3-24-2016

A Framework for Incorporating Insurance into Critical Infrastructure Cyber Risk Strategies

Derek R. Young

A FRAMEWORK FOR INCORPORATING INSURANCE INTO CRITICAL INFRASTRUCTURE CYBER RISK STRATEGIES

THESIS

Derek R. Young, MAJ, USA

AFIT-ENG-MS-16-M-055

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT-ENG-MS-16-M-055

A FRAMEWORK FOR INCORPORATING INSURANCE INTO CRITICAL INFRASTRUCTURE CYBER RISK STRATEGIES

THESIS

Presented to the Faculty

Department of Electrical and Computer Engineering

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 Computer Science

Derek R. Young, BS

MAJ, USA

March 24, 2016

AFIT-ENG-MS-16-M-055

A FRAMEWORK FOR INCORPORATING INSURANCE INTO CRITICAL INFRASTRUCTURE CYBER RISK STRATEGIES

THESIS

Derek R. Young, BS
MAJ, USA

Committee Membership:

LTC Mason. J. Rice, PhD
Chair

Maj Benjamin. W. Ramsey, PhD
Member

Dr. Robert. J. McTasney, PhD
Member

AFIT-ENG-MS-16-M-055

Abstract

Critical infrastructure owners and operators want to minimize their cyber risk and expenditures on cybersecurity. The insurance industry has been quantitatively assessing risk for hundreds of years in order to minimize risk and maximize profits. To achieve these goals, insurers continuously gather statistical data to improve their predictions, incentivize their clients' investment in self-protection and periodically refine their models to improve the accuracy of risk estimates. This paper presents a framework which incorporates the operating principles of the insurance industry in order to provide quantitative estimates of cyber risk. The framework implements optimization techniques to suggest levels of investment for both cybersecurity and insurance for critical infrastructure owners and operators. This analysis can be used to quantitatively formulate strategies to minimize cyber risk.

AFIT-ENG-MS-16-M-055

For my daughter.

Acknowledgements

I would like to thank LTC Mason Rice, Maj Benjamin Ramsey and Dr. Robert Mactasney for all the insight and guidance that was provided throughout the course of this research. I would like to give a special thanks to Juan Lopez Jr. who provided much of his time and expertise in assisting me with this endeavor.

Derek R. Young

Table of Contents

Page

List of Figures

List of Tables

List of Abbreviations

A FRAMEWORK FOR INCORPORATING INSURANCE INTO CRITICAL INFRASTRUCTURE CYBER RISK STRATEGIES

I. Introduction

In the late 17th century, London's growing importance as a center for trade increased demand for marine insurance. In the late 1680s, Edward Lloyd established a coffee house business venture in London which soon became a popular locale for maritime businessmen. The coffee shop served as a venue to share the latest information on shipping-related news (e.g., wars, pirate activity and weather patterns). This information allowed them to factor risk into their business decisions. Eventually, Lloyd's emerged as a market where members joined together to form syndicates to insure (and pool) the risk associated with maritime shipping. Today, Lloyd's continues to exist as an insurance institution that analyzes risk quantitatively, shares and gathers information and pools risk amongst its clients.

Similar to how England faced the emerging threat of maritime risk corresponding to their increased prominence on the seas, critical infrastructure owners and operators face a similar risk of emerging cyber-induced incidents. The U.S. President's executive order, Improving Critical Infrastructure Cybersecurity [34], calls for a cybersecurity framework that provides a cost-effective approach to help critical infrastructure owners and operators manage cyber risk. The art and science of balancing risk and costs is something that the insurance industry has been doing for hundreds of years. The quantitative risk management methods developed and used by the insurance industry reveal patterns and processes that have been proven to mitigate risk in an uncertain world.

1.1 Motivation

In PwC's Global State of Information Security Survey 2015 [37], the authors find that Cybersecurity is now a persistent business risk. They categorize respondents to the survey into small, medium and large companies and reveal that incidents, financial impacts, and security budgets grew from the previous year with the exception of small companies which show small decreases. In the Global State of Information Security Survey 2016 [38], PwC reports that there was a 38% increase in detected information security incidents amongst survey respondents and that 59% of them had purchased cyber insurance.

It may be perceived that the surveys from PwC mostly apply to companies who are protecting digital data and not critical infrastructure control systems which monitor and manage business processes. There has not been a cyber incident involving critical infrastructure sector as large as the high profile data breaches of recent years. However, in a survey conducted by the Aspen Institute, Intel Security, and McAfee [45] of security professionals belonging to 625 critical infrastructure organizations internationally it was reported that almost nine out of 10 experienced at least one attack on their secure systems during 2014. More than 59% of these attacks resulted in physical damage and more than 33% resulted in business process disruption.

The question is no longer if a cyber-induced incident on critical infrastructure will occur, but when will it occur. Insurance has played an important role in mitigating business risk for centuries and should be considered in a holistic cyber risk management strategy.

1.2 Objective

This thesis presents a framework used in making critical infrastructure cyber risk strategies through the incorporation of insurance industry operating methods. Insur-

ance is incorporated into the proposed framework in three ways: (1) as an incentive to increase levels of investment in self-protection; (2) by emphasizing the importance of gathering and sharing data; and (3) by incorporating the insurance industry's cycle of continuously refined quantitative models.

The research goals of this thesis are:

1. Demonstrate that the proposed framework considers the perspectives of both the insured and the insurer.

2. Provide a demonstration of the feasibility of the framework by applying it to a historical example.

3. Provide a demonstration of the applicability of the framework in formulating cyber risk strategies through specific scenarios.

It is hypothesized that the inclusion of insurance industry operating methods into a quantitative cyber risk management process will result in an improved capability of critical infrastructure organizations to make cyber risk mitigation strategies.

This paper uses historical examples to demonstrate the framework's feasibility and three specific scenarios to show its applicability in formulating cyber risk strategies. Given the current environment of limited empirical data regarding cyber incidents in critical infrastructure, the demonstrations are not intended to highlight the framework's accuracy. The purpose of this research is to present concepts from insurance industry operating methods that can be incorporated into a quantitative risk framework that can be refined with time and experience.

1.3 Thesis Layout

This chapter introduces the motivation behind the thesis research. Chapter 2 provides background information on the insurance industry, cyber insurance, and

quantitative risk management methods. Chapter 3 presents the proposed framework and the optimization problem used to link the separate framework processes together to obtain outputs. Chapter 4 presents an analysis of the framework outputs obtained by using a historical example as well as three specific scenarios developed for this research. Chapter 5 discusses conclusions from the results of the research and offers suggestions for future research.

II. Background and Literature Review

This chapter provides the background information used to build the framework presented in chapter three. The inputs to the proposed framework are the outputs from a cyber risk assessment process. It is assumed that the reader has a basic knowledge of cyber risk assessments and its outputs (e.g., identifying threats, threat actors, vulnerabilities and formulating controls to reduce risk).

Section 2.1 provides a background on the modern insurance industry and discusses some of its core driving principles. Section 2.2. provides a discussion of the emerging cyber insurance market, the challenges it faces (2.2.1, 2.2.1.1 and 2.2.1.2) and cyber insurance as an incentive for cybersecurity (2.2.2, 2.2.2.1 and 2.2.2.2). Section 2.3 discusses current quantitative cyber risk analysis methods. Because there exists a large array of methods from public, private and academic sources, the discussion focuses on methods which contributed to this thesis. Section 2.4 presents the contributions of this thesis to the existing body of research. Section 2.5 provides a conclusion for this chapter.

2.1 Modern Insurance Industry Background

The insurance industry has been influencing quantitative risk decisions for centuries. Modern insurance has its roots in 17th century England. Property insurance in the form of fire insurance saw its birth from the Great London Fire in 1666 [12]. The practice of fire insurance soon became widespread and later found its way to the U.S. where the first fire insurance policies were sold in 1732 and popularized by Benjamin Franklin. Concurrent to the development of property policies, business insurance was developed as maritime trading companies sought to insure against storms, piracy and other perils that affected their shipments [36]. By the turn of the 20th century, many

of the major lines of insurance commonly recognized today had been developed by insurers.

The function of insurance is to spread the losses of the few amongst the many; whereby, the actual loss value is substituted by the average loss value [39]. This function is also referred to as risk pooling. In theory, the insurance premium, or rate, charged by an insurer should distribute the cost of insurance fairly amongst the pool of the insured. The rate can also be expected to encourage the reduction of loss through the implementation of controls (i.e., investment in self-protection) [22].

From a business perspective, insurance takes on two views: that of the insurer and that of the insured. The insurer seeks to make a profit from the premiums which exceed the losses spread over time and many different clients. An insurer's profits are in jeopardy if it is inaccurate in quantifying risk or if it insures clients who engage in inappropriate risk behaviors (e.g., negligence and fraud). The insured seek to manage the risk of uncertain loss events and maximize their profits through the transfer of risk to an insurer [27]. The market's response to these two views are the economic functions of putting a quantitative price on risk and setting incentives for risk-appropriate behavior [5]. To achieve these functions, the insurance industry guards against adverse selection and moral hazard.

Adverse selection is the inability of the insurer to distinguish between different client types, those who take risk-appropriate behaviors and those who do not [40]. It is the tendency of persons with higher than average losses to seek insurance at average rates which result in higher than average losses for the insurer [39]. An example of adverse selection would be for an insurer to charge the same rate for flood insurance to two homeowners, one whose home was in a flood plain and the other whose home was built on higher ground. Insurers minimize the effects of adverse selection by

screening for acceptable clients and by charging premiums appropriate for the client's risk-behavior.

Moral hazard results when the insurer is uninformed of a client's risk level [40] which may derive from dishonesty or character/system defects of the client that increase the frequency and/or severity of a loss event [39]. It can also result from a lack of incentive for the insured to take actions to reduce the impact and/or likelihood of risk incidents [17]. Negligence and fraud, on the part of the insured, are both examples of moral hazard. Insurers minimize moral hazard through policies that incentivize clients to reduce risk.

2.2 Cyber Insurance

The cyber insurance market has experienced notable growth over the last few years [13, 19, 28]. This is due in large part to the recent prevalence of high-profile, high-cost data breaches. Despite this growth, accurately quantifying cyber risk into an adequate insurance premium is a difficult task as the value of the data being protected is difficult to quantify. The exposure to threats changes rapidly and assessing the security posture of potential and current clients can be resource intensive [27].

As cyber incidents emerged as a significant business risk, insurers began incorporating cyber exclusion clauses into their existing lines of insurance (see Table 1). Since traditional commercial lines of insurance typically exclude cyber threats from their policies, cyber insurance is offered as a "stand alone" product [10].

Cyber insurance policies provide coverage against many of the losses associated with a cyber incidents (e.g., data destruction/theft, extortion, malicious code, denial of service attacks, response activities and legal claims resulting from the incident). However, of concern to critical infrastructure owners and operators is that few policies cover physical damage and bodily harm that could result from a cyber-induced

Table 1. US Cyber exclusion clauses.

Clause Title	Description
Institute Cyber Attack Exclusion Clause (CL380)	Excludes coverage when the means of inflicting harm is a computer system, computer software, malicious code, computer virus, or the process of an electronic system.
Terrorism Form T3 LMA3030 Exclusion 9	Excludes coverage of cyber attacks motivated by terrorism.
Electronic Data Exclusion NMA2914	Excludes coverage for losses associated with electronic data.

incident [10]. The prospects are improving with the government calling for better options for critical infrastructure [10] and the insurers themselves conducting research into the effects of cyber threats on critical infrastructure and their policies [25].

2.2.1 Challenges with Cyber Insurance.

The key challenges which make cyber risk unattractive to insurers are interdependent security [23], correlated risk [2] and information asymmetries [47]. Interdependent security takes two forms: an entity's IT infrastructure is connected to others and many cyber incidents exploit a vulnerability in a system used by many organizations. This interconnectedness results in an organization's security being undermined by the failure of others. Correlated risk is akin to interdependencies but refers to the systemic nature of some vulnerabilities (i.e., worms and viruses) which are unattractive to insurers because they are globally rather than locally correlated [3]. Information asymmetries arise when one of two parties has inferior information regarding the other. Moral hazard and adverse selection are both information asymmetries. These asymmetries are prevalent in cyber risk management.

This research does not attempt to address all the issues which are associated with these challenges. For a full treatment of these challenges, the reader is referred to the

references cited. The issues that will be discussed are the lack of historical data which provides statistical analysis of cyber-induced incident frequency (likelihood) and the difficulty in predicting the costs of an incident (severity).

2.2.1.1 Lack of Trend Data to Accurately Predict Likelihood of Incident.

The insurance industry relies heavily on actuarial science to develop mathematical and statistical models to empirically or technically estimate risk. Skogh, in his analysis of the insurability of industrial hazards [41], defines two types of risk: actuarial risk and development risk. Actuarial risk, referred to as old risk, has been experienced repeatedly in the past resulting in developed trend data. Development risks are new risks that have arisen due to technological or social changes and are rife with information asymmetries. Cyber risk falls into the latter category and the difficulty in predicting the probability of a cyber-induced incident is well documented [1, 15, 42]. Despite this challenge, the insurance industry has encountered development risks repeatedly in the past.

Insurers have learned that initial premium prices are often inaccurate and that adjustments must be made as new data is gathered. When jetliner insurance was first introduced, premiums were set at 8% of hull value, but with time and experience this rate was reduced to 1% [6]. Homeowner insurance pricing, initially offered in the 1950s, was based largely on insurer judgment and it was not until a decade later that more detailed and accurate statistical policies were released [48]. After the attacks of 9/11, where the insurance industry paid out billions of dollars, many insurers greatly increased their rates for terrorism coverage or declined to offer it [30]. And more recently, cyber insurance premiums for traditional Information Technology (IT)

systems were increased in response to the high-profile data breaches of the last few years [14].

Walters [48] proposes that insurance policies go through three stages: (1) no data; (2) actual experience; and (3) changes in coverage. In the first stage, insurers use their best judgment to determine rates. In stage two, the insurer has paid numerous claims against policies and gained insight into actual losses (actual experience). The transition to stage three occurs as additional experience is gained by the insurer. Periodic refinements to estimations and policy changes are typical during stage three.

A problem faced by the cyber realm is the difficulty in gathering data due to the reluctance of organizations to share information regarding past security breaches [17] (another information asymmetry). This can be attributed in large part to the sizable monetary impact companies suffer due to loss of trust with their customer base resulting from compromises.

The reluctance to share data has been directly addressed by the private and public sectors and even in an Executive Order from the President of the United States [35]. The Department of Homeland Security (DHS), under direction from the President, has developed and implemented numerous information sharing programs [11]. With these programs, DHS seeks to improve the current information sharing environment for the private sector which operates the majority of the nation's critical infrastructure.

Similarly, the World Economic Forum, seeking to promote quantitative risk analysis methods for cyber risk and data sharing, introduced the virtuous circle of cyber quantification [49] as seen in Figure 1. The cycle follows the pattern set by the insurance industry of gathering data, making quantified estimates regarding risk, and then continuing to improve upon these estimates as new data is gathered with time.

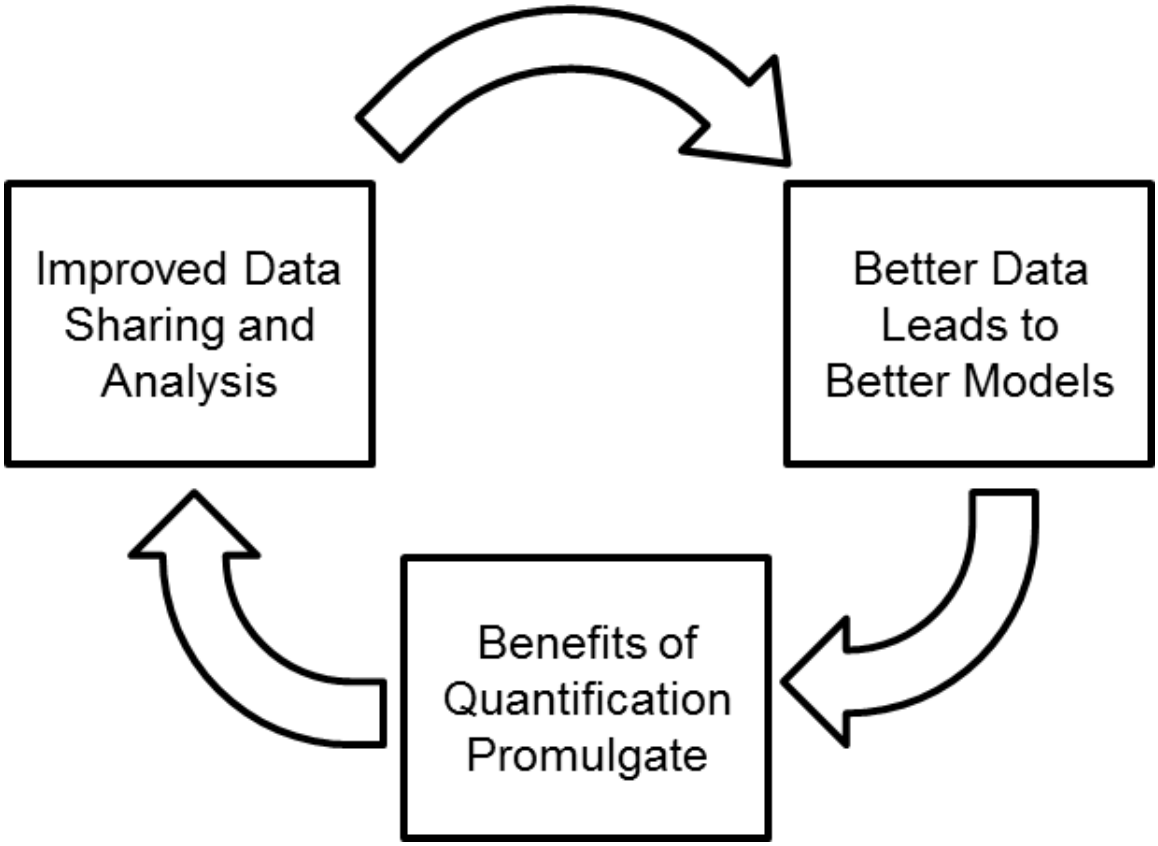


Figure 1. Virtuous circle of cyber quantification.

The insurance industry also relies on reinsurance as a means of risk management. Just as is done between the insured and the insurer, the primary insurer transfers to another insurer (called the reinsurer) potential losses associated with their polices. The purpose of reinsurance is to stabilize profits amidst uncertainty and to provide protection against catastrophic incidents [39].

2.2.1.2 Difficulty Assessing the Severity of Impact Costs.

The costs of a realized cyber incident can include breach of customer privacy, business interruption, damage to physical infrastructure, response costs, law suits, and loss of market value. Unfortunately, accurately predicting the costs of some of the intangible consequences such as loss of brand value or electronic customer data can prove difficult [1, 4, 15, 44]. There exists the assumption that estimating the cost severity of cyber incidents is so difficult that cyber insurance will remain as a niche line of insurance [24].

The insurance company, Lloyd's, and the University of Cambridge's Centre for Risk Studies issued a report, Business Blackout [25], which considers the insurance implications of a cyber attack on the U.S. power grid. In the report, the authors make estimates for the monetary impact of a cyber attack by consulting with insurance and energy industry experts. The estimates take into account the second and third order losses incurred by those dependent on the services of the power companies as well. This is a marked advantage over traditional cyber incidents who may have difficulty in predicting the extent of the effects of a breach. In an interview with Digital Bond [9], two of the authors commented that critical infrastructure is in a good position because it can more easily estimate costs than traditional IT systems.

Critical infrastructure is in a better position because the costs associated with the interruption of an industrial process (e.g., cyber-induced oil pipeline disruption) can

be estimated because they are thoroughly understood by system owners. Additionally, cost estimates can be based on past disruptions to the business process which were caused (at least in part) by a failure in control messaging. Butts *et al.* [8] developed a model for expressing control system failures and attacks that involve the exchange of messages and showed that past control system failures can be used to model current and future cyber threats to their systems. The authors apply the model to a pipeline rupture at Fork Shoals, SC in 1996 [31] that resulted in part from a failure of control and show that the effects of the rupture could also have been produced by cyber means. An analysis of other pipeline ruptures reveals other incidents involving control system failures which could have been produced by a cyber means using the methods from Butts *et al.* (e.g., Murfreesboro, TN [32] and Knoxville, TN [33]).

2.2.2 Insurance as an Incentive for Cybersecurity.

Insurance as an incentive for cybersecurity has two perspectives: the insurer and the insured. The commonality that both perspectives share is the ultimate goal to protect profits. The insurer achieves this through cybersecurity assessments of potential and current clients whereas the insured is incentivized to invest in protective controls.

2.2.2.1 Insurer Perspective.

In order to avoid the dangers of moral hazard, adverse selection and fraud, the insurance industry relies heavily on authenticated, audited, or certified assessments of potential and current clients [24]. Adverse selection requires the insurer invest in an underwriting processes which screens potential clients in order to avoid client risk-behavior beyond the insurer's tolerance. In contrast, moral hazard requires the

insurer to invest in methods to continuously audit potential and current clients for unacceptable risk practices [27].

In order for a company to enjoy the benefits afforded by insurance, they must be willing to be subject to assessments by the insurer. Through this process, system vulnerabilities are identified, mitigated, and the system's security posture is increased. These assessments are of particular importance to critical infrastructure as simply applying accepted traditional IT best practices to the network may not be sufficient for their unique, custom-designed networks [43]. The assessments may also determine that certain controls must be implemented (minimum levels of investment in self-protection) in order for the client to be eligible for coverage.

2.2.2.2 Insured Perspective.

Many researchers believe that cyber insurance can be a incentive to invest in self-protection which leads to an increase in the level of security and thus the level of the security of the Internet in general [5, 21, 27]. The authors claim that insurance can further promote greater levels of investment in security by offering rebates on premiums for clients who meet criteria such as implementation of industry adopted best practices. Gordon and Loeb [17] state that the problem of moral hazard can be directly addressed by offering premium reductions for making increases in security posture and by imposing deductibles which ensure the insured suffer some loss in the event of an incident. Because of the dependence on critical infrastructure as a nation, DHS is currently working with stakeholders to improve the coverage provided by cyber insurance because it is a means to reduce the number of successful cyber-induced incidents [10].

The practice of offering reduced rates for increased levels of self-protection is a well exercised technique employed by the insurance industry. For example, auto insurance

providers typically offer discounts for anti-theft measures, passive restraint measures and participation in an accident avoidance courses.

It may also be the case that minimal controls may be required by the insurer before insurance coverage is offered. In the case of many critical infrastructure operators, their exist mandatory regulations that stipulate what measures an organization will take towards self-protection (similar to mandatory seat belts in cars). These requirements and their effectiveness in changing an organization's security posture can be taken into account when determining potential insurance discounts.

2.3 Quantitative Cyber Risk Assessment Methods

Hoo [18] seeks to answer the question how much security is enough and in doing so defines two generations of cyber risk modeling and introduces a third. First generation methods evolved from the National Bureau of Standards' Annualized Loss Expectancy (ALE) metric introduced in 1974 [20] in its Federal Information Processing Standard (FIPS) 31, Guideline for Automatic Data Processing. ALE is defined in Equation (1) as the product of the Annual Rate of Occurrence (ARO) and the Single Loss Expectancy (SLE); stated otherwise, the product of likelihood and severity.

$$ALE = ARO * SLE \tag{1}$$

SLE is further defined in Equation (2) as the product of the Asset Value (AV) and the Exposure Factor (EF).

$$SLE = AV * EF \tag{2}$$

EF is the percentage loss that an asset would suffer in the event of a realized threat. ALE is a simple model which represents an amortized view of risk; the expected loss averaged according to its expected frequency of occurrence. Because of its simplicity,

ALE is a common metric used in many methods and models. According to Hoo's analysis, the ALE-based methodologies eventually declined in usage because they were deemed as infeasible to implement due to their complication, lack of incorporating uncertainty into the predictive values, and the lack of accurate predictive data for use in the models.

Second Generation approaches attempted to simplify the ALE-based methodologies by reducing their complexity. This was accomplished by focusing on fewer predictive factors, relying on more qualitative approaches, or by not using formal model and simply implementing industry-accepted best practices. Hoo views the generation two approaches as short-term solutions as they do not attempt to adequately tackle the fully quantitative nature of the first generation approaches.

Hoo observed at the time of writing his paper in 2000 that the insurance industry, legal realm, and business executives were becoming increasingly involved in cyber risk management. With their increased presence, he defines a new third generation which returns to the quantitative methods of the first generation but which seeks to overcome its weaknesses by incorporating uncertainty in the models, modeling risk as a management decision, and by recognizing the importance of gathering statistics.

This thesis is based on third generation approaches and so the remainder of this section discusses these methods. Because there exists a large number of methodologies developed by public, private and academic organizations it is not feasible to give an exhaustive overview of all methods. Therefore, the remainder of this section will discuss the methods that influenced this thesis.

Hoo introduces his own third generation method and discusses an econometric approach in which uncertainty and flexible modeling tools can be used with available data to determine appropriate levels of investment in cybersecurity. He proposes a new ALE-based framework which attempts to overcome the weaknesses identified in

Table 2. Gordon-Loeb model variables and expressions.

Variable Name	Description
λ	Monetary loss to a firm caused by a security breach.
t	Probability of an attempted breach of a security system.
v	Probability that an attempted breach is successful (also referred to as vulnerability).
$\lambda t v$	Expected loss conditioned on no new additional security investment.
z	Monetary investment in security.
z^*	Optimal monetary investment in security.
$S(z, v)$	Security breach probability function which denotes the probability that security will be breached given a monetary investment in security z given an initial vulnerability v.
$S(z, v)\lambda t$	Expected loss conditioned on the additional security investment, z (also referred to as residual risk).
α	Measure of effectiveness of security controls.

the previous generations by incorporating uncertainty, modeling the risk as management decisions and by recognizing the importance of gathering statistics. His model does not explicitly incorporate the use of insurance though the recognition of the importance of statistics is a nod to the needs of the insurance industry.

Gordon and Loeb [16] present an economic model for the optimal amount to invest in security to protect information (hereafter referred to as the Gordon-Loeb model). Table 2 provides a summary of the variables and expressions introduced. The model accounts for the effectiveness of increases in security spending with the security breach probability function, $S(z, v)$. The optimal security investment, z^*, is precisely where the marginal benefits from the security investment no longer outweigh the marginal cost. Mathematically, z^* is defined as where the first derivative of $S(z, v)\lambda t$ is equal to one.

Implementation of a specific function for $S(z, v)$ must adhere to three assumptions regarding its properties:

1. $S(z,0) = 0$ for all z. If a system is not vulnerable then it will remain so for any amount of security investment in an ideal case.

2. $S(0,v) = v$ for all v. If there is no investment in additional security controls there is no change to the likelihood of a successful breach.

3. For all $v \in (0,1)$, as z increases the system is made more secure but at a decreasing rate. Additionally, $lim\ S(z,v) \to 0$ as $z \to \infty$. By investing a sufficient amount in security the probability of breach can be made arbitrarily close to zero.

Gordon and Loeb introduce two classes of functions for $S(z,v)$ to model the effectiveness of security control investments. The Class I set of functions represent systems where regardless of the value for v, an investment in security will return equal reductions in expected loss. Class II functions are more practical and better reflect existing systems because the reductions in vulnerability are not linear as in Class I. Class II characterizes systems where increasing investments in security result in reductions of vulnerability but at a decreasing rate as $v \to 1$. Class II systems with initial high values for v may be prohibitively expensive to adequately secure against cyber incidents. For these reasons, this thesis uses the Class II set of functions to model the effectiveness of security controls. Class II functions are given by Equation (3).

$$S^{II}(z,v) = v^{\alpha z+1};\ \alpha > 0 \tag{3}$$

The optimal level of investment, z^* for Class II functions is expressed in Equation (4).

$$z^{II*}(v) = \frac{ln\left(\frac{1}{-\alpha\lambda tv(ln\ v)}\right)}{\alpha\ ln\ v} \tag{4}$$

In a later paper, Gordon and Loeb provide a framework for using insurance in cyber risk management [17]. The model involves the initial assessment of risk, the

reduction of risk through the implementation of security controls, the reduction of financial risk via insurance, and then maintaining risk at acceptable levels. They state that there exists a trade-off between the amount invested in security controls and the amount spent on cyber insurance as constrained by a budget. Higher levels of security control spending will necessitate lower levels spent on insurance and vice versa. The authors did not link their previously published mathematical economic models to this framework.

Arora *et al.* [1] introduce a framework that evaluates the costs and benefits of IT security based on risk avoided rather than increases in productivity. The framework consists of three phases: (1) calculate the net bypass rate for security solutions, (2) calculate total damages incurred from the bypasses of security, and (3) calculate the Risk-based Return on Investment (RROI). The net bypass rate for each security solution is calculated by taking the ratio of successful breaches to the total number of all attempted breaches of security. RROI is the ratio of net monetary benefit of the security controls divided by their implementation costs. The RROI is used to measure how effectively resources are used to avoid or reduce risk similar to how ROI is used to measure the effectiveness of monetary investments with higher values of RROI indicating better investments. Insurance is not incorporated into the framework.

McQueen *et al.* [29] from Idaho National Laboratory introduce a quantitative methodology for small Supervisory Control and Data Acquisition (SCADA) control systems which employs a directed graph where nodes represent stages of the graph and the edges represent the expected time-to-compromise. The methodology includes a 10 step process which includes incorporating an application of an ALE-based quantitative model, identifying system device vulnerabilities and forming a graph based on their categorization, estimating time to compromise for each device, and generating compromise graphs based on the information gathered. The estimated time-to-

compromise is the primary measure of system security and risk used by the authors. They believe that as the time-to-compromise is increased, the likelihood of a successful attack decreases. The methodology is meant to be applied to a small SCADA system as the analysis may become overly burdensome on large control systems. Insurance is not incorporated into their methods.

Bojanc and Jerman-Blažič [4] describe a method for the economic modeling of cyber risk management with the goal of influencing management decisions. The four risk minimization strategies that can be employed by management are acceptance, avoidance, transfer and reduction of the risk. The authors' model uses ALE to quantitatively express risk. The benefits of cybersecurity investments are determined by using the popular accounting metrics Return on Investment (ROI), Net Present Value (NPV) and Internal Rate of Return (IRR). The method uses a flowchart to describe the process by which ALE, ROI, NPV and IRR are used to set quantitative values that are used by an organization's management in deciding how to employ the risk minimizations strategies.

Brecht and Nowey [7] discuss the challenges with accurately quantifying the benefits of information security measures and then present four ways to categorize and determine information security costs to an organization. The first method, a balance sheet oriented approach, is to straightforwardly calculate the personnel, hardware, software, and outsourcing costs of cyber security. The second approach builds on the first but adds the element of time by calculating costs that occur with change and time. The third approach, developed by the authors, presents two new metrics, determinability and security-cost-ratio. Determinability, on a scale from easy to hard, describes how difficult it is to determine security-related costs. Information security-cost-ratio describes the percentage of costs that are cyber security related. The final approach is the ISO/IEC 27001 approach as presented in the standard of the same

name. The authors state that each method has different occasions for which its use is appropriate. For example, when comparing different security implementations, one method may hold advantage over the other.

The Open Group's Risk Taxonomy Standard [46] seeks to set the Factor Analysis of Information Risk (FAIR) model developed by the company, CXOWARE, as single logical and rational framework to be used in quantitative risk analysis. The taxonomy breaks down the factors that drive risk into their quantitative subcomponents. At the top of the hierarchical taxonomy is risk, which has two parts: loss event frequency (likelihood) and loss magnitude (severity). This is equivalent to $ALE = ARO \times SLE$; however, the FAIR model builds upon ALE by further dissection of its subcomponents into deeper layers of abstraction. The model is used to calculate risk based on the level of knowledge the user has of the quantitative factors. If there is a high degree of confidence in data (e.g., it is known how frequently cyber threats are realized against an organization) the model-users do not need to use the deeper abstraction layers of the taxonomy. Likewise, if there is a lack of confidence in the estimates, deeper layers of the taxonomy are systematically used to attempt to build best estimates for the quantitative predictors of likelihood and severity.

Estimates using the FAIR model are done by providing a range of values, including the least likely values at the maximum and minimum and the most likely values lying at the median or mean. The range of values is assigned a probability distribution (e.g., normal, lognormal, triangular, etc...) and is then analyzed through a Monte Carlo simulation performed using software packages. Estimates of risk are provided as a range of output values based on the inputs with assigned confidence intervals.

2.4 Research Contributions

This research extends the econometric quantitative risk management methods discussed in the previous section by incorporating insurance industry operating methods. Specifically, the ideas presented by Gordon and Loeb [15], Bojanc and Jerman-Blažič [4] and ALE are incorporated into this research. Chapter 3 of this thesis presents a framework to be used in formulating risk strategies which incorporates the insurance industry methods of incentivizing investments in self-protection; sharing and gathering data; and continuous refinements and improvements to predictive models.

The framework also takes advantage of critical infrastructure's ability to more accurately predict incident costs to provide risk estimates and influence risk strategies. By using the methods introduced by Butts *et al.*, past disruptions to a business process that resulted in failures of control can be shown to also result from cyber means. These past incidents are then used as inputs to a quantitative risk analysis process as a range of possible loss values.

2.5 Conclusion

This chapter provides a background on the modern insurance industry, cyber insurance and quantitative risk management methods. The methodology described in Chapter 3 builds on the concepts and research presented in this chapter to accomplish the research goals of this thesis.

III. Methodology

3.1 Introduction

This chapter introduces the framework that incorporates insurance and is used in formulating risk strategies. The framework is presented as a flowchart which integrates multiple models to quantitatively express risk. The models used within the framework are linked together using an optimization problem with the objective of minimizing the total risk. Example implementations of the framework are provided in Chapter 4 which demonstrate the feasibility and applicability of the framework.

Section 3.2 provides the research goals of this thesis. Section 3.3 presents the quantitative cyber risk framework, the model used to estimate threat likelihood and severity (3.3.1), the model used to estimate the effectiveness of the reduction of threat likelihood and severity through the implementation of controls (3.3.2), the model used to incentivize investments in controls through insurance premium discounts (3.3.3) and the optimization problem used to link the separate models together (3.3.4). Section 3.4 provides a summary for this chapter.

3.2 Research Goals

The research goals of this thesis are:

1. Demonstrate that the proposed framework considers the perspectives of both the insured and the insurer.

2. Provide a demonstration of the feasibility of the framework by applying it to a historical example.

3. Provide a demonstration of the applicability of the framework in formulating cyber risk strategies through specific scenarios.

It is hypothesized that the inclusion of insurance industry operating principles into a quantitative cyber risk management process will result in an improved capability of critical infrastructure organizations to make cyber risk mitigation strategies. One of the key advantages of using insurance is that an individual organization's actual loss value is substituted by a population's averaged loss value. This is a direct result of risk pooling. Risk pooling is accomplished when there exists both an insurer and the insured.

The proposed framework therefore needs to consider the perspectives of both the insured and the insurer who both desire to protect their profits. The implementation of investments in security controls incentivized with rebates to insurance premiums provides for this protection. An optimization of money spent on security controls and insurance provide the insured with a strategy that will minimize their overall risk. The insurer is protected through the inclusion of appropriately priced premiums and rates of incentivization which ensure adequate profits.

3.3 Quantitative Cyber Risk Framework

The proposed framework in this thesis builds on previous methods by incorporating the principles employed by the insurance industry to influence the risk minimization strategies (accept, reduce, transfer and avoid). The framework employs the use of discounts on insurance premiums based on a client's risk behavior and allows for the flexibility to adjust models with time and experience.

Key assumptions of the framework include:

1. There exists general acceptance by the public and private sectors to adopt efforts that contribute to quantifiable risk analysis.

2. Sharing of cyber incident information and statistics exists between organizations (private, public and academic).

3. A market exists to insure critical infrastructure against cyber-induced incidents and claims are being made against policies.

4. Investments in an organization's cybersecurity posture are incentivized by reductions in insurance premiums by the insurers.

The proposed framework is displayed as a flowchart in Figure 2. Once the threats have been identified, the flowchart traverses through three key models (labeled as 1, 2, and 3 in Figure 2) that are applied to the identified threats so that minimization strategies can be formatted quantitatively. In order to obtain outputs, the models are linked together using an optimization problem.

The first model integrated into the framework is the threat likelihood and severity. After the threat is modeled the framework can follow two paths. When the analysis reveals that the risk is less than or equal to a threshold value set by management (i.e., risk tolerance), the decision can be made to accept the risk as the "cost of doing business." If the risk is accepted, no further attempts are made to minimize the risk. Otherwise, if the threshold is exceeded, model two is applied.

The second model integrated into the framework is the reduction of likelihood and severity. Risk is reduced through the implementation of security controls (e.g., software, hardware, security personnel, security training, policies, and procedures). The model estimates the effectiveness of the security controls by reducing the likelihood and severity values found during the first model resulting in quantitative analysis being applied to the "reduce risk" minimization strategy. The outputs provided by this model are estimates of the amount that the insured should invest in security controls

After reducing the risk, if there exists adequate insurance options which meet the decision makers' goals for cost and coverage amount, the third model of the framework is applied. The model will reduce the cost of transferring risk based on the risk behavior of the organization (i.e., decisions made and actions taken in the

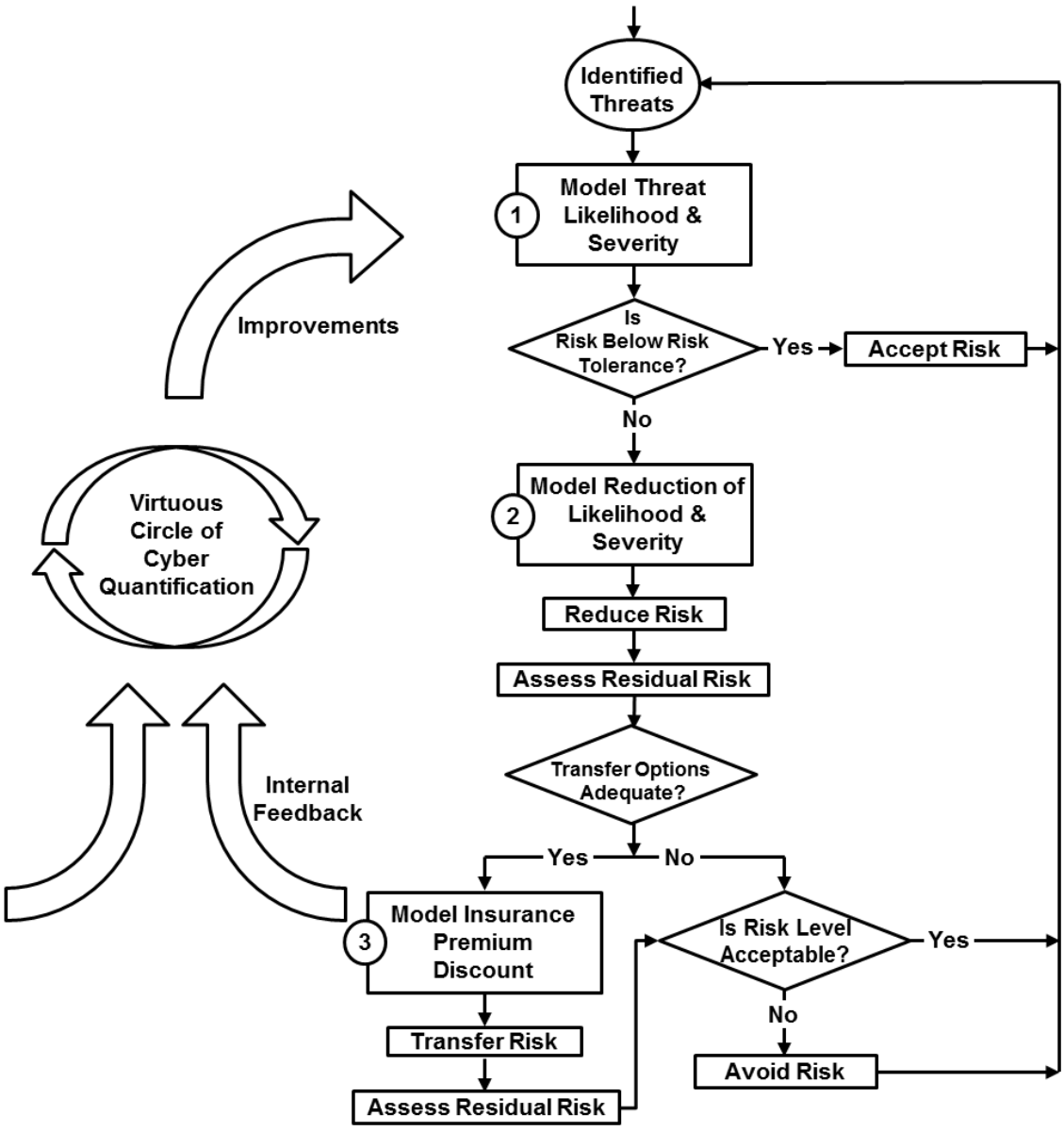


Figure 2. Quantitative cyber risk framework.

"reduce risk" strategy). The outputs from this model can by used by an insurer to set estimates for insurance premiums.

If the residual risk level after the use of controls and insurance is determined to be too high and the severity of the impact of the system threats outweighs the benefits of the system, the decision to avoid the risk should be considered by management.

The outputs from the framework are obtained by linking the models together as an optimization problem where the objective is to minimize the risk. It should be noted that the initial results from the optimization will likely be suboptimal if there is insufficient historical data. However, time, experience and new data will result in more accurate predictions of threat likelihood and severity. This follows the pattern set by the insurance industry and the pattern described by the World Economic Forum's Virtuous Circle of Cyber Quantification [49]. These ideas are included in the framework with the addition of the circle of quantification on the left side of Figure 2.

The models used to implement the framework are ALE, the Gordon-Loeb model, and a newly proposed model for incentivizing security expenditures through insurance premium discounts. ALE has been used as a basis for quantitative risk methods for approximately four decades and was selected for its simplicity and familiarity. The Gordon-Loeb model is considered as the first economic model that determines the optimal amount to invest in security controls and has been widely cited and referenced. Because it determines the optimal amount to invest, it lends itself very well to the optimization problem used in the framework. Additionally, the Class II set of functions defined by Gordon and Loeb are useful in modeling risk strategies due to the diminishing returns on optimal investment for systems that are either highly vulnerable or highly secure as illustrated in Figure 3. This characteristic of the Class II set of functions allows for the optimization to suggest varying ratios

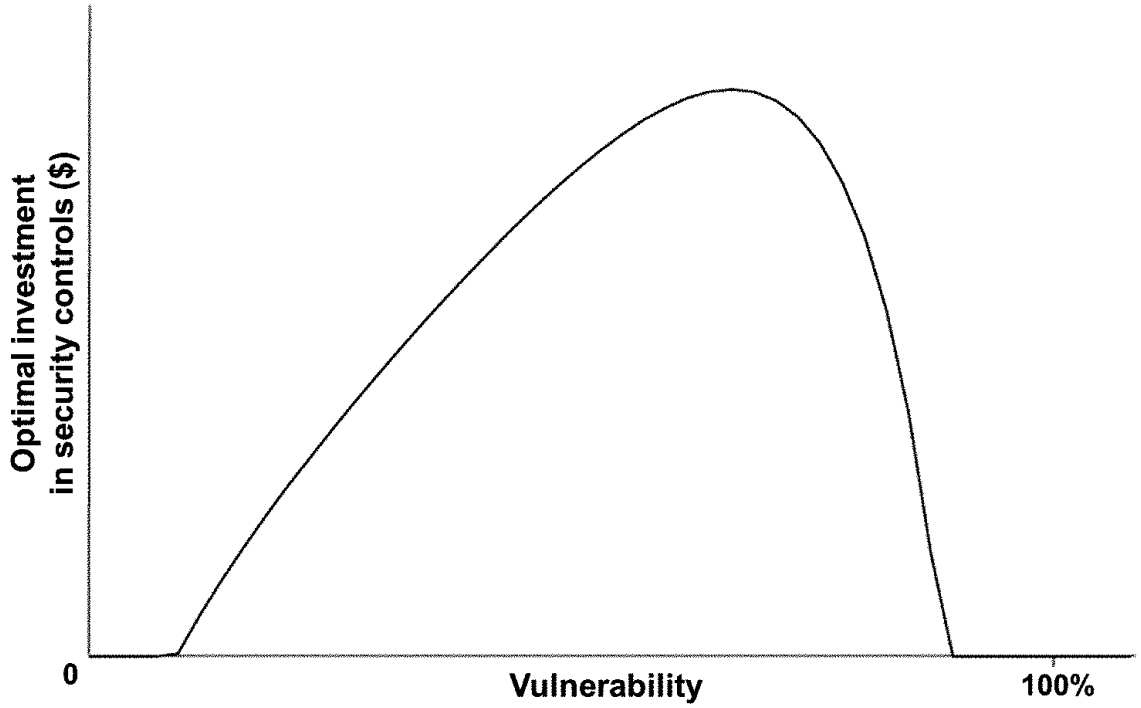


Figure 3. Optimal value of security investments as a function of vulnerability, $z^*(v)$ for Class II.

of security controls and insurance investments according to the input parameters which characterize the system. The simple model for the discount on insurance was developed as part of this research so that it could link directly to the Gordon-Loeb model and thereby incentivize investments in security. Further details regarding these models as well as the optimization problem used to link them together will be shown in the sections that follow.

3.3.1 Threat Likelihood and Severity Model.

The purpose of the threat likelihood and severity model is to represent the identified threats in quantitative terms that are used in subsequent processes and decision points in the framework. The expected outputs are probabilities expressed as percentages for the likelihood and dollar values for the estimated severity.

ALE is used to model the likelihood and severity of the threats with additional layers of abstraction added to SLE by incorporating the Gordon-Loeb model. Specifically, Equation (2) becomes SLE = λtv. Subsequently, by substituting the new expression for SLE into Equation (1) the result is ALE = ARO $*$ λtv.

In order to incorporate uncertainty into the model, ranges of values are selected as inputs to the variables. For example, in Chapter 4, λ will be varied across a range of possible values for the severity of the impact of a cyber-induced incident. The resulting range of values used in estimating ALE as well as the range of values for ALE itself are used as inputs to the other models used at various stages of the framework.

3.3.2 Reduction of Threat Likelihood and Severity Model.

The framework uses the Gordon-Loeb model to quantitatively express the effectiveness of security controls and the reduction of risk. Specifically, the Class II security breach probability function $S^{II}(z, v)$ as shown in Equation (3) is used. The Class II function models a system that becomes increasingly expensive to secure as its vulnerability increases. As stated in Sophos' Security Threat Trends 2015 report [26], ICS are typically ten years or more behind the mainstream in terms of cybersecurity and it is not uncommon when assessing these systems to find that the only viable security strategy is to keep them isolated on air-gapped networks.

A key portion of using the Gordon-Loeb model is the selection of an appropriate value for α (the parameter in $S(z, v)$ which describes the effectiveness of a security investment). The only constraint upon α is that it must be greater than zero. α can also be interpreted as a weight that represents the level of exposure of a network (an exposure parameter). Security controls are less effective on networks with high levels of exposure than those with smaller levels. Subsequently, they will have different α

values assigned. α is inversely related to the level of exposure of the network such that networks with a higher exposure will have smaller values for α. Values for α can be computed by re-arranging Equation (3) to solve for α as shown in Equation (5) and providing estimates for z, v, and $S^{II}(z, v)$.

$$\alpha = \frac{\left(\frac{ln[S^{II}(z,v)]}{ln(v)}\right)}{z} \tag{5}$$

The outputs from this model estimate monetary levels of investment in cybersecurity resulting from the optimal solution from the security breach function, $S(z, v)$. In an optimization, $S(z, v)$ will suggest the Gordon-Loeb optimum z^* as expressed in Equation (4) as the monetary amount to invest in security. However, when the investment is incentivized with discounts to insurance the recommended spending levels exceed z^*.

3.3.3 Insurance Premium Discount Model.

The third model in the framework expresses the discount on insurance premiums as a function of an organization's measures to reduce their risk as illustrated in Figure 4. The variables introduced in this model are summarized in Table 3. The insurer's base rate, P_0 is decreased by a percentage, δ, resulting in the discounted premium, P (assumed to always be an annual rate). This relationship is expressed in Equation (6).

$$P = P_0(1 - \delta) \tag{6}$$

The insured affects the discount, δ, by implementing security controls whose effectiveness in reducing a system's vulnerability is expressed in the function $S(z, v)$. The insurer determines the rate of discount, r $(0 \leq r \leq 1)$, which sets the percentage of the decrease in a system's vulnerability which will apply to δ. For example, if a

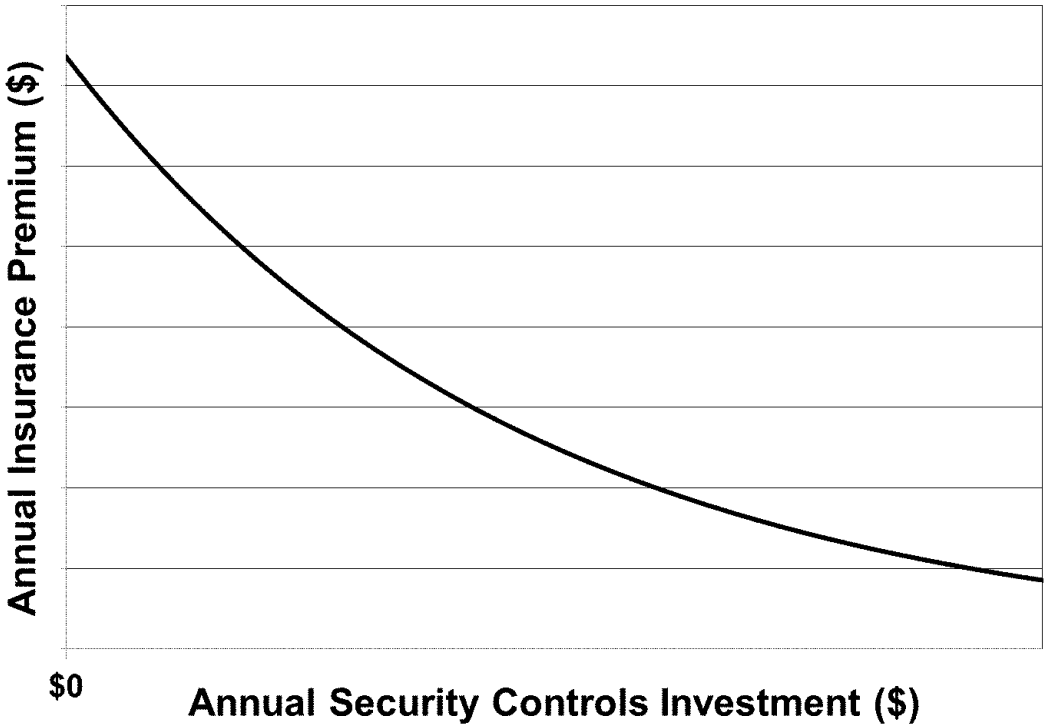


Figure 4. Insurance premium discount as security controls investment increases.

Table 3. Insurance premium discount model variables.

Variable Name	Description
P_0	Base rate insurance premium.
P	Discounted insurance premium.
δ	Percentage discount on the insurance premium.
r	Insurer's rate of discount.

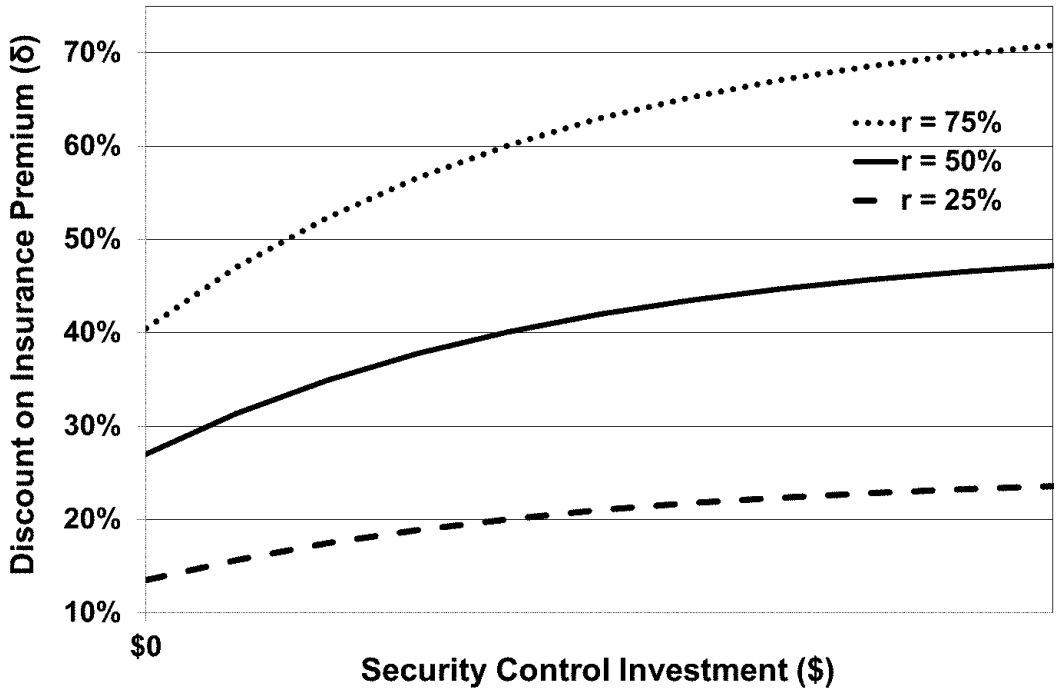


Figure 5. Insurance discount (δ) at an increasing investment in security controls (z) at varying insurance discount rates (r).

system has its vulnerability reduced by 40% through security controls and $r = 50\%$, then a discount (δ) is set at 20%. δ is expressed in Equation (5).

$$\delta = r[1 - S(z, v)] \tag{7}$$

An insurer can vary r to account for how deep of a discount they are willing to offer. The effects of different levels of r are demonstrated in Figure 5 which shows that a higher r increases the discount as the investment in security controls increases. It can also be noted that Equation (7) does not set δ based on the relative change in system vulnerability (i.e., $v - S(z, v)$), but the absolute change in vulnerability. Systems which are inherently secure (the initial value for v is well below 100%) would enjoy deeper insurance premium discounts even if they invested the same amount in security as another less-secure system.

The outputs of this process in the framework estimate levels of spending on insurance premiums. In order to answer the question of how much an organization should be willing to spend on an insurance premium, ALE is used as a guide. It would be reasonable to conclude that an organization should not be willing to spend more on risk minimization than it expects to lose on average. ALE, the averaged view of risk, sets an upper bound on what an organization should be willing to invest in insurance.

3.3.4 Optimization Problem.

The output estimates of the framework use optimization to establish the recommended investments in security controls and insurance premium. The objective of the optimization problem is to minimize the sum of the residual risk after the implementation of security controls, $S(z, v)\lambda t$, the cost of the controls, z, and the cost of insurance, P. The objective function is expressed in Equation (8).

$$minimize[S(z, v)\lambda t + z + P] \tag{8}$$

The optimization is subject to the following constraints and assumptions:

- The cost of security controls and insurance premiums $(z + P)$ cannot exceed the total security budget.
- The amount of coverage purchased should be equal to λ but cannot exceed the maximum coverage amount provided by the insurer.

The optimization was implemented using Frontline System's Premium Solver version 7.0 for Microsoft Excel. The parameters used in Premium Solver are provided in Table 4. The algorithm used to traverse the search space, Generalized Reduced Gradient, is used in nonlinear optimization problems and cannot guarantee that the

Table 4. Options used in Frontline System's Premium Solver 7.0.

Option	Value
Algorithm	GRG Nonlinear
Maximum Time	100 seconds
Iterations	1000
Precision	1×10^{-6}
Convergence	0.0001
Multistart Search	Enabled
Require Bounds on Variables	Enabled
Estimates	Tangent
Derivatives	Forward
Search	Newton
Maximum Subproblems	5000
Maximum Feasible Solutions	5000

solution found is the true global optimum. To overcome this limitation, the "Multistart Search" option was selected to explore multiple local optimums.

Table 5 displays the parameters used in the optimization problem. The input, Security Budget, represents the total budget devoted to cybersecurity and cyber insurance. The inputs Cov and Cov_{Max} respectively represent the amount of insurance coverage to be purchased and the maximum coverage available from an insurer. All the calculations in Table 5 use the equations presented in previous sections. Appendix B contains further details on the use and set up of the optimization within Excel using the Frontline System's Premium Solver.

The optimization adjusts the decision variable, z, until the minimal value for the objective function as defined in Equation (8) is found. In the absence of incentivization through discounts to insurance premiums based on increases of z, the optimization would return the Gordon-Loeb optimum, z^*. When security spending is incentivized with discounts to insurance, the optimization may suggest investments beyond z^*.

Table 5. Optimization inputs, calculations and decision variables.

Inputs
Security Budget
ARO
λ
t
v
α
Cov
Cov_{Max}
P_0
r

Calculations
SLE
ALE
$S^{II}(z, v)$
$S^{II}(z, v)\lambda t$
δ
P

Decision Variables
z

3.4 Conclusion

This chapter provides the framework that incorporates insurance to formulate risk strategies. The framework uses three models to express risk quantitatively. The models provide estimates for the cyber threat's likelihood and severity, estimates of the reduction of likelihood and severity through the implementation of controls and estimates for the discount of insurance premiums as a function of an organization's investment in self-protection. The outputs from the framework are obtained by linking the models together using an optimization problem which seeks to minimize the risk as it is quantitatively expressed monetary values.

An important aspect of the framework is the cycle of refinement and improvement to the predictive models. As time passes and experience gained, it may be necessary to adjust estimates (or possibly adjust the different models).

IV. Results and Analysis

4.1 Introduction

This chapter provides an analysis of the framework presented in the previous chapter by demonstrating its feasibility and applicability. The feasibility of the framework is demonstrated by applying it to a historic example showing how critical infrastructure owners and operators can use past incidents to provide risk estimates for current cyber threats. The applicability is demonstrated through the use of three scenarios which can generally be applied to any critical infrastructure organization. The demonstrations of the framework using the historic example and scenarios includes analysis of the perspectives of the insured and the insurer.

Note that the estimates provided in the historic examples and the scenarios are not intended to demonstrate the accuracy of the framework. Accurate outputs require inputs that properly reflect an organization's and the population's situation. The current scarcity of predictive data as discussed in Chapter 2 is a challenge faced by the cyber insurance industry. Data sharing measures are being promoted by many to include the President of the United States [35], the Department of Homeland Security [11] and the World Economic Forum [49]. The proposed framework also seeks to promote data and information sharing as one of its core tenants.

4.2 Demonstration of Framework Feasibility

In order to demonstrate the proposed framework's feasibility, it will be used to provide analysis using real critical infrastructure incidents which occurred in 1996 and 1999. The examples used will be a series of real oil pipeline ruptures suffered by an individual company that can be shown to also have been cyber-induced using the methods introduced by Butts *et al.* [8]. Using incident reports from the National

Transporation Safety Board (NTSB), a range of estimates for the severity of the loss will be calculated. Specifically, the pipeline ruptures introduced in section 2.2.1.2 (Fork Shoals, SC, Murfreesboro, TN and Knoxville, TN) are used to provide estimates for the severity of the threats.

The first rupture occurred at Fork Shoals, SC [31] on June 26, 1996, spilled approximately 957,600 gallons of fuel oil, and caused damages estimated at $20.5M. The National Transportation Safety Board (NTSB) Pipeline Accident Report states that the rupture of the 36-inch diameter pipeline occurred as a result of the combination of system and control failures. Butts *et al.* specifically use this rupture in their article and show that same results could have been produced by cyber means.

The second incident was a rupture of an 8-inch diameter pipe at Murfreesboro, TN [32] on November 5, 1996. About 84,700 gallons of diesel fuel was released and resulted in $5.7M of property damage. The NTSB report states that the cause of the rupture can be directly attributed to the failure of a controller to open an electric block valve before pumping product through the pipeline.

The third incident at Knoxville, TN [33] spilled 53,550 gallons of diesel from a 10-inch pipe causing about $7M property damage on February 9, 1999. The rupture initially occurred due to structural failures in the pipeline but when the SCADA system did not display a drop in pressure for the pipe section, the controller continued to pump product through the ruptured line through the course of multiple hours.

Based on information obtained from the NTSB reports and adjusting the dollar values for inflation to 2015, the values for λ are $11M for Murfreesboro, $12M for Knoxville, and $135M for Fork Shoals. A more detailed analysis of the estimates of severity is contained in Appendix A. The Fork Shoals estimate is particularly high due to the size of the rupture, the resulting tens of millions of dollars in fines, lawsuits and the repair efforts for the section of ruptured pipeline coupled with the resulting

loss of revenue. Based on these estimates, values assigned for λ range from \$10M to \$150M.

Given the lack of data, the likelihood of a cyber incident is loosely estimated using currently available empirical data and assumptions purely for demonstration purposes. In order to estimate initial values for t (the likelihood of attempted breach of security) and a value for v (the likelihood that breach is successful) the 2015 survey conducted by the Aspen Institute and Intel Security [45] was used. The report stated that nine out of 10 experienced at least one cyber incident, therefore t will be set to 90%. The survey reported that of the detected incidents, 59% resulted in physical damage and 33% resulted in business process disruption. Since it is unclear what overlap exists between these two statistics, an estimate for v of 46% is made by taking their average. Finally, the frequency of incident occurrence is assumed to be once every ten years (ARO of 10%).

Table 6 displays the results of modeling the threat likelihood and severity as a range of possible ALE values based on the range of λ values. These values will be used as inputs at various stages of the framework.

Equation(5) is used to estimate reasonable values for α. Empirical data and assumptions are used to provide estimates for z, v and $S^{II}(z, v)$. Values for z (which is assumed to represent an organization's annual investment) are derived by using statistics from the Global State of Information Security Survey 2015 [37], which provides data on small, medium and large companies' cybersecurity statistics. The survey provided the security budgets for small, medium and large companies over a period of two years. Taking the average of these two years yields reasonable estimates for z for small, medium and large companies of \$825,000, \$2,900,000, and \$10,550,000 respectively. The value of 46% for v is used as it was previously estimated. Finally, it is assumed that 5% of cyber threats successfully breach the system's security ($S^{II}(z, v)$).

Table 6. Range of ALE values with varying values for λ (t = 90%, v=46%, ARO=10%).

Severity(λ)	SLE	ALE
$10,000,000	$4,140,000	$414,000
$20,000,000	$8,280,000	$828,000
$30,000,000	$12,420,000	$1,242,000
$40,000,000	$16,560,000	$1,656,000
$50,000,000	$20,700,000	$2,070,000
$60,000,000	$24,840,000	$2,484,000
$70,000,000	$28,980,000	$2,898,000
$80,000,000	$33,120,000	$3,312,000
$90,000,000	$37,260,000	$3,726,000
$100,000,000	$40,140,000	$4,140,000
$110,000,000	$45,540,000	$4,554,000
$120,000,000	$49,680,000	$4,968,000
$130,000,000	$53,820,000	$5,382,000
$140,000,000	$57,960,000	$5,796,000
$150,000,000	$62,100,000	$6,210,000

Table 7 displays reasonable α values for small, medium and large companies. The α value for a large company is used in this optimization.

Table 7. α value by company size (v =46% and $S^{II}(z, v)$ = 5%).

Company Size	Controls Investment(z)	Exposure Parameter(α)
Small	$825,000	0.000346
Medium	$2,900,000	0.000098
Large	$10,550,000	0.000027

For the purposes of demonstration, the insurer's base rate, P_0, 8% is selected as a starting point in the historic example using pipeline ruptures. This value has historical precedent in the insurance industry as it was used as the initial rate for jetliner insurance [6]. It is assumed that the maximum coverage offered by the insure is $100M. Additionally, it is assumed in this demonstration that the insurer has not placed a requirement on the minimum level of investment in security controls in order to be eligible for coverage.

The optimization results for this demonstration will be shown for an unlimited security budget and a restricted security budget. The unlimited budget results show how the framework is used to estimate recommended spending levels to minimize risk given that an organization does not have set limits. The restricted security budget optimization results provide estimates for the ratio of security controls to insurance which minimize risk when budgetary limits are known.

4.2.1 Optimization Results for an Unlimited Security Budget.

The rate of discount, r, offered by an insurer is varied in the optimization using an unlimited security budget to show which values for r result in a premium not exceeding ALE. During initial trials it was discovered that values of r near 50% resulted in insurance premiums that were near ALE; therefore, the three variations chosen for r are 50%, 55% and 60%. Table 8 displays a summary of the values used as inputs for the optimization with an unlimited security budget.

Table 8. Optimization inputs used with an unlimited security budget.

Inputs	Values
Security Budget	Unlimited
ARO	10%
λ	\$10M - \$150M
t	90%
v	46%
α	0.000027
Cov	\$10M - \$150M
Cov_{Max}	\$100M
P_0	8% of Cov
r	50%, 55% and 60%

Table 9 shows the optimization results for z at three variations of r and a range of λ from \$10M to \$150M. The table also displays the Gordon-Loeb optimum investment (z^*), which does not take insurance into account, as a reference.

Table 9. Unlimited budget optimization results for security controls investment (z).

Severity(λ)	**Optimum(z^*)**	**z ($r = 50\%$)**	**z ($r = 55\%$)**	**z ($r = 60\%$)**
$10,000,000	$0	$0	$0	$0
$11,000,000	$0	$0	$22,628	$42,729
$12,000,000	$209,363	$416,089	$436,276	$456,377
$13,000,000	$589,883	$796,609	$816,796	$836,897
$14,000,000	$942,189	$1,148,915	$1,169,102	$1,189,203
$15,000,000	$1,270,178	$1,476,905	$1,497,091	$1,517,193
$25,000,000	$3,698,622	$3,905,348	$3,925,535	$3,945,636
$50,000,000	$6,993,814	$7,200,541	$7,220,727	$7,240,829
$75,000,000	$8,921,378	$9,128,105	$9,148,291	$9,168,393
$100,000,000	$10,289,007	$10,495,733	$10,515,920	$10,536,021
$125,000,000	$11,349,822	$11,515,916	$11,532,210	$11,548,449
$135,000,000	$11,715,691	$11,869,679	$11,884,807	$11,899,887
$150,000,000	$12,216,571	$12,355,382	$12,369,043	$12,382,665

It can be observed from the results that as r increases, making the discounted insurance premiums more attractive, the optimization suggests that security spending exceed the Gordon-Loeb optimum, z^*, correspondingly. This finding confirms the model appropriately incentivizes security control investments with deeper discounts on insurance premiums.

It can also be observed from Table 9 that the optimization suggests that no money be invested in security controls at the lower levels of λ analyzed (i.e., λ =\$10M and λ =\$11M). This result suggests possible risk tolerance levels for the company as the model determines it is not cost-effective to invest in additional security at these λ for a large company.

The optimization results for the insurance premium are displayed in Table 10 and Figure 6. As would be expected, lower values for r result in lower insurance premiums. The plots in Figure 6 plateau because the maximum coverage amount, \$100M, has been reached. It can be observed from Figure 6 that a value for r of approximately 55% or greater is desirable to achieve the goal of not exceeding ALE provided that λ is greater than approximately \$50M. At values of λ from approximately \$28M to

Table 10. Unlimited budget optimization results for insurance premium (P).

Severity(λ)	ALE	P ($r = 50\%$)	P ($r = 55\%$)	P ($r = 60\%$)
\$10,000,000	\$405,000	\$580,000	\$562,400	\$540,800
\$11,000,000	\$445,500	\$636,727	\$617,582	\$592,706
\$12,000,000	\$486,000	\$676,727	\$653,582	\$624,706
\$13,000,000	\$526,500	\$716,727	\$689,582	\$656,706
\$14,000,000	\$567,000	\$756,727	\$725,582	\$688,706
\$15,000,000	\$607,500	\$796,727	\$761,582	\$720,706
\$25,000,000	\$1,012,500	\$1,196,727	\$1,121,582	\$1,040,706
\$50,000,000	\$2,025,000	\$2,196,727	\$2,021,582	\$1,840,706
\$75,000,000	\$3,037,500	\$3,196,727	\$2,921,582	\$2,640,706
\$100,000,000	\$4,050,000	\$4,196,727	\$3,821,582	\$3,440,706
\$125,000,000	\$5,062,500	\$4,158,733	\$3,778,934	\$3,394,535
\$135,000,000	\$5,467,500	\$4,147,349	\$3,766,143	\$3,380,672
\$150,000,000	\$6,075,000	\$4,133,039	\$3,750,053	\$3,363,226

\$50M, a value of 60% or greater is required. At lower values of λ greater values for r will be required to achieve the goal of insurance premiums not exceeding ALE.

From the perspective of the insured, the optimization provides organizational decision makers with suggested levels of investment in cybersecurity and target rates of discount, r, to seek from an insurer. The optimization also suggests recommended total security budgets ($z + P$) for each value of λ as displayed in Table 11.

From the perspective of the insurer, the optimization provides suggested insurance premiums. The optimization also follows the principle of incentivizing a clients' investments in self-protection which helps the insurer guard against adverse selection.

4.2.2 Optimization Results with a Restricted Security Budget.

The optimization results as previously shown suggest spending levels for security controls and insurance in the absence of budgetary limits. However, it may be the case that resources are limited to the degree that the budget constrains how money is invested. Assume that the oil pipeline company determines that the expected severity of loss (λ) is \$50M and wants to determine the optimum spending on a

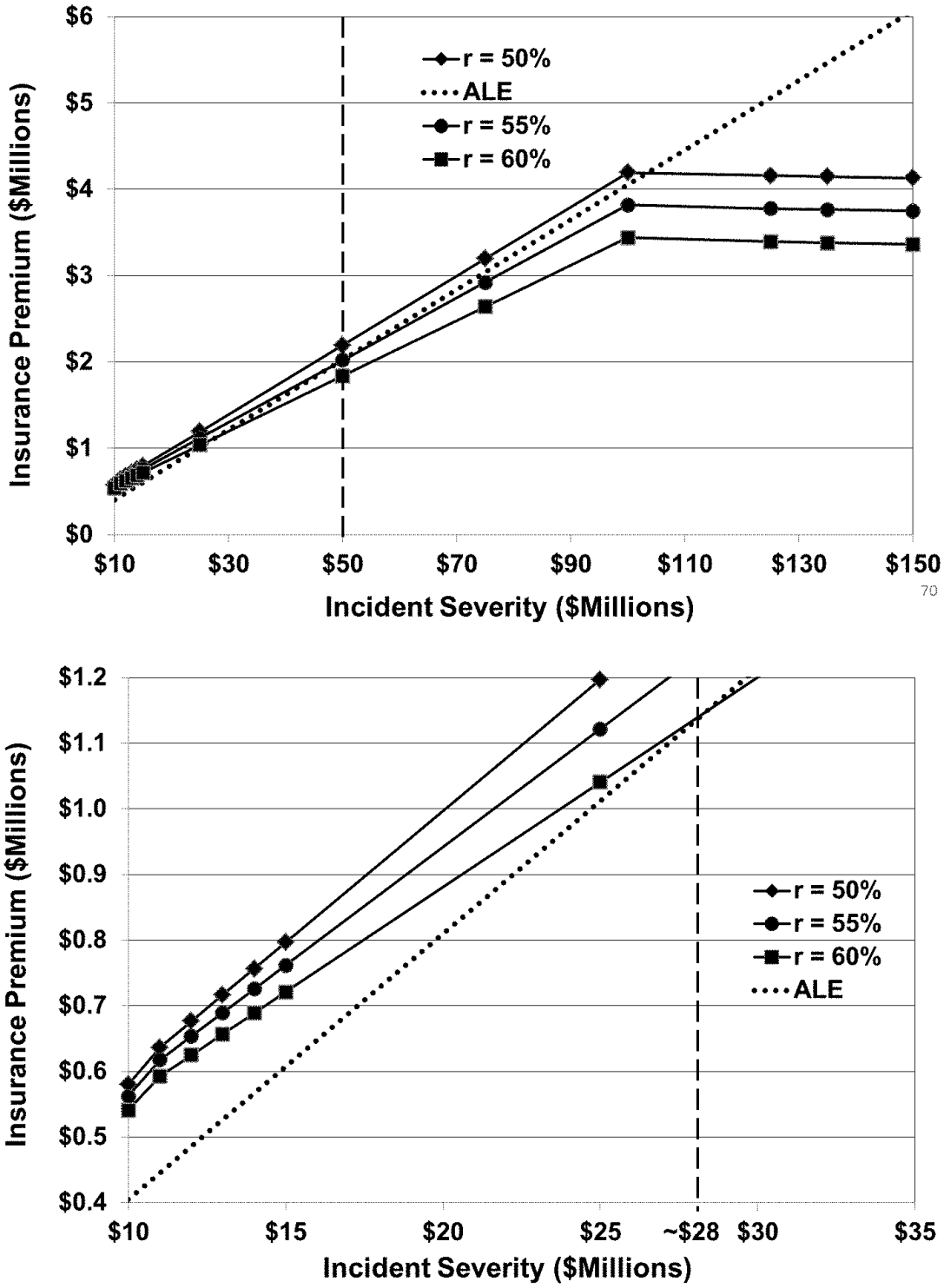


Figure 6. Unlimited budget optimization results for insurance premium (P).

Table 11. Optimization suggested security budget (z+P).

Severity(λ)	r **= 50%**	r **= 55%**	r **= 60%**
$10,000,000	$580,000	$562,400	$540,800
$11,000,000	$666,526	$640,210	$635,436
$12,000,000	$1,108,789	$1,089,859	$1,081,084
$13,000,000	$1,518,834	$1,506,379	$1,493,604
$14,000,000	$1,901,443	$1,894,685	$1,877,910
$15,000,000	$2,260,405	$2,258,674	$2,237,899
$25,000,000	$5,022,005	$5,047,117	$4,986,343
$50,000,000	$9,226,498	$9,242,310	$9,081,535
$75,000,000	$12,101,006	$12,069,874	$11,809,099
$100,000,000	$14,430,990	$14,337,502	$13,976,728
$125,000,000	$15,385,098	$15,311,145	$14,942,985
$135,000,000	$15,717,740	$15,650,950	$15,280,560
$150,000,000	$16,175,764	$16,119,096	$15,745,891

restricted security budget. A value of 55% is chosen for r because as shown in Table 10, P does not exceed ALE at λ = $50M.

The range of security budget values analyzed is $2.8M to $12M. $2.8M is chosen because it is the maximum cost of insurance given the current parameters used in the optimization. Table 12 displays a summary of the values used as inputs for the optimization with an unlimited security budget.

Table 12. Optimization inputs used with a restricted security budget.

Inputs	**Values**
Security Budget	$2.8M to $12M
ARO	10%
λ	$50M
t	90%
v	46%
α	0.000027
Cov	$50M
Cov_{Max}	$100M
P_0	8% of Cov
r	55%

Figure 7 displays the suggested levels of security spending at varying levels of budget and the resulting residual risk ($S(z, v)\lambda t$). Note that the optimization result for an unlimited security budget is also displayed as a reference. Security investment levels should be balanced with the resulting residual risk in order to determine a desirable cost to benefit ratio. For example, as observed in Figure 7, increasing the security investment from the suggested level of \$0 at a budget of \$2.8M to a suggested investment of \$2.5M at a budget of \$5M, the residual risk is reduced by approximately \$9M.

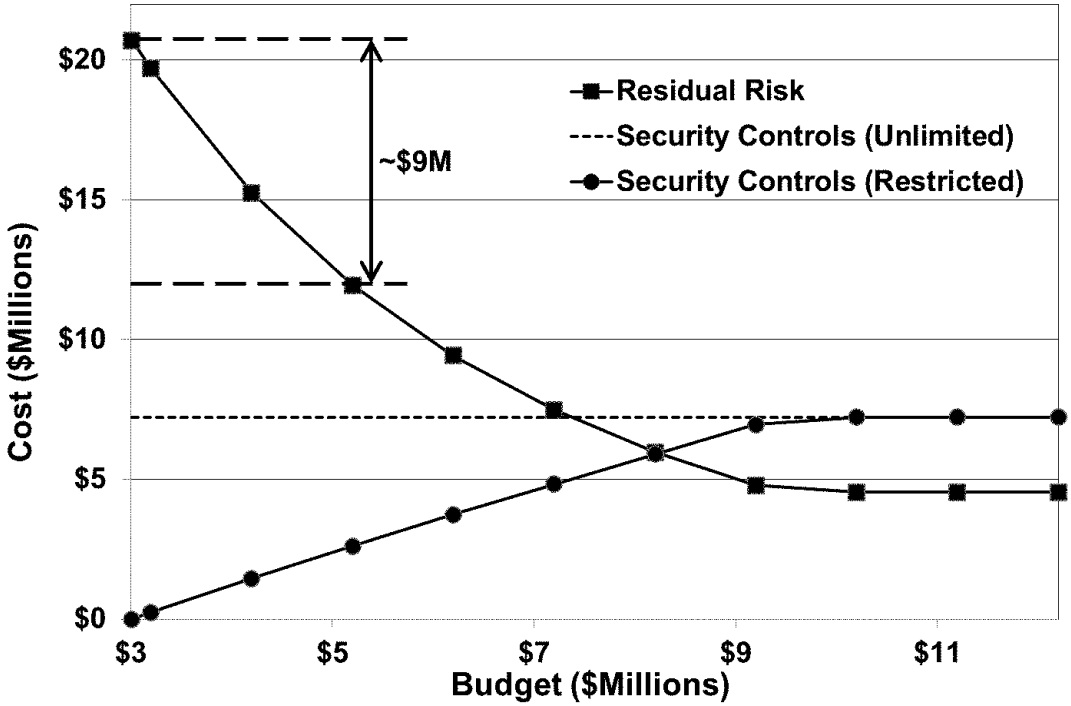


Figure 7. Restricted budget optimization results for security controls (z) and residual risk ($S(z, v)\lambda t$).

Figure 8 displays the suggested expenditures on insurance premiums at varying levels of budget (optimization results for an unlimited security budget are also displayed as a reference). Note that suggested expenditures for insurance are not below ALE until the budget is greater than \$8.5M. The decision now before management is

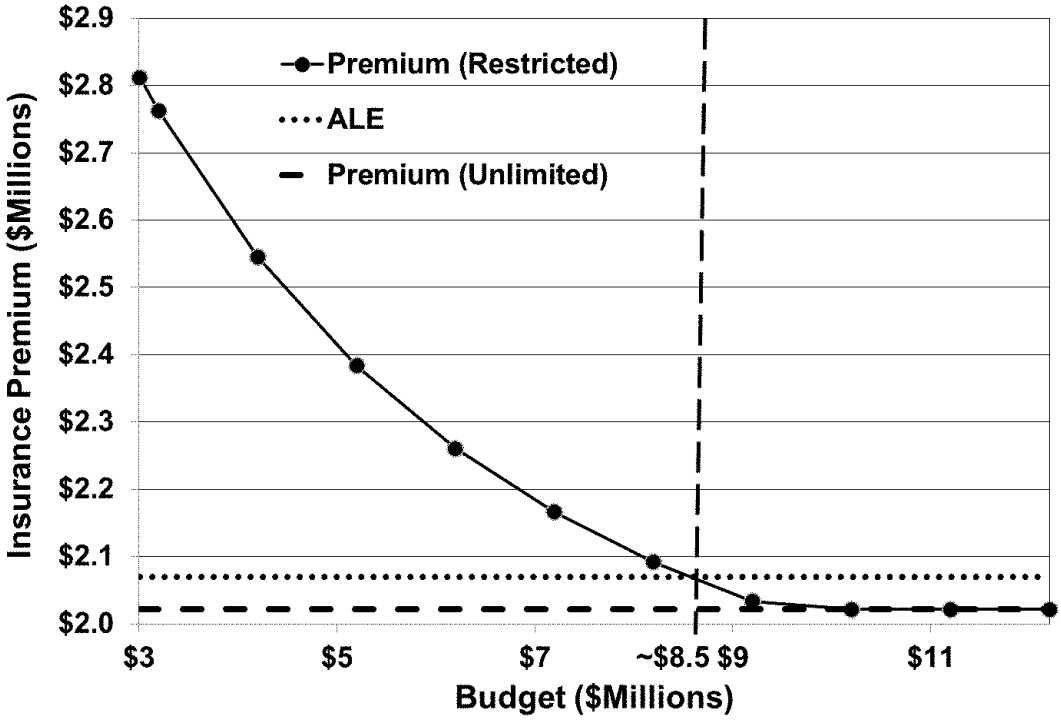


Figure 8. Restricted budget optimization results for insurance premium (P).

what level of budget to choose given the information presented optimization outputs as well any previously set risk thresholds.

From the perspective of the insured, the optimization recommends a budgetary ratio between security controls investment and insurance premiums. These ratios are displayed in Table 13. The optimization favors investments in insurance over investments security controls. This is seen at the lowest budgetary value in Table 13 which devotes 100% of the budget to insurance. It is also noted from the tables and figures that the suggested investments in controls and insurance plateau recommending a budget of approximately $9M is the maximum that should be considered. For the insured, the optimization again suggests insurance premium amounts and also provides insight into what the insurer may wish to require as a client's minimum investment in security controls.

Table 13. Optimization suggested ratios of z and P to total security budget.

Security Budget	z as Percentage of Budget	P as Percentage of Budget
\$2,812,000	0%	100%
\$3,000,000	7.91%	92.09%
\$4,000,000	36.37%	63.63%
\$5,000,000	52.33%	47.67%
\$6,000,000	62.32%	37.68%
\$7,000,000	69.06%	30.94%
\$8,000,000	73.85%	26.15%
\$9,000,000	77.40%	22.60%
\$10,000,000	78.13%	21.87%
\$11,000,000	78.13%	21.87%
\$12,000,000	78.13%	21.87%

4.2.3 Model Refinements.

The optimization results suggest a number of observations that could prove useful to an insured's cyber risk management process. However, these estimates were derived with limited empirical data. As more information is gained through data sharing, shared insurance claims details, and an organization's gathered statistics, refinements to the model and predictive values will improve the framework's usefulness.

For example, a small change to the predicted value for v can have large changes to observations from the models used. Figure 9 displays the recommended ratio of insurance premium to security controls investments at varying values of v. The resulting curve shows that at low and high values for v, the optimization suggests that it is more cost-effective to invest in insurance than in security controls. The curve follows the pattern intended by the Gordon-Loeb Class II function.

Additionally, selecting an appropriate α value can have very large effects on the results of the optimization. Figure 10 displays recommended security investments for the oil pipeline company at varying values of λ for the three values of α presented previously in Table 7. Note that mistakenly selecting an α value that is too large (rep-

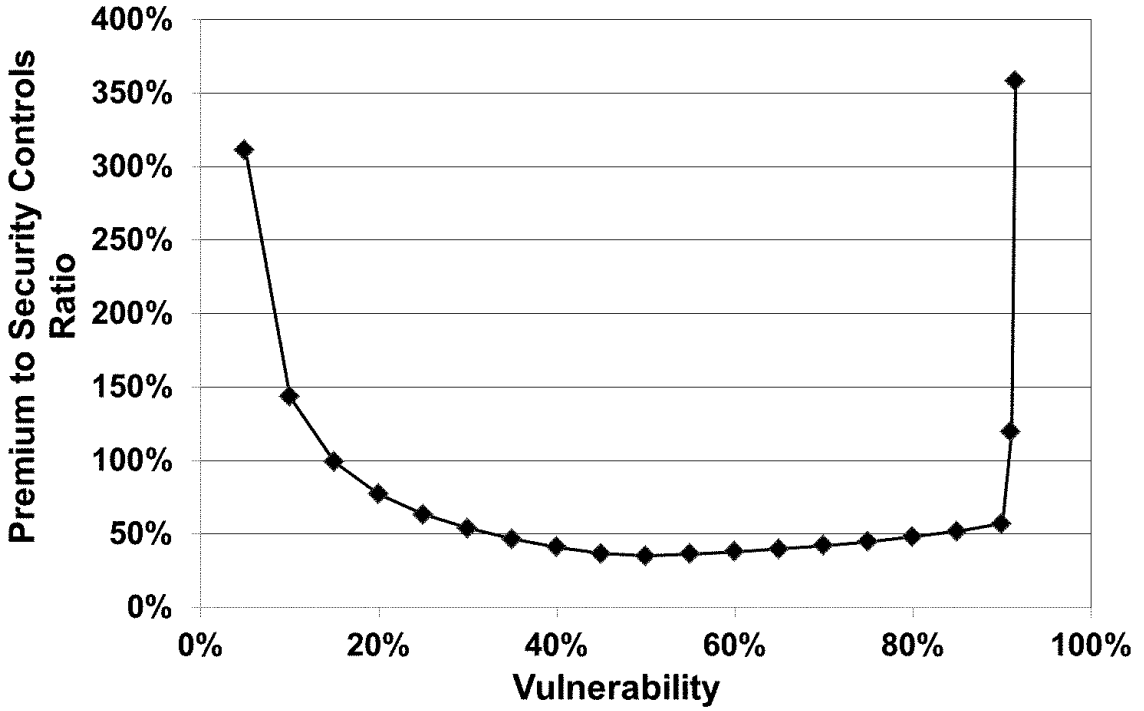


Figure 9. Optimization results for insurance premium (P) to security controls (z) ratio.

resenting a system with low exposure) would result in an organization underinvesting in security controls.

From both the perspectives of the insured and the insurer these observations emphasize the importance of continuous improvement to the framework's models. As previously stated, it may be necessary to select different models to be used in the framework when more accurate methods are discovered. The periodic improvements are aided through data and information sharing conducted between the insured, the insurer and other participating entities (e.g., governmental and academic). Another advantage gained by an insurer through data sharing and model improvements is the ability to provide adequate and competitive insurance rates which ensure their profitability.

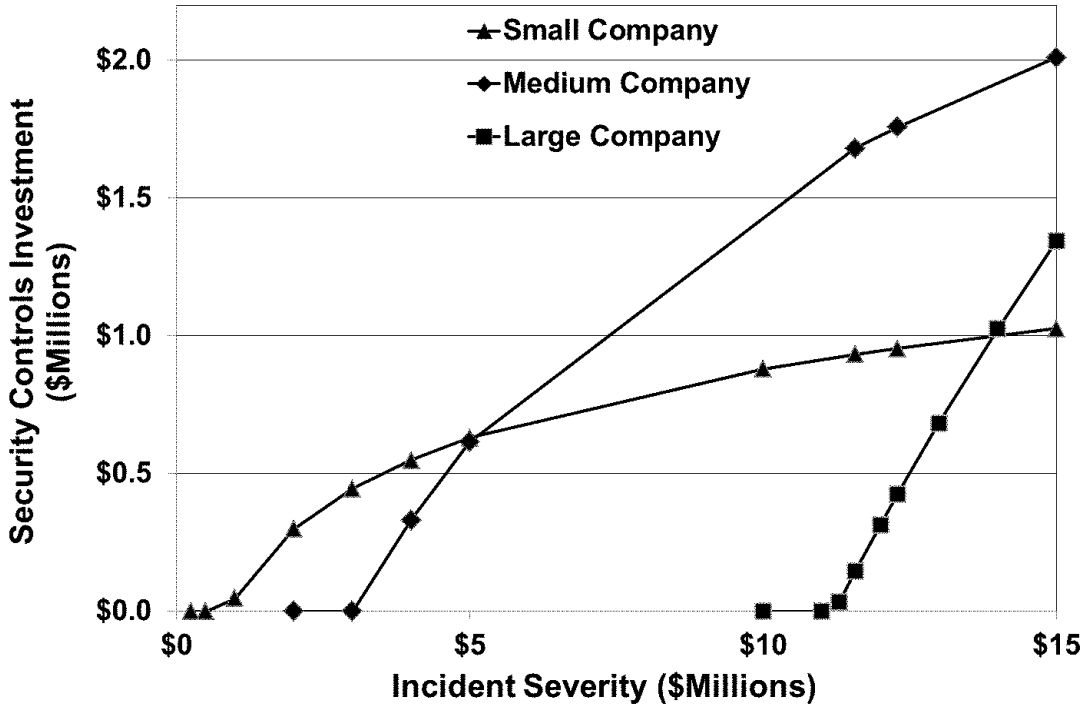


Figure 10. Optimization results for security investment (z) at different values of α.

4.3 Demonstration of Framework Applicability

The applicability of the framework will be demonstrated by applying it to three scenarios which can be generally applied to any critical infrastructure organization in a similar situation seeking to insure and protect against cyber threats. The first scenario describes Company A, an organization which has decided to use quantitative methods in its risk management process for the first time. The second scenario describes Company B which has been using quantitative risk management methods but, in the light of new information, now needs to adjust its models. In the third scenario Company C has an inherently insecure legacy system and is seeking to insure against possible cyber threats.

4.3.1 Company A.

Company A is a small business that distributes natural gas to a three county area. Its distribution network consists of 1,000 networked SCADA devices that share the same network as its traditional IT infrastructure. During the previous year, Company A suffered cyber-induced losses with cumulative costs of $750K and has decided to seek insurance coverage. Company A wants to determine how much it should expect to spend on security controls and insurance.

This is the first year that the company has decided to use the framework and therefore selects the α value for a small company (see Table 7). Information shared through prospective insurers as well as other sources result in values of 10% for ARO, 95% for t, and 45% for v. The insurer reports that the average annual insurance claim made by similar companies is $1.5M. After an assessment performed by the insurer, it is determined that Company A must spend a minimum of $200K on appropriate security controls annually to be eligible for coverage. The insurer provides a base rate of 5% of the coverage being sought for the annual premium and offers a discount where $r = 50\%$. Table 14 displays a summary of the parameters used in the optimization.

Table 14. Optimization inputs used for Company A.

Inputs	Values
Security Budget	Unlimited
ARO	10%
λ	$750K to $3M
t	95%
v	45%
α	0.000346
Cov	$750K to $3M
Cov_{Max}	$100M
P_0	5% of Cov
r	50%

Company A incorporates uncertainty into their estimates by providing a range of losses from $750K to $3M. Table 15 shows the security budget levels recommended by the optimization results. Figure 11 displays the recommended levels of investment

Table 15. Optimization results for Company A.

Incident Severity(λ)	Security Controls(z)	Insurance Premium(P)	Recommended Security Budget
$750,000	$200,000	$23,602	$223,602
$1,000,000	$200,000	$31,469	$231,469
$1,250,000	$200,000	$39,337	$239,337
$1,500,000	$216,577	$46,769	$263,347
$1,750,000	$272,306	$53,019	$325,326
$2,000,000	$320,581	$59,269	$379,850
$2,250,000	$363,162	$65,519	$428,682
$2,500,000	$401,252	$71,769	$473,022
$2,750,000	$435,709	$78,019	$513,729
$3,000,000	$467,165	$84,269	$551,435

in security controls and insurance. The results suggest that if the incident severity (λ) is less than $1.3M, Company A only invests the required minimum of $200K in security controls. At these levels of loss, the optimization determines that it is not cost effective to invest additional money in self-protection. This outcome highlights the importance of the insurer placing minimum standards of cybersecurity on potential clients in order to ensure that they are not practicing bad risk behaviors. Levels greater than or equal to $1.3M for λ suggest increasing levels of security spending to reach the optimized results.

4.3.2 Company B.

Company B is a business that processes clean water for distribution in a large metropolitan area. They use a distributed control network which monitors and manages hundreds of processing, purification and distribution points. Company B has been using quantitative cyber risk methods and held insurance policies against cyber

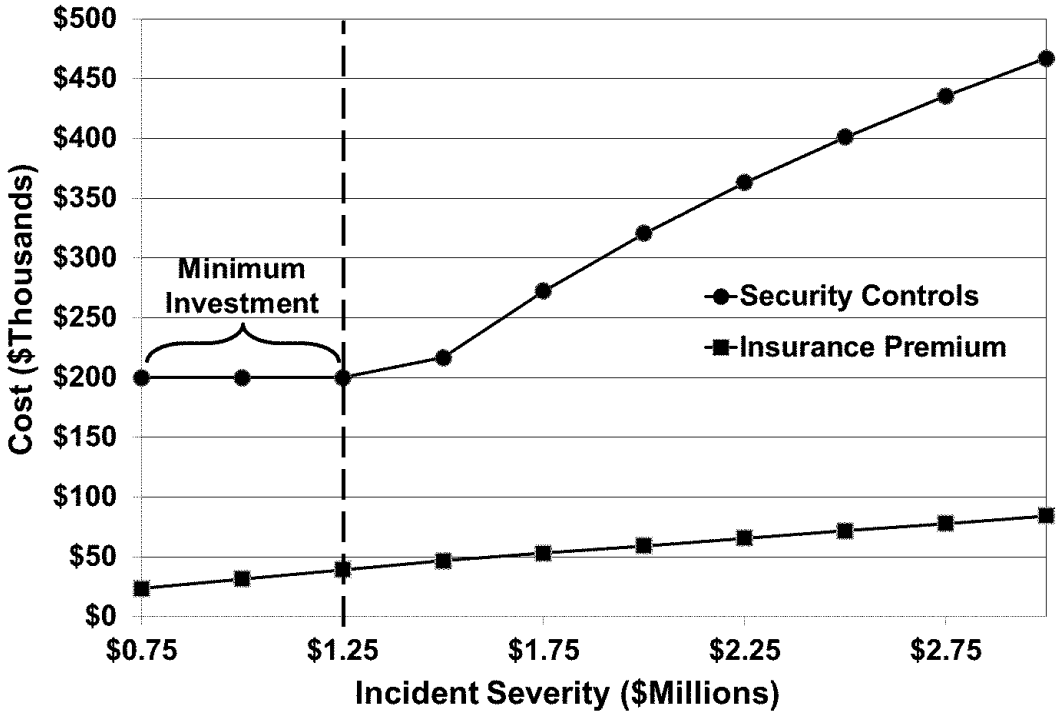


Figure 11. Optimization results for Company A.

threats for a number of years. However, during the last year the losses ($18M) exceeded projections ($11M) due in large part to a cyber-induced incident realized from a disgruntled employee. The insurance policies did not sufficiently cover the losses.

Company B is seeking to better balance its risk minimization strategies. During the previous year, the security budget was approximately $1.8M. They had determined their α value to be approximately 3.3×10^{-6} at an estimated 2% of threats successfully breaching security controls (i.e., $S(z, v)$). However, the actual percentage of successfully realized breaches during the previous year was 30% of detected threats. With this new value for $S(z, v)$, Company B now solves for α using Equation (5) and calculates a higher exposure level for its system and adjusts its α value to be 6.8×10^{-7}. Additionally, Company B decides to analyze a range for λ of $10M to $25M with the most likely value being near their actual losses of $18M.

During the previous year, the insurer had offered a base rate of 7% with $r = 40\%$. After the claims had been made with the insurer, the base rate was adjusted upward

Table 16. Optimization inputs used for Company B.

Inputs	Values
Security Budget	Unlimited
ARO	10%
λ	\$10M to \$25M
t	80%
v	60%
α	6.8×10^{-7}
Cov	\$10M to \$25M
Cov_{Max}	\$100M
P_0	7% of Cov
r	40%

to 10% of coverage while r was maintained at 40%. Table 16 displays a summary of the parameters used in the optimization.

Table 17 shows the previous year's recommended security budget and the new estimates for the current year. The results suggest that Company B has been underinvesting in security. The updated optimization suggests that the security budget be increased by \$1M at the previous year's expected loss value (λ = \$11M) and an increase of about \$2M at the actual loss level (λ = \$18M).

Figure 12 compares the estimated costs for security controls and insurance premiums using the estimates from the previous and current years. Note from Figure 12 that if Company B had continued to use the prior year's parameters and planned for a new expected loss level of \$18M, the optimization would recommend that they increase their security controls investment by about \$0.3M. However, the updated optimization suggests that they increase security controls spending by \$1.5M over the previous year. This outcome highlights the importance of periodic improvements to models.

Also of possible concern to management is the increase in insurance premiums. It may be the case that if Company B had invested in security controls as the updated optimization suggests, the breaches of their security would not have occurred and

Table 17. Optimization Recommended Security Budgets for Company B from the Previous and Current Year.

Incident Severity(λ)	Prior Year Security Budget	Current Year Security Budget
\$10,000,000	\$1,694,735	\$2,516,419
\$11,000,000	\$1,792,780	\$2,794,153
\$12,000,000	\$1,885,946	\$3,052,930
\$13,000,000	\$1,975,013	\$3,295,786
\$14,000,000	\$2,060,591	\$3,525,085
\$15,000,000	\$2,143,160	\$3,742,699
\$16,000,000	\$2,223,111	\$3,950,137
\$17,000,000	\$2,300,760	\$4,148,633
\$18,000,000	\$2,376,371	\$4,339,211
\$19,000,000	\$2,450,164	\$4,522,727
\$20,000,000	\$2,522,325	\$4,699,906
\$21,000,000	\$2,593,015	\$4,871,367
\$22,000,000	\$2,662,371	\$5,037,641
\$23,000,000	\$2,730,509	\$5,199,191
\$24,000,000	\$2,797,536	\$5,356,418
\$25,000,000	\$2,863,540	\$5,509,675

their insurance rates would not have risen. These outcomes highlight the importance of continuous and periodic improvements predictive models in order to ensure their accuracy.

4.3.3 Company C.

Company C is a business that operates multiple oil refineries along the Gulf Coast. They are seeking to modernize their operations and have connected their legacy control network to their corporate network. With potential cyber threats to their control network, Company C seeks to insure against cyber threats. The cybersecurity assessments performed by the insurer (and other experts) reveal that the system is highly vulnerable with an estimated 90% of threats successfully breaching the limited security of their legacy network. It is also estimated that potential damages would range from \$30M to \$50M. System exposure is estimated with an α value of 2.7×10^{-7}. Due

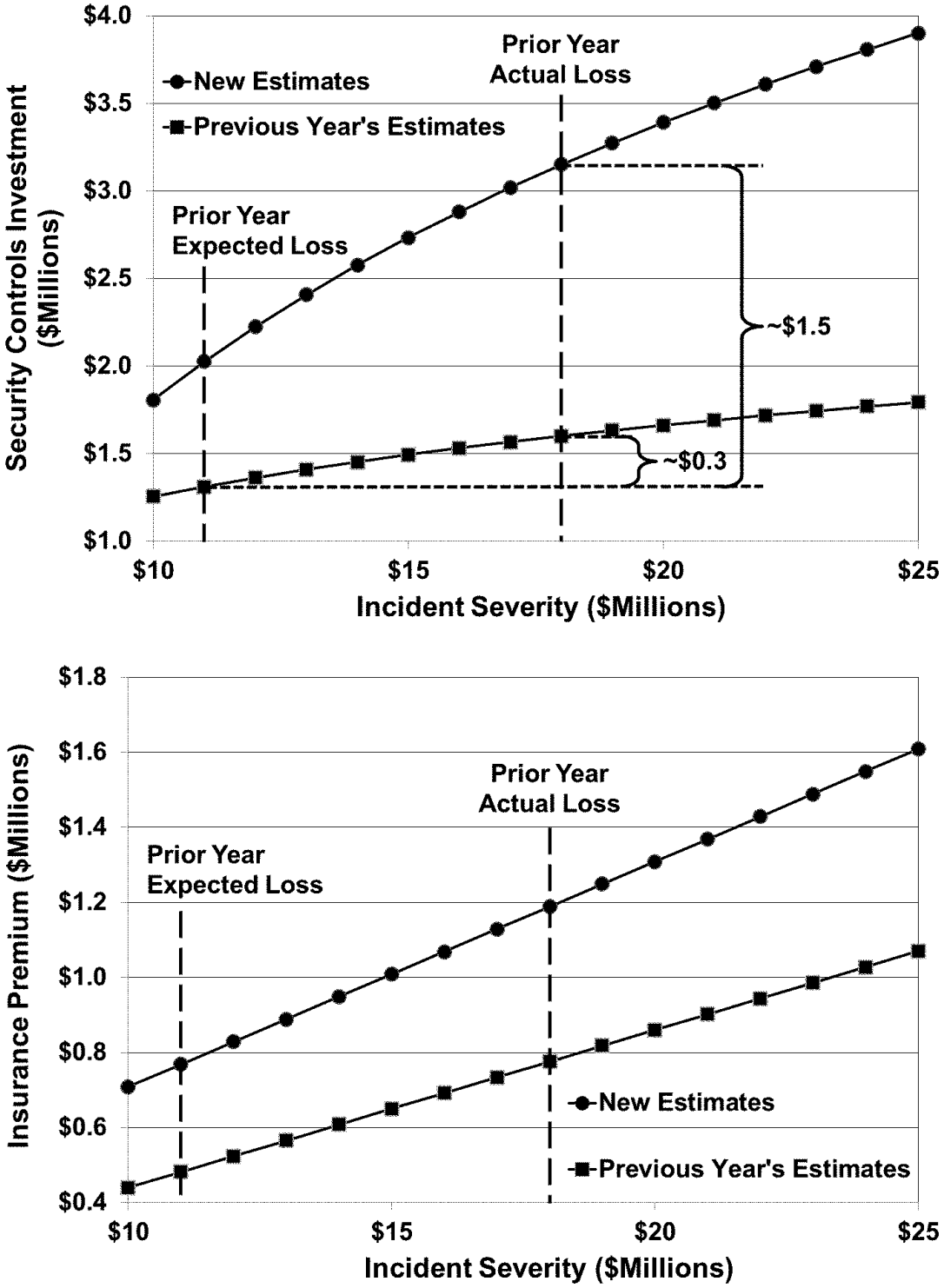


Figure 12. Optimization results for Company B.

to the system's high exposure and vulnerability, the insurer offers a base rate of 20% and heavily incentivizes investments in self-protection with $r = 75\%$. Additionally, the insurer has required that Company C implement a set of controls which cost a minimum of $500K annually. Company C has decided on a security budget of $3M for controls and insurance.

Because the budget chosen is restrictive to the point that it may not be possible to purchase full insurance coverage, the amount of coverage purchased in the optimization Cov is used as a decision variable. The objective function from Equation (8) is modified to also maximize the amount of coverage purchased. The new objective function is $minimize[S(z, v)\lambda t + z + P - Cov]$. Table 18 displays a summary of the parameters used in the optimization.

Table 18. Optimization inputs used for Company C.

Inputs	Values
Security Budget	$3M
ARO	10%
λ	$30M to $50M
t	80%
v	90%
α	2.7×10^{-7}
Cov	Becomes a decision variable
Cov_{Max}	$100M
P_0	20% of Cov
r	75%

The results from the optimization can be seen in Table 19. The optimization suggests that only the minimum of $500,000 be invested in security controls. Company C should devote the remaining security budget to insurance and maximize the amount of coverage purchased. If the insurer had not placed the minimum requirement on security controls the optimization would have recommended that no money be invested. This outcome highlights the importance of an insurer requiring minimum levels of security.

Table 19. Optimization results for Company C.

Incident Severity(λ)	Security Controls(z)	Insurance Premium(P)	Coverage Purchased	Total Budget Used
\$30,000,000	\$500,000	\$2,197,046	\$30,000,000	\$2,697,046
\$32,000,000	\$500,000	\$2,444,541	\$32,000,000	\$2,944,541
\$34,000,000	\$500,000	\$2,489,985	\$34,000,000	\$2,989,985
\$36,000,000	\$500,000	\$2,500,000	\$34,136,742	\$3,000,000
\$38,000,000	\$500,000	\$2,500,000	\$34,136,742	\$3,000,000
\$40,000,000	\$500,000	\$2,500,000	\$34,136,742	\$3,000,000
\$42,000,000	\$500,000	\$2,500,000	\$34,136,742	\$3,000,000
\$44,000,000	\$500,000	\$2,500,000	\$34,136,742	\$3,000,000
\$46,000,000	\$500,000	\$2,500,000	\$34,136,742	\$3,000,000
\$48,000,000	\$500,000	\$2,500,000	\$34,136,742	\$3,000,000
\$50,000,000	\$500,000	\$2,500,000	\$34,136,742	\$3,000,000

Also note, the optimized z for λ of \$30M, \$32M and \$34M results in total expenditures below the \$3M budget set by the company. This result is due to the benefits of additional security control investments not outweighing the residual risk. The optimization therefore recommends the money not be further invested in security controls.

Figure 13 displays the estimated insurance premium in relation to ALE. While the premium does become less than ALE at an approximate incident severity of \$35M, note that if the budget were not restrictive and full coverage were purchased the premium would still exceed ALE.

The optimization suggests that it is not cost-effective to invest in security controls and that insurance premiums may be overly expensive. It may be inferred that the prudent risk strategy is avoidance, meaning that the control and corporate networks should be kept segregated. Otherwise, Company C may want to increase its security budget to rectify the flaws in the system or invest in a new, more modernized and security-focused control system.

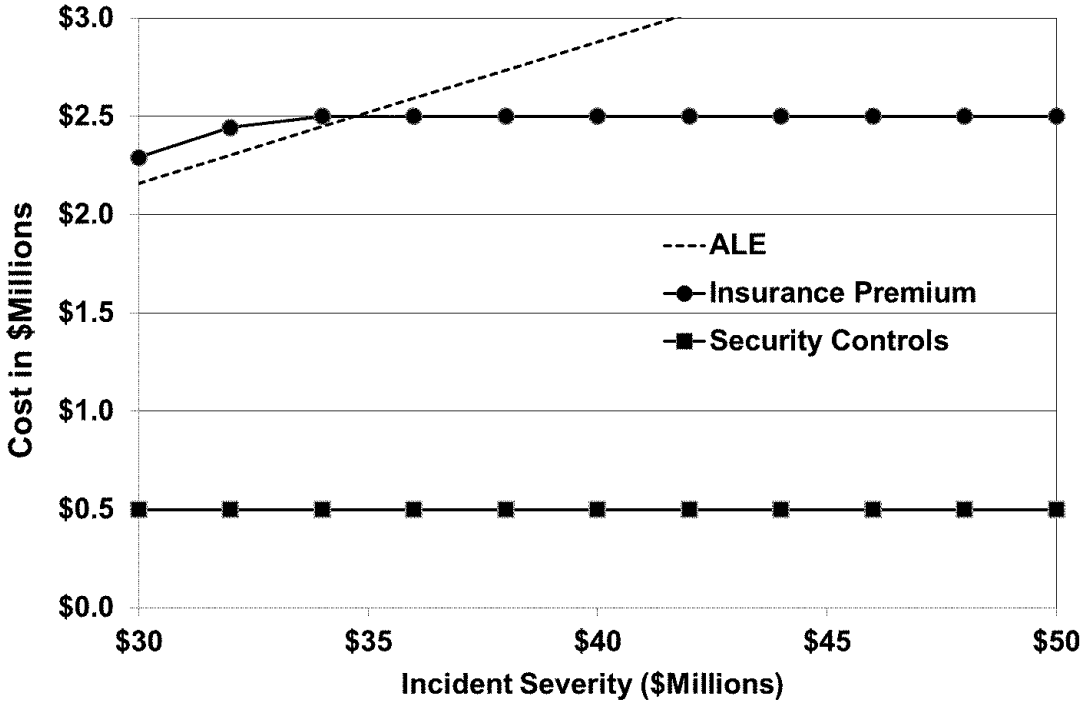


Figure 13. Optimization results for Company C.

4.4 Conclusion

This chapter provides demonstrations of the proposed framework's feasibility and applicability from the perspectives of the insured and the insurer. The framework's feasibility is demonstrated by using it to analyze real oil pipeline ruptures that could have been cyber induced in order to provide estimates for an organization's cyber risk. The applicability is demonstrated by applying the framework to three scenarios which can be generally applied to a critical infrastructure organization.

The outputs obtained from the optimization used within the framework provide suggested levels of investment in security controls, insurance premiums and minimum and maximum recommended security budgets. The outputs also highlight the importance of continuous and periodic refinements and improvements to the models used within the framework. Model refinement is aided and accelerated through information sharing conducted between critical infrastructure stakeholders. All of these outputs

can be used by critical infrastructure owners and operators in forming risk strategies which address their current cyber threats.

V. Conclusions and Recommendations

5.1 Thesis Summary

The following three research goals are presented in Chapter 3 and analyzed in Chapter 4.

1) Demonstrate that the proposed framework considers the perspectives of both the insured and the insurer.

The optimization used within the framework links the separate models together and provides outputs which show insurance is used as an incentive to increase levels of investment in self-protection, the importance of gathering and sharing data is emphasized and a cycle of continuous refinement to quantitative models is adopted. By incorporating these methods from the insurance industry, the interests of both the insured and the insurer are promoted.

The insured pays adequate rates for insurance, avail themselves of the experience shared by the insurer and are able mitigate business risk through its transfer to the insurer. The insurer is able ensure their profitability by guarding against adverse selection through the incentivization of cybersecurity and is also to be able to provide competitive rates as claims are made and trends established.

2) Demonstrate the feasibility of the framework by applying it to a historical example.

Three domestic oil pipeline ruptures that were suffered by an individual company were used to analyze the cyber risk with the proposed framework. The ruptures were caused (in part or in total) by errors in the company's control systems. Because of this, the ruptures can also be shown to have resulted from cyber means and can

be used to provide estimates of the severity of a cyber incident. Estimates for the likelihood of a cyber-induced incident were provided using publicly available empirical data on critical infrastructure.

The optimization used the estimates for severity and likelihood as inputs to provide recommendations for levels of investment in security controls, target rates for discount of insurance premiums and totals for appropriate security budgets in order to demonstrate the framework's feasibility. The framework's quantitative outputs can be used by an organization's decision makers to prepare risk strategies with the goal of minimizing their cyber risk.

3) Demonstrate the applicability of the framework in formulating cyber risk strategies through specific scenarios.

Three specific scenarios were developed which can be generally applied to any critical infrastructure organization seeking to minimize cyber risk through insurance. The scenarios demonstrate that the framework can be applied to diverse situations and aid management in the risk decision-making process.

5.2 Recommendations for Future Research

The limitation of the proposed framework is readily acknowledged in that the outputs from the framework are based on a paucity of data and many assumptions input into a combination of disparate models. There is much work that can be done to improve the accuracy and plausibility of the framework outputs. Therefore, this research can be furthered in the following ways:

- Different models for threat likelihood and severity, the reduction of threat likelihood and severity, and the discount on insurance should be incorporated into the framework presented in Chapter 3 that more accurately reflect current trends

in cybersecurity and cyber insurance. The inclusion of knowledge of the cyber insurance underwriting process as well as current methods used in actuarial science as they apply to cyber insurance would also be beneficial in increasing the accuracy of the outputs from the framework.

- Apply specific ratemaking techniques currently employed in cyber insurance to the framework. Ratemaking is the process used by the insurance industry to set insurance premiums. The model presented in this thesis simply sets the rate as a percentage of the coverage being sought and then applies discounts based on the percentage reduction of risk. More robust methods currently employed by cyber insurers or other new methods should be researched and applied to the framework to improve its accuracy.

- The method in this thesis uses approximation techniques to explore multiple local optima and cannot guarantee that the global optimum is returned as the solution. An algorithm design process using metaheuristics and heuristics specific to the problem could be used to find the global optimum.

5.3 Final Thoughts

The insurance industry has been using quantitative analysis to influence risk decisions for centuries. In order to ensure their own profitability, insurers protect themselves against adverse selection and moral hazard by gathering data, incentivizing clients to invest in self-protection and by continuously refining their assumptions and models. The framework presented in this research incorporates these operating methods in order to quantitatively assess cyber related risk and devise mitigation strategies.

Critical infrastructure owners and operators need to determine whether or not they should invest in insurance given the reality that they implement security controls and have a limited security budget. The question is no longer if a critical infrastructure cyber incident will occur, but when will it occur. The advantages gained by pooling risk and sharing data through insurance result in minimized risk. As more policies are created which cater to critical infrastructure cyber threats, insurance should be considered as an important component of mitigating business risk and as a part of a holistic cyber risk management strategy.

Appendix A. Calculation of Oil Pipeline Incident Severity

The severity of the impact of the three oil pipeline ruptures at Fork Shoals, SC [31]; Murfreesboro, TN [32]; and Knoxville, TN [33] is estimated using the categories employed by the FAIR model [46]. These categories are:

1. Loss of Productivity
2. Response Expenses
3. Replacement and Recovery Expenses
4. Fines and Judgments
5. Loss of Competitive Advantage
6. Loss of Reputation.

The NTSB reports were used as the only reference in conducting the estimates. Any information not available in the reports was estimated using assumptions and judgment. All values from the NTSB reports are adjusted for inflation to 2015 values.

A.1 Estimate for Fork Shoals, SC

Estimate for Fork Shoals, SC

Loss Productivity		
loss of revenue due to immediate impact	$1,778,263.20	957,600 gallon spill. **Assume** $1.857/gal wholesale price.
loss of revenue due to interruption of business process	$62,395,200.00	**Assume** 10 days time to repair. **Assume** avg flow = 840,000 gal/hr. **Assume** operation for 4 hr/day. **Assume** $1.857/gal wholesale price.
Response Expenses		
cost of clean-up operations.	$21,293,384.00	From NTSB report
revenue returned from recovered product	-$418,408.10	901,256 gallons recovered. **Assume** 25% was resellable.
Health-related expenses	$0.00	None in this case
Replacement and Recovery Expenses		
equipment replacement and repairs,	$353,429.00	**Assume** 500 feet of pipeline replaced. **Assume** replacement cost = $100/ft3. 500 ft. of 36" pipe = 3534.29 ft3.
Fines and Judgements		
fines levied (federal)	$31,117,270.00	From NTSB report
fines levied (criminal)	$10,248,258.00	From NTSB report
non-frivolous lawsuits filed against organization	$9,664,468.00	From NTSB report
cost of legal team	$150,000.00	**Assume** $500/hr; 300 hours
Loss of Competitive Advantage		
Loss of customers	$0.00	**Assume**: lack of competition
Loss of Reputation		
depressed share price	$0.00	Private company
cost of public relations campaign	$250,000.00	**Assumption**

Total (λ): **$135,053,600.90**

A.2 Estimate for Murfreesboro, TN

Estimate for Murfreesboro, TN

Loss Productivity		
loss of revenue due to immediate impact	$119,427.00	84,700 gallon spill. **Assume** $1.41/gal wholesale price.
loss of revenue due to interruption of business process	$423,000.00	**Assume** 2 days time to repair. **Assume** loss of opportunities is 150,000 gal/day **Assume** $1.41/gal wholesale price.
Response Expenses		
cost of clean-up operations.	$8,357,751.43	$5.7 mil (1996) inflated for 2015
revenue returned from recovered product	-$12,866.25	36,500 gallons recovered. **Assume** 25% was resellable.
health-related expenses	$0.00	None in this case
Replacement and Recovery Expenses		
equipment replacement and repairs,	$0.00	*Included in cost of clean-up operations by NTSB report*
Fines and Judgements		
fines levied (federal)	$1,986,068.97	November 2000 Federal fine
non-frivolous lawsuits filed against organization	$0.00	No record found
cost of legal team	$150,000.00	**Assume** $500/hr; 300 hours
Loss of Competitive Advantage		
loss of customers	$0.00	**Assume**: lack of competition
Loss of Reputation		
depressed share price	$0.00	Private company
cost of public relations campaign	$250,000.00	**Assumption**

Total (λ): **$11,273,381.15**

A.3 Estimate for Knoxville, TN

Estimate for Knoxville, TN

Loss Productivity		
loss of revenue due to immediate impact	$75,505.50	53,550 gallon diesel spill. **Assume** $1.41/gal wholesale price.
loss of revenue due to interruption of business process	$564,000.00	**Assume** 2 days time to repair. **Assume** loss of opportunities is 200,000 gal/day **Assume** $1.41/gal wholesale price.
Response Expenses		
cost of clean-up operations.	$10,013,277.31	$7 mil (1999) inflated for 2015
revenue returned from recovered product	-$15,515.64	44016 gallons recovered. **Assume** 25% was resellable.
Health-related expenses	$0.00	None in this case
Replacement and Recovery Expenses		
equipment replacement and repairs,	$0.00	*Included in cost of clean-up operations by NTSB report*
Fines and Judgements		
fines levied (federal)	$1,255,655.17	November 2000 Federal fine
non-frivolous lawsuits filed against organization	$0.00	No record found
cost of legal team	$150,000.00	**Assume** $500/hr; 300 hours
Loss of Competitive Advantage		
Loss of customers	$0.00	**Assume**: lack of competition
Loss of Reputation		
depressed share price	$0.00	Private company
cost of public relations campaign	$250,000.00	**Assumption**

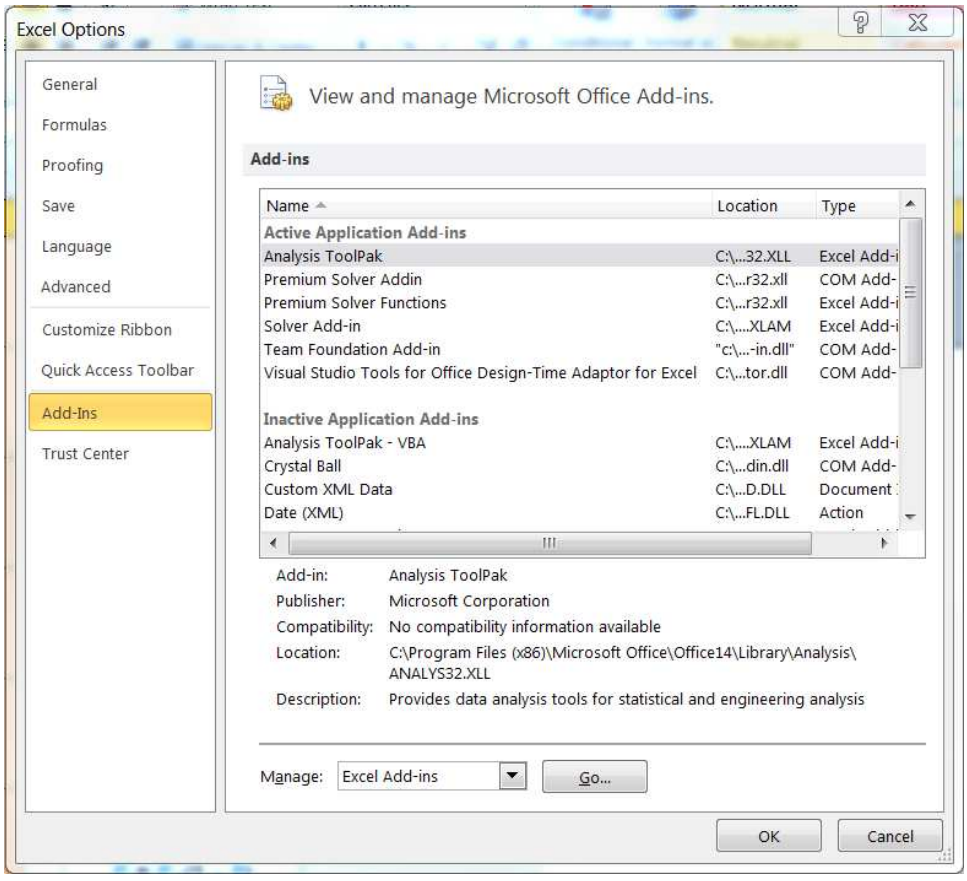
Total (λ): **$12,292,922.34**

Appendix B. Frontline Premium Solver 7.0 for Microsoft Excel

This Appendix briefly describes how Frontline's Premium Solver is installed within Microsoft Excel as well as how to configure the spreadsheet for the optimization discussed in Chapter 3.

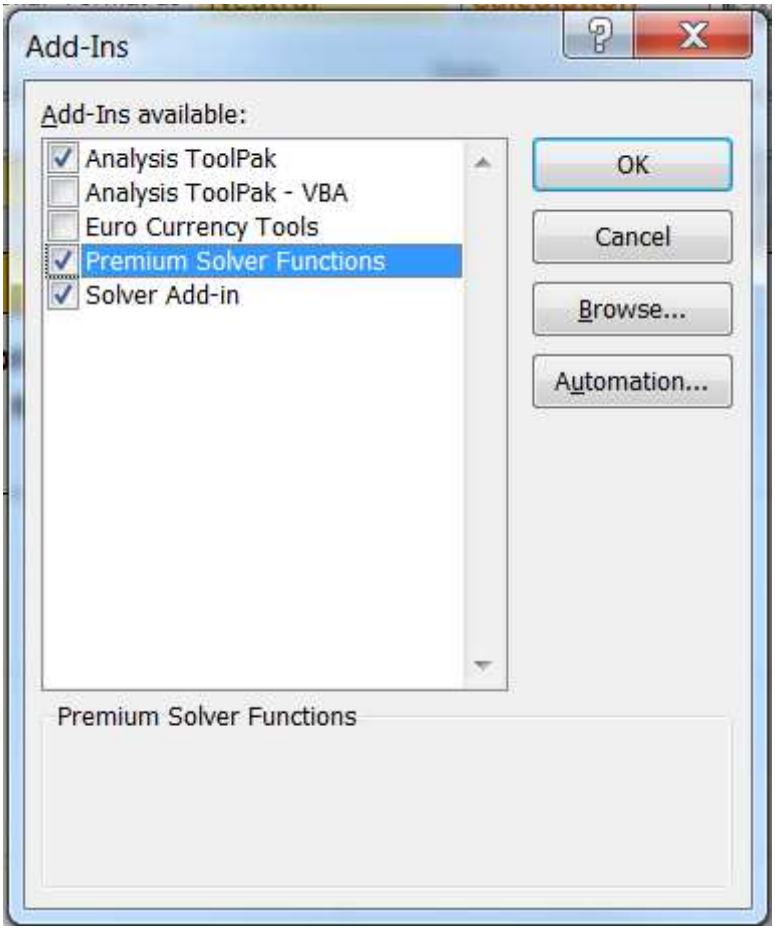
Once the Frontline Premium Solver for Microsoft Excel is obtained and installed on the computer it needs to be included as an add-in within the Excel program using the following steps:

- Open Excel options from the menu and select "Add-Ins" as shown in the following image.



- Manage the Excel add-ins from the drop down menu.

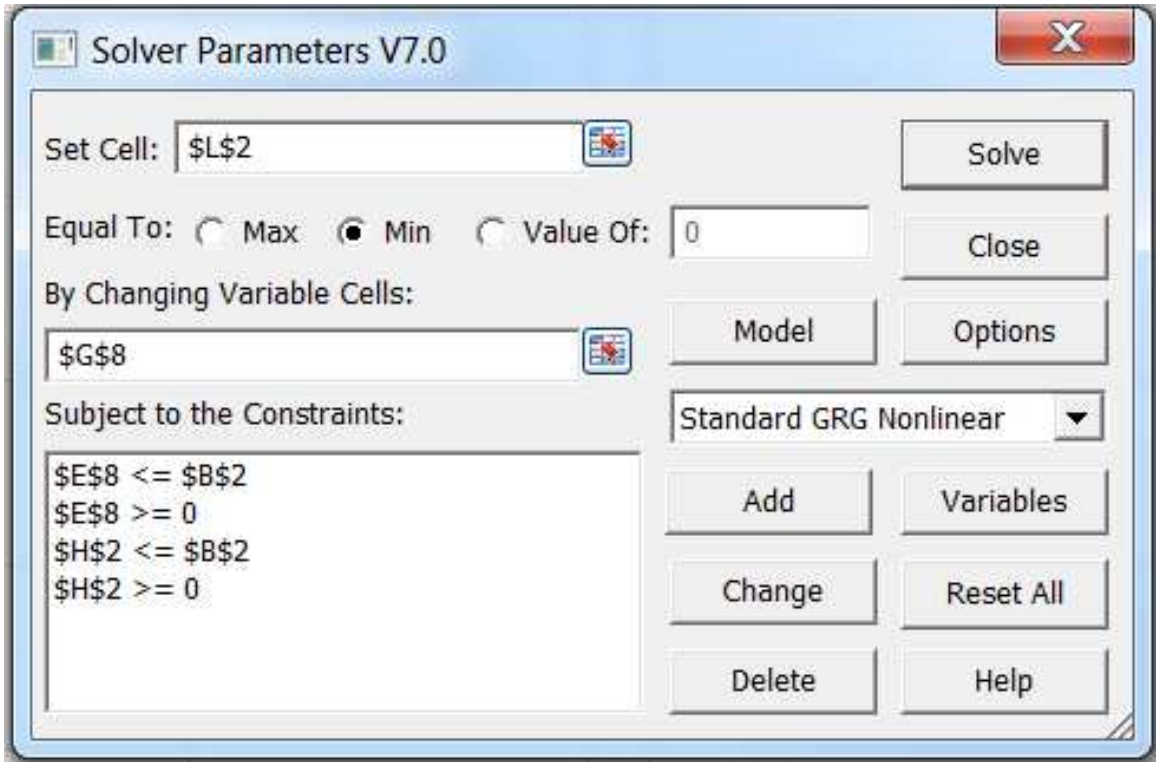
- Under available add-ins, select "Premium Solver Functions" as shown in the following image.



After Premium Solver is properly installed in Excel, build the spreadsheet after the manner discussed in Chapter 3 and as demonstrated in the following image:

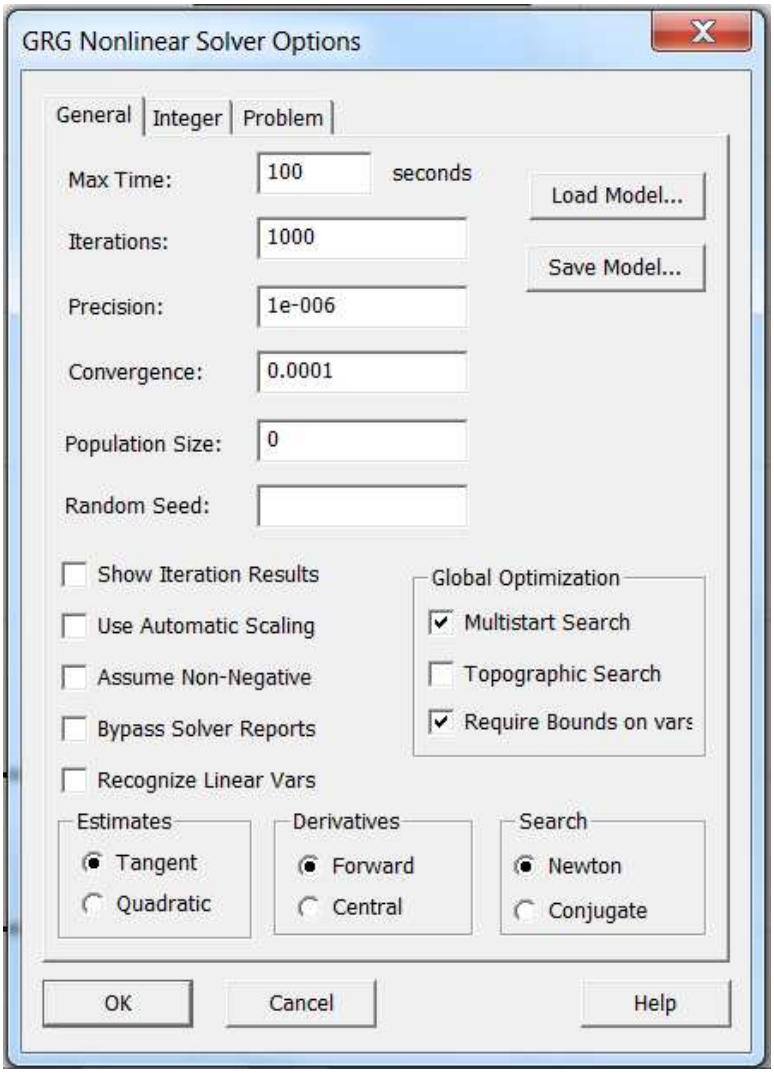
	A	B	C	D	E	F	G	H	I	K	L
1	**Inputs**			**Calculations**			**Decision Variables**			**Objective**	
2	Security Budget	0		Single Loss Expectancy: $SLE = EF \times AV = \lambda t v$	=B4*B5*B6		Monetary investment in security controls: z	0		Minimize residual risk and the costs of controls and insurance: $minimize\ (S(z,v)\lambda t + z + P)$	=E6+H2+E7
3	Annual Rate of Occurrence: ARO	0		Annualized Loss Expectancy: $ALE = ARO \times SLE$	=B3*E2						
4	Impact of cyber attack: λ (aka AV)	0		Security breach probability function: $S''(z,v)$	=(B6^(B7*H2+1))						
5	Probability of attempted cyber security breach: t	0		Residual Risk: $S(z,v)\lambda t$	=E4*B4*B6						
6	Prob that realized threat results in successful attack: v	0		Percentage discount on insurance: $\delta = r * (1 - S(z,v))$	=B11*(1-E4)						
7	Weight representing exposure of network: a	0		Discounted insurance premium: $P = P_0(1 - \delta)$	=B10*(1-E6)						
8	Insurance Coverage to be purchased: Cov	0		Total expenditures: $z + P$	=H2+E7						
9	Maximum insurance coverage available: Cov_{max}	0									
10	Insurance premium base rate: P_0	0									
11	Insurance rate of discount: r	0									

Once the spreadsheet is built, open Premium Solver from the Add-Ins tab in Excel. The dialog box containing the parameters to be used in the optimization should be populated after the manner shown in the following image:



The constraints can be modified to account for minimum investments in security by altering the "H2 >=" item in the parameters dialog box.

Finally, open the options within Solver Parameters and select options after the manner discussed in Table 4 and as displayed in the following image:



Once the spreadsheet has been filled with the appropriate data the outputs are obtained by selecting "Solve" from within the Solver Parameters dialog box.

Bibliography

[1] Ashish Arora, Dennis Hal, C. Ariel Pinto, Dwayne Ramsey, and Rahul Telang. An ounce of prevention vs. a pound of cure: How can we measure the value of it security solutions? Published by Lawrence Berkeley National Laboratory, January 2004.

[2] Rainer Böhme. Cyber-insurance revisited. In *Workshop on the Economics of Information Security*, Cambridge, MA, 2005. Harvard University.

[3] Rainer Böhme and Gaurav Kataria. Models and measures for correlation in cyber-insurance. In *Fifth Workshop on the Economics of Information Security*, Cambridge, MA, June 2006.

[4] Rok Bojanc and Borka Jerman-Blažič. An economic modeling approach to information security risk management. *International Journal of Information Management*, 28(5):413–422, 2008.

[5] Jean Bolot and Marc Lelarge. Cyber insurance as an incentive for internet security. In *Managing information risk and the economics of security*, pages 269–290. Springer, 2009.

[6] Karl Henrik Borch, Agnar Sandmo, and Knut Kristian Aase. *Economics of insurance*, volume 29. Elsevier, 2014.

[7] Matthias Brecht and Thomas Nowey. A closer look at information security costs. In *The Economics of Information Security and Privacy*, pages 3–24. Springer, 2013.

[8] Jonathan Butts, Mason Rice, and Sujeet Shenoi. Modeling control system failures and attacks–the waterloo campaign to oil pipelines. In *Critical Infrastructure Protection IV*, pages 43–62. Springer, 2010.

[9] Jennifer Copic Dale Peterson and Eireann Leverett. Unsolicited Response Podcast: Cyber Insurance. Published by Digital Bond, August 2015. Available at `www.digitalbond.com/blog/2015/08/27/unsolicited-response-podcast-cyber-insurance`.

[10] Department of Homeland Security. Cybersecurity Insurance. World Wide Web Page, 2015. Available at `www.dhs.gov/cybersecurity-insurance`.

[11] Department of Homeland Security. Information Sharing. World Wide Web Page, 2015. Available at `www.dhs.gov/topic/cybersecurity-information-sharing`.

[12] Peter G. M. Dickson. *The Sun Insurance Office, 1710-1960: The history of two and a half centuries of British insurance*. Oxford University Press, 1960.

[13] John Ficenec. Cyber risk the most serious threat to business, says lloyd's chief. World Wide Web Page, April 2015. Available at www.telegraph.co.uk/finance/11516277/Cyber-risk-the-most-serious-threat-to-business-says-Lloyds-chief.html.

[14] Jim Finkle. Cyber insurance premiums rocket after high-profile attacks. World Wide Web Page, October 2015. Available at www.reuters.com/article/2015/10/12/us-cybersecurity-insurance-insight-idUSKCN0S609M20151012.

[15] Lawrence Gordon. Incentives for improving cybersecurity in the private sector: A cost-benefit perspective. World Wide Web Page, October 2007. Available at hsc-democrats.house.gov/SiteDocuments/20071031155020-22632.pdf.

[16] Lawrence Gordon and Martin Loeb. The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC)*, 5(4):438–457, 2002.

[17] Lawrence Gordon, Martin Loeb, and Tashfeen Sohail. A framework for using insurance for cyber-risk management. *Communications of the ACM*, 46(3):81–85, 2003.

[18] Kevin J. Soo Hoo. *How much is enough? A risk management approach to computer security*. Stanford University Stanford, CA, 2000.

[19] Insurance Information Institute. U.S. Cyber Insurance Market Demonstrates Growth, Innovation in Wake of High Profile Data Breaches. World Wide Web Page, October 2015. Available at www.iii.org/press-release/us-cyber-insurance-market-demonstrates-growth-innovation-in-wake-of-high-profile-data-breaches-102015.

[20] Robert Jacobson, Peter Browne, and William Brown. FIPS PUB 31, Guidelines for Automatic Data Processing Physical Security and Risk Management, 1974.

[21] Jay Kesan, Ruperto Majuca, and William Yurcik. Three economic arguments for cyberinsurance. In L. Gelman A. Chander and M. Radin, editors, *Securing Privacy in the Internet Age*, pages 345–366. Stanford University Press, Stanford, CA, 2005.

[22] Clarence A. Kulp. The rate-making process in property and casualty insurance. goals, technics, and limits. *Law and Contemporary Problems*, pages 493–522, 1950.

[23] Marc Lelarge and Jean Bolot. A new perspective on internet security using insurance. In *INFOCOM 2008*, pages 1948–1956. IEEE, 2008.

[24] Marc Lelarge and Jean Bolot. Economic incentives to increase security in the internet: The case for insurance. In *INFOCOM 2009*, pages 1494–1502. IEEE, 2009.

[25] Lloyd's and the University of Cambridge Centre for Risk Studies. Business Blackout: The Insurance Implications of a Cyber Attack on the US Power Grid. World Wide Web Page, 2015. Available at `cambridgeriskframework.com/getdocument/29`.

[26] James Lyne. Security threat trends 2015. World Wide Web Page, 2015. Available at `www.sophos.com/threat-center/medialibrary/PDFs/other/sophos-trends-and-predictions-2015.pdf`.

[27] Ruperto P. Majuca, William Yurcik, and Jay P. Kesan. The evolution of cyberinsurance. *arXiv preprint cs/0601020*, 2006.

[28] Marsh and McLennan Companies. United States Insurance Market Report 2015. World Wide Web Page, 2015. Available at `https://www.marsh.com/us/insights/united-states-insurance-market-report-2015.html`.

[29] Miles A. McQueen, Wayne F. Boyer, Mark A. Flynn, and George A. Beitel. Quantitative cyber risk reduction estimation methodology for a small scada control system. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*, volume 9, pages 226–237. IEEE, 2006.

[30] Erwann Michel-Kerjan and Burkhard Pedell. Terrorism risk coverage in the post-9/11 era: A comparison of new public–private partnerships in france, germany and the us. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 30(1):144–170, 2005.

[31] National Transportation Safety Board. Pipeline Rupture and Release of Fuel Oil into the Reedy River at Fork Shoals, Pipeline Accident Report PB98-916502/NTSB/PAR-98/01, 1996.

[32] National Transportation Safety Board. Pipeline Accident Report 99-03, Pipeline Accident Number DCA-97-FP-002, 1999.

[33] National Transportation Safety Board. Pipeline Accident Brief PAB-01/01, Pipeline Accident Number DCA-99-MP005, 2001.

[34] Barack Obama. Executive Order 13636 – Improving Critical Infrastructure Cybersecurity, 2013. Available at `www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf`.

[35] Barack Obama. Executive Order 13691– Promoting Private Sector Cybersecurity Information Sharing, 2015. Available at `www.gpo.gov/fdsys/pkg/FR-2015-02-20/pdf/2015-03714.pdf`.

[36] Sarah Palmer. *Lloyd, Edward (c.1648-1713), Oxford Dictionary of National Biography*. Oxford University Press, London, United Kingdom, 2007.

[37] PricewaterhouseCoopers. Managing Cyber Risks in an Interconnected World: Key Findings from the Global State of Information Security Survey 2015, 2014. Available at www.dol.gov/ebsa/pdf/erisaadvisorycouncil2015security3.pdf.

[38] PricewaterhouseCoopers. Turnaround and Transformation in Cybersecurity: Key findings from the Global State of Information Security Survey 2016, 2015. Available at www.pwc.com/gx/en/issues/cyber-security/information-security-survey/download.html.

[39] George Rejda and Michael McNamara. *Principles of risk management and insurance*. Pearson Education, 12th ed. edition, 2011.

[40] Galina A. Schwartz and Shankar S. Sastry. Cyber-insurance framework for large scale interdependent networks. In *Proceedings of the 3rd international conference on High confidence networked systems*, pages 145–154. ACM, 2014.

[41] Göran Skogh. Development risks, strict liability, and the insurability of industrial hazards. *Geneva Papers on Risk and Insurance. Issues and Practice*, 23(87):247–264, 1998.

[42] Standard and Poor's. Looking Before They Leap: U.S. Insurers Dip Their Toes In The Cyber-Risk Pool, June 2015. Available at www.globalcreditportal.com/ratingsdirect/renderArticle.do?articleId=1403078&SctArtId=320678&from=CM&nsl_code=LIME&sourceObjectId=9194506&sourceRevId=12&fee_ind=N&exp_date=20250609-19:35:11.

[43] Keith Stouffer, Suzanne Lightman, Victoria Pillitteri, Marshall Abrams, and Adam Hahn. Guide to Industrial Control Systems (ICS) Security. *NIST Special Publication 800-82 Revision 2*, 2015.

[44] Xiaomeng Su. An overview of economic approaches to information security management. Published by the Centre for Telematics and Information Technology University of Twente, 2006.

[45] The Aspen Institute and Intel Security. Critical infrastructure report readiness report: Holding the line against cyberthreats. Published by the Aspen Institute, 2015. Available at http://www.mcafee.com/us/resources/reports/rp-aspen-holding-line-cyberthreats.pdf.

[46] The Open Group. Open Group Standard: Risk Taxonomy, Version 2.0, 2013. Available at pubs.opengroup.org/onlinepubs/9699919899/toc.pdf.

[47] Vijay Mookerjee Tridib Bandyopadhyay and Ram Rao. Why IT managers dont go for cyber-insurance products. *Communications of the ACM*, 52(11):68–73, 2009.

[48] Michael A. Walters. Homeowners insurance ratemaking. *Proceedings of the Casualty Actuarial Society LX1*, pages 15–57, 1974.

[49] World Economic Forum. Partnering for Cyber Resilience: Towards the Quantification of Cyber Threats, 2015. Available at `www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf`.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704–0188

1. REPORT DATE *(DD–MM–YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From — To)*
24–03–2016	Master's Thesis	Aug 2014 — Mar 2016

4. TITLE AND SUBTITLE

A Framework for Incorporating Insurance into Critical Infrastructure Cyber Risk Strategies

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Young, Derek R., Major, USA

5d. PROJECT NUMBER

15G264

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT-ENG-MS-16-M-055

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Department of Homeland Security ICS-CERT
POC: Neil Hershfield, DHS ICS-CERT Technical Lead
ATTN: NPPD/CSC/NCSD/US-CERT Mailstop: 0635
245 Murray Lane, SW, Bldg 410, Washington, DC 20528
Email: ics-cert@dhs.gov phone: 1-877-776-7585

10. SPONSOR/MONITOR'S ACRONYM(S)

DHS ICS-CERT

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

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

13. SUPPLEMENTARY NOTES

14. ABSTRACT

Critical infrastructure owners and operators want to minimize their cyber risk and expenditures on cybersecurity. The insurance industry has been quantitatively assessing risk for hundreds of years in order to minimize risks and maximize profits. To achieve these goals, insurers continuously gather statistical data to improve their predictions, incentivize their clients' investment in self-protection and periodically refine their models to improve the accuracy of risk estimates. This paper presents a framework which incorporates the operating principles of the insurance industry in order to provide quantitative estimates of cyber risk. The framework implements optimization techniques to suggest levels of investment for both cybersecurity and insurance for critical infrastructure owners and operators. This analysis can be used to quantitatively formulate strategies to minimize cyber risk.

15. SUBJECT TERMS

Cyber risk management, cyber insurance, critical infrastructure

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Dr. Mason J. Rice, AFIT/ENG
U	U	U	UU	90	19b. TELEPHONE NUMBER *(include area code)* (937) 255-3636; mason.rice@afit.edu