Management Systems & Software Vulnerability

A cross sectional study on IT managers in the energy sector

Dalton Knapp
Rene Rodriguez

Supervisor: Rickard Wilhelmsson
Preface

The contributions of this study included 50 respondents from the Amazon platform Mechanical Turk. This is an online community where mostly software engineers and information technology professionals conduct work for requesters who collect data such as market research. This study focused on IT managers in which many are active on the platform. Mechanical Turk is well known in the information technology community and a majority of workers come from the United States.

This study could not have been completed without the assistance from this community and its respondents.

In addition to these respondents the researchers would like to thank Rickard Wilhelmsson for issuing helpful seminars and guidance.
Summary

Results:
The researchers want the results to support the management systems theory and the growing need to apply strong standards. Upper level energy managers in the U.S need to be concerned because there are constant infrastructure risk disasters that are produced when internal software is compromised. The researchers want our empirical results to display the importance of this problem and see if the management systems theory is being used.

Contributions:
The first hand research was gathered by contributions from IT managers in the U.S energy sector. The respondents are also actively engaged with Amazon’s Mechanical Turk as workers with worker approval rating of 90%< and are all located within the U.S.
Table of Contents

I) Introduction

1. Topic Background 7
2. Problem Statement 9
3. Research Questions 9
4. Hypotheses 9
5. Purpose & Aim 10
6. Limitations 10

II) Theoretical Framework 12

1. Management Systems Theory 12
   1.1 Management Control System 13
      1.1.1 Information Security Management System 13
      1.1.2 Relation to Management Systems Theory 17
      1.1.3 Relation to Management Control System 18
   1.2 Risk Management 19
      1.2.1 Boehm’s Risk Exposure and Risk Resolution 20
      1.2.2 Relation to Management Systems Theory 24

2. Analytical Framework 25
   2.1 Management Systems Theory 25
   2.2 ISMS Practice 25
   2.3 Risk Exposure and Risk Resolution Practice 25

3. Theoretical Summary 26

III) Methodology 27

1. Research Approach 27
2. Replicability 27
3. Validity 28
   3.1 Measurement Validity 28
   3.2 Internal Validity 28
   3.3 External Validity 28
   3.4 Ecological Validity 29
4. Research Design 29
5. Research Method 30
6. Research Sampling 32
7. Data Gathering 33
   7.1 Primary Data 33
   7.2 Secondary Data 33
8. Methods Critique 34

IV) Empirical Data 36
1. Questionnaire Part 4 36
2. Questionnaire Part 5 39

V) Analysis 43
1. ISMS Comparison 43
   1.1 Security Policy 43
   1.2 Management Control System Scope 44
   1.3 Risk Assessment*(Boehm’s Comparison)* 44
   1.4 Risk Management*(Boehm’s Comparison)* 45
   1.5 Selection of Controls 46
   1.6 Statement of Applicability 46
2. Test Hypothesis 47
   2.1 Hypothesis 1 47
   2.2 Hypothesis 2 48
3. Summary of Analysis 48

VI) Conclusions 49
   Further Research 50

VII) Bibliography 51

VIII) Appendix 54
   A) Survey Questions 54
   B) Coded Answers 58
   C) Figures 61
I) Introduction

1. Topic Background

A rise in the interconnectivity of machines and devices to networks has been taking the world by storm. Dubbed the “Internet of Things”, this phenomenon can be defined as machine to machine communications that is automated and does not require a person to operate (Brown 2016). In industry, the Internet of Things involves attaching sensors to everything and using the data collected from the sensors to make better informed decisions. One industry incorporating this technology quickly is the energy utility industry (Lapping, 2018). Although this trend creates solutions to existing problems, it brings with it a new kind of problem. This kind of problem is a type of software risk and it is leading to an increase in infrastructure risk.

A software risk is an expectation of loss or a problem that may or may not occur in the future of the software development process. Software risks are generally caused by a lack of information, control, or time (Test Institute, 2018). An infrastructure risk is defined as the potential for loss due to failures of basic services, organizational structures, and facilities (Spacey, 2015). An example of this is an office losing power. With these definitions in mind, it is clear why the problem created by an energy company using software to interact with their infrastructure is becoming a serious issue. However, this is not theoretical, there are a litany of real word examples that can demonstrate the severity of the issue. Some examples of this problem can be shown by what are known as spear phishing attacks. Spear phishing is known as an email that tricks the user into giving away vital information through a malicious link which can then be used to access networks and software systems (Wueest 2014). This is a growing issue as many normal employees are being targeted and without protection methods a hacker can generate custom code or script malicious overrides. The 2012 spear phishing attack data from Symantec displayed the energy sector at 16.3% of all attacks in the last half of 2012 (Wueest 2014). A most recent cyber incident that is applicable to this study is the russian government targeting the energy sector with spear phishing campaigns etc. (US-CERT 2018). Another example of what can happen from negligent software risk management is an online attack in 2013 on the Austrian & German power grid because a control command was misused. A requesting command packet from the German gas company found its way into the Austrian
energy power control network and flooded the system (Wueest 2014). This type of attack can lead to major power outages and infrastructure compromisations. In other words, it can lead to what is known as infrastructure risk which can directly affect the well being of citizenry.

The researchers wanted to address the energy sector concerns because it is an ever growing issue for many firms around the world and because energy suppliers can directly affect the livelihood of surrounding populations. The rising threat is well explained in the excerpt from the Council of Foreign Relations “Cyber threats from oil and gas suppliers pose an increasingly challenging problem for U.S national security and economic competitiveness. Attacks can take many forms, ranging from cyber espionage by foreign intelligence services to attempts to interrupt a company’s physical operations” (Clayton & Segal 2013 p1). The researchers believe that all countries are at risk if companies from the U.S are having their networks penetrated. Network threats are borderless and if a company’s physical operations are compromised then infrastructure risk increases explained in the excerpt “Once in the system, an infiltrator could in theory cause the flow of natural gas through a pipeline to grind to a halt, rig an explosion at a petrochemical facility, or do damage to an offshore drilling rig that could lead to an oil spill. Such threats now have the potential to cause environmental damage, energy supply outages for weeks or for months, and even the loss of human life (Clayton & Segal 2013 p2). This is why it is important to see if there are management control methods to mitigate against these factors and investigate how they are being used. A proper management control system standard could prevent or mitigate against these factors.

Information security management is a major concerns for companies to be able to implement their organization's strategies and achieve goals (Eloff and Solms, 2000). A management control system could provide a guideline or framework for IT managers to follow when they are preparing software risk management protocols to make sure that the organization’s strategies are being implemented. The theoretical section explains what a management control system is. The management systems theory explains why a management control system is needed in the theoretical section as well. The management systems theory connects to the problem because it shows that an organization should follow an information security management system (ISMS) to protect information assets (Shing-Hong et al. 2003).

The researchers wanted to look at the internal software risk practices that energy firms are currently using to monitor and prepare for external threats. It is important to note that
software risk management falls under the umbrella of the ISMS. Software risk management is obviously not recent a phenomena, however, the rise smart grid networks have made the concept a key factor for energy suppliers.

The following definitions establish context and are used throughout the paper. A management control is defined as “the systematic process by which the organization’s higher-level managers influence the organization’s lower-level managers to implement the organization’s strategies”(Anthony et al. 2014 p30). A management control system is the “systematic way in which organizations do and should exercise management control”(Anthony et al. 2014 p27). Software risk management is a part of the main risk management mission which is to Identify Risk, Reduce the impact of Risk, Reduce the probability of Risk, and Monitor risk(Test Institute 2018). It is unique in the sense that it focuses on quantitative risk which includes Describing a Risk Event, Defining the probabilities of that Risk to occur, Defining the loss of the risk event, and Defining the liability of the Risk(Test Institute 2018).

2. Problem Statement
The problem is that a firm's adherence to standards can affect a firm’s ability to protect itself from software vulnerability.

3. Research Questions
   - Can the risk management process correlate to software vulnerability?
   - How do top level managers influence the risk management process?

4. Hypothesis
H₀ - The top level managers have moderate or more influence over the risk management method
H₁ - The top level managers have less influence over the risk management method

H₀ - The risk management process does not correlate to software vulnerability
H₁ - The risk management process does correlate to software vulnerability
5. Purpose & Aim

This study aims to comprehend how management systems theory is being used to protect against software risk in the U.S energy sector. The researchers are interested in this study because the standards being used in the U.S may not be adhering to a practice that is based from theory. This is an issue because this means that the management control systems in the U.S might vary greatly. This can lead to greater software vulnerability in the U.S because a greater number of firms will have a broader range of management control practices that might not be following management systems theory. The researchers aim to find a management control practice that does follow management systems theory. In this sense, the researchers strive to compare the standardized management control system of Europe (ISMS). Then the researchers aim to see if risk management practices are influenced less by the top level managers in the U.S energy firms. The study aims to display if this is true in the hypothesis testing. The researchers aim to explain why the statistical analysis is appropriate and why it was chosen. The researchers aim to explain why ISMS is a useful comparison tool and why it was chosen as well. In addition, the researchers aim to find software risk management practices that do follow management systems theory. It is for this reason that the researchers can use Barry W. Boehm’s work as a comparative tool. The researchers then hope to see if a risk management process can correlate to software vulnerability. The study aims to see if this is true in the hypothesis testing. The researchers aim to explain why the statistical analysis is appropriate and why it was chosen. The researchers then aim to draw conclusions from the hypothesis testing.

6. Limitations

The study was limited to an online questionnaire to U.S IT managers in the energy sector. The study results can only be limited to those respondents who have their assets connected to smart grid technology. The study was limited to an online U.S platform called Amazon Mechanical Turk. The researchers did not conduct follow-up interviews.
II) Theoretical Framework

1. Management Systems Theory

The researchers are using management systems theory developed by Eugene Schultz, Robert W. Proctor, Mei-Ching Lien, and Gavriel Salvendy. Proctor and Salvendy are academic references from Purdue University (Schultz et al. 2001). The researchers have chosen this theory because the ENISA ISMS and Boehm’s software risk management practices are supported from this framework. This theory is focused on the importance of setting management control practices to protect against information vulnerability (Schultz et al. 2001). The authors describe the main reason for issuing a theoretically secure system is to “provide protections against intrusions and a method for detecting intrusions when the protection fails” (Schultz et al. 2001 p629). Setting up the system involves setting up a protection practice to avoid intrusions (Schultz et al. 2001). The researchers would not know what a quality management control practice consisted of without the connection to this framework. The theory additionally outlines the functions necessary to accomplish a secure system:

Information Security = information security policy, the scope of information security, risk management, implementation.

Risk Management = risk assessment, risk control

Information Security Policy = environment inside and outside of an organization, standards.

Figure 1
Source: Shing-Hong et al. 2003 p245 in reference to Schultz et al. 2001 Theory
1.1 Management Control System

The implementation of management control happens with a management control system. A management control system is the “*systematic way in which organizations do and should exercise management control*” (Anthony et al. 2014 p74).

1.1.1 Information Security Management System

The management control system that the researchers use is the European ISMS (Information Security Management System) practice. The researchers use the European ISMS because it is a practice that carries out the functions needed in the management system theory and is adopted by the International Standards Organization as the ISO-27000 series of protocols. The researchers are using this European practice to compare to the U.S practices to see if they follow the steps in the management systems theory. The ENISA ISMS is aligned with the theory so if the U.S practices do not align with an ISMS standard then conclusions can be drawn and vice versa.

This management control system is primarily used to provide a strong indication that a company is using a systematic approach for the identification, assessment and management of information security risks (ENISA Technical Department 2006). Its main message is that security is not strictly technical, but managerial (ENISA Technical Department 2006). The need for ISMS is because IT administrators should be devoting about ⅓ of their time to technical aspects and ⅔ spent developing policies, analyzing risk, and addressing contingency planning (ENISA Technical Department 2006). This practice is built to handle those requirements. Some critical success factors for a successful ISMS are constant approval and confirmation from top management, centralisation of tasks, reflect the organization's approach to risk management, and continuous training (ENISA Technical Department 2006). The establishment of an ISMS can begin after these success factors are determined (ENISA Technical Department 2006). The requirements for proper establishment include management framework, implementing selecting controls, finding a way to document the system, documentation control, and maintaining records (ENISA Technical Department 2006). The process in which this framework is performed
is demonstrated in Figure 3. They can be broken down into six steps that will now be explained according to ENISA.

![Figure 2](image)

**Figure 2**

Source: ENISA Technical Department 2006 p10 Figure 3

Step 1 is the Definition of a Security Policy. This contains the necessary plan that should detail the type of security needed and the risks associated with the procedures (ENISA Technical Department 2006). It should really explain the WHY to the rest of the organization and serve as a clear guideline for employees (ENISA Technical Department 2006). This is usually a managerial or strategic decision because it serves a longer time frame and it is not concerned with everyday functions as in the Risk Management process (ENISA Technical Department 2006).

Step 2 is the ISMS Scope. This also occurs on a longer time frame and it sets the parameters for the ISMS (ENISA Technical Department 2006). The ISMS Scope consists of defining the external environment, defining the internal environment, generating the Risk Management Context, and the Formulation of Risk Criteria (ENISA Technical Department 2006). These first two steps are developed by upper management and corporate personnel (ENISA Technical Department 2006).
Step 3 is the Risk Assessment which is within the Risk Management process. This step is concerned with the identification of risks, the analysis of relevant risks, and the evaluation of risks (ENISA Technical Department 2006). This is where risks can be assigned value and ranked by threat levels. It is important to identify the risks scientifically because there cannot be any guesswork during this assessment (ENISA Technical Department 2006). It will critically influence the way the risk management strategy is formulated (ENISA Technical Department 2006).

Step 4 is the actual Risk Management step where possible protocols and controls are generated. This takes the Risk Assessment and other reporting measures into account to determine a risk response plan. This step consists of Definition of Scope, Risk Assessment, Risk Treatment, Risk Communication, and Monitor & Review (ENISA Technical Department 2006). Risk Treatment is the measure the organization can modify its risks. It includes avoiding, optimizing, transferring or retaining risk (ENISA Technical Department 2006). Risk Communication is the process to exchange information about risk between the decision maker and the stakeholders inside/outside an organization (ENISA Technical Department 2006). The Monitor & Review process is to ensure that the risk management action plans remain updated (ENISA Technical Department 2006). The visual model and the internal functions of the process are shown below.
Step 5 is implementation of controls. This is where either established techniques or new methods are actively put into practice (ENISA Technical Department 2006). The previous risk treatment will help determining the most effective method to handle the areas of vulnerability and should set the appropriate controls within an action plan (ENISA Technical Department 2006). This is why the Risk Management is so important. It allows technical managers to narrow down what kind of resources they should devote to control. These controls may be derived from information security standards or be a mix of controls fitted for the organizations needs (ENISA Technical Department 2006).

Step 6 is the Statement of Applicability. This is the documented mapping of the identified risks which are applied to the organization with the technical security tools that the organization has decided on (ENISA Technical Department 2006). This is seen to be in the short term as reports are part of the daily operations (ENISA Technical Department 2006). Steps 5 & 6 are more concerned with technical maintenance than the finding information risks (ENISA Technical Department 2006). It is important to mention that the relevance of an ISMS varies to the size of a
given company (ENISA Technical Department 2006). The large firms where misinformation can be harmful to assets are very interested in Information Security Risk (ENISA Technical Department 2006). The smaller firms will not be as reliant on their information technology and will therefore not be as exposed to risk impacts (ENISA Technical Department 2006).

1.1.2 Relation to Management Systems Theory

ENISA ISMS connects to management systems theory in the following way

Information Security = information security policy, the scope of information security, risk management, implementation. *(Steps 1,2,5,6)

Risk Management = risk assessment, risk control *(Steps 3,4)

Information Security Policy = environment inside and outside of an organization, standards. *(Step 1)

Figure 4
Source: Shing-Hong et al. 2003 p245 in reference to Schultz et al. 2001 Theory
* = Steps from ENISA ISMS to show relation

The ENISA (European Network and Information Security Agency) ISMS practice implements all the theoretical functions of the management system theory. There may be other practices that could be used to implement this theory, however, ISMS clearly follows the functions and puts them into practice. The ENISA ISMS that is used in this paper may not have been directly inspired from this theory, but it is being used to solve the same theoretical functions that management system theory expresses. This theory is, therefore, used because the study comparison shows whether the U.S management control system practices are aligned with the theoretical functions of the theory. The ENISA ISMS is a relevant practice to compare with because it is used to solve the same functions with this theory.
1.1.3 Relation to Management Control System

ISMS is a management control system because it fits the definition by Anthony et al discussed earlier. The management control system is the information security management system (ENISA ISMS) which is displayed in the element comparison below to the book by Anthony et al. 2014 *Management Control Systems*. This system has a six step process that is discussed in the above section 1.1.1 of theoretical framework. It outlines the elements of a controlled system. The element comparison is as follows

**Detector** - *a device that measures what is actually happening in the process being controlled*(Anthony et al. 2014 p75)

**ISMS Detector** - This is the security policy (Step 1) as higher level management is detecting the current situation within the organization (ENISA Technical Department 2006)

**Assessor** - *a device that determines the significance of what is actually happening by comparing it with some standard*(Anthony et al. 2014 p75)

**ISMS Assessor** - This is the ISMS scope (Step 2) because higher level managers assess current risks and develop a standard of what should be (ENISA Technical Department 2006)

**Effector** - *a device that alters behaviour if the assessor indicates the need to do so*(Anthony 2014 et al. p75)

**ISMS Effector** - This would fall under the processes of Risk Assessment, Risk Management, and Selection of Appropriate Controls (Steps 3, 4 & 5) as there are actions taken place after the realization that risk standards are not being met (ENISA Technical Department 2006)

**Communication System** - *devices that transmit information between the detector and the assessor and between the assessor and the effector*(Anthony et al. 2014 p75)

**ISMS Communication System** - This could be the Statement of Applicability (Step 6) because documented outcomes are sent to higher level management (ENISA Technical Department 2006)
Predictive Model - *knowledge about the effect of the behavioural changes made by the effector* (Anthony et al. 2014 p75)

ISMS Predictive Model - This could be Statement of Applicability (Step 6) as well because effective changes of the actions taken will be documented (ENISA Technical Department 2006)

**Figure 5**
Source: Anthony et al. 2014 p75

### 1.2 Risk Management

The concept of risk management that is be used is from ENISA. ENISA (European Network and Information Security Agency) defines Risk Management as “a process aimed at an efficient balance between realizing opportunities for gains and minimizing vulnerabilities and losses” (ENISA Technical Department 2006 p1). The risk management processes are developed within the design of the management control system (ENISA Technical Department 2006). Since the researchers are interviewing U.S firms, the results are compared to the risk management principles of European Network & Information Security Agency because they have a standard of risk management which is necessary in the management system theory. This helps to determine how the top level managers are influencing the risk management processes in the U.S firms.

In addition, the researchers compare software risk management practices that aligned with theory to the risk management practices being used by the U.S IT managers. These practices are from Barry W. Boehm which are studied and compared to the practices that IT managers are currently using in the U.S. The risk management comparison can be used to see if the number of Boehm steps that are followed might correlate software vulnerability.

Barry W. Boehm is a distinguished professor at the University of Southern California teaching computer science and systems engineering (USC Web Archive 2014). He wrote the document used in this section while he was the director of the Defense Advanced Research Project Agency’s (DARPA) Information Science and Technology Office (Boehm, 1991). DARPA is an agency that has been credited with the invention of the internet and the GPS and played a large role in the invention of Windows, the world wide web, Google Maps technology, and cloud computing (Winder, 2018). He has developed methods for software risk management
known as *Software Risk Management: Principles and Practices*. The researchers connect two of his practices to Steps 3 & 4 of the ISMS because the risk exposure table carries out what is needed for risk assessment and risk resolution carries out what is needed for risk management. This is true because risk assessment is concerned with the identification of risks, the analysis of relevant risks, and the evaluation of risks (ENISA Technical Department 2006). Risk exposure is concerned with measuring unit(s) of risk that can be quantified and assessed appropriately (Boehm 1991).

1.2.1 Risk Exposure Table and Risk Resolution

The identification of risk exposure is extremely vital when talking about energy suppliers. Risk Exposure is a measurable unit(s) of risk that can be quantified and assessed appropriately (Boehm 1991). There needs to be a way to calculate the loss associated with a potential software action plan as well as its probability of occurring (Boehm 1991). A Risk Exposure Table can be used to find these levels of exposure to prioritize which outcomes are the most undesirable (Boehm 1991). A table such as this would fit under the Risk Assessment process. This is because it is directly identifying risk outcomes, evaluating probability & loss of risk outcomes, and is able to display objective data from graphical analysis (Boehm 1991). This is shown in the table provided by Boehm

<table>
<thead>
<tr>
<th>Unsatisfactory outcome</th>
<th>Probability of unsatisfactory outcome</th>
<th>Loss caused by unsatisfactory outcome</th>
<th>Risk exposure</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Software error kills experiment</td>
<td>3-5</td>
<td>10</td>
<td>30-50</td>
</tr>
<tr>
<td>B. Software error loses key data</td>
<td>3-5</td>
<td>8</td>
<td>24-40</td>
</tr>
<tr>
<td>C. Fault-tolerant features cause unacceptable performance</td>
<td>4-8</td>
<td>7</td>
<td>28-56</td>
</tr>
<tr>
<td>D. Monitoring software reports unsafe condition as safe</td>
<td>5</td>
<td>9</td>
<td>45</td>
</tr>
<tr>
<td>E. Monitoring software reports safe condition as unsafe</td>
<td>5</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>F. Hardware delay causes schedule overrun</td>
<td>6</td>
<td>4</td>
<td>24</td>
</tr>
<tr>
<td>G. Data-reduction software errors cause extra work</td>
<td>8</td>
<td>1</td>
<td>8</td>
</tr>
<tr>
<td>H. Poor user interface causes inefficient operation</td>
<td>6</td>
<td>5</td>
<td>30</td>
</tr>
<tr>
<td>I. Processor memory insufficient</td>
<td>1</td>
<td>7</td>
<td>7</td>
</tr>
<tr>
<td>J. Database management software loses derived data</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
</tbody>
</table>
Figure 6

This is a tool for risk managers to correctly examine all the probable outcomes and rank losses from 1-10 (Boehm 1991). It can simplify the Risk Assessment process by creating key rating of $P(UO)$ for Probability and $L(UO)$ for Losses that can be plotted into final Risk Exposure shown in the following example given by Boehm.

Figure 7

Software Risk Managers focus on outcomes with either a high probability or a high loss factor, however, these are not always accurate indicators for a high Risk Exposure level (Boehm...
The RE yield from the multiple of the two ratings is what should be considered for as a high priority risk item (Boehm 1991). These are the assessments that IT managers could be using in their risk management process and the results display if IT managers implement similar methods.

Risk Resolution would pertain more to Risk Management (Step 4) in the ISMS framework. It carries tangible response plans that can be exercised from the risk item data and the prioritization done in the Risk Exposure Table (Boehm 1991). Boehm portrays a table for sorting Risk Items by Identifying, Ranking, and Resolving them in a Top Ten Table shown here.

**Figure 8**

Boehm explains “*This technique concentrates management attention on the high risk, high leverage, critical success factors rather than swamping management reviews with lots of low priority detail*” (Boehm 1991 p38-39). This allows higher priority risk factors to be managed more closely and save time as a software risk manager as rankings will be constantly updated.
The results show whether IT managers are managing high priority risk factors and ranking their risk.

1.2.2 Relation to Management Systems Theory

Boehm’s software risk management connects to management systems theory in the following way:

Information Security = information security policy, the scope of information security, risk management, implementation.

Risk Management = risk assessment, risk control + (exposure & resolution)

Information Security Policy = environment inside and outside of an organization, standards.

Figure 9
Source: Shing-Hong et al. 2003 p245 in reference to Schultz et al. 2001 Theory
+ = Steps from Boehm to show relation

The Boehm steps satisfy the theoretical functions of the management system theory. Risk exposure connects to risk assessment because it is concerned with detecting risk and risk resolution connects to risk control because it is concerned with managing risk outcomes (Boehm 1991). These two practices are an accurate example of the risk management process and how it should be implemented at an operational level. The researchers see these as a standard of risk management that can be compared to the practices of the U.S IT managers because these are the practices that the I.T managers are in charge of. The researchers would not know how to choose a quality standard of the risk management process without the management systems theory.
2. Analytical Frame

2.1 Management Systems Theory
The management system theory is used to serve as a foundational theory for the ENISA ISMS. It proves that the ENISA ISMS practice is relevant because it follows all the theoretical functions necessary for the practice of the theory. The theory is needed to show what are quality practices and what are not in terms of management control systems. If the results do not align with the ENISA ISMS risk management practice steps(3&4) then they might not following be management systems theory which can be used to address the research questions.

2.2 ISMS Practice
The researchers will use the method of the ENISA ISMS by comparing empirical data taken from our study to the six step model. ISMS is relevant especially because it follows the management system theory and the system is standardized by the ENISA. The resulting practices from the U.S either resemble those of ISMS or cannot be aligned with management systems theory. The goal is to relate these practices to the six step model. The analysis section of these comparative steps help highlight if the management control system is maintaining the ENISA standard. The top level manager influence on the risk management process can address this issue. The level of influence deviation is tested in the analysis with the hypothesis statements. This testing can help the researchers examine how the top level managers are influencing the risk management process.

2.3 Risk Exposure Table and Risk Resolution Practice
The researchers use these two Risk Management concepts given by Barry W. Boehm’s *Software Risk Management: Principles & Practices*. These methods are for IT managers to use during the Risk Management process. They fit as Steps 3 & 4 of the ISMS because they are used as a methods to prioritize and resolve risk(Boehm 1991). In relation to the theory, the risk exposure is the risk assessment and the risk resolution is the risk control. Theses calculative methods can be used by energy suppliers and the researchers examine how the risk management process might correlate to software vulnerability with a statistical test. This can answer the research question.
Conclusions can be drawn from correlation value relating to the software vulnerability data in the analysis section.

3. Theoretical Summary

The study to (make these frameworks testable) to the research questions draw from quantitative research findings, secondary hand data, and academic texts. The data that is gathered is compared to the ENISA ISMS model and Boehm’s risk exposure/risk resolution tables. These lay the foundation of the quantitative questions. The responses are then served to address the research questions. The problem of poor risk management leading to infrastructure risk is seen as a managerial problem and a technical problem (ENISA Technical Department 2006). This is why the researchers use both the ISMS (managerial) and Boehm (technical). The Boehm risk management practices are a quality standard because they align with steps 3 & 4 of the ENISA ISMS and they align with the risk management function in the management system theory. The ENISA ISMS practice is a quality standard because it fulfills the theoretical design needs of the management system theory. The theory is the foundation for determining proper practice.
III) Methodology

The methods being used in this paper are explained in the following approach and strategy sections. They describe how the researchers collected the data in the study. They also tell how the collected data is relevant to the research questions and why these strategies correctly serve the study. The samplings for the research are then be described as well as the data collection technique. The analysis section takes the finding from the study and compares them to models from theory. This allows the researchers to deduce scientific conclusions based from the hypothesis statement. The last section portrays any criticism, pitfalls, or unforeseeable events that occurred during the course of the study.

1. Research Approach
This research will be using the **deductive approach** because “the accent is placed on the testing of theories” (Bryman & Bell 2011 p27). In addition, a deductive approach is used when “The researcher, on the basis of what is known about a particular domain, deduces a hypothesis that must be subjected to empirical scrutiny” (Bryman & Bell 2011 p11). The research questions have been prepared and can be tested with the comparison of results to the theoretical concepts. The quantitative data that comes from the questionnaire allows the researchers to compare theory using statistical testing. This will create a range of relevant inferences to the research questions after the hypothesis is tested.

2. Replicability
The study can be replicated. The only aspect that may confound replicability is the American population of Amazon Mechanical Turk workers may change, so the sampling of workers that answer the questionnaire may represent a different part of the population than the one that was sampled for the initial study.
3. Validity

3.1 Measurement Validity
This study is a quantitative and does have quantifiable questions such as demographic regions, age range, binary yes/no, and numerical scaling. These questions, however, should simply support the rest of the quantitative response gathering where inferences can be made.

3.2 Internal Validity
In the hypothesis, there are three null statements to answer the two research questions. In the first hypothesis there is one variable which is the influence from top level managers. In the second hypothesis the dependent variable is software vulnerability and the independent variable is the risk management process.

3.3 External Validity
This results of the study will be typically unique in that two questions (Q13/17) are explanatory. This means there are specific responses from each manager who answer this question in a general manner. The Bryman & Bell definition of external validity is “whether the results of the study can be generalized beyond the specific research context” (Bryman & Bell 2011 p43). In that sense, the generalizability of results that is described in Bryman & Bell will be present for these two questions because there is no specific set requirement for how to answer and results may differ in following studies.

3.4 Ecological Validity
The study is for managers at energy firms so it concerns worklife across all energy companies and the practices of management control. This study can be ecologically valid because the managerial practice responses are not disturbed. The one concern is that the natural habitat of the managers during the completion of the questionnaire varies. The questionnaire can be completed in a variety of environments since it is online, so the manager may not be in their workplace during work hours when completing the questionnaire, so the ecological validity of the study is subject to further scrutiny.
4. Research Design

The researchers have chosen to implement the **cross sectional design** for the quantitative study. This design has been chosen for the study because it resembles the tactics used in the survey research framework of cross sectional design defined here as “the collection of data on more than one case and at a single point in time in order to collect a body of quantitative or quantifiable data in connection with two or more variables, which are then examined to determine patterns of association” (Bryman & Bell 2011 p53). The researchers have conducted a quantitative questionnaire to a number of IT managers in the U.S energy sector. The questionnaire carries fifty respondents and was supplied at a single point in time (Bryman & Bell 2011). The questionnaire is typically seen as quantitative in cross research design and it is used in a quantitative context in this study. This being the case, the main rule that the researchers have adhered to is the accurate representativeness of the sample of managers in connection to the population. The ecological validity explained previously will stay the same due to the fact that the researchers will not be completing follow up interviews after the initial study.

The generated responses from IT managers are assessed and observed. These are interpreted in a cross sectional format to establish the connection between Boehm’s risk management strategies and to discover how the recorded practices relate to his theory. The design is similar to that of Bryman & Bell in the following structure

<table>
<thead>
<tr>
<th>Theory 1</th>
<th>Theory 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Observation(w/results)</td>
<td>Observation(w/results)</td>
</tr>
<tr>
<td>Observation(w/results)</td>
<td>Observation(w/results)</td>
</tr>
</tbody>
</table>

Source: Bryman & Bell 2011 Figure 2.2

Figure 10

5. Research Method

This research used a quantitative method of study. Quantitative studies consist of quantification in the collection and analysis of data that: entail a deductive approach, natural science model, and objectivism (Bryman & Bell 2011). The quantitative questions the researchers use in the
study are binary responses of yes/no and numerical ratings to support the analysis. There are also two questions built to determine the level of influence from upper management on software risk assessment/management. Quantitative research most commonly stem from deductive approaches as the focus is on testing theory. This study has issued a quantitative questionnaire to managers in which their responses are used for further analysis of the research questions.

This research was conducted by issuing an online questionnaire with pre-screeners for IT managers in the U.S energy sector. The platform that the researchers used was Amazon’s Mechanical Turk for the professional responses and Qualtrics for the creation and distribution of the questionnaire. Mechanical Turk automatically screened out the respondents that were not currently located in the United States. There are 50 respondents that took the questionnaire with 24 questions issued. The number of questions allowed the researchers to gather simple information about a wide range of policies in place throughout the United States. Responses that were deemed inadequate or incomplete were thrown out so legitimate responses could replace them. Due to a constraint with the mechanical turk service, this was a necessary step so a full quota of 50 serious responses could be filled. The results are tested in the analysis section where these responses are applied to the research questions and the theoretical framework.

The questionnaire was conducted in the following way:

Part 1 Pre-Screener
The question was asked whether the respondent was an IT manager in the energy sector or not. The respondents that answered no were not allowed to continue the rest of the questionnaire.

Part 2 Demographics and Experience
This section entailed the region that the respondent was currently working in. These included Western, Midwest, South, Northeast, or Alaska/Hawaii. It also asks for the age and the years of experience that the respondent has had in the energy industry.

Part 3 Details of the Study and Anonymous Response Claimer
This section explains the details of the study and what it is about. It explains the reason for the study and the goal of the step by step comparison. There is a statement regarding the fact that the responses will remain anonymous as well.

Part 4 Software Vulnerability at the firm
This section strives to identify the network and infrastructure risk that the IT manager has experienced. The questions that are asked are whether the infrastructure assets are connected to a network, whether or not they can become vulnerable when software is compromised, whether there have been any spear phishing or malware attacks, and if so how many. These questions help gauge the risk management process relation to software vulnerability. They also help identify negative number of attacks to the Boehm steps being taken in the risk management process.

Part 5 Management Control and Risk Management
This section is where the step by step questions were asked in relation to the ISMS model. It is the final section of the questionnaire. There are a number of short answer quantitative questions and two long answer questions where the respondent is asked to explain his/her answers. The quantitative questions include two questions which ask for the level of influence from superiors on a 1-5 scale. There are also questions that ask for binary yes/no responses to compare whether the U.S based management control systems is adherent to ISMS.

This completes the questionnaire as respondents are given a survey code that must be inputted into Amazon’s Mechanical Turk page to show that the respondent has indeed taken the questionnaire to be reviewed.

6. Research Sampling

The goal of the sampling approach was to represent organizations by a single respondents. The sampling method of this study is complicated. An argument can be made that the sampling method is convenience sampling, since the sample of people chosen to take the questionnaire was based on accessibility by the researchers (Bryman and Bell 2011).
Convenience sampling generally means that the sample taken does not represent the larger population the data from the sample is supposed to represent. However, due to using the Mechanical Turk platform, the population of American IT managers the researchers have access to is much larger than the stereotypical examples of convenient sampling such as surveying friends and family members, or students in a classroom. Even with this consideration in mind, the researchers still acknowledge the bias and the possibility that the sample misrepresents the population (Bryman and Bell, 2011).

Even though there is clearly a bias, the researchers will treat the sample as though it was from a probability sampling method for purpose of analysis. The perfect sample would be created by taking every IT manager employed in the energy sector and selecting a sample at random from the population. Conclusions made from the data collected from this sample could then be generalized to represent the population with high confidence. Unfortunately, access to every IT manager is not possible. However, with some secondary data from the United States Bureau of Labor Statistics, the sampling data of the study can be put into proper perspective. The BLS tracks data about 803 occupations in the United States of America and classifies all economic activity into twenty industry sectors, some with subsectors. The sector this study is interested in is the Utilities industry, but more specifically the subsectors of Electric Power Generation, Transmission and Distribution, and Natural Gas Distribution. This excludes Water, Sewage, and Other Systems as it is outside the scope of the study. Based on the May 2017 Occupational Employment Statistics report, an estimated 1,580 IT managers are employed in Electric Power Generation, Transmission and Distribution sector, and another estimated 470 IT managers are employed in the Natural Gas Distribution sector for a total of an estimated 2,070 IT managers being employed in the United State’s energy sector (Bureau of Labor Statistics, 2018). The study sampled 50 American IT managers of the energy sector who are workers for Amazon Mechanical Turk, so the question is whether or not the population sampled from Mechanical Turk represents the general American IT manager from the energy sector. If so, then the study is able to make claims with a level of confidence not only about the Mechanical Turk population, but about the general population that the study is seeking.
7. Data Gathering

7.1 Primary Data
The primary data that was collected for this study included 50 responses from IT managers in the energy sector. They were asked 24 questions where they were asked to answer several practices related to software risk management and management control. These responses serve as the main drivers for the quantitative data that is displayed in the empirical section. These responses were also completed anonymous for the respondents sake.

7.2 Secondary Data
The secondary data is generated from online articles, books, journals. The population size that was found above was calculated from the census bureau of labor & statistics. This then created the sample/population ratio to above 2%. This piece of secondary data was critical for the correct sampling. The remaining pieces of data were collected to establish the importance of the problem. This was shown with several examples about previous attacks and a professional take on the rising problem for energy suppliers. The examples came from Wueest, US-Cert, and Clayton & Segal. The authenticity of these secondary sources is clear as the researchers use professional articles that relate to the topic. Credibility and representativeness are developed from the typical use of the Census Bureau and the attack statistics described in the topic background.

8. Methods Critique
This section is to explain the possible criticism that the researchers may face in their method of research. Follow up interviews were not conducted as stated in the limitation section. Further investigative interviews would be helpful for this study because in-person expertise could confirm the data representation and add in different perspectives.

The reason the researchers commenced a questionnaire for a U.S working population is because they might not have a standard practice. The researchers use a standard of practice that is supported by theory to be able to see if the U.S results are adhering to this standard.
The contributions of this study included 50 respondents from the Amazon platform Mechanical Turk. This is an online community where software engineers and information technology professionals can conduct work for requesters who collect data such as market research (Amazon Mechanical Turk Inc 2018). This study focused on IT professionals. The top industry for linkedin members who are also mturk workers is Information Technology (Linkedin 2018). This means that the professionals on linkedin who are also Mturk workers are in the majority of IT services (Linkedin 2018). These workers are motivated to not only work for financial incentives, but to build a reputation status so that requesters will value their work. It is also seen as plus if the workers can contribute to the rest of the information technology community by answering questions about their industry and so forth. Mechanical Turk is well known in the information technology community and a majority of workers come from the United States (Ipeirotis 2018).

One fault in the method of research is that the data relies on the honesty of the Amazon Mechanical Turk workers to not lie about their credentials in order to take the survey. There are a couple of factors that mitigate this risk however. The Mechanical Turk platform incentivizes honesty by rating each worker by the rate of approval on their tasks. Workers carry a financial incentive from their requesters for proper work. Workers who are dishonest will have the work denied and it will negatively impact their rating. A low rating disqualifies workers from future work so they cannot work on higher quality requests, so it is in the interest of workers to be honest if they want to continue work. The responses were also screened by the researchers so that any people who took the survey and gave incomplete or extremely low quality responses were rejected so they did not take up room in the 50 worker quota. With these factors accounted for, the risk of dishonesty that appears on the surface of design is mitigated and low enough to not sacrifice reliability.
IV) Empirical Data

This section displays the data that was collected in the questionnaire or primary data. The researchers explain the relevance of the results that are used for the influence and correlative or non-correlative findings in the analysis section. This data is used in the analysis section for the comparisons of the practices, the influence of the top level managers to the risk management process, and the correlation the risk management process might have on software vulnerability. The figures shown in this section are developed from the questionnaire which are displayed in the Appendix. The two parts below carry summarizations below and detailed descriptions for the reader. These figures all come from specific parts of the questionnaire. They are grouped by parts 4 and 5.

1. Part 4 Software Vulnerability

Are your infrastructure assets connected to a network?

IT Manager Questionnaire

Figure 11

Question 5
IT Manager Questionnaire

Figure 12
Question 6

Does your infrastructure become vulnerable when or if software is compromised?

IT Manager Questionnaire Part 4

Figure 13
Question 7

Have there been any successful malware or spear phishing incidents at your firm?
Part 4 Summary

The results show from the figures in Part 2 show that 96% of respondents have their infrastructure assets connected to a network and 92% of respondents are susceptible to infrastructure vulnerability if software is compromised. This data alone goes to show that external network threats are thoroughly prevalent in the energy sector for these U.S managers.

This part also shows the IT management results from the study for the number of incidents. The number of incidents are important because they are tested to see if there is a correlation between the amount of steps followed from Boehm’s practices to the amount of incidents had.

If there is a correlation then the researchers might be able to attribute the number of attacks with the software risk management practices that are followed. Thus serving Hypothesis 2.
2. Part 5 Management Control and Risk Management

IT Manager Questionnaire Part 5

Figure 15
Question 14
Risk Assessment Method Influence

Do you have a way to calculate the likelihood of the risk, or do you estimate the risks?
Figure 16
Question 15

Do you have a way to calculate the impact of the risk or do you use more subjective criteria?

IT Manager Questionnaire Part 5
Figure 17
Question 16

Top Level Manager Influence Over Risk Management

Risk Management Method Influence
Figure 18
Question 18
IT Manager Questionnaire Part 5

Do you have a way to use calculations to rank the priority of your risk?

IT Manager Questionnaire Part 5
Figure 19
Question 19

Do you have a resolution process for the high priority risk items?

IT Manager Questionnaire Part 5
Figure 20
Question 20

Part 5 Summary
The questions 15, 16, 19, 20 in part 5 are used to display the level at which the IT managers are following Boehm’s standard practices. The 4 Boehm practices are in the questions 15, 16, 19, 20. The results from these questions are used to determine whether the respondents are following 0, 1, 2, 3, or 4 of the Boehm practices calculated from the coded data. The level to which they are following can show if there are any patterns between the number of steps being used and the number of attacks that have been had. These results serve Hypothesis 2.

The questions 14 and 18 are used to determine the level of influence from the top level managers to the risk management process. This is to see how the top level managers are influencing the risk management process. These results serve Hypothesis 1.
V) Analysis

1. ISMS Comparison

This is the main comparison that is used to show what degree the managers in the U.S are following the certain standard steps in their management control systems. The purpose of the step by step comparison of the ENISA ISMS to the US practices is an observation of respondents following theory. It simply adds a background perspective to the hypothesis testing. The comparative results show a level of congruence with the ENISA ISMS. The ISMS comparison section shows to what degree that level of congruence is. In addition, the risk management process is displayed by the two practices used by Boehm since they align with the ENISA ISMS as well as the management systems theory. In that case, a comparison is made to those two practices in a matter of 4 criteria. Risk exposure(2 criteria) and risk resolution(2 criteria).

1.1 Security Policy
Step 1

<table>
<thead>
<tr>
<th>ENISA ISMS(EU)</th>
<th>IT Manager Control Systems(U.S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Is generated by top level managers because it is a strategic decision and serves as a clear guideline for lower departments.</td>
<td>The results show that the IT manager's did in fact obtain more security policies from top level their managers, however, this was not by a large margin. The proportion out of 45 top level/department responses was shown to be ~ 56% in favor of top level managers.</td>
</tr>
</tbody>
</table>
1.2 Management Control System Scope
Step 2

<table>
<thead>
<tr>
<th>ENISA ISMS(EU)</th>
<th>IT Manager Control Systems(U.S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>The ISMS scope consists of defining the external environment and the internal environment.</td>
<td>The results show that 84% of the respondents do have a clear definition of the internal and external environment within their system scope.</td>
</tr>
<tr>
<td>The ISMS scope has a clear risk management context.</td>
<td>The results show that 68% of the respondents have a clear risk management context.</td>
</tr>
<tr>
<td>The ISMS scope lists risk criteria.</td>
<td>The results show that 68% of the respondents have a system scope that lists risk criteria.</td>
</tr>
</tbody>
</table>

1.3 Risk Assessment
Step 3

<table>
<thead>
<tr>
<th>ENISA ISMS(EU)</th>
<th>IT Manager Control Systems(U.S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>There is a method for identifying, analyzing, and evaluating risk.</td>
<td>There is no definitive method that was gained from this question due to its qualitative nature and variety of responses. The methods explained have some form of identifying, analyzing, and evaluating their software risk but to what degree is unknown.</td>
</tr>
<tr>
<td>Risk assessment method is implemented more from an operational standpoint rather than by superior management.</td>
<td>The results show that 62% of respondents chose the level of influence 3 or 4.</td>
</tr>
</tbody>
</table>
Boehm’s Risk Exposure | IT Manager Risk Exposure Practice
---|---
This practice uses calculations for the likelihood of software risk. | The results show that only 76% of respondents do not use calculative tools for the likelihood of software risk. This percentage was taken from the proportion of 50 responses. A smaller minority are calculating risk at 24%.

This practice uses calculations for the impact of risk. | The results show that only 24% of respondents use calculative tools for the impact of risk. This percentage was taken from the proportion of 50 responses. This means that 76% are using subjective criteria.

1.4 Risk Management

Step 4

| ENISA ISMS(EU) | IT Manager Control Systems(U.S) |
---|---|
There is a method for determining a risk response plan from generating controls & protocols. | There was no definitive method that was gained from this question due to its qualitative nature and variety of responses. The methods carried a way to prioritize risk and act upon it but to what degree is unknown. |

Risk management method is implemented more from an operational standpoint rather than by superior management. | The results show that 32% of respondents chose 3 as their level of influence. 24% chose level 2 and 22% chose level 4 which creates a fairly even spread. |
Boehm’s Risk Resolution | IT Manager Risk Resolution Practice
--- | ---
The results show that 60% of respondents do not use calculations to rank the priority of software risk. | This practice uses calculations to rank the priority of software risk.
The results show that 70% of respondents do have a resolution process for high priority risk items. | This practices has a resolution process for the high priority risk items.

1.5 Selection of Controls
Step 5

ENISA ISMS(EU) | IT Manager Control Systems(U.S)
The results show that 52% of respondents do have a selection process for the application of controls. | This step requires a selection process for the application of controls needed.

1.6 Statement of Applicability
Step 6

ENISA ISMS(EU) | IT Manager Control Systems(U.S)
The results show that 64% of respondents do track the security implementation with proper documentation. | This step is to track the security implementation with proper documentation.
2. Test Hypothesis
The researchers test two hypothesis in this section. The method of statistical significance testing is the T-Score test for hypothesis 1 and the method for hypothesis 2 is the correlation coefficient and the two tailed test.

2.1 Hypothesis 1
Is there evidence of lower influence from top level managers, measured by level of influence of top level managers, to the risk management process at a .05 significance interval?

H₀ - The top level managers have moderate or more influence over the risk assessment method
H₁ - The top level managers have less influence over the risk assessment method
H₀: μ = μ₀
H₁: μ ≠ μ₀

\[ t = \frac{\bar{x} - \mu_0}{\sigma/\sqrt{n}} = \frac{3 - 3}{1.088 / \sqrt{50}} = 0 \]

-2.009 < 0 < 2.009 therefore cannot reject null

H₀ - The top level managers have moderate or more influence over the risk management method
H₁ - The top level managers have less influence over the risk management method
H₀: μ = μ₀
H₁: μ ≠ μ₀

\[ t = \frac{\bar{x} - \mu_0}{\sigma/\sqrt{n}} = \frac{2.9 - 3}{1.182 / \sqrt{50}} = -0.598 \]

-2.009 < -0.598 < 2.009 therefore cannot reject null
2.2 Hypothesis 2
Is there evidence for a linear relationship between risk management processes, measured by number of steps followed, and software vulnerability, measured by number of attacks, at a .05 level of significance?

$H_0: \rho = 0$ (no correlation)
$H_1: \rho \neq 0$ (correlation)

$$r = \frac{\overline{\sigma}(\overline{\sigma}) - (\overline{\sigma})(\overline{\sigma})}{\sqrt{\overline{\sigma}^2 - (\overline{\sigma})^2} [\overline{\sigma}^2 - (\overline{\sigma})^2]}$$

$r = -0.2319608$

$$t = \frac{-0.232}{\sqrt{\frac{1-(-0.0232)^2}{50-2}}} = -1.652$$

$-2.01 < -1.652 < 2.01$ therefore cannot reject null

There is no evidence of a linear relationship at the 5% level of significance.

3. Analytical Summary
The ISMS comparison has provided a congruence comparison to observe the results. This is simply used to display a percentage of respondents that are following the steps. This can be observed before the hypothesis so the reader has an idea of the degree to which these respondents are following the theory. There are no concrete conclusions taken from the ISMS comparison considering not all the results are relevant to the hypothesis. The hypothesis has provided calculations that can be interpreted to provide conclusive statements. The two hypothesis cannot reject the null statements due to the results from this testing.
VI) Conclusions

These conclusive statements are generated with a 0.05 significance level which creates a 95% confidence interval.

It is clear that firms are moving toward smart grid technology and attaching their infrastructure to networks. 96% of these IT managers do in fact have their networks attached to their critical infrastructure. An additional 92% of these firms have vulnerable infrastructure if software is compromised. These results demonstrate that a lack of standards can affect a firm’s exposure to software vulnerability. This is by no means a small problem considering that energy firms can affect surrounding populations. This being the case, firms should be taking an adherence to standards considering they can affect software vulnerability and even worse infrastructure vulnerability.

The top level managers are influencing the risk management processes at these firms at a moderate or high level. There is no evidence to confirm that the department level managers are influencing the risk management process more. The risk assessment method is not being influenced more from the IT departments and the risk management method is not being influenced more from the IT department thus consisting of the entire risk management process. The ENISA ISMS suggests that the risk management processes should be influenced more at the department level, but the statistics show that there cannot be a claim made to assign any high amount of influence from the U.S IT departments to their risk management processes whatsoever. This in fact suggests that the U.S IT managers are not following this standard of practice. The U.S IT departments would in fact have more of an influence in their risk management processes if that were the case. This is troubling considering the amount of these firms that are attached to networks.

The risk management process cannot correlate to software vulnerability. There is no evidence that the number of risk management steps being used at the Boehm standard relate to the number of attacks at these firms. The researchers cannot prove that the correlation is not due to random chance. A number of respondents were following 3 to 4 of the Boehm standard steps, however, it
cannot be said that there was a linear relationship to the number of steps followed to the number of attacks. In that case, it could not be said that a non-standard risk management process could indeed lead to more software attacks at least from this initial study.

Further research of this problem could investigate why the U.S firms have not fully given the IT department the influence needed to oversee their risk management processes which would therefore, implement a management control standard that is supported by theory. If studies can emerge with different research method approaches (interviews, inductive etc.) then there can also be more answers such as if there are non-standard software risk management practices that are actually leading to software vulnerability.

Overall, software vulnerability is apparent in these U.S firms and the integration of a standard management systems theory is designed to protect against it. The researchers have found that the ENISA ISMS standard is not being followed and that software vulnerability cannot be attributed to the risk management process in this study.

**Further Research**

These are certainly problems worth investigating further. The researchers hope that experts in management systems academia can contribute further considering that there is very few information security management studies that are found in literature (Shing-Hong et al. 2003). The lack of theory in this realm of research has led to few empirical studies to examine the effectiveness of management strategies (Shing-Hong et al. 2003). The researchers hope that more of these empirical studies could address the importance of information security management in the energy sector because networks are becoming more prevalent. The researchers hope this study can expose the growing necessity to solve these managerial system related issues and inspire industry experts to investigate further.
VII) Bibliography


https://www.bls.gov/oes/current/oesrcli.htm#00

https://www.cfr.org/content/publications/attachments/Energy_Brief_Clayton_Segal.pdf


VIII) Appendix

This appendix shows the questions asked on the survey, coded answers, and survey data.

A) Survey Questions

Q1 - Are you currently employed as an IT manager in the energy sector?
   Yes  No

Q2 - What region of the US do you live in?
   Western  Central  Southern  Northeast  Other

Q3 - How old are you?

Q4 - How many years of experience do you have in the industry?

Study Disclaimer
This study is to gather data on the management control system and its influence on energy sector IT managers in the U.S. This study aims to compare the management control system of energy companies in the U.S to that of the Information Security Management System(ISMS) established by the European Union Agency for Network and Information Security. The goal is to do a step by step comparison of the ISMS to the U.S based management control systems. The questions in this study will help identify if these systems are using proper risk management methods and whether or not they can be adjusted to prevent software vulnerability.
The respondents in this study must currently be IT Managers within the energy sector and work in the U.S. The responses will remain completely anonymous.

Q5 - Are your infrastructure assets connected to a network?
   Yes   No

Q6 - Does infrastructure become vulnerable when or if software is compromised at your firm?
   Yes   No

Q7 - Have there been any successful malware or spear phishing incidents at your firm?
   Yes   No   Not sure

Q8 - How many can you recall?
   Only shown if respondent answered “Yes” to the previous question

Q9 - Is the security policy in your management control system generated by your top level managers or by the IT department? Please Explain

Q10 - Is the internal and external environment clear within the scope of your risk management system?
   Yes   No

Q11 - Do you feel there is a clear risk management context in your system scope?
   Please Explain
Q12 - Does the system scope list risk criteria?
   Yes  No

Q13 - What method(s) is used to assess your software risk

Q14 - At What level is this method directly influenced by your superiors in the organization?
   1  2  3  4  5

Q15 - Do you have a way to calculate the likelihood of the risk, or do you estimate the risks?

Q16 - Do you have a way to calculate the impact of the risk, or do you use more subjective criteria?

Q17 - What methods are used to manage your software risk

Q18 - At What level is this method directly influenced by your superiors in the organization?
   1  2  3  4  5

Q19 - Do you have a way to calculate the rank of the priority of your risk?
Q20 - Do you have a resolution process for the high priority risk items?

Q21 - Does your IT department have a selection process for the application of controls needed?
   Yes  No

Q22 - Briefly explain
   Only shown if respondent answered “Yes” to the previous question

Q23 - Do you track the security implementation with proper documentation?

Q24 - Briefly Explain.
   Only shown if respondent answered “Yes” to the previous question
This Appendix shows how each respondent answered their survey. An ID number was given to each respondent and their answer was marked below the relevant question. Responses to questions asking for a more detailed response such as question 9 were interpreted into the categories listed in the legend. Questions 13 and 17 are missing because they were long answer, open ended questions with answers that can not be interpreted in a manner appropriate for a table.

| ID # | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | Q8 | Q9 | Q10 | Q11 | Q12 | Q13 | Q14 | Q15 | Q16 | Q17 | Q18 | Q19 | Q20 | Q21 | Q22 |
|------|----|----|----|----|----|----|----|----|----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| 1    | Y  | 25 | 5  | S  | Y  | Y  | N  | -  | M  | Y  | Y  | N  | 3   | C   | C   | 2   | Y   | Y   | Y   | N   |     |     |
| 2    | Y  | 31 | 8  | W  | Y  | Y  | N S | -  | B  | Y  | Y  | Y  | 2   | E   | E   | 5   | N   | Y   | Y   | N   |     |     |
| 3    | Y  | 36 | 5  | C  | Y  | Y  | N  | -  | I T | Y  | Y  | Y  | 4   | E   | E   | 4   | N   | Y   | Y   | N   |     |     |
| 4    | Y  | 36 | 5  | W  | Y  | Y  | Y  | 1  | I T | Y  | Y  | Y  | 1   | E   | E   | 1   | N   | N   | N   | N   |     |     |
| 5    | Y  | 28 | 10 | S  | Y  | Y  | Y  | 1  | M  | Y  | Y  | Y  | 4   | C   | C   | 3   | Y   | Y   | Y   | Y   |     |     |
| 6    | Y  | 36 | 15 | S  | Y  | Y  | Y  | 2  | I T | Y  | Y  | Y  | 4   | E   | E   | 4   | Y   | Y   | Y   | Y   |     |     |
| 7    | Y  | 23 | 3  | W  | Y  | Y  | N  | -  | M  | N  | Y  | N  | 2   | C   | C   | 2   | Y   | Y   | Y   | Y   |     |     |
| 8    | Y  | 25 | 4  | S  | Y  | Y  | Y  | 2  | I T | N  | Y  | Y  | 3   | E   | E   | 3   | Y   | N   | Y   | Y   |     |     |
| 9    | Y  | 38 | 15 | S  | Y  | Y  | Y  | 2  | B  | Y  | Y  | Y  | 3   | E   | E   | 4   | Y   | Y   | Y   | Y   |     |     |
| 10   | Y  | 31 | 5  | W  | Y  | Y  | Y  | 3  | I T | Y  | N  | N  | 5   | E   | E   | 1   | N   | N   | N   | N   |     |     |
| 11   | Y  | 45 | 25 | S  | Y  | N  | Y  | 1  | B  | N  | N  | N  | 2   | E   | E   | 3   | N   | N   | N   | N   |     |     |
| 12   | Y  | 32 | 10 | W  | Y  | Y  | Y  | 5  | I T | Y  | Y  | Y  | 1   | E   | E   | 2   | N   | Y   | Y   | Y   |     |     |
| 13   | Y  | 37 | 1  | S  | Y  | Y  | Y  | 1  | M  | Y  | Y  | N  | 4   | E   | E   | 4   | Y   | Y   | N   | Y   |     |     |
| 14   | Y  | 30 | 8  | N  | Y  | Y  | Y  | 2  | M  | Y  | Y  | Y  | 2   | C   | C   | 3   | Y   | Y   | Y   | N   |     |     |
| 15   | Y  | 28 | 4  | S  | Y  | Y  | N  | -  | I T | Y  | Y  | Y  | 4   | E   | E   | 4   | Y   | Y   | N   | Y   |     |     |
| 16   | Y  | 28 | 8  | W  | Y  | Y  | Y  | 3  | I T | Y  | Y  | Y  | 3   | E   | E   | 3   | Y   | Y   | N   | Y   |     |     |
| 17   | Y  | 25 | 5  | S  | Y  | Y  | Y  | 1  | B  | Y  | Y  | N  | 3   | E   | E   | 3   | Y   | Y   | N   | Y   |     |     |
| 18   | Y  | 32 | 10 | S  | Y  | Y  | Y  | 13 | M  | Y  | Y  | Y  | 2   | C   | C   | 3   | Y   | Y   | N   | N   |     |     |
| 19   | Y  | 27 | 5  | W  | Y  | Y  | Y  | 1  | M  | Y  | Y  | N  | 3   | E   | E   | 2   | Y   | N   | N   | N   |     |     |
| 20   | Y  | 28 | 6  | S  | Y  | N  | Y  | 2  | I T | Y  | Y  | Y  | 1   | E   | E   | 1   | Y   | Y   | N   | Y   |     |     |
Y 24 5 S Y Y N - M Y N Y 4 E E 3 N N Y N
22 Y 29 1 S Y Y N - I T Y N Y 2 C C 1 Y Y Y Y
23 Y 67 15 S Y Y Y 2 M Y N Y 3 E E 3 Y Y Y Y
24 Y 23 1 S Y Y NS - M Y Y Y 3 C C 3 N N N N
25 Y 55 16 S Y Y Y 17 I T Y Y Y 4 E E 4 N N N N
26 Y 26 3 N Y N Y 3 M Y N N 4 E E 3 N N N Y
27 Y 35 11 N Y Y NS - M Y N N 5 E C 5 Y Y Y Y
28 Y 29 5 W Y Y Y 5 M Y N Y 3 C E 4 Y Y Y Y
29 Y 25 10 S Y Y Y 10 M Y N Y 4 C C 2 Y N N N
30 Y 35 7 S Y Y N - I T Y Y N 3 E E 4 Y Y Y Y
31 Y 30 7 C Y Y Y 1 M Y Y N 5 C E 5 Y Y Y Y
32 Y 28 7 N Y Y Y 1 M N N Y 4 E E 4 N N N N
33 Y 42 18 N Y Y Y 2 M Y Y Y 3 E E 3 Y Y Y Y
34 Y 25 2 C Y Y N - I T Y Y Y 4 E E 5 Y Y Y Y
35 Y 38 22 C Y Y N - M Y Y N 3 E E 2 Y Y N N
36 Y 30 5 W Y N N - I T Y Y Y 2 E E 1 N Y N Y
37 Y 35 12 C Y Y Y 1 M Y Y Y 4 E E 5 N Y Y N
38 Y 35 9 S Y Y Y 1 M Y N N 2 E E 2 N Y Y Y
39 Y 25 4 S Y Y N - M Y N N 4 E E 4 Y Y Y Y
40 Y 29 3 S Y Y N - M Y Y Y 2 E E 2 N N Y Y
41 Y 35 10 W N Y NS - I T Y Y Y 3 E C 2 N Y N Y
42 Y 32 9 S Y Y N - I T Y Y Y 3 E E 3 Y Y Y Y
43 Y 52 30 C Y Y Y 3 M Y N Y 2 E E 2 N N Y N
44 Y 38 19 W Y Y NS - B Y N Y 2 E E 2 Y Y N Y
45 Y 47 5 C Y Y Y 5 M Y Y Y 4 E C 3 N N Y N
46 Y 35 7 N Y Y Y 2 M N Y Y 1 C E 1 N N N Y
47 Y 36 16 W Y Y NS - I T Y Y N 3 C C 3 Y Y N Y
48 Y 33 10 W Y Y Y 5 I T N Y N 1 E E 1 N Y N N
49 Y 35 10 S N Y Y 1 I T N N Y 4 E E 3 N N Y N
50 Y 35 8 S Y Y N - I T N N N 3 E E 3 N Y N N
Legend: All Q's - Y=Yes N=No NS=Non Satisfactory
Q4 - S=South W=West C=Central N=Northeast
Q14/18 - Level of Influence
Q15/16 - C = Calculate E = Estimate
Q9 - M=Management IT=Department B=Both
C) Figures

1. Part 2 Demographics and Experience

IT Manager Questionnaire Part 2

Question 3

IT Manager Questionnaire Part 2
Question 4
This figures resembles the years of experience in industry for the questionnaire.

IT Manager Questionnaire
Question 5

IT Manager Questionnaire
Question 6
IT Manager Questionnaire Part 4

Question 7

Have there been any successful malware or spear phishing incidents at your firm?

IT Manager Questionnaire Part 4

Question 8

Number of Incidents

0 2 4 6 8 10 12
1 2 3 4 5 Over 5
3. Part 5 Management Control and Risk Management

IT Manager Questionnaire Part 5

Question 9

Is the security policy in your management control system generated by your top level managers or by the IT department? Please Explain

- Top Level Management
- IT Department
- Both

IT Manager Questionnaire Part 5

Question 10

Is the internal and external environment clear within the scope of your risk management system?

- Yes
- No
IT Manager Questionnaire Part 5
Question 11

Do you feel there is a clear risk management context in your system scope?

16 Yes | 34 No

IT Manager Questionnaire Part 5
Question 12

Does the system scope list risk criteria?

16 Yes | 34 No
The next question in the questionnaire was Q13. It asked for what method(s) were being used to assess software risk which generated a variety of responses. These included monthly audits to the active software, risk screening based on impact and probability, and risk factor analysis for problems such as malware.

**IT Manager Questionnaire Part 5**

**Question 13**

![Bar chart](chart.png)

**Question 14**

**Risk Assessment Influence**
IT Manager Questionnaire Part 5

Question 15

Do you have a way to calculate the likelihood of the risk, or do you estimate the risks?

- Calculate (38)
- Estimate (12)

IT Manager Questionnaire Part 5

Question 16

Do you have a way to calculate the impact of the risk or do you use more subjective criteria?

- Calculative (38)
- Estimate (12)
The next question in the questionnaire was Q17. It asked for what method(s) are being used to manage software risk which generated a variety of responses. These responses included the prioritization of risks and software action plans. One example of this is given by an excerpt from respondent in the questionnaire “Classify and prioritize all risks then Craft a plan that links each risk to a mitigation Monitor” (Respondent Q17).

IT Manager Questionnaire Part 5

Question 17

![Bar chart showing the level of influence over risk management](chart.png)

IT Manager Questionnaire Part 5

Question 18
IT Manager Questionnaire Part 5

Question 19

Do you have a way to use calculations to rank the priority of your risk?

- Yes: 30
- No: 14

IT Manager Questionnaire Part 5

Question 20

Do you have a resolution process for the high priority risk items?

- Yes: 35
- No: 15
IT Manager Questionnaire Part 5

Question 21

Does you IT department have a selection process for the application of controls needed?

- Yes: 26
- No: 24

IT Manager Questionnaire Part 5

Question 22

Do you track the security implementation with proper documentation?

- Yes: 32
- No: 18