3-6-2007

Developing a Framwork for Evaluating Organizational Information Assurance Metrics Programs

Adam R. Bryant

DEVELOPING A FRAMEWORK FOR EVALUATING ORGANIZATIONAL INFORMATION ASSURANCE METRICS PROGRAMS

THESIS

Adam R. Bryant, Captain, USAF

AFIT/GIR/ENV/07-M5

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the United States Air Force, Department of Defense, or the United States Government.

AFIT/GIR/ENV/07-M5

DEVELOPING A FRAMEWORK FOR EVALUATING ORGANIZATIONAL INFORMATION ASSURANCE METRICS PROGRAMS

THESIS

Presented to the Faculty

Department of Systems and Engineering Management

Graduate School of Engineering and Management

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the Requirements for the

Degree of Master of Science in Information Resource Management

Adam R. Bryant, BS

Captain, USAF

March 2007

AFIT/GIR/ENV/07-M5

DEVELOPING A FRAMEWORK FOR EVALUATING ORGANIZATIONAL INFORMATION ASSURANCE METRICS PROGRAMS

Adam R. Bryant, BS

Captain, USAF

Approved:

//SIGNED//_____	_6 Mar 07
Michael R. Grimaila, PhD (Chairman)	Date
//SIGNED//_____	_6 Mar 07
Robert Mills, PhD (Member)	Date
//SIGNED//_____	_6 Mar 07
Maj. Paul D. Williams, PhD (Member)	Date

Abstract

The push to secure organizational information has brought about the need to develop better metrics for understanding the state of the organization's security capability. This thesis utilizes case studies of information security metrics programs within Department of Defense organizations, the United States Air Force (USAF), and the National Aeronautics and Space Administration's (NASA's) Jet Propulsion Lab to discover how these organizations make decisions about how the measurement program is designed, how information is collected and disseminated, and how the collected information supports decision making.

This research finds that both the DOD and USAF have highly complex information security programs that are primarily focused on determining the return for security investments, meeting budget constraints, and achieving mission objectives while NASA's Jet Propulsion Lab seeks to improve security processes related to compliance. While the analytical techniques were similar in all of the cases, the DOD and USAF use communication processes still based mostly on manual data calls and communications. In contrast, NASA's JPL information security metrics program employs a more automated approach for information collection and dissemination.

Acknowledgments

I would like to say thank you to my sweet wife as well as my children for supporting me in my decision to pursue separate degrees, and for being patient with me when my class work and this thesis often took so much of my time that I couldn't spend with you. Thank you to the U.S. Air Force for giving me this unique and excellent set of opportunities and to my bosses for supporting me. Thank you to AFIT and its faculty for providing me with a very worthy challenge, and for forcing me to push myself even harder. Thank you to my parents for the independence and perseverance you taught me at an early age, for my brothers and sisters for shaping my world. Thank you to my HQAX band mates and the many new friends I've made in the Dayton area through my music life, which have helped me see the world in different ways and helped me keep everything in perspective. I also would thank my Lord for watching over me whenever times are difficult, for giving me strength when I've had nothing left to give, and for constantly reminding me how little I know and how much I have left to grow.

Adam Bryant

Table of Contents

Page

List of Figures

Page

List of Tables

Page

DEVELOPING A FRAMEWORK FOR EVALUATING ORGANIZATIONAL INFORMATION ASSURANCE METRICS PROGRAMS

I. Introduction

Background on Information Security Metrics

Organizations spend a lot of money on information security related expenditures in many different areas. In the United States, companies and private organizations spend millions of dollars each year on measures to protect their information and information systems. Nearly all organizations responding to the 2005 CSI/FBI survey agree that information security is an important component of their organizational strategy and it is a critical capability. In this survey, as well as other similar security surveys, respondents report spending between two and five percent of their budget on information security (Dinnie, 1999; CSI/FBI, 2004; CSI/FBI, 2005; Deloitte Touche Tohmatsu, 2003; Deloitte Touche Tohmatsu, 2005; Department of Trade and Industry, 2004) .

Information security is vital to the success and survival of modern organizations because the world is more connected than it ever has been. Because of the rapid advances in information technology, computers and information systems have become ubiquitous. Information and information systems bring great capabilities to the modern world, but they also introduce a great dependence on those capabilities (Tiwari and Karlapalem, 2004).

In many cases, this dependence is so great that many organizations could not function without the information technology support they enjoy today. Some types of organization such as banking depend so heavily on the security of their systems and the transactions that users make with them that they could not function if their information systems were severely compromised. Other organizations, such as the U.S. Department of Defense (DOD) and the Department of Homeland Security (DHS) depend on information security to establish continuity of operations and to prevent the loss of human life.

Information Security Metrics

There are many different areas that organizations can focus on to make their information systems more secure. The International Information Systems Security Certification Consortium $(ISC)^2$ lists access control systems, secure software development, physical security, network security, operations security,

law, ethics, and privacy as some of their ten domains of information security ((ISC)², 2006). Organizations can also spend money to improve their communications security through cryptography and security protocols or with key management infrastructures such as the public key infrastructure. They could also devote money and resources to training users in order to eliminate vulnerabilities that users can introduce into their information systems.

The International Standards Organization (ISO) says that organizations can focus on management and policy measures, personnel measures, operational measures, business continuity planning measures, or physical security measures (ISO/IEC TR 13335-4, 2000).

In addition, most organizations spend money on virus protection and firewalls, and many organizations have elaborate intrusion detection systems to prevent external adversaries from gaining access to their information systems (CSI/FBI, 2005). These organizations also spend money on access controls, measures to prevent physical theft, identity management, network security, policy management, and many other areas. Unfortunately, in most cases there are more areas to protect than there are resources available.

Despite all of these ways to spend money, few organizations can say exactly what level of security they have (Geer, Soo Hoo, & Jaquith, 2003). It is

difficult to establish a baseline or extract performance measures from the performance of the security solutions above. It is also difficult to define exactly how those solutions help the organization achieve its mission, or the business to achieve its bottom line. Since the effects of an organization's work and spending on information security is unknown, many organizations see information security as a sunk cost with no return on investment (CSI/FBI, 2005).

Furthermore, it is very difficult to see any tangible results from work spent on information security. Since security involves preventing events or acts from happening, successful security solutions will seem to have no effect at all. The organization's leadership is then left with the task of determining whether the lack of effects they experienced was due to the security solution, in which case they made a great decision, or due to chance, in which case they squandered millions of dollars that could be better used for other purposes.

If an organization's leadership should decide the security solution was wasted money, they may decide to cut the security budget until they feel they are getting a better return on investment, but currently there are no generally accepted measures to determine return on investment so this would be a gut-feel guess at best (Berinato, 2005). This phenomenon is only complicated by the fact

that many information security and IT departments have difficulty proving that they achieve any results with the security money in their budget.

Hamilton (1998) points out that in 1996 and 1997, the FBI and the Computer Security Institute of San Francisco put out the first and second FBI/CSI surveys, with results that shocked management and led to the current practice of using fear, uncertainty, and doubt as primary mechanisms to justify information security solutions, rather than measures that provide evidence of return on investment.

It is possible for an organization to spend millions of dollars on security solutions and still leave numerous vulnerabilities unprotected because it chose the wrong approach or the wrong solutions. Thus, organizations want to find the optimal strategy for how to spend their information security budget which will provide them the highest level of protection for the least cost. Standards such as ISO/IEC 17799 and ISO/IEC 27001 provide guidance on the domains that security management should consider when developing an organizational security program but they don't choose the mix of security controls that is right for each organization (NIST 800-12, 1995; ISO/IEC 17799, 2000; ISO/IEC 27001, 2005).

In order to attempt to find this optimal mix, organizations can make risk decisions weighing the threat, vulnerability, and potential impact of negative events occurring and plan their controls accordingly. This problem is more complicated than it first appears though, because each security control is designed to only protect against a certain type or small set of threats. Threats are also aimed at vulnerabilities that the organization has which they may or may not know about.

Finally, organizations may not know what the potential impact for a certain event is, or the probability that it will occur. Since this information often is lacking, the task of protecting information systems becomes a guessing game in order to determine which vulnerabilities are the most important, and which threats are the most likely to occur.

This is where security metrics come into play. The National Science and Technology Council's 2006 report explained that security metrics offer the ability for organizations to "isolate problems with an information security program, justify budgets and spending, and target investments." The council's report also says security metrics can help organizations tie their high-level goals and investments to the security events and the tactically-focused implementation of

each specific security measure or investment (The National Science and Technology Council, 2006).

But more basically the council said that security metrics should be used "to identify security weaknesses," "determine trends," to "better utilize security resources," "measure success or failure of implemented security solutions," and to "help characterize the organization's overall security posture from risk/threat/vulnerability, budgetary, and regulatory standpoints" (The National Science and Technology Council, 2006).

To consolidate and summarize their points, according to the NSTC (2006), the basic purposes of a metrics program are to:

- Identify and isolate security problems
- Determine security trends
- Measure effectiveness of security measures
- Provide security accountability
- Justify security spending
- Link high-level goals and investments to security events and measures

Security metrics are also important because laws and regulations demand reporting on information security programs. After corporate scandals in the early 2000's, the Sarbanes-Oxley Act was signed into law mandating stricter accounting by corporate-level officers in publicly-traded organizations. Since

this law requires executive-level officers to certify their financial statements, the executive level in organizations typically requires this same type of reporting from lower echelons in the company.

The National Institute of Standards and Technology (NIST) holds that a strong information security risk management plan requires the collection of good and meaningful metrics about the organization's information security posture and practices, but there is still little agreement about what those metrics should be, what themes should underlie them, how the metrics should be organized, and which metrics are the most effective for managing which aspects of information security (Swanson, 2003; Seddigh et al., 2004).

Metrics have been used for years as inputs to decisions in fields such as logistics, manufacturing, software engineering, and customer service. However, with information security, metrics are needed that are reliable enough on which to base multi-million or multi-billion dollar decisions which in some cases may have life-or-death consequences.

Regardless of the reason for developing and collecting metrics, since metrics are designed to support decisions, it is sensible that any metrics program should have (1) a methodology for gathering data, (2) processes for analyzing and interpreting the data, and (3) a process by which that data is used to support

decision making. This really is just one type of process for turning organization data about information security into actionable, decision-level knowledge. Papadopoullos (2004) presents one process of turning data into knowledge:

- Data capture or *gathering*
- Data normalization and transformation or *organizing*
- Data analysis or *refining*
- Data reporting or *disseminating*

Because of the simplicity of this approach, this research will use these steps as a starting point to discover more about how organizations implement their information security systems and why they do it that way. Since many organizations have involved themselves with information security metrics, but there are no standard practices, processes, or measures, the goal of this research is to discover more about what organizations have actually done in their security metrics programs and to find some common threads among those programs that may be used to develop general propositions that may apply to other public sector security metrics programs.

Investigative Questions

Using these steps as a starting point, the intent of this thesis is to discover answers the following questions:

- Q1: How do organizations make decisions and communicate decisions about what and how to measure?
- Q2: How do organizations perform:
    - Data gathering
    - Data normalizing and transforming
    - Data analysis
    - Data reporting
- Q3: How do organizations use the information provided by metrics support information security-related decisions?

In this thesis, we will explore a review of relevant academic and practitioner literature in order to lead us to a model and a qualitative case study methodology which are appropriate to this type of inquiry. This thesis will then present cases from the U.S. Department of Defense (DOD), the U.S. Air Force (USAF), Air Force Materiel Command (AFMC), and the National Aeronautics and Space Administration's (NASA) Jet Propulsion Lab and draw inferences from the cases to develop a set of propositions which may be tested in later research.

Scope

This thesis will seek to answer questions about the domain of metrics, measurement, information assurance and security, and management, but will

focus specifically on how organizations have designed and operate their information security metrics programs by a sample of organizations in the public sector. Furthermore, this research will focus only exploring and investigating rather than evaluating approaches to some of the problems related to information security metrics.

Thesis Overview

Chapter one has been a look at the background of security metrics and it established the goals of this research. It introduced the importance of information security metrics and focused on some of the purposes and uses of a security metrics program, such as demonstrating return on security investment, improving information security, and providing a reportable measure of the security of an organization's systems. This chapter also briefly introduced the research questions, and explained the scope of this research problem.

Chapter two contains a more in-depth review of literature related to security metrics. Chapter two also goes into what metrics really are and discusses the nature of data collection, normalization, analysis, and reporting. Chapter three provides an overview of qualitative methodology, and the case study methodology used in this study. It explains the rationale behind the

research design and its appropriateness to answer the research questions. It also reviews guidelines for ensuring rigorous case study research.

Chapter four outlines the results from the research, providing the reader access to the aggregated information collected from the case study and chapter five provides a discussion on the research results and presents implications for future research.

II. Literature Review

In order to understand any problem, it is important to understand how the problem is organized. In computer science problems, knowledge of the architecture of a software program, or knowledge of the data structures and algorithms used can help the problem solver frame the problem and come up with possible solutions (Michaelewicz and Fogel, 2000). In this thesis, we will frame the problem by seeking to develop a theory of how decision processes and communication processes interact with an organizational security metrics program and how they are manifested in the capture, normalization, analysis, and reporting of metrics.

Hong, Chi, Chao, and Tang (2003) claim that the process of developing a theory involves "developing concepts, constructs, and propositions at the same time," and that is the goal of this chapter. We will explore the different concepts related to information security management, and tie those into the decision processes where they are considered. The constructs we provide will be combined from an extensive search of relative literature.

Concerning theory development, Hong et al. (2003) say that theories can be built by intension, which is modifying an existing theory, or extension, which is look for a better explanation of a theory. This thesis will develop its theory by

intension, modifying and combining several different concepts and theories to form a model.

Since the questions guiding this research are exploratory in nature, this theory will take the form of a model that we can present graphically. Rather than present cause and effect relationships, it will present a model of organizational communication and decision-making flow that may be used to better understand the organizational contexts presented in the cases that follow.

We will present this model in parts by introducing concepts and phenomena that are critical to understanding information security. We will then examine the concepts that may influence data collection, normalization, analysis, and reporting processes in information security metrics programs. Finally, we will explore concepts and constructs that may be relied upon in the decision processes. We will then present the model.

In order to understand the concepts that underlie a theory, one of the first things needed is a set of definitions and a grouping of ideas that provide boundaries as to what each concept covers. This commonly is called a taxonomy. One example of a taxonomy comes from the field of psychology. Within field of psychology, numerous theories and models explain how to conceptualize a human's personality. Each of the theories of personality comes with its own set

of definitions and constructs. Ewen's text (1998) on *Theoris of Personality* defines a construct as "a term or principle that is created (or adopted) by a theorist." It says that a theory is composed of "a set of constructs that are related to each other in a logical and consistent way."

Some examples of theories of personality in psychology are Sigmund Freud's psychoanalytical view, Jung's analytic view, Adler's individual perspective, various clinical-based theories from Karen Horney, Erich Fromm, etc., and B. F. Skinner's behavioral perspective (Ewen, 1998).

Since information security management is more practical than academic, there is not a great deal of existing theoretical research in the discipline. However, user behavior, decision making and risk all have their theoretical backing.

Definition of Information Assurance and Information Security

NIST defines information assurance as a "set of measures" employed with the goal of ensuring confidentiality, integrity, and availability of information and likewise, the International Standards Organization (ISO) defines information security as the "preservation of confidentiality, integrity and availability of information" (NIST 800-12, 1995; ISO/IEC 17799, 2005). The ISO defines those three constructs as follows:

- Confidentiality - ensuring that information is accessible only to those authorized to have access
- Integrity - safeguarding the accuracy and completeness of information and processing methods
- Availability - ensuring that authorized users have access to information and associated assets when required (ISO 17799, 2005)

The DOD and the Committee on National Security Systems follow suit with NIST and ISO in their view, but say that information assurance also includes "providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" (Committee on National Security Systems, 2005; Swanson, 2001; U.S. Department of Defense, 2002). Ameri (2004) adds to this saying that the five pillars of information security are protection, detection, reaction, documentation, and prevention.

Not all definitions for information assurance are the same. Seddigh, Pieda, Matrawy, Nandy, Lambadaris, and Hatfield (2004) developed their own information assurance taxonomy based on a review of other information assurance taxonomies. They define information assurance as being composed of "security, quality of service, and availability" and define these across organizational, operational, and technical areas (Seddigh et al., 2004).

Sometimes, instead of giving different definitions for the same term, researchers give the same definition for different terms. Sometimes these definitions are similar and sometimes they overlap. For instance, Soo Hoo (2000) describes *information security* with a similar definition we used for *information assurance*: measures that ensure availability, confidentiality, integrity, and authenticity.

Hong et al. (2003) offer a different definition for information security: they say it is the act of combining systems, operational, and internal controls for the purpose of ensuring confidentiality of data and operation procedures. They also cite management systems theory saying that an organization should establish and keep an information security management system to "control and protect information assets". Hong et al. (2003) incorporates Tudor (2001) in that there are five parts to information security architecture:

- Security organization and infrastructure
- Security policy, standards, and procedures
- Security baselines and risk assessments
- Security awareness and training programs
- Compliance

Although these are small differences, the boundaries are blurred between information assurance and information security. Similar confusion exists with

the terms *computer security, network security, cybersecurity,* and *information systems security*.

Not having a commonly accepted definition of information assurance or information security makes it very difficult to create a taxonomy around which to organize a set of metrics (Seddigh et al., 2004). To be as clear as possible, for the purpose of this research we will combine the above terms into a single construct: information security, which we will use to mean: a set of measures that has the goal protecting information and information systems by ensuring confidentiality, integrity, and availability of information and information systems, and which incorporates protection, detection, and reaction capabilities.

Related Constructs and Taxonomies of Information Security

We've seen that many sources agree that the goals of information assurance have to do with ensuring confidentiality, integrity, and availability of information (Committee on National Security Systems, 2005). The International Standards Organization (ISO) and NIST agree, but break integrity further down into authentication, accountability, and non-repudiation (IEC, 2000; NIST 800-12, 1995). Each of these terms, however, actually represents a construct that information security has as its goal to protect.

Although it is not necessarily advertised as a taxonomy, it is interesting to note that the International Information Systems Security Certification Consortium $(ISC)^2$ website lists ten domains of information security that the organization expects all candidates for the Certified Information Systems Security Professional (CISSP) certification to be proficient in (Table 1).

Table 1. The $(ISC)^2$ Ten Domains of Information Security

Access control systems and methodology	Applications and systems development security
Business continuity planning and disaster recovery planning	Cryptography
Law, investigation, and ethics	Physical security
Operations security	Security management practices
Security architecture and models	Telecommunications and network security

($(ISC)^2$, 2006)

As another conceptual taxonomy, the DOD's defense-in-depth concept compares information security systems to a medieval castle. It focuses on three principles to implement defense-in-depth: "people, technology, and procedures" (Jones, 2005). The DOD divides the areas of responsibility into "network infrastructure, enclave boundary, computing environment, and supporting infrastructure" and compares these functions and technology with medieval tools, weapons, and attacks of the dark ages (Jones, 2005).

The International Standards Organization (ISO/IEC TR 13335-4, 2000) divides the focus areas of information security management into (1) management and policy measures, (2) personnel measures, (3) operational measures, (4) business continuity planning measures, and (5) physical security measures.

Combining aspects of those models, we come up with something that looks like the Table 2 for the goals of information security.

Table 2. Purpose, Mechanism, and Domain of Information Security

<table>
<tr><th colspan="2">Protection of:</th><th colspan="2">By using the mechanisms of:</th></tr>
<tr><td colspan="2" rowspan="3">Data
Information
Information assets
Information systems
Operational procedures</td><td>People</td><td>Education and training</td></tr>
<tr><td>Technology</td><td>Understanding security architecture</td></tr>
<tr><td>Procedures</td><td>Management measures/practices
Policy measures
Operational measures
Business continuity planning measures
Physical security measures
Application and system development measures</td></tr>
<tr><th colspan="2">By ensuring their:</th><th colspan="2">In the following environments:</th></tr>
<tr><td>Confidentiality</td><td>Operations security
Law and ethics
Cryptography
Access controls</td><td>Computing environment</td><td>Enclave boundary</td></tr>
<tr><td>Availability</td><td>Business continuity planning
Disaster recovery planning</td><td rowspan="2">Network infrastructure</td><td rowspan="2">Supporting infrastructure</td></tr>
<tr><td>Integrity</td><td>Authentication
Accountability
Non-repudiation
Cryptography</td></tr>
</table>

(Adapted from Hong, 2003; Soo Hoo, 2000; Seddigh et al., 2004; Committee on National Security Systems, 2005; Swanson, 2001; (ISC)², 2006; ISO 17799, 2005; NIST 800-12, 1995)

To summarize, the problem of information security is to prevent negative events from happening that would compromise the confidentiality, integrity, and availability of information, data, information resources, or operational procedures. This is the essence of risk management.

To frame this problem in risk management terms, the manager fears negative events, which are composed of the matching of a threat, a specific vulnerability, the impact of that vulnerability being exploited, and the probability that that event would actually occur. The manager has a choice of controls which can protect, detect, or react to the negative event. Of course, each of these controls involves a cost "in terms of executive and employee time, supporting technology, and financial resources," (ISO 17799, 2000) but they are employed through the people, technologies, and procedures we discussed above. To break down the negative events, we can look at each of its parts.

Negative Events

There are four ways to understand negative events based on whether they are successful or not, and whether they are detected by the potential victims or not. This can be illustrated with a table:

Table 3. The Nature of Negative Events

	Unsuccessful	Successful
Detected	1 - Known	2 - Known
Undetected	3 - Unknown	4 – Unknown

Events that are unsuccessful but detected may represent a large proportion of all negative events, but it is impossible to tell what proportion. Organizations can prevent events that are successful but detected (the second category) after they occur the first time. The third and fourth categories are unknowns, which is one of the reasons that an organization's security is difficult to measure. The undetected and unknown category is less serious because it causes no damage, but the events that are undetected and unknown can be very scary.

An example of the fourth category events were the Allied powers intercepting German Enigma traffic during World War II. It was a great situation for the Allied Forces, as the attackers, but not so great for Germany as the victims. Since the attack went undetected, the Allied forces were able to intercept German communications for a long period of time. In this same way, an undetected negative event can affect an organization's information systems for days, months, or years without the organization knowing about it.

Hamilton (1998) mentions how the U.S. Senate recommended vulnerability assessment for safeguarding information security across the country. They outlined a risk assessment process which had five variables if interest:

- What to protect, how much it's worth, and how much depends on it?
- What could potentially threaten an asset?
- What weaknesses exist?
- If a malicious event occurs, what kind of loss could the company have?
- What controls can be put into place to reduce loss or eliminate threat?

We will discuss each of these variables in the context of our discussion of risk and what constitutes a negative event.

Vulnerability

According to the Committee on National Security Systems, vulnerability is "a weakness in an (information system), system security procedures, internal controls, or implementation that could be exploited" (Committee on National Security Systems, 2005). Vulnerability is an important component of a negative event, because it takes vulnerability in order for a negative event to happen.

Organizations have many different types of vulnerabilities. An organization could be vulnerable to fire or flood, vulnerable to viruses, or

vulnerable to insiders misusing their user privileges and exploiting trust relationships between computers in a network.

The most commonly understood type of vulnerability is the software vulnerability that allows viruses and intruders to either take control of a computer system or to disrupt, deny, or degrade its capability. Many times, these vulnerabilities are exploited from the very process of patching them. Typically, someone detects a security flaw that can be exploited in a piece of software. The company that maintains the software releases a patch which closes the vulnerability, but hackers reverse engineer that patch to discover the security flaw that caused the patch in the first place. After they reverse-engineer the patch, they can target systems that are still vulnerable. The difference in time between when a patch is released and when a vulnerability is closed is called "patch latency."

Once a patch or vulnerability is released, the number of attempts to exploit those vulnerabilities grows exponentially (Qualys Inc., 2006). So the longer an organization waits after a technical vulnerability is discovered, the higher the probability that their systems will be exploited.

Sometimes a virus is written and released to target a specific vulnerability which has been known about for months. Any systems that are not patched have

a high risk of being compromised. Unfortunately, the exploiters' reverse-engineering loop is getting smaller faster than the repair and recovery loop of organizations, meaning it will continue to be more and more difficult to defend against this type of attack (Qualys Inc., 2006).

Many times, executive management assumes that their security vulnerabilities will be fixed just because they ask. Also many times system administrators don't know how to secure the systems properly. Some argue that it takes a combination of upgrades, updated systems, effective patch management, and knowledgeable staff to secure a network (McCarthy, 2003).

Meyer (2001) says the problem is exacerbated by the fact that the security community focuses on patching vulnerable software instead of making sure that the software that the organization uses is secure to start with. This problem is more economic than technical though, as Alderson and Soo Hoo (2005) point out.

Vulnerabilities can exist in services like Amazon.com, applications such as e-mail and word processing software, service-level protocols such as HTTP and SMTP, networking protocols such as TCP or IP, operating systems, physical hardware, or basic infrastructure like electricity (Perry, Casado, Coleman, and Wendlandt, 2004). Many organizations feel that they just need to concentrate on

getting the operational mission done, and that they don't have time for security (Erwin, 2002).

Field (2000) mentions a survey at a conference of chief information officers where 59 percent of the executives (CIOs) responded that their information systems had never been hacked into. Field claims that they had been hacked into, but that the executives just didn't know it.

Threat

The Committee for National Security Systems (2005) defines a threat as "any circumstance or event with the potential to adversely impact an (information system) through unauthorized access, destruction, disclosure, modification of data, and/or denial of service." This is similar to our understanding of a negative event, but it is important to understand the fact that a threat is aimed at a specific vulnerability.

There are many threats to organizations' information security. According to the U.K.'s Department of Trade and Industry's Information Security Breaches survey (2002), 78 percent of UK business suffered a malicious security incident in 2002. 42 percent of those businesses experienced virus infections from e-mail attachments, and twenty percent of businesses got viruses from employees downloading files from the web.

In another more recent survey, 39 percent of respondents said their systems have been compromised somehow in the last year (Deloitte Touche Tohmatsu, 2005). The Computer Emergency Response Team (CERT) lists several reasons for the difficulty in protecting information systems in Table 4.

Table 4. Reasons for Difficulty in Protecting Information Systems

Intruders are prepared and organized, internet attacks are easy, low risk, and hard to trace
The complexity of the Internet, protocols, and applications are all increasing along with our reliance on them
Source code is not required to find vulnerabilities
Intruder tools are increasingly sophisticated, easy to use, especially by novice intruders and designed to support large-scale attacks
System and network administrators not prepared due to: • Insufficient resources • Lack of training
Critical infrastructures increasingly rely upon the Internet for operations
Intruders are leveraging the availability of broadband connections: • Vulnerable home users computers • Collections of compromised home computers are good weapons

(CERT Coordination Center,Carnegie Mellon University, 2003)

LaRocca and LaRocca (2002) say that information security concerns itself with four main types of threats:

- Viruses
- Outside intrusions
- Damage from insiders
- Equipment theft

Another type besides equipment theft is the theft of information. Winkler (1996) mentions several illegal methods to steal information: using an insider or mole, digging through trash, surveilling the organization, and by using technical methods.

Although there has been a decline in the number of successful system break-ins, San Francisco's Computer Security Institute says threats from insider and outsiders are roughly equal (CSI/FBI, 2005). The computer security industry's focus on external threats may be because of intrusion detection technologies, since intrusion attempts by external agents are readily accessible to be counted and measured.

Managers may just be naive though. For instance, Wilson (2004) found that there is generally a discrepancy between what risk managers think about employee dishonesty in general, and to what degree they believe employee

dishonesty exists in their organization. Also in the 2005 CSI/FBI Survey, most respondents said that they were more concerned about external threats than internal ones.

Impact

The impact of an event is the cost or loss that the victim will incur after the event happens. Different types of threats have different potential impacts, and in many cases it is specific to the context of the organization that is the victim of a threat. Of all the threats though, the Computer Security Institute's 2004 survey says that viruses cost the respondents to their survey the most in terms of repairing damage. A separate study found that virus infection was the largest cause of security-related damage, even though 83 percent of respondents used anti-virus software in their organization (PriceWaterhouseCooper, 2004).

The 2005 CSI/FBI survey reported that viruses, unauthorized access, and the loss of proprietary info are the first, second, and third most costly negative events, but it reported those events have declined sharply in cost from the previous year. The survey indicated that 95 percent of respondents experienced more than 10 web site incidents, which cause two types of loss: the perception of risk and loss from unavailability of systems (CSI/FBI, 2004).

Although the risk of lost business is great, the CERT Coordination Center identified the following as additional possible impacts from a negative security event:

- Denial-of-service
- Unauthorized use or misuse of computing systems
- Loss, alteration, or compromise of data or software
- Monetary or financial loss
- Loss or endangerment of human life
- Loss of trust in computer/network system
- Loss of public confidence (CERT Coordination Center, Carnegie Mellon University, 2003)

For many companies, all security breaches may not have the same impact. Campbell, Gordon, Loeb, and Zhou (2003) found that although there is evidence to support companies' stock prices dropping after their security was breached, there is stronger support for the hypothesis that stock prices drop more due to breaches where private customer information is disclosed. They categorize the types of losses as:

- Lost business
- Detecting and correcting
- Potential legal liability

Raul (2001) tells us that even though companies can protect themselves from some measure of legal liability when they take due care in securing their systems, it's still a big guess as to whether the company is secure or not. As of his article, the company could still be held legally liable if a hacker or a computer glitch releases personal, proprietary, or customer information.

Determining the cost of the impact requires some way to valuate the things that are compromised. As we discussed, in an information security attack, many times information is what is compromised. Poore (2000) gives us some ways to put a value to information assets for the purpose of information security risk management. He says that value is generally determined by one or more of the following:

- Market forces
- Official value established by an authority
- Expert opinion/appraisal
- Contract
- Cost of creation or re-creation (replacement cost) (Poore, 2000)

These are hardly discrete categories though. An information asset may have different values for each of these areas making the total value of

information more difficult to assess. Poore (2000) says the following may also be factors:

- Exclusive possession
- Utility
- Cost of creation/re-creation
- Ability to interchange in trade
- Operational impact

Hamilton (1998) says information has a value which can be expressed in many different ways, such as by:

- Confidentiality requirements
- Expectations of availability
- Requirements for integrity of information

Besides the value for information, there is also a value or a cost associated with the consequences if something were to go wrong. These can exist on a small scale or on a national scale. A white paper from Cisco Systems, Inc. (2001) describes some of the economic consequences or impacts on a national scale related to network security. The paper discusses immediate impact, short-term, and long-term impacts. They point out that different types of negative security events have different impacts:

> The theft of national security information from a government agency or the interruption of electrical power to a major metropolitan area would have greater consequences for national security, public safety, and the economy than the defacement of a website. But even the less serious categories have real consequences and, ultimately, can undermine public confidence in web-based commerce and violate privacy or property rights. (Cisco Systems Inc., 2001)

Controls

An organization responds to or defends against negative information security events by employing controls. Controls are safeguards that are intended to protect the information and information systems of an organization. The National Institute of Standards and Technology (NIST) lists three different types of controls on information systems: management controls, operational controls, and technical controls (NIST 800-53, 2005).

Management controls are those aspects of security that can be managed with policy. An example of a management control is a policy requiring all users of an information system to have an account and be registered with the system administrator. Operational controls are those aspects that can be managed with good practices, such as not writing down passwords or using weak passwords. Technical controls are those controls which can be managed with hardware and

software, such as patch management software, virus scanning software, intrusion detection systems, or an access control system.

Though managers can apply controls to information security risks, many managers do not know what types of controls exist (Straub, 1993). Even if they do, they may be guilty of paying little attention to the mechanisms that must be put in place to fix them (McCarthy, 2003). Even in the public sector, "governmental agencies currently have wide latitude in determining which security controls to implement and measure" (Bentley, 2005).

Straub (1993) writes further about security controls, saying that controls can be put in place for deterrence, prevention, detection, and recovery. He describes deterrence as a form of active and visible policing. Deterrence can take the form of policies and guidelines which must be adhered to by company mandate.

Prevention is the next line of defense after deterrence, and prevention includes such controls as passwords and locked doors (Straub, 1993). In other words, prevention simply keeps good people good.

Detection is the next level of controls which is put into place after something negative has already happened. Detection consists of investigative work and the use of system logs to find and fix problems, but most importantly,

to discover and punish offenses. Recovery is the final control level, and it involves cleaning up the mess and restoring things as close as possible to their initial state (Straub, 1993).

Even with all these different controls available, Straub (1993) says controls should be targeted at a specific pairing of threat and vulnerability pair in order to be the most valuable. May (1997) describes the selection of security controls as an iterative process where organizations choose security controls based upon their understanding of which of their existing controls are not working and where the organizations' information systems vulnerabilities are.

Some threat/vulnerability pairs are so common that it is almost unheard of for an organization to not implement appropriate security controls. Some examples are password cracks, hacker intrusions, and virus exploits. Yet still, Field (2000) finds that many companies don't even have the basics like firewall and virus protection covered, and this may be in spite of knowing better.

The Corporate Information Security Working Group (2006) defined the "Fundamental Five" security controls as:

1. Malware protection, including worms and viruses
2. Change management, including patch management
3. Identity and access management, including privilege assignment and authentication

4. Firewalls including workstation, host, sub-network, and perimeter as required
5. Configuration management

In a 1999 international security survey, responding companies had firewalls, but very few had encryption systems to secure confidential or sensitive information (Dinnie, 1999). In 2004, PriceWaterhouseCooper consulting performed a security breaches survey for the Department of Trade and Industry (DTI) in the United Kingdom. In the survey, thirty-three percent of respondents said that "virus infection was the single largest cause of serious security breaches," but only 83 percent of businesses used antivirus software. Also, only 33 percent had intrusion detection systems and only 51 percent of responding transaction system companies encrypted their transactions over the web (Department of Trade and Industry, 2004).

Strangely, the same year CSI and FBI reported that most companies were up to speed, using antivirus software and firewalls as well as conduct security audits (CSI/FBI, 2004). The survey reported that most responding organizations, however, had a patch-and-repair approach to security, attempting to fix security breaches by patching technical vulnerabilities as they are announced.

Even with controls in place users can still defeat them, knowingly or not. For instance, in a study on password security, Zviran and Haga (1999) found that user passwords are often easy to guess, and sometimes written down. These user behaviors defeat the usefulness of having password controls in place. Because of these user behaviors, Straub (1993) maintains that a goal of an information security program should be that it is ready and able to punish the abuser.

Even when controls are selected appropriately, they are difficult to manage:

> Ensuring effective implementation of security policies requires active monitoring through metrics. However, it appears that military and governmental agencies have fallen short in this area. A series of recent reports by the General Accounting Office (GAO) found repeated deficiencies in information security, especially in the area of controls and measures. In fact, the GAO found that many government agencies have not implemented a program for testing the effectiveness of the controls they use. (Bentley, 2005)

Risk Management

Risk management is the process of identifying risks to the organization's information systems and choosing and applying the appropriate controls. Each risk has a probability value whether known or not, and leaders should consider this when making risk management decisions. "Risk measurement involves

complex consideration of threat event frequency, probability of attack, exposure from vulnerabilities (mitigated in part by controls), and magnitude of potential loss" (Interagency Working Group on Cyber Security and Information Assurance, 2006).

One example of risk management in action is the circumstance that many companies find themselves in where they fear that deploying a software patch on their information systems may cause harm to their systems. However, in many cases the probability of implementing a bad software patch may be less than the probability of being the victim of a worm or other virus attack, and the losses will be much greater with the work or virus attack. Risk management is concerned with weighing those risks and the potential for damage in order to make the best decisions possible (Tiwari and Karlapalem, 2004).

Because organizations depend more than ever on their information systems, information security is important to the organization in proportion to its dependence on information technology. The more reliance an organization has on information technology, the more attackers attempt to compromise the confidentiality, integrity, and availability of that organization's information assets (Tiwari and Karlapalem, 2005).

Tiwari and Karlapalem (2005) claim metrics can also be used to make risk management decisions from the attackers' points of view. This means that leaders can analyze the risks that attackers must take in an attempt to increase the cost that a potential attacker must bear for each exploitation step he must take to compromise the organization's information systems. They claim that this can be done with the use of classical risk management techniques, but that one important element is necessary in order to use those techniques: the quantification of risks.

Information assurance is closely related to organizational risk management. This function involves decision-makers making a series of trade-offs which need to be weighed in order to optimally protect resources without spending more than it is worth to do so (Gordon & Loeb, 2002; Soo Hoo, 2000). Those decisions will ultimately affect how an organization is able to meet the goals of information assurance.

NIST (NIST 800-53, 2005) points out that there are costs for information security decisions as well. These are called investment costs and opportunity costs, meaning you pay if you invest in security and you pay if you don't invest in security. For example, sometimes, organizations completely abdicate or outsource their responsibility for making risk management decisions and leave

them to contractors, consultants, or other outside agencies. Jaquith (2006) says that unfortunately many "risk management" companies exploit this and offer organizations risk management *solutions* that don't actually manage or mitigate the risk that these organizations face.

Jaquith (2006) says that these companies help identify the organizations' *technical* vulnerability risks and attempt to patch them. Once they have that set of risks taken care of, then they proclaim that the organization is ready for the next round of risk assessment and evaluation, and they start the cycle over again. Jaquith says that these companies and their software are missing the point and in scorn refers to this cycle as the *Hamster Wheel of Pain*.

Geer et al. (2003) say also that some of the popular approaches to selling organizations security solutions which are based on cryptography or technology measures alone are not sufficient, but that risk management should be done, based on quantifiable factors. They say "the issue is getting a handle on the risk such that it can be priced."

Risks can also be shared between organizations. For instance, Henning (1999) brings up the point that when IT services are outsourced, security can be a major issue for both organizations and their customers. She says the organization is only as secure as its vendors or service providers.

As one way to mitigate this type of risk, Henning (1999) promotes the idea of using security service level agreements to specify and quantify security when it is outsourced. She compares security service level agreements to purchasing insurance, or analogizes insurance and information assurance. She proposes that security service level agreements do not replace electronic assurance measures, but that they ensure process-based measures in an organization are being implemented to control security.

Another type of risk mitigation is cybersecurity insurance. Gordon et al. (2003) explain some of the ways that insurance companies can offer insurance for cyber risks. The authors explain how risks are divided between first party, such as loss to the company, and third party, such as liability to the company for damage caused elsewhere.

A way to mitigate certain types of technical risk is through a strategy like defense-in-depth. Jones (2005) discusses the Department of Defense's defense in depth strategy. Like other authors, he finds that three basic principles to defense in depth are people, technology, and procedures.

For the "people" category, the areas of interest are training, certification, awareness, system security administration, physical security, personal security. For the "technology" category, the areas are defense in depth strategy layers,

security criteria, acquisition, risk assessments, and C&A. For the "procedures" category, the areas of interest are assessments, monitoring and analysis, warning, response, reconstitution (Jones, 2005).

Business Continuity Planning

Many organizations approach information security and risk management in the context of business continuity planning. For these organizations, their goal in this type of exercise is to enable the ability of the organization to carry out their mission. In the 2002 DTI survey 43 percent of respondents said that "most security incidents could have been prevented by better systems configuration and 32 percent said they could have been mitigated by better backup and contingency plans. However in a 2005 survey, only 43 percent of organizations responding characterized themselves as "very confident" that their backups either work or are being stored off-site in accordance with policy" (Deloitte Touche Tohmatsu, 2005).

Top-Down or Bottom-Up

Swanson in NIST SP 800-18 (1998) advises that organizations should have policies to outline how to make security policy. There are many different approaches to policy in the context of information security. Usually these are

laid out in terms of top-down, or bottom-up approaches. In a pure bottom-up approach, the low-level technical abilities and capabilities that the organization has enable a certain type of mission and vision. In a purely top-down approach, the problem is to take high-level policy statements and turn them into low-level technical specifications which will support the strategic vision and mission.

There have been a number of approaches to taking a top-level view to low-level implementations, either iterative, like the Zachman Enterprise Architecture Framework (Zachman, 1987), or integrative. Tsoumas et al. (2004), offer the idea of a "text to knowledge" system that will help transform general high-level policy statements on information security into more concrete specification or a "well-defined policy language."

It seems that neither of these approaches is easy or optimal though. Many approaches may start at the top and bottom and try to find some meeting ground in the middle of the organization and operational hierarchy.

Strategic Alignment

Across strategic information management and enterprise information architecture literature, authors and researchers say it is vital that business or mission goals and information technology goals are aligned (Somogyi and Galliers, 1994).

Somogyi and Galliers, (1994) say that organizations need to align their business needs, what they do with IT, and the triad of human resources, organizational structure, and processes. He advocates using return-on-investment by matching IT investments to their business or organizational value, or using risk assessments in evaluating IT investments.

NIST says that computer security should support mission of organization. It claims that security is a means to an end, it "ought to increase the firm's ability to make a profit" and "help improve service provided to the citizen" (NIST 800-12, 1995).

Executive Buy-in is Critical to Security Policy Success

In any IA or security management program, executive-level buy-in has been shown to be critical to success (Boeckmann, 2003). Often, this must be done from the middle of the organization, by selling the value of information security to the organization.

Foster and Yong-Gon (2004) say there should be a strategic security plan which ties to the strategic plan for the organization. They say it should that type of plan should answer questions about

- The most serious potential outcomes and their impact
- The most common threats

- The costliest aspects of the current security program
- The risks that are happening
- How much security events are costing the organization

Investment in Information Security

A problem most organizations face is how much money to invest in information security. For instance, a PriceWaterhouseCooper survey (DTI, 2002) reported that "the UK appears to be suffering from under-investment in IT security (Department of Trade and Industry, 2002). For instance, "only 27 percent of UK businesses spend more than 1 percent of their IT budget on information security" (Department of Trade and Industry, 2002).

This type of result may be because of the way management views information security. The survey's authors claimed that "security (was) treated as an overhead rather than an investment" (Department of Trade and Industry, 2002). In a separate survey, 63 percent of respondents indicated that their general management perceives spending on IT security in realistic terms, or as a necessary cost of doing business. Twenty-two percent said it was a discretionary expense, and 13 percent saw it as an investment in enabling infrastructure (Deloitte Touche Tohmatsu, 2003).

In many surveys, respondents indicate their organization's IT security budgets are a very small percentage of the total IT budget (CSI/FBI, 2004; CSI/FBI, 2005; Deloitte Touche Tohmatsu, 2003).

Costs and Benefits

NIST (NIST 800-12) points out that "by investing in security measures, an organization can reduce the frequency and severity of computer security-related losses, but cautions that computer security should be cost-effective. NIST says that "costs and benefits of security should be carefully examined in both monetary and non-monetary terms to ensure that the cost of controls does not exceed expected benefits." Stated another way, "solutions to security problems should not be chosen if they cost more, directly or indirectly, than simply tolerating the problem" (NIST 800-12, 1995).

The people, technologies, infrastructure, policies, and processes that support an organization's information assurance all have a cost, as does the certification and accreditation process prescribed by NIST and mandated by the DOD (Takewell, 2005).

The reality is that implementing controls cost money, and that is where the risk comes in with implementations. Gordon et al. (2002) present an economic model concerning how managers should spend IT security dollars.

The authors state that the most value could be gained by protecting information assets that only have a medium level of vulnerability: highly vulnerable assets are not worth the protection, nor are nearly invulnerable assets. They also say that an organization should only spend a small fraction of what their expected loss is on security controls (Gordon & Loeb, 2002).

In many contemporary journal articles and trade publications, the stated purpose of developing metrics is to develop proven return on investment. The purpose of a return on investment is to optimize investments in order to get a "good deal" for your security spending. Return on security investment can tie the expense of the systems, programs, policies, and personnel to achieving the goals of information assurance and to the awareness, integration, and alignment of the organization. Chan (1993) suggests, in relation to information systems alignment, that this financial tie is "critical to organizational effectiveness."

Payne (2001) says that metrics are important because security is forefront in the minds of leaders, and thus return on investment is important because it helps ensure an organization is getting its worth from the spending.

What are Metrics?

In the National Science and Technology Council's 2006 report, the council states that metrics are "tools designed to facilitate decision making and improve

performance and accountability, such as through the collection, analysis, and reporting of performance data" which are "diversified, multidimensional data collected in real time and analyzed."

The Corporate Information Security Working Group (2006) says that "metrics report how well policies, processes, and controls are functioning, and whether or not desired performance outcomes are being achieved."

One of the areas in which management compliance is required is Information Technology (IT). Specifically, a company must show that it is providing due diligence to secure its information and information systems, and it must stand up to an external audit (The National Science and Technology Council, 2006). The Corporate Information Security Working Group (2006) points out the requirements for compliance:

> U.S. federal government agencies must demonstrate compliance with the Federal Information Security Management Act of 2002 (FISMA). Private sector organizations are subject to the information security implications of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Gramm-Leach-Bliley Act of 1999 (GLB), and the Sarbanes-Oxley Act of 2002 (SOX).

In the health care industry, laws also dictate the protection of confidential patient information which is maintained on information systems. The Health Insurance Portability and Accountability Act of 1996 (HIPPA) set legal standards

for data security in health care transactions and concerning patient information (The National Science and Technology Council, 2006).

Organizations that deal with these types of organizations must also show that they have an adequate level of security over their information and information systems. These requirements have led organizations to seek for easier and more audit-friendly security metrics that can provide quantitative information about how healthy its information security program is.

Besides mandatory reporting requirements, effective management of any program requires performance measures to keep the program on track. Information security is no different. Program management which lacks metrics to guide it is based on intuition, guesses, and "gut-feel." These are, no doubt, important tools for managers, but programs that are consistently managed with no regard to performance measurement will lack the efficiency and effectiveness that better-controlled programs will have. These types of inefficiencies can manifest themselves in the form of unrealistic budget estimates or incorrect schedules or milestones. At any rate, it makes for very poor and inefficient management.

Unfortunately, the FBI and Computer Security Institute found up to 25 percent of their respondents were from organizations that manage information

security this way (CSI/FBI, 2005). A majority of organizations do not use performance measures to manage information security, so their security level and the effectiveness of their controls are usually optimistic guesses (CSI/FBI, 2005). This means that managers are making and accepting risks based on a high degree of uncertainty.

Because of this need for good performance measures for information security (or security metrics), this research is aimed at exploring how organizations implement security metrics. Research in security metrics offers promise for helping managers determine return on investment for information security, provide evidence of due diligence with respect to legal requirements, help managers make risk management decisions and focus their attention to more effectively and efficiently secure their organizations' information and information systems.

The National Science and Technology Council's (NSTC) Federal Plan for Cybersecurity and Information Assurance Research and Development of 2006 (2006) recommended that federal agencies make developing information assurance metrics one of their priorities. The working group determined that the development of security metrics is necessary because of the requirement for IT security reporting mandated by laws and regulations like the Information

Technology Management Reform Act (ITMRA), Government Paperwork Elimination Act (GPRA), Federal Information Security Management Act (FISMA), and the Healthcare Insurance Portability and Accountability Act (The National Science and Technology Council, 2006).

The council also determined that security metrics development is a key requirement to securing our nation's critical process control systems (PCS) and supervisory control and data acquisition (SCADA) systems and because of the "'national and homeland security implications of IT infrastructure vulnerabilities" (The National Science and Technology Council, 2006).

Closely related with the securing of PCS and SCADA systems, the United States' General Accounting Office (GAO) gave a report on the use of cybersecurity for critical infrastructure protection. The nation's critical infrastructure includes those systems that would, if compromised, cause destruction or loss on the regional or national scale, such as PCS and SCADA systems, as well as the transportation, economic, power, and other systems that the United States depends on (U.S. General Accounting Office, 2004).

In the report, the GAO cautions that since it is "impossible to protect computer systems from all attacks," an organization must rely on selecting the proper controls to protect against the attacks that are most likely to occur and to

cause the most damage. It advises organizations to identify these controls "through a risk management process" (U.S. General Accounting Office, 2004). The GAO says this risk management process "must support three integral concepts of a holistic security program":

- Protection: guarding against known or unknown threats and remedying vulnerabilities to those threats
- Detection: searching out new threats with the goal of discovering them as soon as they appear or before they are realized and cause damage
- Reaction: once a malicious event occurs, repairing and cleaning up the damage and preventing the problem from spreading (U.S. General Accounting Office, 2004)

Figure 1. Protection, Detection, and Reaction are Components of Cybersecurity (U.S. General Accounting Office, 2004)

A majority of the United States' critical infrastructure, much like the Internet, is controlled by non-governmental organizations. In most cases, these organizations are publicly traded companies that provide a service for profit. In 1996, President Clinton established an executive order establishing the President's Commission on the Critical Infrastructure Protection (PCCIP). The PCCIP issued their report in 1998 which identified eight critical infrastructures in the United States: telecommunications, electrical power, gas/oil storage and transport, banking/finance, transportation, water supply, emergency services, and continuity of government (Hamilton, 1998).

The GAO recognizes that it must make good business sense in order for private companies to improve their information security, even if those companies provide the United States' critical infrastructure. In order to discover whether or not a particular security control makes good business sense, the GAO recommends leaders analyze the cost effectiveness and the threat, vulnerability, impact and other risk factors involved with implementing each security control. The GAO admits that though it is possible to determine the costs of information security, it is not as easy to determine its cost effectiveness (U.S. General Accounting Office, 2004).

Alderson and Soo Hoo (2005) paint a darker picture. They expound upon the need for economic incentives in securing information systems. They claim the Internet is not suitable as a critical infrastructure, and further that government security measures have failed to take into account the economics of information security. Further, they argue that the free market will not force products and systems to be more secure and that, like the GAO report expresses, proper security is too expensive for developers to include it for altruistic reasons. They show that since most breaches and exploits have been focused at vulnerabilities that were already widely known, it follows that adequate incentives do not currently exist for companies to provide adequate security for their systems.

The GAO (2004) report determines that this is the case because in many organizations, "decision makers...lack baseline data on the costs, benefits, and effects of security controls from an economic and technical perspective." The GAO maintains that this problem exists because "good and consistent security metrics are not available".

What does it mean to have a "good and consistent security metric" though? First, we must understand the purpose of security metrics. The National Science and Technology Council (2006) offers some insight in that

regard. The council mentions in its report that metrics are important "to improve (an) organization's security accountability." It says that security metrics can also help organizations find problems with the way they have implemented their "operational, technical or management controls," or circumstances in which they have failed to implement the proper controls at all (The National Science and Technology Council, 2006).

The Air Force Systems Command's *Metrics Handbook* (1991) says that "metrics are nothing more than meaningful measures." It also says they must be "actionable (and)...support…organizational goals and objectives." But to draw a distinction between measurement and metrics, it says "measurement does not necessarily result in process improvement...good metrics always will." Payne (2001) differentiates measurements from metrics. She says that measurements are done at one point in time, whereas metrics show trends.

NIST describes three types of security metrics:

- Implementation metrics
- Effectiveness/efficiency metrics
- Impact metrics "to measure business or mission impact of security events" (Swanson, 2003).

Furthermore, a roundtable discussion at the Mini-Metricon security metrics conference revealed the following purposes for collecting information security metrics:

- Steering business decisions
- Creating direction
- Cost reduction
- Measuring against a plan
- Comparing to self (over time to show progress)
- Comparing against industry/peers to show relative position (Marty, 2007)

Characteristics of Good Metrics

In *Winning with Quality* (1994), John Wesner introduces the concept that metrics should be S.M.A.R.T.: Specific, measurable, actionable, relevant, and timely. NIST says that "data supporting metrics must be readily available," "only repeatable processes should be considered for measurement," and "metrics must be useful for tracking performance and directing resources" (Swanson, 2003).

NIST provides many guidelines for managing an information security metrics program. "Metrics must yield quantifiable data, data supporting metrics must be readily available, only repeatable processes should be considered for measurement, and metrics must me useful for tracking performance and directing resources" (Swanson, 2003).

Bob Blakley (2002) states that it is impossible to manage information security investments without being able to quantify them. But he claims it is impossible to quantify them without knowing more information about losses, projections, and information to make statistical statements from.

Antanitus (2003) says that the purpose of metrics is to improve performance. "A good metric is measurable." He provides an example of a naval organization which "saw error rates drop by as much as 50 percent" after using metrics to find the weak areas in a process. He also claims that "the metrics you develop and track need to be part of your everyday job."

Metrics need to be comprised of "quantifiable, observable, and measurable data to apply corrective actions and improve performance" (NSTC, 2006). Also, when metrics are visible, they "provide a positive influence on human behavior by invoking the desire to succeed and compare favorably with one's peers" (Interagency Working Group on Cyber Security and Information Assurance, 2006).

In contrast, Campbell and Gutterman (1993) found that many of the metrics in use in organizations across the U.S. Air Force in the early 1990's were not focused on improving processes. This was unsettling, because that was the goal of the Air Force's metrics programs in the first place.

A security metrics mailing list described the following characteristics of good metrics from a recent mini-conference:

- Metrics must have a purpose.
- Must fit within the decision making process – enhance decision making process.
- Simple to collect – not costly to obtain
- Repeatable
- Demonstrated relationship to other metrics
- Qualitative metrics are acceptable
- Independently verifiable
- Metrics should be transparent (not black box)
- Consensus of how the metrics will be gathered (will hot backup count?)
- A metric should have coverage (lamp post effect)
- Must answer a question
- How do you mediate conflicting metrics
- Different metrics for different people
- Metrics should be hierarchical
- Metrics can lead to discovery and discovery can lead to metrics
- Prescriptive versus descriptive
- The Metric should be actionable (Kadrich, 2007)

Also from the same mailing list, Kadrich (2007) brought up an audience participation survey from the RSA conference with computer security officers and information systems security officers in attendance: "An interesting statistic from the group was that 20% thought that they had mature metrics programs

while the rest was split between emerging metrics programs and no metrics program."

How to Generate Metrics

Metrics generation in security is difficult because luck plays a role. "Asset value, threat, and vulnerability are critical elements of overall risk and are (or should be) weighted in most decisions having to do with security" (Payne, 2001).

Payne (2001) claims that a top-down, strategy-based method or bottom-up, measurement-based approach can be used in the absence of a clearly defined framework. The top-down approach is better at finding what the organization's true metrics should be, and the bottom-up approach is better at producing quickly obtainable metrics. Either way, the organization needs to know what it wants to measure, why, and how it relates to the organization's mission (Payne, 2001).

Hong et al. (2003) caution that "a top-down approach may not be consistent with reality." They also claimed that context is important in implementing an information security metrics program because it is difficult to adapt "structured methods…to highly dynamic environments."

The Corporate Information Security Working Group (2005) defined a large group of metrics that it claims are ready-made for either large or small organizations. They explain that metrics can be generated and used as follows:

> A carefully chosen set of information security metrics for management reports of information security status to the board will clarify to management what the board members consider important and on which they wish to be kept informed. Board members can choose their information security metrics from those defined above and/or create others they consider appropriate for the organization. For large enterprises, it is assumed the metrics will be calculated by various units of the organization and aggregated at various levels up to the entire enterprise.

Geer (2003) argues that each organization has a responsibility to share their data about information security lapses, problems, and breaches. He also says that the data has been collected, but organizations have not used it properly in order to develop a statistically significant baseline of data to make informed security decisions off of.

Bryant and Grimaila (2007) describe three approaches for developing metrics:

- Using automated analysis, such as an executive information system (EIS) or business analysis portal (BAP);
- Have staff mine available data to see if it can provide insight into the problem or;
- Making a data call for a subordinate organization to answer

Metrics from Already Established Disciplines

Dan Geer (2004) argues that organizations should strive to adopt metrics from already established disciplines, such as physics, medicine, public health, and economics. For instance, the Center for Disease Control maintains metrics on how bad a disease is based upon how quickly it spreads, what kind of immunity builds up, what the chance of infection is, etc. Geer describes most worms as a "perfectly pessimistic disease."

Geer (2004) contends that vulnerabilities are directly related to the amount of complexity in the coding, which has increased exponentially. Geer claims patch latency and vulnerability exploitation can be modeled after the concept of half-life in chemistry. His example is that if a patch has a shorter half life and a longer time to exploit it has a lower risk, but if a patch has a greater latency and a shorter time to exploit, the system may be at a much greater risk. Geer describes latency in different forms, interarrival rates, intrusion tolerance, comparands, cost effectiveness, and the scope of data measurement.

Geer (2004) argues that information security should have models like portfolio management, quality assurance, public health, and accelerated failure testing, such as stress testing a toaster to see how much it can handle. He claims organizations should learn how to hedge their security investments from the

field of portfolio management, how to insert quality from the beginning from quality assurance, how to treat and prevent mass infections from public health, and how to discern what the "level-of-effort" is to attack a system instead of whether or not they can.

In military aircraft maintenance, metrics are at the forefront of leaders' daily activities. Leaders watch leading indicators which tell of a problem that will soon take place, and lagging indicators, which tell of a problem that is already happening, or has already happened. These types of indicators help maintenance leaders make decisions as far as what resources to allocate to which aircraft, and which organizations are performing their maintenance duties better than others.

Aircraft maintenance metrics gives commanders an ability to see the health and status of the different aircraft, and they can also judge the health and status of their maintenance workforce (Rainey, et al, 2001).

Return on Investment

Return on investment is a very important concept related to metrics, but sometimes very difficult to assess. With regard to general IT investments, Willcocks (1999) remarked that:

> Organizations have found it increasingly difficult to justify the costs surrounding the purchase, development and use of IT. The value of IT/IS investments are more often justified by faith alone, or perhaps what adds up to the same thing, by understating costs and using mainly notional figures for benefit realization.

Soo Hoo (2000) in his thesis said there have been three major phases in the life of return on investment (ROI) measures. He claims the first generation approaches were estimates of annual loss expectancy (ALE), but they lacked sufficient data to be useful, and used decision trees which were cumbersome, and very difficult to implement for risk management. The second generation consisted of an approach to use a valuation type of ROI, which ignored unknowns completely. It tended to err on the side of safety though. The final generation was the best practices approach, which works, and has the primary goal of preventing corporations from having liability for computer security incidents, so long as they are following the current best practices (Soo Hoo, 2000).

Soo Hoo claims the first stage was brought about in 1979, with the advent of the Federal Information Processing Standard (FIPS) 65, which enabled risk managers to calculate annual loss expectancy (ALE). ALE was an attempt to put a quantitative value on a set of unknown variables:

> The metric's appeal rests in its combination of both risk components into a single number. Unfortunately, this blending of quantities has the disadvantage of being unable to distinguish between high-frequency, low-impact events and low-frequency, high-impact events. In many situations, the former may be tolerable while the latter may be catastrophic (Soo Hoo, 2000).

Chan (2000) claims that "because systems are dynamic, an assessment of IT value that relies heavily on a few key numbers at a single point in time will be incomplete and misleading."

Annual Loss Expectancy suffered from other problems as well. Scott Berinato from CSO magazine online says, "in Annual Loss Expectancy (ALE), the L and the E are a joke" (Berinato, 2005). Soo Hoo (2000) also points out that the first-generation "event tree" models were too "deterministic," using "single-point estimates rather than . . . probabilistically weighted or parameterized ranges of values." He argues that those measures are too simplistic to capture what was really going.

Soo Hoo (2000) explains that the second generation computer security risk models were the "integrated business risk-management framework," which approached computer security risk like any other business risk and suggested that it should be managed like any other strategic level risk. He offers that these "valuation-driven methodologies" were easier to implement than the complex

ALE trees, but they were not very precise. These types of measures "could result in either over-securing assets or under-securing them."

Soo Hoo (2000) explained that third-generation models eschewed risk management altogether and adopted "best practices" which promised to protect companies from any liability due to security negligence as long as they followed them. He offers a fourth-generation model which allows analysts to assign quantitative costs and Bayesian probability estimates to various variables, which has the benefits of "flexibly allowing for varying levels of modeling detail (and) placing the modeling focus squarely on the management decision."

Berinato (2002) suggests that using return on investment (ROI) is the key to selling a security budget, however, May (1997) however, says that classical return on investment needs to be replaced by spending behaviors that consider calendar, infrastructural, temporal, security, knowledge, accountability, and connectivity issues.

Berinato (2002) discusses modified ROI (mROI) which adds a risk factor into the standard return on investment equation. He also discusses that a lot of factors are not captured with that kind of ROI though, like soft returns, such as brand image, etc.

In many operations, the information systems department must justify spending in numerous ways and to numerous players with different agendas in order to get their upper management levels to allocate resources toward improving information assurance (Hall, 2001). For years, information security professionals found themselves selling their practice based on principles of fear, uncertainty, and doubt, but any attempts at hard numbers were either guesses or complete fabrications (Cavusoglu, Mishra, & Raghunathan, 2004).

Thornton May (1997) says there are three organization types in the commercial world: (1) those that view underperforming IT investments as problems that can and must be solved, (2) those that view them as just a condition of our complex world, and (3) those that are in denial that IT moneys aren't being spent wisely.

May (1997) suggests also measuring returns on time investments, because "projects fail not because of technology glitches, but because key people did not have time to devote to them." He claims that ignorance in matters of information security "has an enormous cost multiplier -- it will slow you down, it will hamper your ability to connect, collaborate and exchange information with value-creating entities both internal and external to the organization."

NIST says that information security measures should be cost effective in monetary and non-monetary terms. In other words, the solutions should not cost more than the cost of tolerating the problem it is intended to fix (NIST 800-12, 1995).

In the U.K.'s Department of Trade and Industry (2002) survey mentioned previously, only 30 percent of companies surveyed evaluated return on investment for their information security expenditures. Also, only 65 percent carried out a "detailed risk assessment of IT systems and the threats to them."

The 2004 CSI study found that "most organizations conduct some form of economic evaluation of their security expenditures, with 55 percent using Return on Investment (ROI), 28 percent using Internal Rate of Return (IRR), and 25 percent using Net Present Value (NPV)."

In the 2005 CSI study, 75 percent of respondents reported using ROI, NPV or IRR to quantify security expenditures with 38 percent using ROI, 18 percent using NPV and 19 percent using IRR. Deloitte Touche Tomatsu's Information Security Breaches survey (2003) pointed out a critical absence of key performance indicators for information security functions, and said "the most effective way to cost justify the security function is to assess the value and impact delivered to the business (Deloitte Touche Tohmatsu, 2005).

Willcocks (1999) says that one way to measure return on investment is to relate IT investment to business or organizational value, and another way is to include risk assessment in evaluation procedures for IT investment (or information security investment).

Chan (2000) posits that "in order to fully harvest economic benefits of IT investments, ongoing management processes must be established," and that "IT evaluation approaches are also systems" which "should evolve with the organization, and be adapted to specific information systems under consideration.

Measurement

With the focus on return on investment and ensuring security controls provide value to an organization, it goes along that there should be some sort of measurements with which to evaluate return on investment or value. Measurement is at the heart of metrics.

There are many potential sources of security information. The NSTC (2006) points out that "much information must be gathered, collected, analyzed by hand." It recommends automated approaches to collect, organize, and analyze data for security metrics. The NSTC's report (2006) says, "the reality is that researchers don't yet understand how to quantify, measure, or evaluate

cybersecurity to inform decision making." They further state that "without metrics and tools to automate collection of significant data and streamline its analysis, security effectiveness is speculative at best."

How to Measure.

Leedy and Ormrod (2005) mention several properties that measurement must have in order for the results to be inferentially useful. In academic research, validity and reliability help the researcher prove cause and effect relationships from correlations in order to make a statement of causality. In performance measurement, these constructs are essential to ensuring the continuation of research into the future.

One of the important characteristics of good metrics is reliability (Wesner, 1994). Reliability is ensuring that you can measure something the same way each time. It is paramount to be objective in measurement, especially when those measurements will be correlated and aggregated into a metric which will be used to make decisions.

What to Measure

Construct validity is the term for measuring what you intend to measure. This is property is lacking in many metrics programs. Many programs in the U.S. Air Force during Quality Air Force were doomed to failure because the

personnel managing those programs did not measure precisely what their organization's leadership intended to manage (Campbell and Gutterman, 1993).

When management provides a tangible reward, based on their measurement, the results change according to the reward offered. An example from Kerr (1995) is how promotion systems that reward individual effort do not foster teamwork. This is because what is measured and rewarded is at odds with what managers desire.

A metric measurement can be derived from data or used as information, but many organizations keep metrics long after the usefulness of the metric is gone. It is important not to lose sight of the goal of the metrics. Even with new metrics, there are many things that an organization can measure which provide no valuable information to the organization. However, when an organization measures something, there is a desire to ensure that the measurement looks favorably upon those who are responsible for the metric.

In one particular USAF organization familiar to the author, a slight change in the display of metrics at a staff meeting completely changed the way the leadership of the organization did business because none of the leadership wanted to be seen as falling behind.

Bryant and Grimaila (2007) point out the similarity between organizational metrics collection and statistical research:

> In an organization, each type of data that is required to be collected is analogous to a data point in a research problem. What data is collected really does matter. If two pieces of data are put together, they may show a relationship, but it may be moderated or mediated by another relationship which is unseen to the investigator. In this case any attempts to solve the problem will come up short because the true relationship between the data has not yet been discovered.

Types of Data

The field of research methods defines four different types of variables: nominal, ordinal, interval, and ratio. Nominal data can be categorized as discreet data, or bin-type data, where an item falls into one of several bins. Ordinal data is data which is arranged in a hierarchy, with some items having a greater value than other items.

Interval data is like a temperature scale, which is calibrated to provide a measure of difference between different items, and ratio data is data based on an interval scale that has an absolute zero. Ratio data can be ranked, multiplied, and most easily analyzed. Nominal data provides the least information, while ratio data provides the most (McClave and Benson, 2003; Leedy and Ormrod, 2005).

Variables exist as independent variables and dependent variables. With a relationship between the variables, a change in the independent variable makes a change in the dependent variable. Qualitative measurement is used to measure nominal or ordinal variables, where quantitative measurement is most appropriate for interval and ratio variables.

Data can also be continuous or discrete. Continuous data implies a measurement where discrete data implies a count or enumeration (McClave and Benson, 2003). Statistics can be descriptive, which can tell you about an event, or inferential, which can help predict events (McClave and Benson, 2003).

The data is analyzed and drawn into conclusions based on either deductive or inductive logic. Finally, deductive logic starts with a premise and expands that to different instances, and inductive logic starts with specific instances, then attempts to draw a conclusion, which those instances would support (Leedy and Ormrod, 2005).

Soft Issues

Even though there are many things that can be measured and managed in order to provide an estimate of return on investment, there are some things which defy measurement. These are things that cannot be adequately expressed with a number, and which evade capturing in a discrete format, comparing

against time, or running a regression on. One example of this is what Kahraman (2006) calls an "evaluation of minds." An evaluation of minds is what users or personnel in the organization are thinking or feeling, what their perceptions are, and how they like or don't like something. These type of issues make information security very complicated.

Security Awareness

Munley (2004) says that most companies focus on the technology of security and neglect the holistic approach, including security awareness. He claims that the human factor is the weak link and that organizational culture must be considered and understood.

Kahraman (2006) says that the "biggest problem of the companies are derived not from the technical difficulties but from lack of control over the work flow and the employee behaviors." Hinson (2003) says that a technology-only approach to managing information security is not suitable because technology is fallible and "very few organizations understand their information security problems in sufficient detail to ensure that they specify appropriate technical solutions." Further, Hinson states that for every technology, there are risks associated with the people who use that technology, which comprises the "human element of information security."

Contribution to Program Success or Failure

In 1996, Wilson (1996) reported that many federal computer security programs were born soon after an inspector general's (IG) visit during which an agency is cited for not having a required program. He said that "some agencies begin a computer security program following a major security incident, or just prior to an IG visit, hoping to avoid yet another adverse finding." He says the new project is either thrown under an existing program for nurturing or "thrown to the wolves" on its own, but that it is seen as a knee-jerk reaction, or an unnecessary overhead function, which "does not contribute to other agency functions" and which "should not be taken seriously."

Siponen (2000) says that certain parts of information security programs or campaigns may be met with negative results from end users when user buy-in is not achieved and Hamilton (1998) notes that in conducting surveys about compliance, "there is little point to asking questions unrelated to requirements because the organization would find it difficult to enforce compliance if it was not a requirement."

Communication

McCarthy (2003) states that alignment failures sometimes cripple information security programs. One example from her book gives a description

of how a museum security system lacked proper security controls because the security and IT personnel did not have adequate intra-organizational communications, so they neglected many responsibilities that were shared between them.

Everett (2006) says that managers and information technology professionals need to understand each others' positions to reach a compromise on the security aspects of their systems. Everett says that these groups can do this by analyzing the risks against the liability that comes from having their systems breached. Hall (2001) points out that a failure of management to understanding security issues is a result of a lack of communication.

Decision Making

In ensuring that an organization's information and information systems are protected, managers must make many decisions which take into account the threat, the level of risk, vulnerability, security controls that are in place, costs associated with security and many other factors. But even if the best metrics are available, it is important to realize that not all decision-makers approach risk in the same way. Not all decision-makers are capable of making optimal decisions, especially in high pressure environments.

Kahneman and Tversky (1979) found that people tend to make risk decisions irrationally. They found that people tend to under-weight their expected losses and over-weight their expected gains. For instance, if a person's expected gain is 40 dollars and expected loss is 60 dollars, they will likely consider the chance to win 40 dollars more strongly than the chance they could lose 60 dollars.

Kahneman and Tversky (1979) also found that people under-weight both their expected losses and gains when compared to a outcome that they know is certain. This is like when they have to make a decision to take 40 dollars that they will definitely receive or to choose from the chance to make either no money or 100 dollars, with the ability to repeat the experiment indefinitely. The expected outcome in the second instance is actually higher than the first, but it seems like a less attractive option to many people.

This type of behavior is described by prospect theory, which asserts that people will make suboptimal decisions in order to avoid risk, even when the probability of the risky choice would make it the better choice (Kahneman & Tversky, 1979).

Sitkin and Weingart (1995) say that the way a decision-maker frames the problem affects the outcome of his or her decision. They found that decision-

makers also base their decisions on how they perceived the outcome of previous decisions. They found, however, that an individual's propensity for taking risks and his or her perception of the severity of the risk actually mediate the effects of both problem framing and the history of previous outcomes (Sitkin & Weingart, 1995).

Sitkin and Weingart (1995) found that a decision-maker's decision depended on whether "a situation is presented to a decision maker as an opportunity or a threat. . . or in terms of gains or losses." They found that situations that were set in a positive light were seen as high risk, but negatively-framed situations were seen as lower risk. They also found that those who tend to more often make risky decisions will not perceive as much risk as someone with a more risk-averse nature (Sitkin & Weingart, 1995).

In another study, managers faced with a risk decision about introducing a new product relied on their perceived level of outcome control, along with how they categorized the problem or decision, to help predict what level of risk they are willing to tolerate (Forlani, 2002).

Even if someone has good decision-making abilities, he or she may still make errors because decisions can only be as good as the information upon

which they are based. One problem many decision makers may come into contact with is the challenge of interpreting information correctly.

Ricketts (1990) found that people tend to make decision errors more frequently based on information which is incorrect by powers of 10. In other words, they are less likely to catch an error when it involves a decimal place or a zero than if it involved another kind of numerical error.

Moreno, Kida, and Smith (2002) found that in the financial world, auditors with less experience use more affective information, such as how much they feel a person is "likeable," in order to make risk management decisions than auditors with more experience. The implication seems to be that in the absence of reliable and valid information or knowledge, decision-makers rely on their less-optimal fallback mechanisms in order to make decisions. When decision makers are making risk management decisions about information security with a lack of clear, reliable data, it is very easy to see how there could many sub-optimal information security decisions.

Schroeder (2005) discusses different ways that Designated Approval Authorities in the Air Force approach information security risk management decisions. He uses prospect theory as a way to understand their decisions and finds that they tend to risk more when things are going downhill in an attempt to

"fix" things. He finds that affective context has a great impact, and operations personnel are more risk averse after a negative scenario. Also, non-operators (non-pilots) place more decision weight on background than non-operational personnel (Schroeder, 2005).

Organizational Culture

The context and culture of an organization has a great deal to do with how well metrics work as decision-making tools in an organization. Hobbs (2005) described fifteen major barriers to electronic records management (ERM) in a deployed military environment. Many of these barriers may apply to information assurance programs as well. Among the findings were that organizational guidance, organizational structure, information technology, and organizational culture were major determinants of how effectively electronic records management was implemented at a deployed location (Hobbs, 2005).

Hobbs (2005) also found a lack of policy, standardization, and accountability, inadequate training, organizational guidance, lack or misuse of information technology capabilities, complexity of the systems involved, an insufficient support structure, prohibitive workload, misuse of personnel, high turnover rate, non-reinforcing behaviors, beliefs, and values, minimal collaboration, low prioritization, generation gap, and a high operations and

personnel tempo. These are many of the same issues that plague information security program implementation as we have discussed.

Organizational culture also involves the organizational environment. Earl (1993) discusses five types of organizational environments as he discusses strategic information systems planning:

1. Business-led
2. Method-driven
3. Administrative
4. Technological
5. Organizational

Earl (1993) claims the business-led approach has as its assumption that the current business direction or plans are the only basis upon which information systems plans can be built, therefore business planning should drive the planning processes. The method-driven approach is the approach used in many government organizations, where the planning processed is enhanced by, or depends on use of a formal technique or method. Earl shows that these goals can seem unreal or high-level to users. It's often the "xyz strategy," where xyz is the name of the consultants.

Earl (1993) explains that the administrative approach is found in government bureaucracies. It is bottom-up rather than top-down in its approach,

and takes a financial requirements or budgeting process. Earl's criticism is that this type lacks ideas for radical change and strategic thinking, enterprise-level applications are in the background and business as usual and the status quo were the driving forces.

Earl (1993) says the technological approach is about modeling the processes and the organization. He claims the drawbacks to this approach are that sometimes management is confused and unsure of what the blueprints mean, and that it is difficult to determine the most important thing to focus on.

Finally, Earl (1993) says the organizational approach involves continuous integration between information systems and the organization. In this approach, teamwork is the main driver of strategy making. In his case study, he found that in organizational-approach organizations, occasional project cost and time overruns were acceptable if they allowed evolving ideas to be incorporated and that sometimes new strategies were discovered through implementation. Earl claims the organizational approach is the most effective, efficient, and flexible.

Examples of Security Management Frameworks

There are several information security management frameworks which exist to help organizations manage their information security assets and close vulnerabilities more effectively. Some of these frameworks were derived from

the others, and some can be very useful for helping an organization find all the big security issues that need immediate attention. Many of these offer their own sets of metrics which organizations can pick and choose.

The existence of several frameworks though implies that all are possibly incomplete in their approach to helping managers deal with information security in their organizations. We present several with some of the major points that each provides.

National Institute of Standards and Technology (NIST)

NIST provides several guides to IT management in their 800 series of publications. Two of these are the *Security Self-Assessment Guide for IT Systems* and the *Computer Security Handbook*. Their *Security Self-Assessment Guide for IT Systems* (NIST Special Publication 800-26) is based off the Federal IT Security Assessment Framework presented to and issued by the federal CIO Council. It can help managers and agencies understand the security of their systems and can aid in decision making. It references the control activities found in the U.S. General Accounting Office's Federal Information System Control Audit Manual (FISCAM). It is also the document that inspectors use when auditing a U.S. federal agency's information security program.

NIST maintains that before auditors can assess an information system's security, the organization needs to perform a risk assessment. Also, before an organization starts assessing a system, it needs to identify the boundaries of the system and sensitivity and criticality of information used by that system and that goes into and out of the system.

NIST Special Publication 800-26 divides the self-assessment into management controls, operational controls, and technical controls and provide five levels of achievement for each of these topic areas, like in a capability maturity model: Level 1 involves documenting the objectives; level 2 involves documenting the objectives as procedures; level 3 consists of implementing procedures; level 4 is when procedures and security controls are tested and reviewed; and level 5 is when procedures and security controls are fully integrated into a comprehensive program (NIST 800-26, 2001).

NIST's *Introduction to Computer Security: The NIST Handbook*, (Special Publication 800-12) Chapter 7 goes further into discussing management, operational, and technical controls. It also is a general purpose guide to computer security, covering everything from cryptography to management responsibilities, how to handle sticky user issues when an employee is fired, and how to handle incident investigation.

NIST's *Security Metrics Guide for Information Technology Systems* (NIST Special Publication 800-55) discusses not just the information security program, but the information security metrics program. It states that a metrics program should include:

- Strong upper management support
- Practical security policies and procedures
- Quantifiable performance metrics
- Results-oriented metrics analysis (Swanson, 2003).

NIST's guide also suggests prioritizing metrics based on those that affect security, where the data is readily obtainable, and "measures existing and stable processes" (Swanson, 2003). The guide gives a general model for timing and implementation of metrics collection, and the process that drives it:

- Prepare for data collection
- Collect data an analyze results
- ID corrective actions
- Develop business case
- Obtain resources
- Apply corrective actions (Swanson, 2003)

International Standards Organization (ISO)

The International Standards Organization provided a standard for information security named ISO 17799. It defines the following factors as "critical to the successful implementation of information security within an organization:"

- Information security policy, objectives, and activities that reflect business objectives
- An approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with the organizational culture
- Visible support and commitment from all levels of management
- A good understanding of the information security requirements, risk assessment, and risk management
- Effective marketing of information security all managers, employees, and other parties to achieve awareness
- Distribution of guidance on information security policy and standards to all managers, employees, and other parties
- Provision to fund information security management activities
- Providing appropriate awareness, training, and education
- Establishing an effective information security incident management process
- Implementation of a measurement system that is used to evaluate performance in information security management and feedback suggestions for improvement (ISO/IEC 17799, 2005)

We have talked about each of these issues and concepts in detail from the relevant literature related to information security management, so it serves as a tidy summary of our information security model so far.

ISO/IEC 17799 also discusses risk assessments with regard to information security systems. It says organizations should consider:

- The criticality of the application processes
- The value, sensitivity or criticality of the information involved
- The past experience of system infiltration and misuse
- The extent of system interconnection(IEC, 2000)

GAO's General Framework

In 2004, the General Accounting Office developed a cybersecurity framework which includes:

1. Determining the business requirements for security
2. Performing risk assessments
3. Establishing security policy
4. Implementing a cybersecurity solution that includes people, processes, and technology to mitigate identified security risks; and
5. Continuously monitoring and managing security. (GAO, 2004)

The GAO's model (Figure 1) shows how risk assessments and business requirements feed into the security policy, and then how information security management practices feed back into future risk assessments.

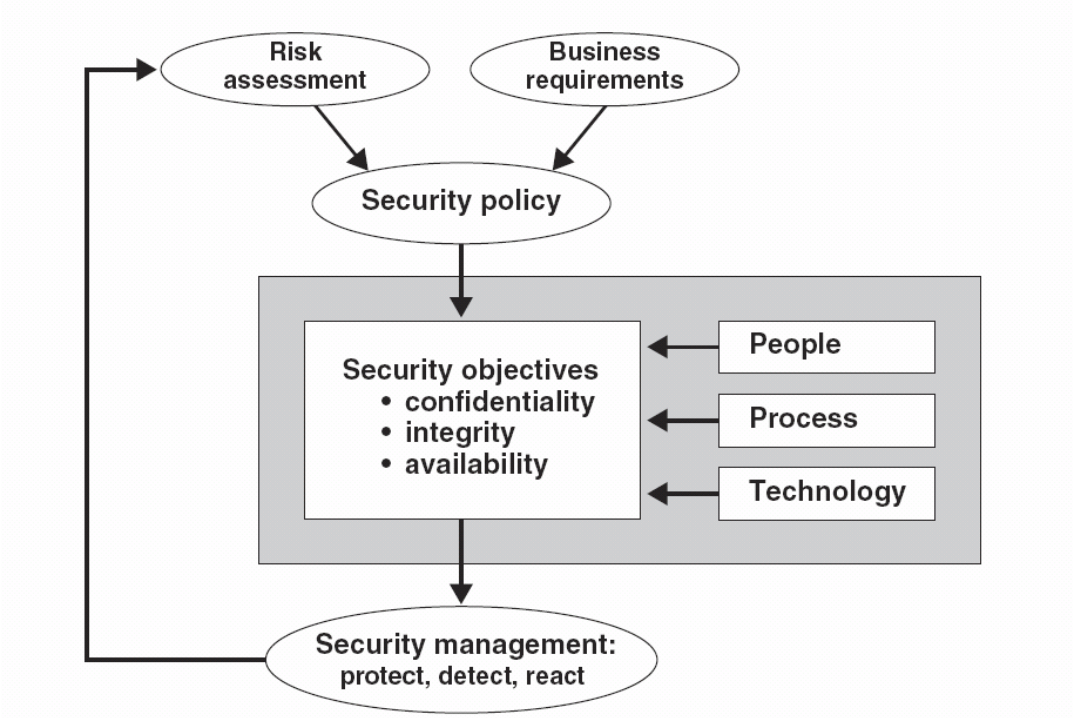


Figure 2. GAO's Overall Framework for Information Security

(U.S. General Accounting Office, 2004)

Cognitive Model

In order to better understand the environment of an organizational information security management program, we develop a first attempt at a cognitive model of how the data collection, organization, analysis, and reporting processes would work. The following model (Figure 1) will help in organizing the data collection in the research. It outlines how strategic, and operational-level organizations make data calls to lower-level organizations, and how the

strategic, operational, and tactical organizations organize and analyze the data, and then report it as information in a more refined form. That information is also used to support management decision-making at each level.

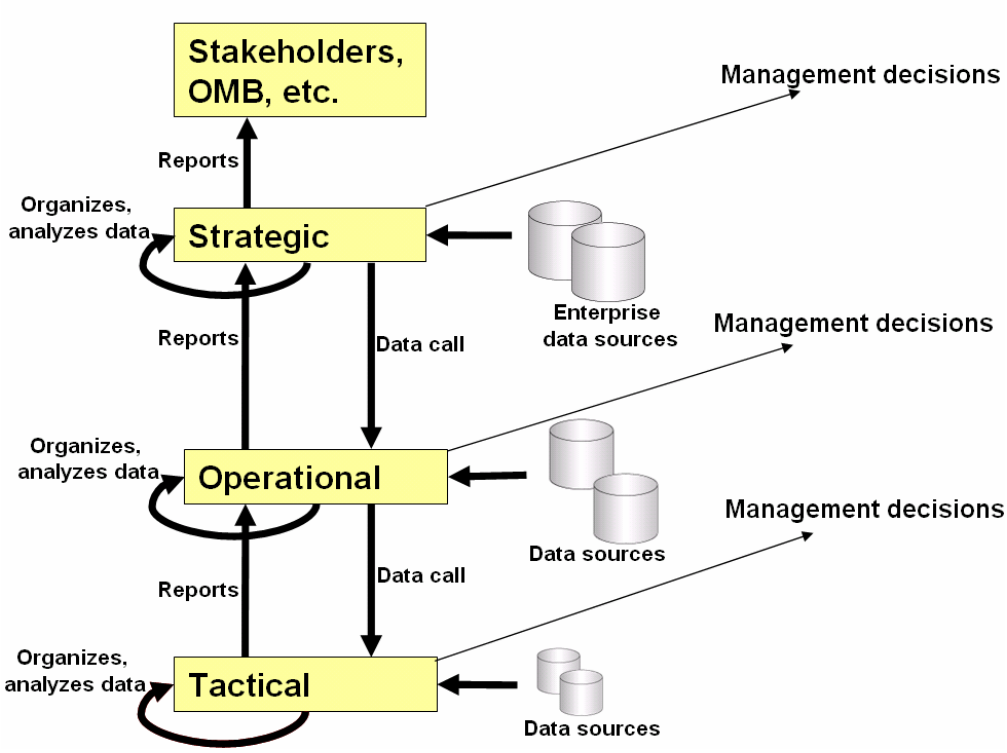


Figure 3. Conceptual Model of the Metrics Collection Process

In summary, we've learned about what general characteristics of security programs, security metrics programs, and metrics should be. A consolidated grouping of characteristics that are desirable is drawn from the literature and listed in Appendix I, II, and III.

These lists of desirable qualities will be taken into account as we impose our methodology to describing the communication and decision processes in some real information security metrics programs.

III. Methodology

This research uses the case study methodology as a method of inquiry. The case study is one of several types of qualitative research methods which is particularly suited to the kinds of goals, problems, and data in this research.

Using a Qualitative Method

In choosing the methodology to guide this inquiry, many different ideas were evaluated. Three main factors which were considered when deciding what type of method of inquiry should be used were the goals of the research, the type of research questions, and the nature of the expected data.

First, the goals of this research lend themselves best toward a qualitative design two major reasons. First, the major goals of this research are to explore an area that is not well established theoretically. The goals of this research are to explore how organizations have implemented their information security metrics programs. This type of understanding is difficult to analyze without considering the context of the organization. Human factors, decision making, intuition, and organizational culture have a lot to do with the way that an information security metrics program is implemented. These areas are part of the context of the organization and cannot be divorced from the actual implementation. As Yin

(2003) states, "a holistic approach is also desired in order to examine the events and processes within the context of the organizations in which they are carried out, and this is best provided with a qualitative approach" (Yin, 2003).

Also, this research seeks to inductively draw inferences or conclusions from a set of correlated events, ideas, or phenomena rather than testing a preconceived hypothesis by deductively applying an experimental research method to a set of data to see if the data supports the hypothesis.

The questions that this research poses are "how" and "why" questions related to the processes and methods of measuring and converting data into information and knowledge to make decisions. As Yin (2003, p. 22) states, these types of questions lend themselves to qualitative analysis more so than any other method. A quantitative analysis would only provide support or non-support for a pre-defined set of hypotheses. "How" or "why" questions can not be adequately answered with a binary answer.

The questions in this research explore various aspects of how information security metrics programs are implemented rather than measuring the effectiveness of such a program. Both Benbasat (1987) and Yin (2003) say that these types of "how" questions lend themselves to qualitative analysis rather than quantitative methods.

The type of data expected will be narrative and a rich understanding of the processes and ideas surrounding information security metrics. It is difficult, if not impossible to capture this type of data with quantitative methods.

The nature of the data expected also lends itself to a qualitative form of measurement (Leedy & Ormrod, 2005). The data expected from this study come in the form of explanations, stories, rationale for decisions, and intuition. The data will also be very context dependent. Each organization will have its own reasons and rationale for implementing their metrics program the way it has, and that kind of data would not be captured with a quantitative approach.

Finally, the questions in this research may open the way for further investigation. Lines of questioning in the interviews and information discovered through analysis of documents may provide insight into questions already asked, and when combined may lead to a richer sort of inferences when the data are combined to inductively develop propositions.

Yin (2003) says the "distinctive need for case studies arises out of the desire to understand complex social phenomena. In brief, the case study method allows investigators to retain the holistic and meaningful characteristics of real-life events--such as individual life cycles, organizational and managerial

processes, neighborhood change, international relations, and the maturation of industries."

Case Study Method

The case study method has been used for years in the areas of social science, and has in the past twenty years been applied to the area of information systems management. Benbasat (1987) says that the case study method is useful for generating "theories from practice."

The case study methodology is also useful for developing a holistic view of a problem or process, particularly if done with a single unit of analysis, which is one of the stated goals for this research (Miles and Huberman, 1994, p.10; Yin, 2003).

Benbasat et al. (1987) found "case research is particularly appropriate for certain types of problems: those in which research and theory are at their early, formative stages, and "sticky, practice-based problems where the experiences of the actors are important and the context of action is critical." Benbasat et al. (1987) say there are three main reasons why case study research is a viable form of inquiry in the domain of information systems:

1. The researcher can study information systems in a natural setting, learn about the state of the art, and generate theories from practice

2. The case method allows the researcher to ask "how" and "why" questions, that is, questions about the nature and complexity of the processes taking place
3. A case approach is an appropriate way to research an area in which few previous studies have been carried out (Benbasat, 1987)

In addition to the reasons why case study research is appropriate, Benbasat et al. (1987) give a definition of what case study research is all about. They say a case study examines:

> a phenomenon in its natural setting, employing multiple methods of data collection to gather information from one or a few entities (people, groups, or organizations). The boundaries of the phenomenon are not clearly evident at the outset of the research and no experimental controls or manipulation is used (Benbasat, 1987)

This description is a fitting description of this research which matches the goals, expectations, and limitations of this research. Since it has been demonstrated that the case study is appropriate for this type of research, it is important to understand what the key characteristics of the case study are. Again, Benbasat et al. (1987) answer, describing the key characteristics of case studies as follows:

Table 5. Benbasat's Key Characteristics of a Case Study

Phenomenon is examined in a natural setting.	The investigator may not specify the set of independent and dependent variables in advance.
Data are collected by multiple means.	The results derived depend heavily on the integrative powers of the investigator.
One or few entities (person, group, or organization) are examined.	Changes in site selection and data collection methods could take place as the investigator develops new hypotheses.
The complexity of the unit is studied intensively.	Case research is useful in the study of "why" and "how" questions because these deal with operational links to be traced over time rather than with frequency or incidence.
Case studies are more suitable for the exploration, classification and hypothesis development stages of the knowledge building process; the investigator should have a receptive attitude towards exploration	The focus is on contemporary events. (Benbasat, 1987)
No experimental controls or manipulation are involved.	

(Benbasat, 1987)

Sources of Evidence

Yin (2003, p. 86) describes six sources of evidence that are appropriate for case study research:

- Documentation
- Archival Records
- Interviews
- Direct Observations
- Participant-Observations
- Physical Artifacts

Due to time and availability restrictions on the researcher, the major form of investigation used in this research are documentation, archival records, and interviews. The following are also used in this research to triangulate the findings in each case: policy memoranda, strategy documents, presentations, charts and spreadsheets, conversations, and e-mails (Yin, 2003).

The case study method is one of the most popular qualitative methods used in research science. This method is appropriate for use whenever a subject of inquiry is to be searched in a very detailed manner, without clear cause-and-effect relationships to guide or test. In exploratory research like this study, there are not well-grounded or proven theories to guide the research.

- The case study is for looking at a problem in depth
- The case study looks at a few data points in depth rather than a cursory look at many data points.
- The case study is important for problems where the interaction between the context and the case plays a significant role

Case Study Design

Yin (2003, p. 20) states that "a research design is the logical sequence that connects the empirical data to a study's initial research questions and, ultimately, to its conclusions." The case study design can be either a single case or multiple case design, and it can either be holistic or embedded. A holistic design uses

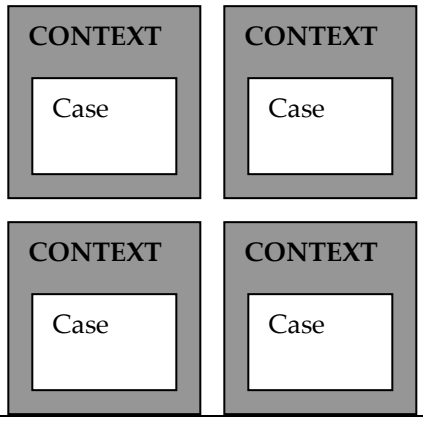
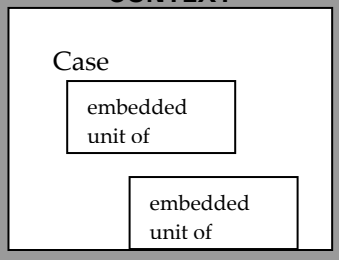
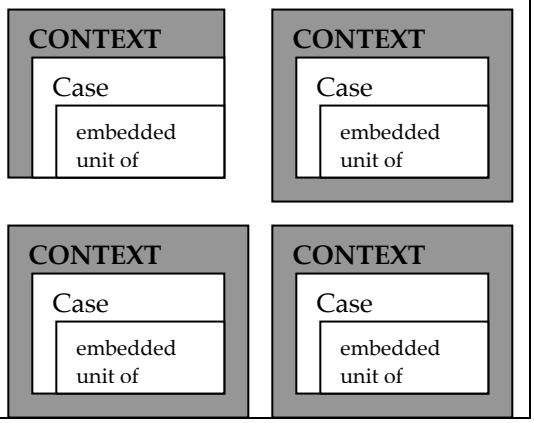
single units of analysis in its approach to cases, where an embedded design uses multiple units of analysis

This research uses a multiple-case design with a holistic approach, using the information security metrics program as the single unit of analysis. This unit of analysis will be investigated across multiple organizations in order to be able to draw inferences from the data. As Yin states, a multiple case design has the benefit of being more capable of providing inference than a single case design (Yin, 2003). Benbasat et al. (1987) say that "multiple-case designs are desirable when the intent of the research is description, theory building, or theory testing." Yin (2003, p. 21) describes five key parts to ensuring a rigorous research design:

1. Determining the study's questions
2. Developing propositions
3. Determining units of analysis
4. Developing logic linking data to propositions
5. Developing and applying criteria for interpreting the findings

This chapter will go on to explain the design of this case study and how each of these components were developed or chosen.

Table 6. Basic Types of Designs for Case Studies

	single-case designs	multiple-case designs
holistic (single unit of analysis)		
embedded (multiple units of analysis)		

(Yin, 2003)

Determining the Study's Questions

As outlined in Chapter 1, the primary questions guiding this research are:

- Q1: How do organizations make decisions and communicate decisions about what and how to measure?
- Q2: How do organizations perform:
    - Data capture or *gathering*
    - Data normalization and transformation or *organizing*

- Data analysis or *refining*
- Data reporting or *disseminating* (Papadopoullos, 2004)

- Q3: How do organizations use the information provided by metrics support information security-related decisions?

These questions are decomposed using the themes introduced in Chapter 2 and developed into a series of questions to be used as a guideline in the interview. The interviews of this case study are designed to be semi-structured. These questions are meant to provide a direction, focus and general flow of the interview; however, other lines of questioning may develop based on interviewee responses. Questions are grouped by process as follows:

Developing Propositions

Yin (Yin, 2003, p. 22) states that propositions point "attention to something that should be examined within the scope of the study." These are in a way pseudo hypothesis which an investigator can gather his or her ideas around in order to approach a case study. However, for exploratory research, propositions are difficult to get at. The purpose of exploratory research is to discover what is not known about a subject, so the idea of developing propositions for

exploratory research would involve making educated but uninformed guesses, which would not contribute to the quality of the research design.

Nevertheless, even in exploratory research, Yin (Yin, 2003, p. 22) continues:

> every exploration…should still have some purpose. Instead of propositions, the design for an exploratory study should state this purpose, as well as the criteria by which an exploration will be judged successful.

The purpose behind this research is to develop a general theory of how organizations make decisions concerning what and how to measure with regard to information security, as well as how those organizations convert data into information and information into knowledge and how that data, information, and/or knowledge is communicated and transported throughout the organization and finally used to support information security decision making.

Determining Units of Analysis

The unit of analysis for this study is the information security program in the organization. Several potential units of analysis were examined in order to determine which would be the best way to approach this type of exploratory research, but most lacked potential in one way or another.

One method examined was to use the security decision-maker as the unit of analysis. This approach suffered from several flaws. First, as we discussed before, the decision-maker has challenges of his or her own with making decisions, mostly based on human nature, personal preference, and habit. Secondly, findings from analyzing security decision-makers would be applicable to other decision-makers, but would lack external generalizability to information security metrics programs as a whole. This approach would also not provide the ability to examine organizational processes or technologies that contribute to an information security metrics program.

A second method was to examine the processes operating within the organization. Intuitively, this approach suffered from many of the same problems as examining the decision-makers. There would be a lack of generalizability to information security metrics programs, because programs also deal with the people that engage in processes and the technologies that support them. Also, a stated organizational process may not be consistently used or enforced in some instances, and many processes interleave and interact with each other. This makes the process a difficult unit of analysis.

While this research does draw data from both processes and decision-makers, it does so through the lens of the metrics program. The metrics program

was chosen because its scope is the entire organization, even if that organization is the subordinate of a larger organization. Also, the program deals with people, processes, and technologies, so each of these areas can be investigated while still examining the metrics program.

Data Collection

Data is collected in this thesis by two primary means: the first is a series of telephone interviews with personnel in the organizations who are intimately familiar with the processes and assumptions in the organization and concerning the information security metrics program. Also, data from this thesis will be drawn from examining documents and information available on websites maintained by the organizations being studied, and by examining documents provided by personnel in each of those organizations.

Developing Logic Linking Data to Propositions

It is important to create a logical tie between what is being studied and what is being proposed. For each type of data he or she collects, a researcher must be prepared to answer the question, "why did you decide to collect that particular data, and how does it relate to the goals of your study?"

Yin (2003) says that although developing the logic linking the data to the propositions is the least well developed component in many case studies, one way to accomplish this is through pattern matching. Patterns will be examined in interview responses, artifacts, documents, and so forth to see what the connection is between those findings and the exploratory goals stated above.

Interview data will uncover anecdotal information about how people make decisions and have made decisions in each organization concerning what and how to measure. Documents, policy memoranda, presentations, and so forth will reveal official intentions, which can be analyzed to inductively reveal what decisions went behind them were. Artifacts of different types can be interpreted in many different ways, but one way is through examining why artifacts exists in the state they are in.

Often, there can be a hypothetical chain which logically links the artifact and its state to a decision which was made previously which resulted in the artifact and its state. Although by themselves, these types of hypothetical chains are not sufficient for explanatory research, they can assist in providing a "chain of evidence" when put together with documents, interviews, and other sources of data.

Interview questions are developed to address directly the areas of data capture, normalization, analysis, reporting, and decision support.

Developing and Applying Criteria for Interpreting the Findings

Yin (2003) suggests using criteria to aid in pattern matching. For this thesis, the following questions are used to aid the research in the process of organizing case study data into categories related to the domain of the thesis' investigation.

- How do these answers relate to the literature?
- How does the decision process relate to the literature?
- How do the communication processes relate to that cognitive model?
- Where are the gaps between the model and the answers to the questions?

The major criteria for interpreting the data and analyzing it in this research is the lists of desired qualities for a strong *security program*, the desired qualities for strong information security *metrics programs*, and desired qualities for the individual *metrics,* as listed at the end of Chapter 2.

Measures to Ensure Rigor in the Case Study

Yin (2003, p. 19) says that in order to provide scientific rigor, case study designs need to take measures to maximize (a) construct validity, (b) internal validity when demonstrating causality, (c) external validity, and (d) reliability.

Yin (2003, p. 34) provides the following table which illustrates how these concepts relate and how the methodological issues are controlled.

Table 7. Case Study Tactics for Four Design Tests

Tests	Case Study Tactic	Phase of research in which tactic occurs
Construct validity	• Use multiple sources of evidence • Establish chain of evidence • Have key informants review draft case study report	data collection data collection composition
Internal validity	• Do pattern-matching • Do explanation-building • Address rival explanations • Use logic models	data analysis data analysis data analysis data analysis
External validity	• Use theory in single-case studies • Use replication logic in multiple-case studies	research design research design
Reliability	• Use case study protocol • Develop case study database	data collection data collection

(Yin, 2003)

Construct Validity

Construct validity is how well a measurement represents the concept, or construct that it is intended to represent. In this study, the cases have been chosen to represent the organizations. The level of analysis in a case study is important to match the level of analysis of the question that you are analyzing. Since this research deals with information security on an organizational level, the cases that are presented are organizations, usually at the headquarters,

command, or department level, dealing with problems that affect the entire organization.

Internal Validity

In research, internal validity "is the extent to which its design and the data it yields allow the researcher to draw accurate conclusions about cause-and-effect and other relationships within the data" (Leedy & Ormrod, 2005, p. 97). In this research, there is no cause and effect relationship being tested, however this study will lead to inferences in cause and effect relationships which may be tested in future research efforts.

The internal validity in a qualitative study is often achieved by the use of triangulating many data sources so that the relationship between data and conclusions is better supported (Leedy and Ormrod, 2005, p. 99; Scandura and Williams, 2000). In this study, the data from each case is triangulated against data from the other case, and within each case, multiple sources of evidence are used in order to draw stronger conclusions from the data collected. These sources of evidence, such as interviews, records, documents, e-mail discussions and perspectives from multiple people in the organization when available and appropriate.

External Validity

External validity is a measure of how well the findings from the case generalize to the real world. Leedy and Ormrod (1999, p. 99) say that "the external validity of a research study is the extend to which its results apply to situations beyond the study itself." This is also understood as the generalizability of a study. In this study, the replication in two different cases from two different contexts are used to improve the study's reliability. Also, the cases take part in a real-life setting which improves the degree to which the findings can be generalized to other organizations (Leedy & Ormrod, 2005, p. 100).

Reliability

Reliability is "the consistency with which a measuring instrument yields a certain result when the entity being measured hasn't changed" (Leedy and Ormrod, 2005, p. 99). In case study research, reliability is the ability for the case study to be repeated and result in the same conclusions. With case study research, this is achieved by documenting the methods and case study design as closely as possible and following a case study protocol.

This chapter has provided an explanation about why qualitative research is appropriate for this study. It also discussed the case study methodology in

general, and then in how it pertains to this study. Finally, methodological issues were discussed and the appropriate measures were described.

IV. Analysis and Results

This study examined three cases to learn more about the information security metrics programs of the organizations involved. As mentioned in Chapter 3, the unit of analysis was the organization's information security or information assurance metrics program. The three programs that were analyzed were from the DOD, the Air Force, and NASA's Jet Propulsion Lab (JPL).

The major differences in the organizations were the sizes of the organizations. The DOD is a very large government organization which employs close to three million military and civilian personnel. The Air Force employs nearly 740,000 personnel, being the second smallest military service component of the DOD. NASA's JPL is very small in comparison to either of those, employing around only 5,000 personnel and a few thousand contractors. That kind of difference in size makes a difference in scale for the different organizations, and it changes what each organization means when it discusses their *enterprise.*

The DOD is the principle defense and war-fighting element for the United States, while the Air Force is its air component, and a member of the Department of Defense. NASA's JPL, or JPL for short, is a research laboratory run by

California Institute of Technology, with oversight, guidance, and funding by NASA.

The cases were chosen to draw a rich comparison and contrast. The IA metrics programs from the defense organizations can be analyzed because of their commonalities in law, regulation, purpose, and in some ways, organizational culture. The two organizations have a lot of similarities which will allow us to hold those factors constant and look at the differences between them. The two cases have enough differences to draw contrast from and to make unique observations about how the different contextual factors dealing with the style, size, affiliation, or mission of an organization affect their security metrics program.

NASA's IA metrics program was included to contrast the other two. While JPL is a federal organization, it is not under some of the same requirements and constraints that DOD and Air Force are, and it is not nearly as large or complex.

This chapter presents a brief overview of each of the cases, including the organization's purpose for collecting metrics if known, and then examines the case with respect to six major variables of interest:

- Measurement planning
- Data capture
- Data normalization and transformation
- Analysis
- Reporting
- Decision making

The measurement planning variable describes the assumptions, processes, and factors involved in how metrics are selected for inclusion in the program, and some of the rationale for why metrics are included. It also describes how measurement is planned, and how the planned measurements tie into the purpose for measurement. The data capture variable describes a major overview of how the different organizations actually collect the data to support metrics. Normalization and transformation involves how the organization ensures that the data makes sense coming from different contexts and how data standards are applied to make the data more useful. This can be seen in Figure 4.

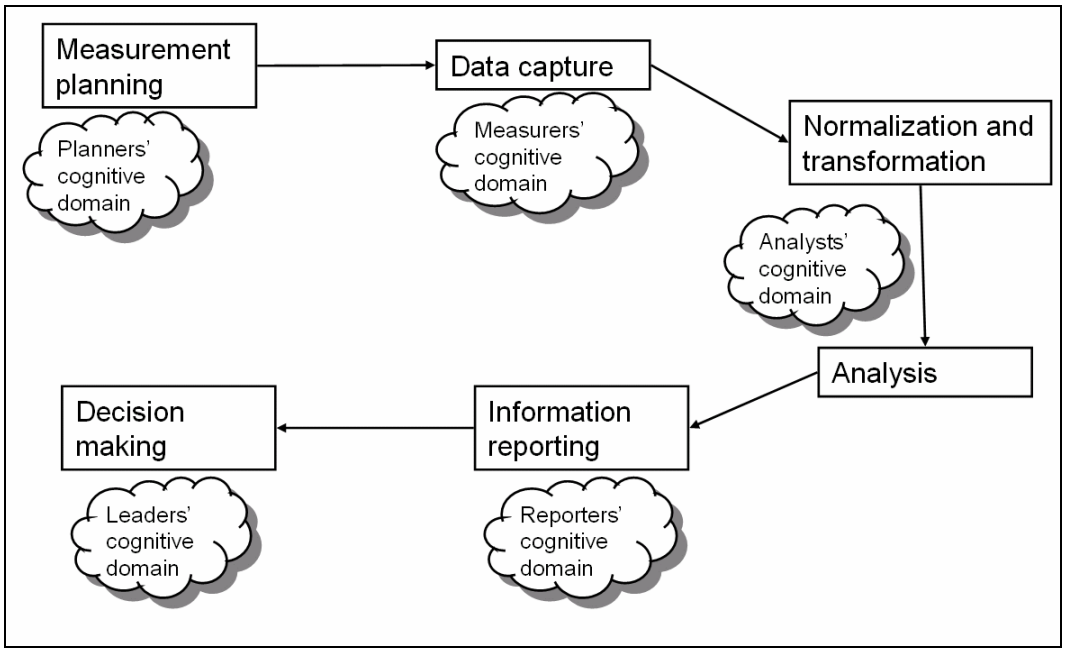


Figure 4. Research Model

The analysis variable is a measure of how the organization makes sense from the data it collects. Reporting involves how the analysis information gets to the decision makers, and the decision making variable describes how decisions are made with the information that is gleaned from the collection of metrics. Ideally this should be directly related to the measurement planning processes and assumptions.

The Department of Defense's Information Assurance Metrics Program

The Department of Defense has several organizations committed to information assurance, and which are involved in the department's overall

information assurance metrics program. These organizations are the Assistant Secretary of Defense for Networks and Information Integration, the National Security Agency's Information Assurance Division, and the Defense Information Systems Agency (DISA).

Each of these agencies has particular responsibilities with regard to the DOD's information assurance posture, and through coordinated processes, these organizations have come up with guidance, policy, instructions, and directives. Each of these is examined with the exception of DISA.

In the Department of Defense, the Office of the Secretary of Defense is "the principle staff element" of the Secretary of Defense "in the exercise of policy development, planning, resource management, fiscal, and program evaluation responsibilities," and within OSD, the Assistant Secretary of Defense, Networks & Information Integration, or ASD(NII)/DOD CIO, among other things provides guidance on networking, command and control, information resource management, IT, and most relevant to this research, information assurance (DOD, 2007; DODD 5144.1, 2005).

The goal of this office, through the Defense-wide Information Assurance Program (DIAP) to "ensure DOD's vital information resources and net-centric operations are secure and protected through information assurance enablement

of the global information grid" (DOD, 2006). They do this through primarily through the establishment of DOD policy and fiscal control over DOD information resources.

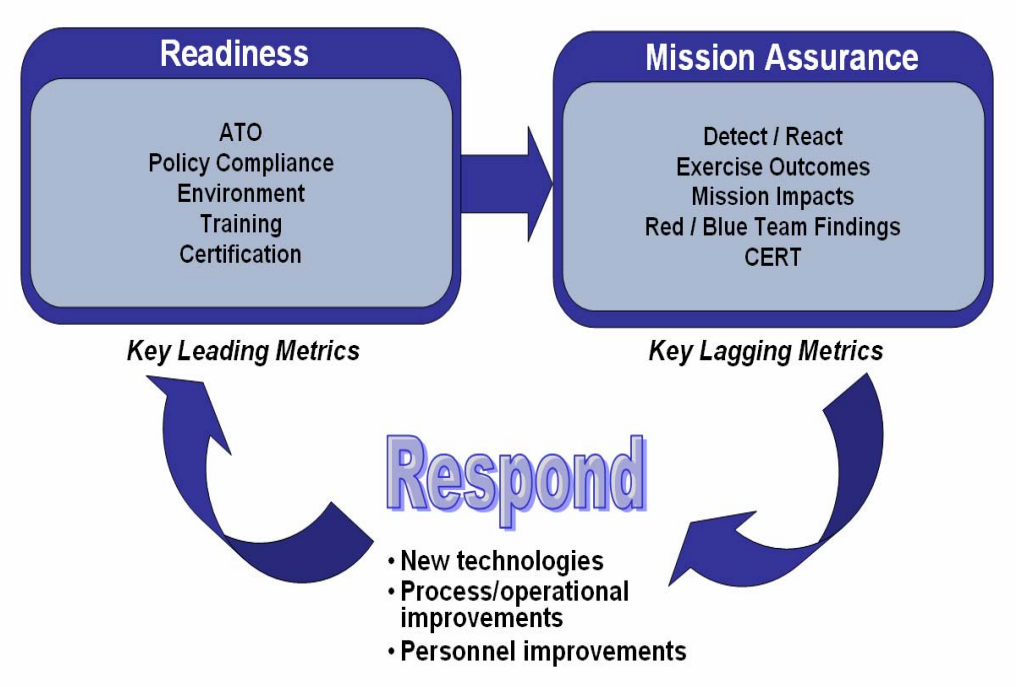


Figure 5. DOD Measurement Framework

(ASD(NII)/DIAP, 2007)

The National Security Agency's Information Assurance Directorate (IAD) works together with the ASD(NII)/DOD CIO's office to provide the "information assurance solutions" that keep DOD networks safe from harmful events. The IAD's mission involves preparation for and reaction to cyber threats, developing

encryption systems, enacting network IA measures, developing secure systems, and system testing. The NSA provides information security knowledge, products, and services. Examples of products are their security configuration guides, which cover how to configure applications, database servers, operating systems, routers, switches, voice over internet protocol, and internet protocol telephony, web servers and browsers, wireless devices and more (NSA.gov/IA).

The NSA's Information Assurance Division looks at how different network threats impact Department of Defense networks and tries to determine what the types of attacks infer about the different types of nuisance code that exists. To understand what nation state information assurance threats could be, the IAD takes the information about the attacks and elevates the threat level up to what an aggressor nation state could and would do.

The IAD also has 'red teams,' which perpetrate attacks against DOD networks in order to measure the protection level of the networks and 'blue teams,' which attempt to discover network security vulnerabilities in a cooperative effort with the installation and do their work from inside the network. The IAD representative mentioned that they increase the threat level because the IAD's red teams are bound by a limited set of objectives and a limited amount of resources while a nation state has many more resources with

which to reduce its own risk to attacking DOD networks, while increasing the risk to DOD networks.

The NSA's IAD provides "services, knowledge, and guidance." The red teams and blue teams provide the services, the NSA develops a repository of technical security guidance which comprises the knowledge aspect, and the products are the systems, architectures, and policies.

The Joint Task Force for Global Network Operations (JTF-GNO) is responsible for directing the "operation and defense of the Global Information Grid across strategic, operational, and tactical boundaries in support of DoD's full spectrum of war fighting, intelligence, and business operations." They also "identify and resolve" computer security issues, "identify significant threats" to networks and "disseminate and implement countermeasures" to those threats. They also assess the posture of combatant commands, services, and agencies computer network defense (CC/S/A CND), coordinate responses to threats, and identify threats (JTF-GNO, 2007).

Measurement Planning

In the DOD, the measurement planning process typically begins when high-level leadership asks questions attempting to determine how well that investment is performing. The key is that the DOD sees information assurance

controls, especially enterprise controls, as investments in the organization's security, which should return something in the way of a measurable impact to improving information assurance.

Once these types of questions are asked, someone or even a working group tries to identify what the goals of the IA investment are at a high level and then tries to develop indicators based off of that goal. Once those indicators are developed, they try to find ways that they can measure how well the system or networks are performing as related to those indicators. If it can be measured directly, it will be tasked and reported back through the typical organizational communication processes, usually through a text document containing data.

One example is that a goal for the IAD is to create knowledge, products, and services to make systems more resistant to attack. From that goal, IAD developed an indicator that the probability of successful "basic attacks" would decrease. The general compliance mandates are aimed at these types of "basic attacks," so it is logical that in order to measure how well the IAD is making systems more resistant to attacks, systems should be more resistant to "basic attacks" as a baseline.

It follows that the more the organization protects against basic attacks and if every other type of attack is held constant, the probability of attack would

decrease and IAD's effectiveness with regard to that goal can be talked about. With any given vulnerability, these type of measurements drive the decision as to whether the IAD should focus on improving the performance of existing security investments or moving toward procurement steps for newer security investments. If the IAD identifies an existing vulnerability-threat combination and then applies operational, managerial, or technical controls to it and then subsequently is no longer among the top exploited vulnerabilities, the IAD can determine at least in a categorical way that the controls are effective and are providing some type of security return on investment.

The DOD plans what and how to measure based on many constraining factors. One of those factors is the requirements supplied by regulation. The DOD is a U.S. federal agency which falls under the purview of the Federal Information Security Management Act (FISMA). FISMA requires specific minimum standards to be met with regard to the security of national security systems. FISMA also requires each federal agency to report specifics of its information security management program annually to the U.S. Office of Management and Budget which in turn reports to congress. More specifically, FISMA uses five basic performance measures for agencies:

- Certification and accreditation of systems
- Built in security costs
- Annual testing of system controls
- Contingency planning
- Implementation of security configuration requirements

Additionally, the U.S. Office of Management and Budget, which oversees FISMA requires federal organizations to prepare and report Plans of Actions and Milestones (POA&Ms) or detailed get-well plans "for all programs and systems where a security weakness has been found" (2004 FISMA report to congress, p. 2). FISMA also mandates that federal agencies report about:

- Inventory of systems
- Contractor operations and facilities
- Implementation of security configurations
- Costs for IT investments
- Documentation of adequate security controls in investment life cycles
- Tie POA&Ms directly to the funding request for the system (2004 FISMA report to congress, p. 3)

There are also numerous internal information security and management requirements which must be met, and which require specific sets of performance measures. The Office of the Secretary of Defense reports information security

metrics and performance measures for four services and 22 agencies. Each agency has their own internal drivers, but the agencies for the most part do not collaborate or coordinate in order to develop, measure, or plan to measure their information assurance. Some of these sources of policy, directives, and guidance are as follows:

Table 8. Numerous Sources of DOD-relevant Information Assurance Policy,

Executive Orders	OMB Circulars
National Security Directives	Public Law
White House Policy and Strategy	DOD Level Policy
House of Representatives	NSA Security Guides
Chairman of the Joint Chiefs of Staff Guidance	Department of the Army Policy and Instruction
Department of the Navy Guidance	Department of the Air Force Instruction
Marine Corp Instructions	DISA Instructions
GAO Reports	NIST Publications and Standards
Committee on National Security Systems	STRATCOM Directives

(adapted from DISA, 2006)

Almost universally, the directorate which has the budget mandates the metrics. Often, the directorate passes down tasks and indicators for different mission or cost centers to gather.

Each organization involved in the process has its own processes and drivers for determining what to measure, and thus measures different things. For instance, the JTF-GNO has the goal of defending the network against threats, so it collects very technical data, as does DISA. There are also different agencies

involved in the planning and design of metrics and who carry them out. The NII, Joint Staff, JTF-GNO, and the Director, Operational Test and Evaluation (DOT&E).

In addition, as recently found by Liou, Meeson, Swart, and Adams (2006):

> There are a large number of independent assessment efforts, some loosely connected, others unrelated, often using different metrics (with) findings not easily correlated or compared. It is difficult to obtain a coherent "big picture" of both the assessment efforts and their results.

Some of these different assessments are the enterprise IA posture assessment, the Joint Quarterly Readiness Review (JQRR), the Computer/Network Defense Assessment (CNDA), FISMA, assessments from the Undersecretary for Industrial Affairs and Installations (IA&I), and JTF-GNO reporting.

Each of the services has its own drivers depending on its investment strategy, and the OSD has regulatory drivers as well as investment evaluation drivers. Installation commanders invite "red teams" to attack their networks and discover vulnerabilities, and the discoveries are reported back to the installation commanders to do as the commander wishes with it. There is no coordination

between the combatant commands, services, or agencies within the DOD as to what they will measure or how they will collect the data to measure.

Table 9. Independent IA Assessment Efforts

IA Initiative	Sponsoring Organization	Level of Focus	Purpose
Enterprise IA Posture Assessment	ASD/NII DIAP	Executive	To establish a performance evaluation framework and plan that provides an accurate and reliable means of depicting and communicating the "effectiveness" of IA
JQRR	Joint Staff	COCOM & Combat Support Agencies	To report IA readiness, personnel/ training programs, equipment acquisition, and risk assessments at Combatant Commands and supporting agencies
CNDA	DoD CIO, STRATCOM	CC/S/A, CND Service Provider, Component HQ	To evaluate trends in policy compliance, resource requirements, and policy adequacy
FISMA	OMB	DoD and Federal Agencies	To comply with quarterly and annual security reviews & reporting requirements
IA&I Assessments	DOT&E	COCOM & Service fielded networks/sys.	To assess IA&I of fielded systems through Combatant Command and Service exercises
GNO Incident Reporting	JTF-GNO	Global & regional NOSCs	To track and report cyber events and intrusions as well as bandwidth utilization

(Liou et al., 2006)

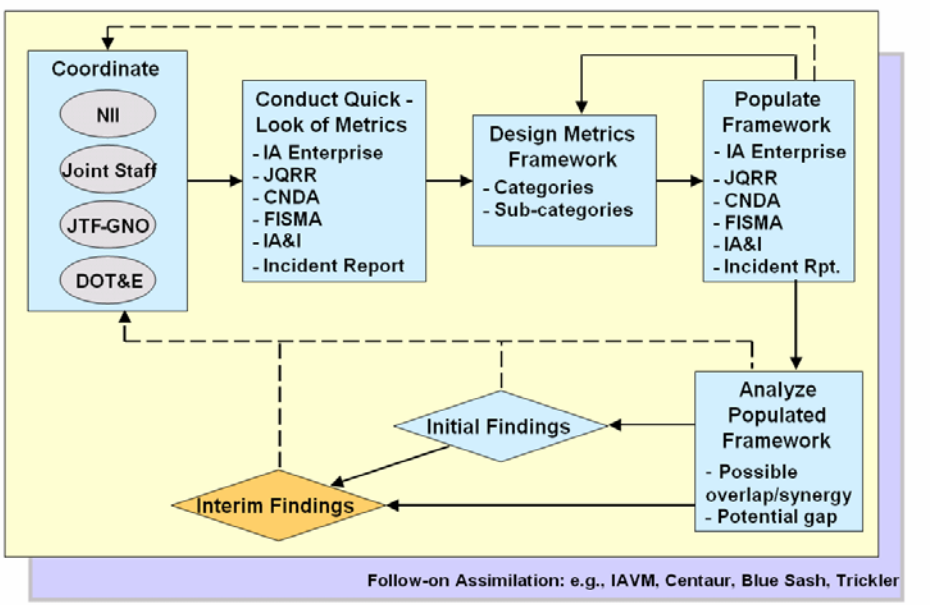


Figure 6. DOD IA Approach

(Liou et al., 2006)

Example: Public Key Infrastructure

One example of a high-level investment question is the DOD Public Key Infrastructure (PKI), which is the cryptography system which exists to provide access control and ensure confidentiality and integrity of communications across DOD networks. Specifically, PKI "is a service of products which provide and manage X.509 certificates for public key cryptography." The high-level question involved how well the Department of Defense tell if PKI is addressing the specific vulnerabilities that are present in DOD networks. This question concerned the costs of PKI and how well PKI was performing at securing DOD networks (DISA, 2007).

The PKI is only able to protect against certain types of vulnerabilities, so measurements of its effectiveness should be constrained to its intended use. In other words, it would be inaccurate to measure how well PKI protects *information security*, but it might be more appropriate to investigate how well PKI protects *authentication* or *non-repudiation*. The PKI system was not designed to handle many types of attacks that exist, although PKI makes it more difficult for attackers to pull out password files from networks. The IAD representative claimed that PKI doesn't help detect, protect against, or respond to attackers who exploit network-aware code; although it does offer the ability to find data easier with failed authentication logs after an attack is discovered through other means.

Data Capture

Despite the measurement planning, a technical representative in IAD mentioned that "there's no way to collect metrics the 'right' way" where the organization starts with a high-level problem to solve and then maps it to specific metrics. Like many other organizations, it is easier to "start with the data that's available and go from there" (NSA IAD, 2006).

The data that is available is the blue team and red team data. The blue teams capture vulnerability information from within the network and the red teams capture external vulnerability information related to their attempts to

penetrate the network. Many red team and blue team efforts are by invitation from the installation commander, and it is at the commander's discretion as to whether or not that information is released. Also, sensors at network gateways provide yet another perspective of network-related activity. Finally, IAD uses simulation events to fight against systems, which provides data about what the systems are most vulnerable to.

The IAD representative mentioned that they were able to collect three sets of data with regard to PKI. When red teams attacked a military installation's networks, they would encounter the PKI systems. Sometimes PKI was in place before the red team arrived on site, sometimes the base began implementing PKI after the attackers had begun their penetration tests, and sometimes the base began deploying PKI on top of them, which provided three sets of data on how PKI affects attackers.

Another source of data is the standard organizational data call. Usually, data calls come from an attempt to justify a budget. A call for data comes down from higher level management to lower levels of management. One example is "how many vulnerabilities exist in each computer." The tasking is formulated specifically which provides the lower levels in the organizational hierarchy information about what to collect, how to collect it, and how to report it. A

former line of thinking in the DOD was "no new data calls." But representatives from the ASD(NII) report that that is not feasible. In the future, they expect that there will be a requirement for services, agencies, and combatant commands to report. It is an "extremely manual process" which relies on data owners across the DOD for the metrics (DOD IAD, 2006).

Data that is collected by mandate is another source of information. Organizations must already collect data and information to support FISMA compliance reporting, which can be a useful data source to feed into the analysis step. Computer Network Defense Assessment is a self-report survey which is derived from Chairman of the Joint Chiefs of Staff Instruction 6510.01D (15 June 2004). The regulation guides the survey, but it also constrains the survey by only allowing the survey to ask specific sets of questions which relate directly to the regulation. The survey cannot be more specific than the regulation. Basically, DOD's aim is to collect data from end user sites which are required by mandate to gather various types of security data, and determine in what ways it can be used for more than one purpose.

Knowledge discovery in databases (KDD), otherwise known as data mining, is another method for collecting data, but it is not currently used in the DOD. However, representatives claimed "this is the direction we're going." One

IAD member claimed that using KDD is the only way to get out of managing IA by the use of "stories." In other words, anecdotal evidence lacks the ability to make statements with any degree of internal validity or confidence level. Data gathering through data mining is also more efficient. Databases and data stores can allow automatic data gathering so more time can be spent by people doing analysis. A representative from ASD(NII) speculated that the new project of Defense Online may be successful if it is built correctly. The representative expects that it will provide the option of automated analysis as well as automated reporting.

Some of these data repositories are the Defense IT Portfolio Registry, accreditation data bases which track approvals to operate (ATOs) and interim approvals to operate (IATOs), databases which hold FISMA-related data, and the Global Network Operations incident reporting database. SNAP is an IT budget repository for progress assessments and evaluation groups in NII. SNAP DIAP (Defense Information Assurance Program) contains budget data, and is linked to programs, goals, and capabilities which are listed in initial capabilities documentation.

According to representatives from IAD and OSD, the DOD collects a lot of data, but only a small portion of it is relevant.

Data Normalization and Transformation

One of the most important parts of the DOD's information security metrics processes is that of normalization and transformation, where the data is turned into information, and added to knowledge. This is the realm of business and technical analysts.

One analyst at NSA's IAD remarked that the data must have what could be seen as "points of consistency, which must be defined into the standards, so the data can tell you what you can ask and how to interpret the answers you get. Without indicators you can't do IA metrics that mean anything."

In IAD, it is the analyst's job to ensure the data is maintained and consistent, and to contact organizations which supply the data when there are problems. With an existing data architecture, the analyst's job is more focused on formulating analysis and finding relationships in the data instead of fixing data integrity issues. If this data architecture exists as data standards, then the analyst can refer to the data by way of metadata standards. This ensures the assets, alert information, vulnerabilities, and so on are discussed using the same language. They also do cross-correlations with the data to see if linkages exist between reports and trends that are discovered in DOD networks.

Analysis

Analysis in the IAD involves marrying the data that is available to the mission goals and indicators in order to determine whether or not the trends in the data relate to the mission goals or to evaluate whether or not an investment is actually meeting its information security-related goals according to the data.

In IAD there is a combination of business analysis with traditional business tools as well as technical analysis with more technical tools. The main goals are to see that there is a match between what is being measured and strategic-level goals.

Dealing with analysis is the business of creating meaning from data relationships. The representative cautioned that there is a lot of room for moving back and forth with regard to collected metrics and what they can mean. "With what data is available, it is very easy to create the metrics you want in order to back the cause you want to. For instance if some in the Department of Defense want to decentralize, and some want to be more centralized it is an easy task for the metrics to support both."

With the data that the DOD and its agencies collect to support leadership's defined measures of effectiveness, the metrics do not provide tangible definitive return on investment, but only a statement as to whether or

not the measures of effectiveness are met. This creates relative lines and conditional relationships, but no hard numbers or tangible, quantifiable relationships. In other words, "you can do behavior modifications which result in either significant, intermediate, or no results which will show completely valid relationships with defined points and defined rationale, but can't say you have 37 percent confidence with the current spending and 42 percent confidence with 3 billion dollars extra. As a side note concerning financial investments, a CND Assessment review reported that

> Once again components indicated that increased funding was their perceived best remedy for deficiencies, though once again cross-correlating increase in budget with increase in CND Assessment score reveals almost no correlation. Zero would be absolutely no correlation and we come up with only a 0.07, so it is very closely to being completely uncorrelated. (Aldrich, 2006)

One of the limitations in the DOD's program is the cost of measuring and analyzing data. The measurement and processing of data is very expensive. One anecdotal estimate is that it cost 60 million dollars to administer the security metrics program at only a limited level of capability in one organization. This often translates to short staffs and short budgets. In ASD(NII) for instance there is only one full time and two part-time analysts working on information security

metrics. As one official claimed, "you can gather measurements easily but it takes analysis to bridge the gap. Analysis can't be automated."

Information Reporting

When data and processes are standardized, in DOD's IAP, interpretation is a collaborative effort. But after analysis, information is reported through business channels to respond to senior-level requests which initiated the measurement in the first place. Data reporting is done primarily through manual processes in the Department of Defense's IA program. To the highest levels, reports and analysis are briefed to higher level leadership through slideshow presentations and in unstructured documents, and data is captured in spreadsheets.

Automatic report generation from databases and "point instantiations" feed into analysis, but the DOD does not currently use executive information systems in order to report findings at a high-level to senior management.

Leaders in the office of the ASD(NII) mentioned that using an executive information system would be useful and make the task of reporting easier, but that it would be cost prohibitive and it would lack the validity that comes with human data analysis. Executive information systems rely on reports from decision support systems and analyst-generated reports in order to make the

business cases. The personnel claimed that "decisions will never be made solely on a data graph from an EIS."

Ultimately, metrics and their analysis are used for enterprise budgeting decisions. If a metric is valuable in the OSD portion of the DOD's IA program, it is valuable because it relates to budgeting and resources.

At the strategic level, these decisions support primarily resource decisions. They answer questions such as whether the organization needs more money in one capability area or another or more money to be spent in certification and accreditation. The OSD has a relatively small budget divided between 27 agencies and five services. Leaders claimed it is a challenge to prioritize these monies and give them to the right places.

Incentives are from the OSD to the commanders of the various combatant commands, services, or agencies. It is to the commanders' benefit to do the best they can with their IA programs. If the probability of successful attack increases because the commander lacks resources, the commander needs to justify through the metrics of getting back to good network health.

The Office of Management and Budget (OMB) also holds the purse strings at a higher level. FISMA is only done by federal agencies because OMB has the

power to take away resources. "Risk is what's being signed off on: risk that's acceptable to be signed off on under the law."

At different levels such as the JTF-GNO, or tactical and mission areas use metrics to find out if they can sustain mission assurance, respond to threats, and update readiness data. In those agencies, metrics are important if they focus on mission capabilities at a point in time, allowing the agency to spend just enough to successfully complete the mission, and no more. An example of this type of reporting is the Joint Quarterly Readiness Review is a JTF-GNO review which measures capabilities. It took the place of the C-rating system to rate organizations' mission capability and has been in use for the last five years.

One challenge for the DOD's IA program is meeting in the middle. The DOD started their IA program by changing strategic IA objectives to be more outcome-focused. They developed measures to meet newer objectives, but have not developed targets for the objectives or for those measures.

As far as the data that is collected to go into analysis, CNDA data is not used for any senior management decisions outside DOD's information assurance program.

United States Air Force

The Air Force's mission is to "deliver sovereign options for the defense of the United Status of America, and its global interests—in air, space, and cyberspace" (Wynne, 2005). Since the Air Force has asserted that the battlefield of the Air Force extends to cyberspace, it logically follows that the Air Force must protect the information and computing infrastructure which characterizes this domain.

The Air Force Information Resource Management Flight Plan (2004) states that one of the information goals of the Air Force is to "protect Air Force information resources from attack and/or intrusion by both outside forces and internal disruption." Unfortunately, because of the asymmetric nature of information assurance, there is an extremely wide range of possible threats to the information, computers, and infrastructure of the Air Force, but there is only a finite amount of resources, including time, to protect it. The Air Force has thousands of information systems, with varying degrees of criticality that enable the service to operate. The loss of even one critical system could mean catastrophe and lost lives.

One reason the Air Force is interested in information assurance is to enable the Air Force to fulfill its mission. The effectiveness with which the Air

Force ensures confidentiality, availability, and integrity of its information and information resources is a required, though not sufficient, precondition to the Air Force being able to provide "sovereign options" and accomplish the military goals of the nation. Information security is important to the Air Force particularly for combinations of the following reasons:

Table 10. Some Motivations for Air Force Information Security

<table>
<tr><td colspan="2">Data processing is done on interconnected systems</td><td>Information security is a prerequisite to information superiority</td></tr>
<tr><td colspan="2">Dependence on information systems is high</td><td rowspan="3">Computer systems and servers are susceptible to viruses</td></tr>
<tr><td></td><td>Command and control systems are too critical to fail</td></tr>
<tr><td></td><td>Support functions are information system driven</td></tr>
<tr><td colspan="2">Air Force systems house sensitive and classified information</td><td>Air Force systems are popular targets for cyber attackers</td></tr>
</table>

(drawn from case analysis)

Measurement Planning

The U.S. Air Force Information Strategy states that the Air Force is interested in developing better accountability of its programs and processes by developing metrics that link investments to "specific payoffs in enhanced mission capabilities" (AF/CIO, 2002). The Air Force wants the freedom to be able to exploit cyberspace, so it must make sure that its information and information resources are secure, but it also must control its processes and ensure that they

are in line with the strategic vision, mission, and goals of the Air Force. The Air Force Chief Information Officer's office declared that

> Internal processes must be improved to reduce the time and complexity involved in executing security patches, procedures, and reporting. Success in this effort will be ensured through the establishment and tracking of critical performance measures that document progress. (AF/CIO 2004)

It is important for the Air Force to understand how to optimally measure and manage information assurance. The U.S. Air Force spends a great deal of resources to ensure that information resources are protected and available, and it is of great interest to Air Force leaders to know if the service is getting a good return on security investment. A successful information security metrics program promises to deliver that information.

It is impossible to know how well these conditions are being met without being able to measure the threats, vulnerabilities, and risks associated with the Air Force's information security. Being able to gather this information is the goal of an information security metrics program.

The Air Force must meet certain regulatory requirements as well. The Air Force, as a federal agency under the DOD, is motivated by the Federal Information Security Management Act (FISMA) reporting requirements (E-Government Act of 2002, Public Law 107-347). The Office of Management and

Budget (OMB) and Congress are required to review how well the Air Force, the Department of Defense (DOD) and the other agencies manage their information resources. Part of that reporting requirement is ensuring the security and assurance of the agencies' information systems (Takewell, 2005).

Headquarters, U.S. Air Force has a department within the Office Secretary of the Air Force, Information, Services, and Integration (SAF/XCI) which deals with evaluation of information assurance. For privacy concerns, they are referred to in this report as representatives from SAF/XCI. A representative from the office reported that the office used metrics through FISMA to identify deficiencies and weaknesses and create funding lines to mitigate the weaknesses. In order to do this, the service develops a Plan of Action and Milestone (POA&M) document, which is a schedule of activities which need to be accomplished before the deficiencies can be considered closed.

A previous Chief Information Officer for the Air Force began looking at information security metrics during his time in the position. The efforts consisted of research to show what the way forward should be, and what the service needed to measure in order to indicate that it had identified a security problem which can be fixed. The service looked at the three categories of goals for information assurance metrics: detection, protection, and response.

Another contact from the Air Force was from SAF/XCA, which is the assessments division within the office of the Secretary of the Air Force. A representative claimed that even though a lot has been done with regard to security metrics, the Air Force still had a long way to go with respect to its security and information assurance metrics.

The representative said that the services had begun coordinated meetings with XCIA (another branch from SAF/XC) to look at what things to use to establish an information assurance metric.

Data Capture

The Air Force sees its information security metrics as divided into managerial, operational, and technical metrics, but the Air Force collects mostly technical metrics.

The Air Force Audit Agency (AFAA) performs ongoing information assurance audits at the major command headquarters level. Its mission is to

> Provide all levels of Air Force management with independent, objective, and quality audit services that include: Reviewing and promoting economy, effectiveness, and efficiency of operations; Evaluating programs and activities and assisting management in achieving intended results; Assessing and improving Air Force fiduciary stewardship and the accuracy of financial reporting. (AF Audit Agency, 2006)

Sometimes the AFAA audits at base-level organizations, but in either case, it reports its findings to the Air Force Chief Information Officer and the senior Information Assurance official.

Some of the challenges SAF/XCI mentioned were that a lot of metrics are not easily quantified. They claim that there are strengths and weaknesses in the metrics program, like any other program. Technical metrics are easily quantified, like vulnerability scans. The representative claimed that these are easily taken care of, because you can perform a scan and quickly pinpoint the security weakness.

A representative from SAF/XCA said that sufficient protection like firewall protection, tools to track viruses, scanners, and response time were not supported throughout the Air Force's major commands. The primary sources of information were still the major command's network operations and security centers (NOSCs), and the base-level network control centers (NCCs), as well as the Air Force Network Operations Center (AFNOC). In the last year, however, those organizations are consolidating into two global Integrated Network Operation and Security Centers (INOSC), which will centralize command and control of Air Force networks.

Representatives from a NOSC at a major command supplied information about how data is captured. Mostly, the AFNETOPS CND (formerly the Air Force Computer Emergency Response Team) monitors Air Force networks for suspicious activity in a technical sense. The NOSC employs "network defenders" which monitor network traffic through a system of sensors inside and outside of an Air Force base's firewall. They also monitor e-mail traffic or manage antivirus activities.

Data Normalization and Transformation

SAF/XCI said that the most needed thing was a standardized set of rules to quantify metrics and consolidate them. They use a "collect everything you can" mentality and have much more data than they can use to make decisions. SAF/XCI mentioned that it is difficult to sort through the multitudes of data to find what is important or what makes sense. So the most necessary thing is organizing and interpreting the data and filtering it down to what's useful.

Reporting

Base network control centers report data from their networks to the major command (MAJCOM) NOSC, and in the future to the INOSCs. The MAJCOM NOSC then reports threats, numbers of port scans, and significant malicious events which are rated on a scale of severity from 1 through 5.

The Air Force developed a type of business analysis portal, or executive information system, which it's CIO used to track and manage deficiencies.

From the strategic level, a representative from the Air Force audit agency said that the Federal Information Security Management Act (FISMA) was the major mechanism the Air Force uses for compiling and reporting information assurance problems up to the Department of Defense, the Office of Management and Budget, and Congress. Once the FISMA report is completed, the Air Force Audit Agency reviews their report, and then sees if there is anything it takes exception to. The agency also reports these results to the Department of Defense Inspector General, who compiles the reports from the services and sends them to congress as well.

Numerous individuals in the process complained that a major hurdle in the Air Force remained the structure, complexity, and competitive nature of the major commands which make up the major organizational forces in the Air Force. One representative at the strategic level remarked that "with each major command having competing requirements and demands, it has been very difficult for the Air Force to mandate compliance with all of the policies."

Further, although some MAJCOMs or bases have strong information assurance programs, there is not yet an enterprise information assurance solution

across the MAJCOMs, forward operating agencies, direct reporting units, and headquarters.

Decision Making

A SAF/XCA representative claimed that the biggest problem was after the metrics were collected was implementing and enforcing policies. He mentioned that the internal threat was the biggest problem in the Air Force, but the real problem was harder to pin down. He said the Air Force did not have problems with network or system availability, assurance of information, or the ability to turn missions using network resources. He characterized the problem as binary: either the Air Force doesn't have the proper policies or procedures in place, or someone or some organization did not follow the policies and procedures correctly.

The representative offered an example of one metric and how it was implemented. The question originated at headquarters to the effect of: "how successful are organizations at remediating an attack. This included (a) how long it takes to identify if a threat is real, (b) how long it takes to mitigate the threat, and (c) how long it takes to restore operations.

Unfortunately, it was difficult to gather this information. The MAJCOM NOSCs tasked this data call to base-level network control centers had the

information, but since it made their organization or their commander's organization look bad, they did not want to provide that information up the chain of command.

The service representative also said there was a greater problem trying to pin down and change non-technical problems, which has to do with the operational mission of the Air Force. The Eighth Air Force Commander, who also serves as the Air Force Network Operations (AFNETOPS) Commander is the Air Force's Designated Approval Authority and has the authority to control whether or not a system can be part of the Air Force's network. The DAA can shut down a base's network or information systems, but has not been willing to do that because of the risk to the operational mission.

The representative claimed that when it comes to taking a commander's base off the network when it would affect the flying mission, security would have to take a second priority every time.

The representative mentioned that one problem with the Air Force's information assurance metrics program was with even the most useful metrics, a commander at any level can decide whether or not to take the risk. Because of the connected nature of the Air Force enterprise, this means that the tactical-level commander's decision can make a risk management decision, which while

locally beneficial for him or her, can put the rest of the enterprise at risk. Since any commander can accept the risk, then the metrics are almost meaningless.

He claims that these types of decisions are also made all across the Air Force in hundreds of squadrons and dozens of wings, directorates, and bases. "With this kind of compliance structure," the representative claims, "our protection to vulnerabilities is going to be limited."

After the interview, an exception to the representative's rule of thumb occurred: web-based e-mail was taken down across the Air Force. Due to negative information security events, the JTF-GNO determined that web-based e-mail, which had been in wide use across the entire Department of Defense, would be taken offline. The Air Force, as part of the DOD, complied.

National Aeronautics and Space Administration's Jet Propulsion Lab

NASA's Jet Propulsion lab is "the leading US center for robotic exploration of the solar system." Managed for NASA by the California Institute of Technology, JPL is responsible for research into planetary exploration, earth science, astronomy and physics, telecommunications, and other technologies (NASA, 2005). The laboratory maintains a Pasadena location at the California Institute of Technology and three "Deep Space Network complexes around the

world," as well as an "astronomical observatory" in California "and a launch operations site at Cape Canaveral, Florida" (NASA, 2005).

In 2005, JPL employed 5,425 personnel as direct employees and "on-site contractors" and maintained a $1.6 billion budget (NASA, 2005). The California Institute of Technology manages all *jpl.nasa.gov* websites and supports all information technology assets for the government agency.

JPL is a lot different than either the Department of Defense or the Air Force, so it provides many points of contrast. The first noticeable difference is the size of the organization. JPL is only one segment of NASA, and NASA is smaller than the Air Force or the DOD. Another major difference is that JPL is not a purely federal agency. JPL's information technology assets are managed by the California Institute of Technology as a federal research partnership. The third difference is that it is not as high-level of an organization as either the Air Force or the DOD, so the perspective of the employees and the nature of work are different. Being partially federal and partially academic, there are other factors that play into how research into security metrics is done, and there is a major difference in the complexity of the organizations: JPL has a much simpler structure.

Due to intellectual property concerns over methods that have not yet been published, the actual metrics and methodologies that are used by NASA's Jet Propulsion Lab are not presented in this thesis, but every attempt has been made to convey the main organizational ideas and concepts that underlie the processes and metrics because of what they add to the community.

Measurement Planning

Measurement planning is less complicated at JPL than in the previous two cases. The IT Security Service Engineer works information technology security issues and implementations on behalf of the Information Security Manager. The IT Security Services Engineer is thus the focal point for the design and collection of information security metrics and presents those metrics to senior management" (Miller and Hope, 2003).

Measurement is planned by understanding the trends of what is reported, why it's reported, and how. When a request for data comes in from the CIO's office or the Information Security Manager, the IT Security Service Engineer has the authority to automate the collection of that data if he believes the request will reoccur.

The Senior Enterprise Manager works for the IT Security Manager and "manages security issues for 'special management attention' items." There are

also security management roles held by the Division Manager, the IT Security Rep, Line Managers, System Administrators, and others. These security management roles are defined in advance, and then security metrics planning can proceed using the same or similar lines of authority and areas of responsibility.

NASA JPL uses the NIST 800-53 guidance referenced in Chapter 2 because it is difficult for managers to select controls on their own.

The representative stated that NIST provides not just technical security controls, but also the management and operational controls which he claimed people don't generally understand well.

The Security Services Engineer stated that mandatory controls are "kind of like insurance…people don't have the ability to evaluate what they need." Having the NIST structure in place makes the process easier to sell to upper management. Instead of being a choice to evaluate, the organization just has to comply with it, so it eliminates on some of the risk decisions being pushed down to a lower level.

JPL defined three sets of metrics, based on three categories: compliance, incident response, and risk assessment. Each category only has a handful of nine metrics it collects as well. The rationale behind this is that even though the data

is available, the management believes there are only certain aspects that need to be looked at from a high-level view which really have much impact on the security of an organization.

JPL is not currently required to report FISMA compliance since the unique reporting structure of the organization. Even though they are not required to report, JPL traces each of their security requirements to a NIST 800-53 control. Another source of guidance for JPL's security planning and security metrics program planning are GAO (General Accounting Office) testimony. The representative stated "if you look at what the GAO is saying, it's good to listen, because it's what the inspector general will come to audit you about."

Data Capture

Whenever possible, JPL automates the collection of data. Manually collecting all sorts of data from numerous people "doesn't work." A representative from JPL says that manual collection often fails or is slow because people aren't responsive. Sometimes, they are too busy, other times, they do not know the required data, and they introduce another source of error into the metric. Automation is also more reliable. The way the data is collected can change from person to person or from organization to organization, but an

automated process collects data the same way every time, unless something changes with the systems that are responsible for it.

While automation is the goal for many organizations, the representative from JPL stated that their success with automation was due to their efforts to align their processes. He claimed that an organization needs to focus on an infrastructure to enable them to collect data for metrics. He also claimed that it wasn't done quickly. "It has to be an evolution…it has to be phased in gently over the years. That way, people understand why they're doing these additional things."

The automated approach led to the creation of a centralized IT Security Database which tracks the location of particular items of information-related property, and then tracks documents, directives, e-mail communications, logs, security plans, and other information. It also generates reports and can help a user generate a security plan, which is required for each department.

One of major initial steps is getting asset accountability under control. The representative stated that "first, property was the biggest thing that we had to get under control." He claims the key to managing information security is "managing the inventory…getting a list of things that (the organization) owns is the first part, and determining the properties of those assets is the second part."

"Once you have the list, you can go to management, or go to the organization with a list of properties and can put it in the security plans. We have so many properties arriving and leaving every week that it is still major work to manage this." The managers of the security metrics program send out weekly notices to line managers to have them enter items into the security plans, or to take care of security plans when employees leave. The JPL representative claims that all the messaging is still automated, but people still have to do stuff."

The reports from the database help management measure how well JPL manages different processes and operational or management controls, and assess how well the different sub-organizations are keeping up with their responsibilities.

One exception to the automated data gathering approach is compliance metrics. In JPL, compliance metrics are almost always done with data calls from sponsors. Many aspects of compliance, including whether or not programs are in place are collected manually, either through looking through a database containing the information, or through the standard series of data calls to the information owner or the responsible individual or department. However, the representative claimed that almost all of the data is contained in the database, so

even manual data gathering only involves having a person look in the database to find information.

Data Normalization and Transformation

The representative from JPL said that setting data standards is important, but that in JPL's process, those standards are implicit. When the data comes from the automated database, management can ensure that the information comes from the authoritative source, since this is how the database was designed to gather input.

This reduces the amount of redundancy in the data and enables a certain measure of uniformity to the data, since it comes from the same source. But like any database, data integrity is always a concern. The representative cautions that the data is all only good to the extent that people comply with the process, which is why some of the other management controls and triangulations are in place.

With vulnerability for instance, there are a lot of different perspectives. Some of these are whether vulnerabilities relate to false positives, whether vulnerabilities are being tracked by system administrators, and where a new vulnerability discovered is at the in the processes. There are a lot of different states to consider. But, the representative claimed, this helps out because it

enables you to better account for what is happening in any given circumstance. "It's like looking at a double sum backwards…you get new insights, and all the things should match up with the books."

The JPL representative stated that those in the organization with security planning roles can see the data and can say if there are data integrity issues. If there are integrity issues, most of the time, the problem is with the source of the data rather than on any processing steps which the data might go through.

Analysis

Analysis is done at different levels depending on the questions. The analysis is of major importance in order to interpret trends and findings in the data and to correlate findings from the different data sources.

An example of an analysis curve is records of historical data which shows how well the organization has done with regard to their information security goals over the last two years. They can see whether their information security is improving or getting worse, but the representative says "it's really hard to quantify this stuff. For example, we can look at incidents and probes to see how well we're deflecting attacks." Even though JPL can plot those types of findings and measure them, they are of limited use since they only represent a part of the whole information security picture.

Analysts spend their time seeking to discover what is wrong with the overall picture of information security management with regard to a particular process or event. If something is broken in the process, the goal is to identify it as soon as possible so it can be fixed.

Reporting

Information reporting is "semi-manual." The reporting capabilities have evolved as the technologies have allowed them to. For instance, the security department used to send out a monthly metrics report to senior management. As it started out, it wasn't information that could be held in the database. The tools that the organization had at the time didn't support the charts that they required for this type of reporting. Now, management can go online and log in at any time and view the metrics for the previous two months.

In JPL, information on security is reported to the CIO and to other people that have security roles in the organization. But for the most part, management doesn't pay attention to the security metrics when things are going well. But people in the information security department can look at the metrics and the information to further refine organizational processes dealing with information security. For instance, the representative for JPL said that they can "see backlogs of things that need to be done in the history of open security log tickets."

JPL's representative said that "compliance metrics get management's attention the most. Management looks at performance metrics, but they may not always know what actions to take based on what they see.

Decision Making

JPL makes decisions about which processes to implement, improve, or discard based on information gained from the security metrics program. It also helps JPL determine whether or not a process is effective before it is implemented completely. The analysis allows management to look at a problem in several different ways, so they can see patterns of consistency in the data, and know whether or not a process is working or not.

Process improvement is a major area of interest to JPL, but measures of return on investment are implicit. Since most of the security metrics program deals with compliance-related issues, the organization has to do it. In this case, efficiency is more important than determining whether it would cost more to have a control or not to have it. These arguments are sold to management by showing how every step in the security management and security metrics/risk assessment process was an outside auditor requirement.

The representative claims that they "haven't had to do the typical ROI calculations because it's implicit in the process." Their feeling is that if the

controls are being carried out as efficiently as possible, since the reporting is a requirement, the organization is achieving a return on its security investment. Another factor is that the data to feed into that kind of equation are guesses anyway and it is difficult to put a dollar value on the various factors in that type of equation. For instance, how do you quantify loss of reputation, or a bad audit report?

Summary

The Department of Defense makes decisions based on how and what to measure based primarily on budget constraints. In this regard, return on investment is probably the primary factor in their program with mission effectiveness a close second. The DOD is concerned about mission accomplishment and does this through measures intended to improve the mission readiness of an organization. The Air Force has similar motivations. NASA's Jet Propulsion lab makes decisions about what and how to measure information security based on a goal of continuous process improvement and a desire for efficiency. Jet Propulsion lab sees return on investment as an implicit goal: if the organization does the right things, they will provide value back to the organization.

The primary objectives of the DOD's program are to determine how to meet high level objectives with existing and available data. This takes the form of attempting to integrate many different independent assessment efforts into one and to streamline them so that they complement rather than compete with each other. Because there is no single office responsible for integrating all of this data and all of these organizational processes, this likely will be difficult or impossible without change from outside the system. The Air Force has the same primary motivations, to tie high-level goals to what the service has been measuring for years. One can speculate as to whether or not this is an attempt to simply justify the current processes and organizational relationships. Jet Propulsion Lab is working to improve the effective security processes already in place.

The DOD's primary challenges are the disparity between numerous data sources, metrics, organizational processes, assessment efforts, sources of funding, organizational chains-of-command, and responsibilities. Thus, the three analysts in OSD's metrics cell do most of their work cleaning, grooming, and trying to get data reported in the same way rather than analyzing trends. The Air Force has problems managing the risks that are present in the system and delegated to the lowest levels of command. A squadron commander or group commander's

acceptance of risk at their level puts the entire enterprise at risk in our laterally-configured networks with their associated information resources. The Air Force also has the problem of trying to sort the massive amounts of data available from its "measure everything" measurement efforts. JPL expressed their challenges as mainly dealing with not being able to completely automate security. Managers still have to do security work, and the processes still involve coordination between the different parties, but in most cases, this coordination is automated as well.

The DOD's process is by far the most complex. Even in doing an 18-month case study on the security metrics program, and reviewing hundreds of documents, the researcher was not able to read all of the relevant, applicable, and enforceable policy and guidance for the DOD. There are just too many documents. With so many different levels of policy and guidance, there are likely many contradictions in policy, procedures, and guidelines. This is inevitable in the way the DOD is organized though. The hierarchical command structure of the military from the 1950s created silos of control. Each of these silos of control is developing their own programs, assessments, and policy independently: there is no glue that can hold all of that together.

The Air Force's complexity is high, but it is for the same reason. The Air Force is on a smaller scale, but even in the Air Force, there is policy at the Squadron, Group, Wing, Numbered Air Force, Major Command, Department, and Service level covering many different aspects of information security. Also, since the Air Force is a sub-organization of the DOD, all DOD policy applies as well. NASA's JPL seemed to escape from this issue somewhat. The organization is hierarchical, but it could be that they are such a comparatively small organization that there is no need to introduce unneeded complexity in the form of task forces, sub-organizations and such. Policy is simple, clear, and specific.

The policy drivers for the DOD and Air Force are primarily FISMA and compliance related issues and congressional oversight facilitated through the OMB. NASA's JPL is responsible primarily to its sponsors, and to NASA, even though it follows NIST guidelines for managing information assurance.

The DOD and Air Force both operate from bottom-up orientations. This means that they style of their strategic IT management processes is "administrative" and inflexible (Earl, 1993). It also means that matching high level goals to the data in the trenches is likely to be impossible, especially with such complex organization.

The factors that DOD has going for its program are the long history with information assurance. Most of the IA standards in place are in place because of the work in the DOD. This includes NIST guidance, CNSS guidance, and so on. The Air Force has an increasing role in cyberspace which may facilitate additional resources and a higher level of attention to the IA metrics program. This is conjecture though. JPL has a track record of success, and has generated credibility with its security programs ever since its successful implementation of Y2K controls. In fact, officials from NIST helped the researcher choose JPL as a case and facilitated contact because of NIST's high regard for JPL's IA metrics program.

The DOD and Air Force both desire automation in their processes, but their process and organizational structure, as well as their enterprise architectures are too immature for that. JPL uses automation effectively to reduce the amount of actual human work that takes place in managing the incredibly complex processes involved in IA management and metrics collection.

The DOD and Air Force take a very long time to go from planning stages to implementation, which is almost measured in decades instead of years or even months. JPL claims that the implementation of their processes were slow and gradual, but in relative terms, they were implemented very rapidly. The fact is,

they are in place today, and each organization started their programs at roughly the same time when information technology and networks started becoming ubiquitous, threats became greater, and vulnerabilities more exposed in the 1980s, 1990s, and early 2000s.

The DOD and Air Force's metrics programs are designed to be self-reports in many cases. The type of data they collect is very technical, consisting of intrusions, machines, and firewall logs. Primarily, both metrics programs are focused not on *information assurance*, but *network security*. Also, due to the self-report nature of the preponderance of assessment tools, the majority of values are Boolean values, representing yes or no questions to whether or not a process is in place. Again, JPL comes out on top, using a mix of management, operational, and technical metrics, but more importantly using a small set of metrics. These metrics are general indicators of health and are many times in ratio form, consisting of percentages and real zero values.

Consequently, from all of these factors neither the DOD nor the Air Force see their programs as successful yet, where JPL does.

Table 11. Comparison of IA Metrics Programs

	DOD	Air Force	NASA JPL
Motivations	Return on investment, mission readiness (surrogate for effectiveness)	Return on investment, mission accomplishment	Process improvement, implicit return on investment
Primary objectives	Determine how to measure strategic objectives, re-use existing data	Determine how to measure strategic objectives, re-use existing data	Improve control over processes
Challenges	Disparity between numerous data sources, too much time spent "cleaning" data, not enough personnel doing analysis, difficult to use massive amount of data collected	Problems managing issues discovered, risks accepted at lower levels make risk unmanageable from enterprise perspective, difficult to use massive amount of data collected	Management intervention still required to enforce policy
Process complexity	Extremely high	High	Medium to Low
Drivers	FISMA, congress, other budget and effectiveness questions	FISMA, congress, DOD questions, improvement of IA posture	Process improvement, responsibility to sponsors
Orientation	Bottom-up, attempting to tie toward high objectives	Bottom-up	Top-down
Strengths and keys to program	Long history - co-developed most standards, many data sources	Air Force has increasing role in cyberspace so program should be put at forefront, many data sources	Track record of success, credibility with leadership as well as other agencies like NIST, asset control
Approach to automation	Desired but not there yet	Desired but not there yet	In place and successful
Time to market **from policy to implementation**	Very slow	Very slow	Moderate
Type of metrics collected	Heavily technical but also containing operational and management metrics	Heavily technical but also containing operational and management metrics	Mix of technical, operational, and management-related
Style of data for majority of metrics	Nominal. Boolean checklist-oriented questions	Nominal. Boolean checklist-oriented questions	Ratio.
Program success as perceived by organization	Not yet successful	Not yet successful	Successful and improving

Communications about what to measure and how to measure it are simplest in NASA's JPL, but most difficult in the Department of Defense. The number of agencies that are required to communicate with is daunting, and they all tend to have standard policies, practices, and cultures which make it very difficult to integrate measurement decisions in one single way. In all cases, these communications are set forth in policy or in a formal way.

Data gathering is largely done manually with the support of very limited automation in the Department of Defense and the Air Force, but at JPL, it is largely done in an automated fashion with supported of limited manual processes to fill in the gaps that automation won't support.

Data normalizing and transformation, and data analysis is done by analysts in all three organizations, but in roughly equal numbers, regardless of the size of the organization. Data standards are set forth in JPL, but have not yet been conceived in the DOD or in the Air Force. Data reporting is done through manual means in most cases in all the organizations; however, automated reports are available on demand to senior managers at JPL.

True to the purposes that brought metrics about in the first place, the DOD and Air Force use metrics information in order to make decisions about how to most effectively allocate resources, and how to improve the information

security for the enterprise. NASA's JPL, since it lacks the enterprise scope that its parent organization, NASA has, is more concerned with continual process improvement as it implements standard sets of security controls, rather than managing each investment and measuring it for optimality conditions.

An inference from this research is that a simpler program is easier to administer. This is intuitive, but easy to forget when the organization is extremely complex to start with. Complex organizations tend to generate complex business process with varied and scattered sources and types of data. Integrating the collection of data across all those sources can prove to be very difficult. In NASA/JPL's program, which was the simplest, the management and administration was easier. In that organization, there was still work which needed to get done in order to manage the security policies and practices, but because so much of the work was smartly automated, the work of the analyst could be spent more on analyzing and interpreting findings, seeking out and correcting negative trends, and contributing to process improvement.

Following that line of thinking, it may be very difficult to make a simpler program without serious organizational change. The structure of the organization and the motivation of the participants has a lot to do with how well any type of program can perform. If the motivations and rewards are not

aligned with the desired outcomes in terms of performance, the organization will probably always have difficulty making the processes and programs work because those processes and programs are designed to fit a system that doesn't work.

Another observation is that contrary to the researcher's prior intuition, low-level detailed and precise risk calculations may not be helpful for high-complexity problems. In the same way that mathematicians and algorithm researchers have been unable to find a polynomial time algorithms to solve the traveling salesman problem and other non-deterministic polynomial or "NP complete" problems, it may be the case that to find a precise measurement of risk to evaluate the future prospect of each combination of potential security controls has so many combinatoric solutions, that the problem would not solvable in an efficient manner with a deterministic solution. The selection of controls and safeguards may very well be an NP-complete problem, but as far as the researcher knows, the problem is not even formalized well enough to evaluate that yet. This is left to future research.

All the organizations studied used heuristics such as using best practices in order to find a reasonably accurate solution, or a best-effort approximate of what needs to be done so they could focus their valuable time on

implementation, execution, and planning rather than getting stuck on the value of the choices of what to focus on. In this line of thinking, an organization can use groups of controls which close off certain very common sets of vulnerabilities. This practice may have more value to a company than a computationally precise measurement of risk, especially when security is a time-sensitive area. All the determinants of security risk change with respect to time, and major parts of the organization's risk model may be obsolete sometimes within weeks or months.

Another intuitive finding is that it is difficult and highly subjective to map organizational goals to data that is available. Many times, the high-level view cannot be supported with accurate and descriptive data without a great cost to the organization, so other data must be used to approximate a solution. In other cases, data can be manipulated and molded in order to support whatever hypothesis the organization wants to support.

This brings us to the next point: rigorous data collection and research methods are not in place in the organizations' information security metrics programs. For example, reliability is often touted as a property of a "good" metric, but reliability only determines whether or not the metric is stable and can be re-measured in the same way with the same result. The concept that is

missing from Wesner's (1994) characterization of "SMART metrics" is validity. If a metric is not valid for what construct is being measured, it doesn't matter how specific, measurable, actionable, relevant, or time-dependent the metric is. It doesn't measure what the organization wants to measure, so it is useless for that purpose.

V. Conclusions and Recommendations

In all of the organizations, automation of some of the more menial data collection and entry processes was a goal. The observation from this is that automation is helpful and good, but automation relies on strong processes to be in place first. In the example of NASA's Jet Propulsion Lab, they were able to automate a great deal of their measurements and metrics all the way down to the workstation level only because they first developed strong processes to control their inventory.

In all the organizations, data that was collected was used for multiple purposes. In this way, compliance metrics can often be used to support effectiveness metrics or process metrics. If an organization has to collect something by mandate, it is logical that their best interest is to get the most out of that collection, since it comes at a cost.

With regard to collecting data, data standards are necessary in order to incorporate multiple sources of data into analysis. However, data standards represent unified organizational processes. If the processes in the organization are aligned, the data should be aligned by design or as an extension of aligning the processes. An effort to align different types and formats of data could fail without considering the organizational processes that make those types of data

formats necessary, and the appropriateness of keeping such varied processes across an enterprise. Patching the data together in a piecemeal fashion may help an organization in the short term, but will probably not be as effective as revising the processes which require the different data standards, and then changing the data standards for each of the data sources to be cohesive.

Organizations seem to do metrics for three reasons: to increase or maintain the organization's ability to carry out its mission by focusing its security controls, to comply with governance or compliance mandates, and third, and most common: to focus investments by determining the return on the security investment as it applies to security controls.

In determining if a security control is cost-effective, an organization needs to know:

1. How much does the security control cost to implement?
2. How much would it cost without the security control?
3. What is the security control providing in terms of value to the organization?

Metrics are really correlations between two or more different measurements. Measurements of any kind require data sources, and in order to

compare multiple data sources and make correlations, there needs to be some way to tie these data sources together. Many organizations do this through an analysis function, with people connecting the data together.

Organizations can answer question number one above by storing contract, acquisition, bill, receipt, or time sheet data, or by calculating it based on a number of those factors as appropriate to the organization. Organizations can answer question number two, "how much would it cost without the security control" by using an identical or close to identical control situation, which did not implement the security control. If there is a sister organization with accessible data, this can be easily estimated based on a comparison between current costs and control costs.

If there's not a sister organization, a peer competitor or similarly sized organization may offer information to their stockholders or in the case of the federal government, in a report to congress or a budget submission. Short of either of these two options, the organization must estimate the cost, using some form of loss expectancy, such as annual loss expectancy or total cost of ownership, but in either case, the estimate of the cost which is a calculation of the probability of loss and the cost of the loss:

Return on investment may be done for many reasons: some reasons benefit an organization's information security, and some do not. For example, when compensations, staffing levels, budget decisions, and authority rest on the perceived return on investment for an information security measure, control, or practice, there may be a tendency for managers to select data and metrics which make the department look good, regardless of the true performance of the department.

In the worst case, this behavior may cover up legitimate information security problems. In some cases, metrics may be established as an attempt by a business unit, or some individual in middle-management to head off budget cuts before they start (Bentley, 2005). This way, the skilled manager will always be able to defend his or her department or business unit from reduced funding.

This can be for many reasons. One reason may be because the unit truly and rightly believes its functions are critical to the operation of the organization as a whole. Another may be that the unit realizes that it only offers tangential and indirect value to the organization and that the unit has a feeling that the leaders of the organization don't understand the value it provides. Sometimes it may be pure and simple tribalism, fostered by the managers' desire to show leadership that their unit is performing better than other units.

While one tenet of measurement is to strive to be more quantitative, quantitative measures lend themselves toward measuring technical problems. The difficulty is that information security is not only a technical problem, but it is also a managerial problem, a resource allocation problem, a user education problem, a compliance problem, etc. An approach to information security is sensitive to the context of the organization, the people making decisions in the organization, and the motivations for securing the information systems and information.

Quantitative metrics alone can not take into account the whole information security picture. They often are correlations of technical measures, like software and hardware systems, antivirus, and intrusion detection trends. They also do not account for personnel and policy safeguards or tell management how to balance the costs to optimize their return on investment.

The U.S. Air Force, as a sub-department of the Department of Defense, was also complicated. The leaders seemed frustrated with the lack of ability to collect certain types of metrics because of the structure of the organization, and how it functions. One of the major features of the structure of the organization is the leadership and management-level reward system used by the Department of Defense and the United States Air Force. Promotions are defined based upon

annual performance reviews, so long-term thinking, while highly valued, is not rewarded. This is not unlike how businesses are responsible to their shareholders on a quarterly basis. Such rewards hinder innovation, risk taking, and critical thinking among the leadership of the organizations, and promote small but measurable management achievements, or continuing previous management's projects.

Insights About Security Models

In developing the model for this thesis, certain information emerged that explains what an information assurance program should be like, what a security metrics or security risk assessment program should be like, and what metrics should be like. This information was presented in Chapter 2 in order to be used as criteria for interpreting the data presented in Chapter 4. Nevertheless, this consolidation of ideas from the literature review is a major benefit from this research.

A more theoretical observation is that it may not be appropriate to fit information, mission, goals, systems, and resources to a hierarchical model. In the researcher's initial view, goals were aligned to strategies and systems existed to support these goals. Information aligned under each of the goals in a tree-like structure. Attack trees (Figure 5) are also arranged this way. In this hierarchical

view, it is difficult to determine what is related to what and to examine the effects of changes in information security policy. A possibly better approach to modeling this problem would be with the use of a graph with nodes and connected edges.

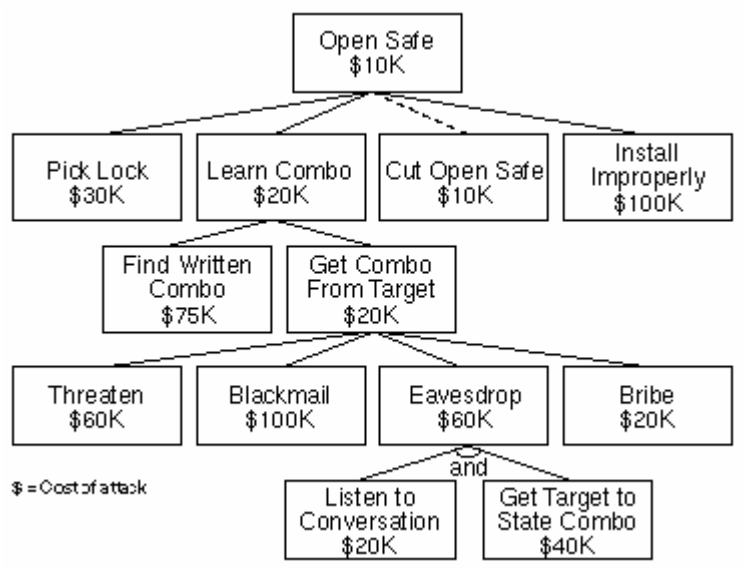


Figure 7. Attack Trees

(Shneier, 1999)

For example, if we picture the problem as a directed graph $G(V, E)$ (Figure 3) with vertices {vulnerabilities v, threats t, assets a, controls c} $\in$ V and edges e $\in$ E with cost function w(c, v) assigned to edges between vulnerabilities and controls, probability function p(t, v) assigned to edges between threats and vulnerabilities, and a severity function s(v, a) assigned to edges between vulnerability and asset nodes. The Threats try to affect the assets, but they must

do so through a vulnerability with a certain probability that they will. The vulnerability has a level of severity with respect to an organizational asset which has a bearing on what the actual probability and cost of loss will be.

This kind of view allows us to formalize problems more precisely, which is a requirement if we wish to effectively automate the process of analysis or measurement.

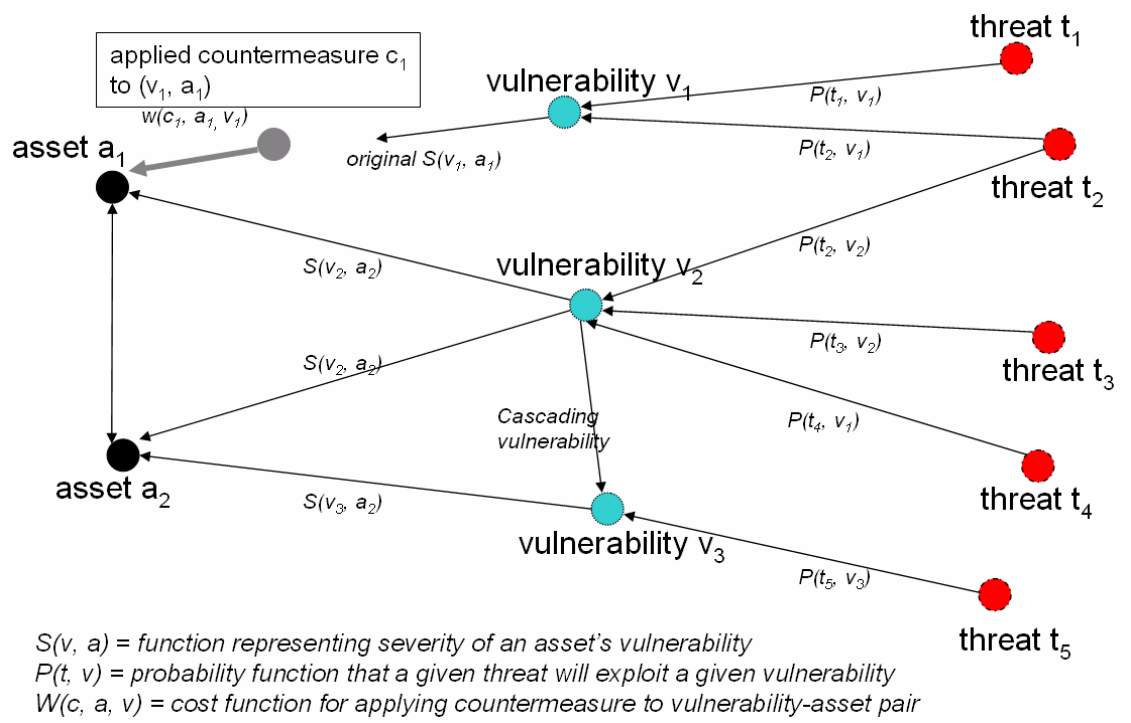


Figure 8. Example Threat Graph Model

Significance of Research

This research should be valuable to those organizations that seek to further refine their information security metrics program. The findings and conclusions of this research can be used by an organization to introspectively examine its own program. The checklists mentioned above, and included in Appendix B will be useful to remind organizations of what is important in an information security metrics program.

The information can easily be converted into a checklist format. The information was derived from a thorough, although still incomplete, review of the literature and represents the lessons learned from over 150 different sources. Duplicate information has been taken out whenever possible, but the checklists should also be checked for discriminant validity before implementing them in a survey instrument or as an organizational tool. This will ensure that the constructs being measured are cleanly and clearly defined and separated, and will help future researchers evaluate different programs. Also, even though the measures came from a review of the literature, it is also important to ensure that though those items should be checked for face validity to ensure they meet standard, current, and accepted practices and taxonomies of information security management.

Limitations of This Research

There are some limitations in this research due to time factors, availability of information, and access. Some of these limitations included the lack of a detailed program review, many issues were left uncovered, there was a limited pool of people to talk to and not all applicable documents were reviewed.

First, this research was only capable of tackling a high-level review of the information security metrics programs. There were many details and issues not covered by the case study. Even though the research gathered a big-picture look of the program, there may be inaccuracies because of the small number of subjects interviewed and the number of documents that could be feasibly analyzed to represent the cases.

The subjects typically came from the same parts of an organization, or were networked in some respects. This may have contributed to a bias related to the interviewees' perspectives of the organization, and their views and mindsets on where problems lie and how to solve them. A more comprehensive organizational study would take accounts of personnel collecting metrics, leaders who use the metrics, analysts, process architects, and so forth. This research relied typically on the process architects' view of the world.

Another limitation is that corporate organizations are not represented. Though all the organizations' cases are not exactly the same, none of the organizations has any involvement with shareholders and the requirements imposed on companies due to Sarbanes-Oxley. Also, the motivations of corporations are different than the motivations for the military or NASA. Although fiscal responsibility is important for all the cases we studied, the *bottom line* is not the primary measure of success in the military or in NASA's JPL.

The final limitation is that even though the organizations involved are extremely complex, it is impossible to capture every aspect of an organization in a case study. A case study simply seeks to investigate an event or circumstance, and does so from a particular model of the world. All that can be presented in this thesis is a model of how the data from the analysis fits together. It may represent some parts of the actual organization, but it may fail to represent, or misrepresent other parts of the organizations studied. It is like the saying "all models are wrong…but some are useful." Hopefully this model can be used to improve information security metrics programs in other organizations.

Suggestions for Future Research

The following are some research problems that present themselves after this effort:

1. Is the IA control selection problem NP complete?

It is very difficult to cover everything in an information assurance metrics program. Constantly, managers have struggled with finding the "optimum" mix. There are many optimality problems that are NP-complete. It may be of interest to discover if the selection of the optimal controls and the optimal spending for those controls is part of the class of problems that are nondeterministically solvable in polynomial-order time.

2. Is greater organizational complexity related to a slower *time to market* for implementation of security controls or configurations?

We have seen how the DOD and Air Force had a difficult time developing, and are still developing their IA metrics programs. Many of the required elements, such as data standards, are not in place yet, and won't be for several years. Is this difficulty due to the complexity of the organization, or is it due to something else, like the cost of upgrading the systems that would support this kind of standardization?

3. How can an organization simplify its existing processes and reduce unnecessary complexity?

Since we've partially demonstrated that DOD and Air Force's complexity has made it challenging for those organizations to create a single, manageable

enterprise information assurance metrics program, how do we fix the problem. It is one part of an answer to identify that a problem exists, but it is an entirely different matter to solve that problem. A standard methodology for doing so would be highly valuable to many organizations, not just the DOD and Air Force.

4. Does the use of different types of data lead to better decisions than others?

There has been a lot of talk that metrics need to be time-focused, or SMART, or quantitative, or meaningful, with data that is primarily ratio data. The question is: does better metrics actually lead to better decisions? What are the factors that are involved with that relationship, if it exists?

5. How important are low-level risk assessments in actually improving the information assurance posture of an organization?

There has been much research about how to characterize information security and assurance and how to make low-level risk calculations. Many of these ideas and methods rely heavily on guesswork or information that is not available. Is this goal of finding the perfect characterization of the problem worth it? Is it valuable to know the percentage of risk, or would it be more valuable to heuristically just fix the problems that the security manager knows

about and can handle. At what level of precision do decision makers need their calculation or risks in order to make good decisions?

6. How are personal or organizational rewards such as compensation, increased staff, budget, and authority related to metrics selected?

This research and the literature review have hinted that rewards are tied to performance. If rewards are tied to metrics as well, and the organizations or people generating and creating those metrics are the people who will benefit from the rewards, does that phenomenon affect what metrics are created? If so, how?

Summary

In this thesis, we have explored three different information security metrics programs with the main goal of finding out what their decision and communications processes really looked like and how they were structured. We have learned what factors the literature suggests are important for an information security metrics program, and we have compared those factors to what organizations think are important for their metrics programs. We have identified the qualities of good metrics from the literature, and in a general sense compared that against what kind of metrics the different organizations are collecting and using to make decisions and manage information assurance.

We found that the Department of Defense had the most complicated and complex organization and thus the most complex information security metrics program. This complexity makes it difficult for the DOD to establish control over the processes that feed in, support, and depend on its metrics program.

We found that the DOD's goals are aligned with commonly accepted literature and standards, but that being at a strategic level of an enormous organization with many budgetary concerns, return on investment is crucial. Mission effectiveness is almost an implicit goal for the DOD's metrics program, because it is such a large part of the DOD's goals and purpose.

The DOD had a great deal to do with creating the standards used by NIST and others, and has been one of the leads in developing research and work in information security and assurance, but in the future, and possibly the present, it may find itself behind its competitors, such as other nation states, if it can't react faster, be more proactive, and much more flexible. Unfortunately, the momentum and political gravity it would take to change these kinds of issues in the DOD are not going to be in the toolset of personnel who would typically be interested in this thesis.

We discussed the U.S. Air Force and its organizational structure and the problems that are associated with that as well. The U.S. Air Force, as a child of

the Department of Defense, has many of the same traits as its parent organization. The bottom-up approach and attempt to organize massive amounts of information characterize the Air Force's program. It is also very slow to market though: the Air Force's program is also just emerging and getting off the ground, even though measurements in management and other programs have been around for many years.

The domain of information security is not much different from the domain of aircraft maintenance, and a discrete set of highly useful and highly effective aircraft maintenance metrics abound in all flying and flying support organizations in the Air Force.

We discussed NSA's Jet Propulsion Lab and the unique challenges it faces to keeping its information systems secure, but also how it used automation to as much advantage as possible. The JPL program really comes out on top in all areas, but in some respects, it may not be a fair comparison. The size of JPL compared to the size of the Air Force represents almost an insignificant fraction. Though JPL operates at the enterprise level, the Air Force, and especially DOD operate at what I would call the *super-enterprise* level. *So* it is not fair to say that the Air Force should copy JPL's programs, because many of JPL's programs

wouldn't translate to that *super-enterprise* level, and may not even be useful for the larger organizations. It is an interesting contrast though.

The research concluded that data calls are prevalent in all the organizations, but most notably in those where automation hasn't taken hold as strongly or as completely. Officials in the U.S. Air Force's and DOD's IA divisions report that they are seeking to apply automation to all areas possible, but they don't see data calls ever going away. It is too much a part of the military and the culture of getting answers fast and getting things done.

It has been the goal of this thesis to explore these areas. It constructed several propositions to develop the ideas, and examined multiple aspects of these different programs, but it is ultimately up to the reader to externalize the data from these case studies and this analysis to the organization that he or she is a part of. Even more important, it is up to the reader to learn how to apply the information in this thesis in creative and effective ways to keep those systems and the information in them safe from harm and useful to the people who need it.

Appendix I. Interview Questions

A: General

What does your organization measure?

- How does your organization measure it?
- Where are counts/measurements taken?
- How often/when are counts/measurements taken?
- Is it a measurement, a count, or a trend?
- What tools does your organization use to measure it?

What trends does your organization track for internal use?

How is this information collected and stored?

B: Measurement planning

How does the organization decide and plan what to measure?

How does the organization decide and plan how to measure?

How often/when does the organization plan measurement or change measurement strategies?

C: Data reporting

How is information reported or upchannelled?

What information security information is reported up?

Who/what organization is information security information reported up to?

Where is information security information briefed or reported?

What are the motivations for reporting the information?

What information may be lost when upchannelled?

D: Data capture

How is data capture done?

How is data analysis done?

What tools are used to collect data?

How are data calls requested?

- What metrics are generated by data calls?
- What types of data calls does this organization request?
- Who/what organization requests data calls?
- Where/through what medium are data calls requested?
- How often/when are data calls requested?

How does data mining or KDD play into the data capture?

Are executive information systems or decision support systems used to make decisions?
How does tacit knowledge feed into decision making?

E: Data normalization and transformation
How is data standardized, normalized, or transformed?

F: Decision making
How do metrics support decision making?
How are decisions made with metrics?
What decisions are made with metrics?
When, how often, and where are decisions made?
Why are particular decisions made based on information security metrics support?

Appendix II. Desirable Properties for Information Security Programs

Enables protection against threats
Enables detection of new threats
Enables reaction to malicious events
Has a goal of confidentiality of information
Has a goal of integrity of information (including non-repudiation and authentication)
Has a goal of availability of information
Manages security organization and infrastructure
Manages security policy, standards, and procedures
Manages security baselines and risk assessments
Manages security awareness and training programs
Manages Compliance
Access control systems and methodology
Business continuity planning and disaster recovery planning
Law, investigation, and ethics
Operations security
Security architecture and models
Applications and systems development security
Cryptography
Physical security
Security management practices
Telecommunications and network security
Uses management and policy measures
Uses personnel measures
Uses operational measures
Uses business continuity planning measures
Uses physical security measures
Guards against viruses
Guards against outside intrusions
Guards against damage from insiders
Guards against equipment theft
Guards against denial of service
Guards against unauthorized use or misuse of computing systems
Guards against loss, alteration, or compromise of data or software
Guards against monetary or financial loss due to negative security events

Guards against loss or endangerment of human life from negative security events
Guards against loss of trust in computer/network systems
Guards against loss of public confidence
Guards against lost business
Guards against detecting and correcting costs
Guards against potential legal liability
Considers people issues
Considers technology issues
Considers procedural issues
Gets executive-level buy in and visible support and commitment from management
Aligns strategically with the organization's goals
Has a strategic security plan
Considers most seious potential outcomes and impacts
Considers the most common threats
Considers costliest aspects of current security program
Considers current risks
Considers cost of security events
Security policy, objectives and activities reflect biz objectives
Approach to implementing security is consistent with organizational culture
Program administrators understand security requirements, risk assessments and risk management
Program is effectively marketed to to all managers and employees
Guidance and policy is distributed to all managers, employees and contractors
Provides appropriate training and education
Involves comprehensive and balanced system of measurement
Incorporates feedback and suggestions for improvement

Appendix III. Desired Properties for Security Metrics/ Risk Assessment Programs

Identifies and isolates security problems
Determines security trends
Measures effectiveness of security measures
Provides security accountability
Determines what to protect
Determines how much assets are worth
Determines what depends on the assets
Determines what potentially threatens an asset
Determines what weaknesses exist
Determines what potential loss exists
Helps decide what controls to put in place to reduce or eliminate threat
Values information based on market forces
Values information based on official value established by an authority
Values information based on expert opinion/appraisal
Values information based on contract
Values information based on cost of creation or re-creation
Values information based on exclusive possession
Values information based on utility
Values information based on ability to interchange in trade
Values information based on operational impact
Values information based on confidentiality requirements
Values information based on expectations of availability
Values information based on requirements for integrity
Measures based on performance criteria
Measures based on temporal criteria
Measures based on process criteria
Measurements and processes align to strategic level organizational goals
Administers implementation metrics
Administers effectiveness/efficiency metrics
Administers impact metrics (business impact of negative events)
Steers business decisions
Creates direction
Reduces costs
Measures against a plan

Compares against self over time to show progress
Compares against industry/peers to show relative position
Uses quantitative measures
Uses qualitative measures
Has a consensus on how metrics are gathered
Metrics are gathered by automated means
Metrics are analyzed to provide insight into problems
Metrics are collected through data calls
Metrics program has strong upper management support
Metrics program includes practical security policies and procedures
Metrics program includes its own quantifiable performance metrics
Metrics program includes results-oriented metrics analysis
Metrics are prioritized according to a standard
Measures existing and stable processes
Considers criticality of application processes
Considers value, sensitivity, or criticality of information involved
Considers past experience of system infiltration and misuse
Considers extent of system interconnection
Uses a security or risk assessment framework
Uses best practices
Uses a risk assessment method
Employs malware protection
Employs patch management and change management
Employs identity and access management including privilege assignment and authentication
Employs firewalls at workstation, host, sub-net, and perimeter levels
Employs configuration management

Appendix IV. Desired Properties of Metrics

Metrics are specific
Metrics are measurable
Metrics are actionable
Metrics are relevant
Metrics are time-determinant
Metrics have a purpose
Metrics fit within decision making process
Metrics are simple to collect
Metrics are not costly to obtain
Metrics are repeatable
Metrics demonstrate relationship to other metrics
Metrics are independently verifiable
Metrics are transparent (not a black box)
Metrics have coverage of the domain
Metrics answer a question
Metrics do not conflict
Metrics are hierarchical
Metrics lead to discovery
Metrics arise from discovery
Metrics are prescriptive

Appendix V. Human Subjects Exemption

DEPARTMENT OF THE AIR FORCE
AIR FORCE MATERIEL COMMAND
WRIGHT-PATTERSON AIR FORCE BASE OHIO

18 December 2006

MEMORANDUM FOR AFIT/ENV (Capt Adam Bryant)

FROM: AFRL/Wright Site Institutional Review Board

SUBJECT: Request for exemption from human experimentation requirements

1. Protocol title: Organizational Security Metrics Case Study

2. Protocol number: F-WR-2007-0024-E

3. The above protocol has been reviewed by the AFRL Wright Site IRB and determined to be **exempt** from IRB oversight and human subject research requirements per 32 CFR 219.101(b)(2) which exempts "research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior."

4. This exemption applies only to the requirements of 32 CFR 219, DoDD 3216.2, AFI 40-402, and related human research subject regulations. If this project is a survey, attitude or opinion poll, questionnaire or interview, consult AFI 36-2601, Air Force Personnel Survey Program, for further guidance. Headquarters AFPC/DPSAS is the final approval authority for conducting attitude and opinion surveys within the Air Force.

5. The IRB must be notified if there is any change to the design or procedures of the research to be conducted. Otherwise, no further action is required.

6. For questions or concerns, please contact the IRB administrator, Helen Jennings at (937) 904-8094 or helen.jennings@wpafb.af.mil OR Lt. Douglas Grafel at douglas.grafel@wpafb.af.mil or (937) 656-5437. All inquiries and correspondence concerning this protocol should include the protocol number and name of the primary investigator.

JEFFREY BIDINGER, Maj, USAF, MC, FS
Chair, AFRL/Wright Site IRB

References

(ISC)2 (2006). (ISC)2 website. www.isc2.org.

107th Congress (2002). Public Law 107-347. December 17, 2002.

AF Audit Agency (2006). Air Force Audit Agency website. Retrieved from the World Wide Web December, 2006. https://www.afaa.hq.af.mil

AF/CIO (2002). Air Force Information Strategy. Office of the Chief Information Officer, United States Air Force.

AF/CIO (2004). Air Force Information Resource Management Flight Plan, Office of the Chief Information Officer, United States Air Force.

Air Force Systems Command. (1991). *The Metrics Handbook*.

Alderson, D., & Hoo, K. S. (2005). The role of economic incentives in securing cyberspace. [Electronic version]. Iis-db.stanford.edu

Aldrich, R. (2006). 2006 CND Assessment. Agencies and Field Activities Workshop, 8 Dec 2006.

Ameri, A. (2004). The five pillars of information security. *Risk Management*. 51 (7). ABI/INFORM Research pg. 48.

Antanitus, D. (2003). The business of metrics--measuring the product of the plan: how do you know what you know? *Management & Measurement. Program Manager*. 32.2 (March-April 2003): p10(5).

ASD(NII)/DIAP. (2006). Telephone and e-mail communications with members and leaders of the Defense Information Assurance Program, December, 2006.

Bensbasat, I. et. al. (1987). The Case Research Strategy in Studies of Information Systems. *MIS Quarterly*, September.

Bentley, R. S. (2005). Security measures and investments. [Electronic version]. Assignment in partial fulfillment of IMGT 684, managerial aspects of information warfare, Air Force Institute of Technology.

Berinato, S. (2002). Finally, a real return on security spending. [Electronic version]. Chief Information Officer (CIO) Magazine.

Berinato, S. (2005). A few good metrics. [Electronic version]. CSO Magazine Online.

Blakley, B. (2002). The measure of information security is dollars. Paper presented at the *Workshop of Economics and Information Security*. [Electronic version]. Cl.cam.ac.uk.

Boeckmann, C. (2003). Achieving executive buy-in: The case for security. [Electronic version]. GSEC Practical Version 1.4b, BPMetricsTeamReportFinal111704Rev11005.pdf

Bryant, A., and Grimaila, M. (2007). Developing a Framework to Improve Information Assurance Battlespace Knowledge. Paper presented at the *Proceedings of the ICIW*.

Campbell, C. A., and Gutterman, G. M. (1993). *The Development and Demonstration of the Metric Assessment Tool*. Master's Thesis. Air Force Institute of Technology.

Campbell, K. (2003). The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. [Electronic version]. *Journal of Computer Security*, 11(3), 431-448.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. [Electronic version]. *Communications of the ACM*, 47(7), 87-92.

CERT Coordination Center,Carnegie Mellon University. (2003). CERT/CC overview incident and vulnerability trends. [Electronic version].

Chan, Y. E. (2000). IT value: The great divide between qualitative and quantitative and individual and organizational measures. [Electronic version]. *Journal of Management Information Systems*, 16(4), 225-261.

Chan, Y. E., & Huff, S. (1993). Strategic information systems alignment. [Electronic version]. *Business Quarterly*, 58(1), 51-55.

Cisco Systems Inc. (2001) Economic impact of network security threats. Cisco White Paper.

Cisco Systems Inc. (2001). The return on investment for network security. Cisco White Paper.

Committee on National Security Systems. (2005). CNSS Instruction no. 4009. National Information Assurance (IA) Glossary. [Electronic version].

Corporate Information Security Working Group (2004). Report of the best practices and metrics team. November 17, 2004.

CSI/FBI. (2004). The 2004 CSI/FBI computer crime and security survey. [Electronic version].

CSI/FBI. (2005). The 2005 CSI/FBI computer crime and security survey. [Electronic version].

Deloitte Touche Tohmatsu. (2003). 2003 Global security survey

Deloitte Touche Tohmatsu. (2005). 2005 Global security survey

Department of Defense. (2007). Department of Defense Organizational Structure. http://www.dod.mil/odam/omp/pubs/GuideBook/DoD.htm #Department%20of%20Defense. Retrieved from the World Wide Web January, 2007.

Department of Defense. (2006). Defense-wide Information Assurance Program. http://www.dod.mil/cio-nii/infoassurance /diap/index.html. Retrieved from the World Wide Web December, 2006.

DOD IAD. (2006). Conversation with members from the Department of Defense's Information Assurance Directorate. December, 2006.

Department of Trade and Industry. (2004). DTI information security breach survey. PriceWaterhouseCoopers.

DISA. (2006). Information Assurance Policy and Guidance. The Defense Information Systems Agency website. http://iase.disa.mil/policy.html. Retrieved from the World Wide Web December, 2006.

DISA. (2007). Public Key Infrastructure. The Defense Information Systems Agency website. (http://iase.disa.mil/pki/. Retrieved from the world Wide Web January, 2007.

Dinnie, G. (1999). The second annual global information security survey. [Electronic version]. *Information Management & Computer Security*, 7(3), 112-120.

Earl, M. J. (1993). Experiences in strategic information systems planning. [Electronic version]. *MIS Quarterly*, 17(1), 1-24.

E-Government Act of 2002 (H.R. 2458/S. 803). December 17, 2002.

Erwin (2002). Citation lost.

Everett, C. (2006). Bridging the gap between computer security and legal requirements. [Electronic version]. Infosecon.net

Ewen, R. B. (1998). *An Introduction to Theories of Personality*. 5th ed. New Jersey: Lawrence Erlbaum Associates.

Field, T. (2000). SECURITY: Protection money. [Electronic version]. *CIO*. Framingham MA, 14(1), 172-180.

Forlani, D. (2002). Risk and rationality: the influence of decision domain and perceived outcome control on managers' high-risk decisions. [Electronic version]. *Journal of Behavioral Decision Making*. 15 (2). pp. 125 – 140.

Foster, N., & Yong-Gon, C. (2004). Justifying security spending: how to make a business case for information security. TruSecure white paper. [Electronic version].

Geer, D. (2004). Security Metrics. Presentation at the 2004 USENIX Conference.

Geer, D. (2004). Metrics, economics and shared risk at the national scale. [Electronic version].

Geer, D., Soo Hoo, K. J., & Jaquith, A. (2003). Information security: why the future belongs to the quants. [Electronic version]. *Security & Privacy Magazine, IEEE*, 1(4), 24-32.

General Accounting Office (2004). *Technology Assessment: Cybersecurity for Critical Infrastructure Protection*. GAO-04-321. [Electronic version].

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. [Electronic version]. *ACM Transactions on Information and System Security (TISSEC)*, 5(4), 438-457.

Gordon, L. A., Loeb, M. P., & Sohail, T. (2003). A framework for using insurance for cyber-risk management. [Electronic version]. *Communications of the ACM*, 46(3), 81-85.

Hall, J. (2001). Selling security to management. [Electronic version]. SANS InfoSec Reading Room. July, 2001.

Hamilton, C. R. (1998). New trends in risk management. [Electronic version]. *Information Systems Security*, 7(1), 70-78.

Henning, R. R. (1999). Security service level agreements: Quantifiable security for the enterprise? [Electronic version]. *Proceedings of The 1999 Workshop On New Security Paradigms*, 54-60.

Hinson, G. (2003). Human factors in information security. NOTICEBOARD white paper. http://www.cisecurity.org/Documents/

Hobbs, B. G. (2005). *Barriers to Electronic Records Management (ERM): An Exploratory Case Study Investigating ERM in the Deployed Environment During Operations Enduring Freedom and Iraqi Freedom* [Electronic version]. Master's Thesis, Air Force Institute of Technology.

Hong, K. S., Chi, Y. P., Chao, L. R., & Tang, J. H. (2003). An integrated system theory of information security management. [Electronic version]. *Information Management and Computer Security*, 11(5), 243-248.

Interagency Working Group on Cyber Security and Information Assurance. (2006). Federal plan for cyber security and information assurance research and development. [Electronic version].

(ISC)². (2006). International Information Systems Security Certification Consortium (ISC)² website. www.isc2.org. Retrieved from the World Wide Web June 2006.

International Organization of Standardization. (2000). ISO/IEC 17799. *Information Technology - Code of Practice for Information Security Management.* [Electronic version].

International Organization of Standards. (2000). ISO/IEC 27001. *Information Technology Security Techniques: Information Security Management Systems Requirements.* [Electronic version].

International Organization of Standards. (2000). TR 13335-4. *Information Technology - Guidelines for the Management of IT Security, part 4: Selection of safeguards.* [Electronic version].

Jaquith, A. (2006). Escaping the hamster wheel of pain: Risk management is where the confusion is. [Electronic version]. www.securitymetrics.org

Jones, B. (2005). Overview of DOD defense in depth strategy. GIAC GSEC practical 1.4c. [Electronic version].

JTF-GNO (2007). Joint Task Force for Global Network Operations web site. https://www.jtfgno.mil/misc/mission.htm. *PKI certificate required*.

Kadrich, M. (2007). Re: Mini-Metricon. Message posted to www.securitymetrics.org mailing list.

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. [Electronic version]. *Econometrica*, 47(2), 263.

Kahraman, E. (2006). Evaluating IT security performance with quantifiable metrics. [Electronic version].

Kerr, S. (1995). On the folly of rewarding A while hoping for B. [Electronic version]. *Academy of Management Executive*, 9(1), 7.

LaRocca, J., & LaRocca, R. (2002). *802.11 demystified.* New York: McGraw-Hill New York.

Leedy, P.D., and Ormrod, J.E. (2005). *Practical Research: Planning and Design.* 8th ed., Upper Saddle River, NJ: Prentice-Hall.

Liou, P., Meeson, R., Swart, W., Adams, M. (2006). DoD IA/CND Metrics Assimilation: In Progress Review Briefing (DRAFT).

Marty, R., (2007). Re: Mini-Metricon. Message posted to www.securitymetrics.org mailing list.

May, T. A. (1997). The death of ROI: Re-thinking IT value measurement. [Electronic version]. *Information Management & Computer Security*, 5(3), 90-92.

McCarthy, L. (2003). *IT Security: Risking the Corporation*. Upper Saddle River, NJ: Prentice-Hall.

McClave, J. & Benson, G. (2003). *Statistics for Business and Economics*. New York: Maxwell Macmillan.

Meyer, G. S., Raul, A. C., & Frank, R. V. (2001). Liability for computer glitches and online security lapses. [Electronic version].

Michalewicz, Z., and Fogel, D. B. (2002). *How to Solve It: Modern Heuristics. Berlin: Springer-Verlag.*

Miles, M. B., and Huberman, A. M. (1994). *Qualitative Data Analysis: An Expanded Sourcebook*. Thousand Oaks: Sage Publications.

Miller, R. L., and Hope, S. A. (2003). ITSDB/SPL: The Management Toolset for Enterprise IT Security Programs. [Electronic version]. JPL/Caltech New Technology Report #40405.

Moreno, K., Kida, T., & Smith, J. F. (2002). The impact of affective reactions on risky decision making in accounting contexts. [Electronic version]. *Journal of Accounting Research*, 40(5), 1331-1349.

Munley, M. (2004). Moving from consciousness to culture: creating an environment of security awareness. [Electronic version]. GSEC Practical Assignment version 1.4b, Option 1. April 10, 2004.

National Aeronautics and Space Administration (2005). NASA Facts: Jet Propulsion Laboratory. [Electronic version]. jpl.nasa.gov

NIST Special Publication 800-12 (1995). An Introduction to Computer Security: NIST Special Publication 800-12. [Electronic version].

NIST Special Publication 800-26 (2001). *Security Self-Assessment Guide for Information Technology Systems*. [Electronic version]. National Institute of Standards and Technology. November 2001.

NIST Special Publication 800-53 (2005). *Recommended Security Controls for Federal Information Systems.* [Electronic version]. National Institute of Standards and Technology. February 2005.

NSA IAD (2006). Conversation with members of NSA's Information Assurance Directorate, December 2006.

Papadopoullos, A. (2004). Information analysis and the content supply chain. [Electronic version]. *Supplement to KMWorld*. November/December 2004.

Payne, S. C. (2001). A guide to security metrics. [Electronic version]. The SANS Institute, July 11, 2001.

Perry, W. J., Casado, W., Coleman, K., and Wendlandt, D. (2004). U.S. National Cybersecurity. [Electronic version]. Presentation, MS&E 91SI, Fall 2004. Stanford University.

Poore, R. (2000). Valuing information assets for security risk management. [Electronic version]. Information systems security, 9(9)

Qualys, Inc. (2006). The laws of vulnerabilities: Six axioms for understanding risk. [Electronic version].

Rainey, J.C., McGonagle, R., Scott, B., and Waller, G. (2001). *The Metrics Handbook for Maintenance Leaders*. Air Force Logistics Management Agency.

Raul, A. C., Volpe, F. R., and Meyer, G. S. (2001). Liability for computer glitches and online security lapses. [Electronic version]. *Sidley Information Law and Privacy Practice.*

Ricketts, J. (1990). Powers-of-ten information biases. [Electronic version]. *MIS Quarterly*, 14(1), 63.

Scandura, T. A., and Williams, E., A., (2000). Research methodology in management: Current practices, trends, and implications for future research. [Electronic version]. *Academy of Management Journal*. Dec 2000. Vol 43 (6). pp. 1248-1284.

Schroeder, N. J. (2005). *Using Prospect Theory to Investigate Decision-making Bias Within an Information Security Context.* [Electronic version]. Master's Thesis, Air Force Institute of Technology.

Seddigh, N., Pieda, P., Matrawy, A., Nandy, B., Lambadaris, J., & Hatfield, A. (2004). Current trends and advances in information assurance metrics. [Electronic version]. *Paper presented at the PST 2004*, 197-198.

Shneier, B. (1999). Attack trees: modeling security threats. [Electronic version]. *Dr. Dobb's Journal.* December 1999. www.shneier.com/paper-attacktrees-ddj-ft.html

Siponen, M. T. (2000). Conceptual foundation for organizational information security awareness. [Electronic version]. *Information Management and Computer Security*, 8(1), 31-41.

Sitkin, S., & Weingart, L. (1995). Determinants of risky decision-making behavior: A test of the mediating role of risk perceptions and propensity. [Electronic version]. *Academy of Management Journal*, 38(6), 1573.

Somogyi, E.K., Galliers, R.D. (1994). Information technology in business: from data processing to strategic information systems edited by Galliers, R.D., and Leidner, D.E. (2003) in *Challenges and Strategies in Managing Information Systems.*

Soo Hoo, K. J. (2000). How much is enough?: A risk-management approach to computer security. [Electronic version].

Straub, D.W., Welke, R.J. (1998). Coping with systems risk: security planning models for management decision making. [Electronic version]. Management Information Systems Quarterly. Vol 22 (4) pp. 441-469.

Swanson, M. (1998). NIST Special Publication 800-18. Guide for Developing Security Plans for Information Technology Systems. [Electronic version]. National Institute of Standards and Technology.

Swanson, M. (2001). NIST Special Publication 800-26: Security Self-Assessment Guide for Information Technology Systems. [Electronic version].

Swanson, M. (2003). NIST Special Publication 800-55: Security Metrics Guide for Information Technology Systems. [Electronic version].

Takewell, S. (2005). Understanding NIST 800-37 and DITSCAP. [Electronic version].

The National Science and Technology Council. (2006). Federal plan for cybersecurity and information assurance research and development. [Electronic version].

Tiwari, R. K., and Karlapalem, K. (2004). Cost tradeoffs for information security assurance. [Electronic version]. Proceedings of the *Workshop on the Economics of Information Security*. June 1-3.

Tsoumas, V., & Tryfonas, T. (2004). From risk analysis to effective security management: Towards an automated approach. [Electronic version]. *Information Management & Computer Security*, 12(1), 91-101.

Tudor, J.K. (2001). *Information Security Architecture: An Integrated Approach to Security in the Organization*. Aurbach Publications.

U.S. Department of Defense. (2002). DOD directive 8500.1 - Information Assurance (IA)

U.S. General Accounting Office. (2004). *Technology Assessment: Cybersecurity for Critical Infrastructure Protection* [Electronic version].

Wesner, J. W. (1994). *Winning with quality: Applying quality principles in product development*. New York: Addison-Wesley .

Willcocks, L. P. IT evaluation: Techniques and processes. In *Strategic Information Management*. Edited by Galliers, R.; Leidner, D.; Baker, B. (eds.). Butterworth, 1999.

Wilson, M. (1996). Marketing and implementing computer security. [Electronic version]. Research Paper. National Institute of Standards and Technology.

Wilson, R. A. (2004). Employee dishonesty: national survey of risk managers on crime. [Electronic version]. *Journal of Economic Crime Management.* Winter 2004, 2 (1).

Winkler, I. S. (1996). Case study of industrial espionage through social engineering. Paper presented at the 19th National Information Systems Security Conference.

Wynne, M. W. (2005). Letter to airmen. [Electronic version]. www.af.mil

Yin, R. K. (2003). Case study research: Design and methods. 3rd ed. Thousand Oaks, CA: Sage Publishers.

Zachman, J.A. (1987). A framework for information systems architecture. [Electronic version]. *IBM Systems Journal*, v.26 n.3, p.276-292.

Zviran, M., and Haga, W. J. (1999). Password security: an empirical study. [Electronic version]. *Journal of Management Information Systems;* Spring 1999; 15, 4; ABI/INFORM Research pg. 161.

Vita

Captain Adam R. Bryant was born in West Palm Beach, Florida. He graduated from Dade County High School, Trenton, Georgia in 1996. He enlisted in the Air Force in 1998 and was assigned to F. E. Warren Air Force Base as a Space and Missile Systems Maintenance Technician. While on active duty he completed his associate's degree from the Community College of the Air Force in Space and Missile Systems Maintenance in 2000 and completed his Bachelor of Science degree from Park University in Social Psychology in 2001. Upon graduation, he attended Officer Training School at Maxwell Air Force Base, Alabama.

After his commissioning in May 2002, Captain Bryant was assigned to the 60th Communications Squadron, Travis Air Force Base, California, where he served as the Secure Network Systems Operations Officer and Network Control Chief before deploying to Afghanistan in December 2002. He attended Basic Communications and Information Officer Training after returning from Afghanistan in 2003 and served as Executive Officer for the 60th Communications Squadron and later the 60th Maintenance Group at Travis Air Force Base until 2005.

In August 2005, Captain Bryant entered the Graduate School of Engineering and Management, Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, to pursue a Masters of Science in Information Resource Management and was accepted to a dual-degree program to pursue an additional Masters of Science in Computer Science in June 2006. Upon graduation, he will separate from the Air Force and work and live in Dayton, Ohio.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
22-03-2007	Master's Thesis	Sept 2005 – March 2007

4. TITLE AND SUBTITLE

Developing a Framework for Evaluating Organizational Information Assurance Metrics Programs

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Bryant, Adam R., Captain, USAF

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
Graduate School of Engineering and Management (AFIT/EN)
2950 Hobson Way, Building 640
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/ENV/07-M5

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

Robert L. Miller, PhD, CISSP
NASA JPL
4800 Oak Grove Dr., M/S: 602-149
Pasadena, CA 91109
(818) 354-4349

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION/AVAILABILITY STATEMENT

APPROVED FOR PUBLIC RELEASE; DISTRIBUTION UNLIMITED.

13. SUPPLEMENTARY NOTES

14. ABSTRACT The push to secure organizational information has brought about the need to develop better metrics for understanding the state of the organization's security capability. This thesis utilizes case studies of information security metrics programs within Department of Defense organizations, the United States Air Force (USAF), and the National Aeronautics and Space Administration's (NASA's) Jet Propulsion Lab to discover how these organizations make decisions about how the measurement program is designed, how information is collected and disseminated, and how the collected information supports decision making.

This research finds that both the DOD and USAF have highly complex information security programs that are primarily focused on determining the return for security investments, meeting budget constraints, and achieving mission objectives while NASA's Jet Propulsion Lab seeks to improve security processes related to compliance. While the analytical techniques were similar in all of the cases, the DOD and USAF use communication processes still based mostly on manual data calls and communications. In contrast, NASA's JPL information security metrics program employs a more automated approach for information collection and dissemination.

15. SUBJECT TERMS

Information Security, Security, Computer Security, Corporate Information Management, Data Management, Risk Analysis, Risk Management, Business Process Reengineering

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. Michael R. Grimaila, Ph.D. (ENV)
U	U	U	UU	216	19b. TELEPHONE NUMBER *(Include area code)* (937) 255-3636, ext 4800; e-mail: michael.grimaila@afit.edu

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39-18