UNIVERSITY OF OREGON
APPLIED INFORMATION MANAGEMENT

Presented to the Interdisciplinary Studies Program:
Applied Information Management
and the Graduate School of the
University of Oregon
in partial fulfillment of the
requirement for the degree of
Master of Science

Key Components of an Information Security Metrics Program Plan

CAPSTONE REPORT

Scott E. Schimkowitsch
Senior Security Specialist
Harland Financial Solutions

University of Oregon
Applied Information
Management
Program

July 2009

Continuing Education
1277 University of Oregon
Eugene, OR 97403-1277

This page intentionally left blank

Approved by

____

Dr. Linda F. Ettinger

Academic Director, AIM Program

This page intentionally left blank

Running Head: KEY COMPONENTS OF IT SECURITY METRICS PROGRAM

Key Components of an Information Security Metrics Program Plan

Scott E. Schimkowitsch

Senior Security Specialist

Harland Financial Solutions

This page intentionally left blank

Abstract

An information security metrics program can provide organizations with a resource to manage, monitor, control, or improve aspects of an information security program. A set of five key components necessary to include when developing a plan for an information security metrics program is presented. Components are framed in relation to criteria from Chew et al. (2008), and include associated tasks designed to a) increase accountability, b) improve information security effectiveness and c) demonstrate compliance.

This page intentionally left blank

Table of Contents

List of Tables

This page intentionally left blank

Introduction

Problem

Information security has become an essential business function that is critical to enabling organizations to conduct their operations and deliver services to the public (Chew, Clay, Hash, Bartol and Brown, 2006). The push to secure organizational information has initiated the need to develop better metrics for understanding the state of the organization's security posture (Bryant, 2007). In explanation, Wang (2007) states "It is widely recognized that metrics are important to information security because metrics can be an effective tool for information security professionals to measure the security strength and levels of their systems, products, processes, and readiness to address security issues they are facing" (p. 284).

However, not all organizations utilize security metrics to measure the effectiveness of the overall security posture, though it is the premise of this paper that they should. Herrmann (2007) states "The initial reaction of some organizations or individuals may be fear — fear of implementing a metrics program because of the perhaps unpleasant facts that metrics may bring to light; that is, the proverbial "emperor has no clothes" syndrome (chap. 2.1). Furthermore, it can be very difficult to see any tangible results from work spent on information security. As noted by Bryant (2007), since security involves preventing events or acts from happening, successful security solutions will seem to have no effect at all.

Significance

The goal of this literature review is to address the value of using performance measures to quantify the effectiveness of an organization's information security program. Chew et al.

(2006) defines performance measures as “indicators, statistics, or metrics used to gauge program performance” (p. 10). According to Payne (2006) “a widely accepted management principle is that an activity cannot be managed if it cannot be measured” (p. 2). The belief in the importance to quantify something is not new. Lord Kelvin, a 19th-century physicist stated, "When you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is a meager and unsatisfactory kind" (Geer, 2006, p. 2).

Herrmann (2007) states “the judicious use of metrics promotes visibility, informed decision making, predictability, and proactive planning and preparedness, thus averting surprises and always being caught in a reactive mode when it comes to security” (chap. 2.13). In addition to these purported goals, there are a number of existing laws, rules, and regulations, including the Clinger-Cohen Act, the Government Performance and Results Act (GPRA), the Government Paperwork Elimination Act (GPEA), and the Federal Information Security Management Act (FISMA), that cite information performance measurement in general, and information security performance measurement in particular, as a requirement (Chew et al., 2008).

Stevens (2005) states that the goal of implementing an information security metrics program within an organization is to improve security management capabilities and attain an adequate level of security that directly supports the accomplishment of the mission and strategic drivers. Payne (2006) suggests that the use of metrics can be a useful tool for determining the effectiveness of various components of a security program. Several other authors agree. According to Chew et al. (2008), the benefits of security metrics include increasing accountability for information security performance; improving effectiveness of information security activities; demonstrating compliance with laws, rules and regulations; and providing quantifiable inputs for resource allocation decisions. Swanson et al. (2003) believes that security metrics can be used to facilitate improved understanding, performance, coverage, and decision making of various security processes, mechanisms and procedures. Wang (2007) states that metrics can also help identify system vulnerabilities, providing guidance in prioritizing corrective actions, and raising the level of security awareness within the organization. However, as noted by Hinson (2006), information security professionals and management find "information security is a notoriously difficult area to measure" (p. 2).

Purpose

The purpose of this literature review is to identify and describe key components necessary to include when developing a plan for an information security metrics program. The notion of a "component" is generically defined as "a constituent part" (Component, n.d.). Based on a preliminary review of the literature, there are a variety of terms used to describe these parts (e.g. stage, step, phase, and component) and various approaches to both the number and description of individual parts. The goal is to select four prominent plans described in the literature, conduct comparisons among the approaches, and extrapolate a set of key components that can function as a pre-selected set for use during the conceptual analysis process. "Prominent", in this case, is defined as "widely and popularly known" in the information security community (Prominent, n.d.). Final presentation of the identified components is framed within criteria provided by Chew et al. (2008), who suggests that performance measures should be designed to (a) increase accountability, (b) improve security effectiveness, and (c) demonstrate compliance.

Audience

Security professionals are now being asked to measure the value of their information security programs and demonstrate the continuing maturity of their organizations (Sundaram, 2008). Payne (2006) believes that the use of metrics can be an effective tool for determining the effectiveness of various components of a security program. This review is intended to be valuable to information technology professionals who need to design an effective information security program and those who manage information security initiatives. These security professionals must see the role of security and asset protection through the eyes of the receiver, corporate management and the share holder, in order to better understand how best to communicate with management and gain management support (Kovacich & Halibozek, 2006).

Outcome

In accordance with the general goals suggested by Hewitt (2002) the outcome of this literature review is a "concise summary of previous findings" that will "provide an up-to-date picture" and "reveal common findings", in this case related to identification of a set of key components necessary to the development of an information security metrics program plan (p. 1-3). Chapin (2005) states it has always been difficult to quantify the effectiveness of an organization's security efforts. In order to provide information security professionals with a tool useful to support their efforts, components are presented in the form of a guide that describes the key components of an information security metrics program plan. Key components are framed with attention to three overarching criteria provided by Chew et al. (2008, p. 10):

1. Increase Accountability: Information security measures can increase accountability for information security by helping to identify specific security controls that are implemented incorrectly, are not implemented, or are ineffective.

2. Improve Information Security Effectiveness: An information security measurement program will enable organizations to quantify improvements in securing information systems and demonstrate quantifiable progress in accomplishing agency strategic goals and objectives.

3. Demonstrate compliance: Organizations can demonstrate compliance with applicable laws, rules, and regulations by implementing and maintaining an information security measurement program.

Limitations

Time frame. Jansen (2009) recently stated that "security metrics is an area of computer security that has been receiving a good deal of attention lately" (p.1). Patriciu (2006) states that an increased interest in using standardized metrics to measure information security has taken place over the last several years. Since the use of metrics to quantify the performance of information security is a relatively new field, material used in this literature review is limited to publications in the last five years (2004 to 2009) (Leedy and Ormrod, 2005, p.65).

Type of sources. Material was selected from academic, government, professional, and association literature including books, journals and Web sites. Academic and government material provides practical and theoretical background for the study. Professional and association literature provides industry best practices and examples of information security metrics currently used. When searching online resources, .edu and .org sites are preferred and ".gov" (government) and ".mil" (military) sites are generally considered reliable (Leedy & Ormrod, 2005).

Selection criteria. The primary search engines for literature retrieved for review were Clusty, Google, Google Scholar, and Yahoo. The primary databases used for the finding literature were ACM Digital Library, Summit, and WorldCat. Online databases were searched using a set of keywords that included "security metrics" or related key terms. During the review process, "other people's conclusions" were not accepted "at face value," but rather "justified based on the data presented" (Leedy & Ormrod, 2005, p. 77).

Resources reviewed were evaluated with the checklist developed by Leedy and Ormrod (2005):

- Did experts in the field review the resource before being published?
- Can the focus of the author's work be determined?
- Does the article describe the collection of data or does it describe and synthesize other studies in which data was collected?
- Is the article logically organized and easy to follow?
- Does the article contain a section that outlines and reviews previous work in the field?
- Is there agreement with the interpretation of the results?

Audience. This document is intended for information security professionals who need to design and manage the effectiveness of an information security program, specifically Chief

Information Security Officers (CISO), security managers, and security consultants. For this review, CISO (also referred to as the Chief Security officer or CSO, Director of Information Security, or Information Security Manager) is defined as the person responsible for the assessment, management, and implementation of the security program that secures the organization's information (Whitman & Mattord, 2008).

Topic definition. Security metrics are an emerging field of study for information security professionals (Jaquith, 2007) and can have different definitions (Sundaram, 2008) throughout the IT security community. Some authors draw distinctions between the term security metrics and security measurements and others use the terms interchangeably. Payne (2006) states, "Measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing to a predetermined baseline two or more measurements taken over time" (p.1). Others, such as Chew et al. (2008) agree that a case can be made for using different terms for more detailed and aggregated items, such as "metrics" and "measures," but standardized in a single term. For this literature review, the term information security metrics is defined as measures used to indicate progress or achievement that can be improved upon (Sundaram, 2008).

Focus selection. Security metrics can be utilized in many ways to benefit an organization, including increasing accountability, improving security effectiveness, and demonstrating compliance (Chew et al., 2008). The focus of this literature review is to identify and describe the key planning components needed to construct a successful security metrics program within an organization, in light of these three criteria. Key components are extrapolated from four prominent plans described in the literature after conducting comparisons among the approaches.

The framing approach of this review is based from the criteria of National Institute of Standards and Technology's (NIST) document, Performance Measurement Guide for Information Security resource (Chew et al., 2008). NIST is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce which is responsible for developing standards and guidelines, including minimum requirements that enhance economic security. Multiple resources used in this literature review cite the NIST publication including (Chapin, 2005), (Garigue & Stefaniu, 2003), (Kark, 2008), (Kahraman, 2005), and (Patriciu, 2006).

Preview of Data Analysis and Writing Plans

Data Analysis. According to Busch et al. (2005), there are two types of content analysis: conceptual analysis and relational analysis. This literature review utilizes conceptual analysis. Conceptual analysis is a type of content analysis in which a concept is chosen and analyzed by quantifying and tallying its presence (Busch et al., 2005). Busch et al. (2005) outline eight coding steps for conducting the conceptual analysis. Details of these eight steps are provided in the Research Parameters section of this paper.

Writing Plan. Leedy and Ormrod (2005) state a literature review "evaluates, organizes, and synthesizes what others have done" (p. 77). Synthesis is a re-organization that gives a new interpretation of old material or combines new with old interpretations (Literature review, 2007, para. 5).

The Writing Plan for the Review of Literature section of this paper adopts a "thematic" approach. (Literature review, 2007, para. 27). In this case, themes are defined as "key components" of an information security metrics program plan. The goal is to provide an ordered guide of components necessary to develop an information security metrics program plan. These identified components are extrapolated from multiple sources and categorized as themes, in relation to three overarching criteria provided by Chew et al. (2008): (a) increase accountability, (b) improve information security effectiveness, and (c) demonstrate compliance. Details of the full Writing Plan are provided in the Research Parameters section of this paper.

Definitions

The specialized terms used within this literature review are defined from the selected literature, academic sources, and reference materials. As noted by Leedy and Ormrod (2005), “Each term must be defined operationally; that is, the definition must interpret the term as it is used in relation to the researcher’s project” (p. 56).

Benchmarking is described as the “process of comparing one’s own performance and practices against peers within the industry or noted ‘best practice’ organizations outside the industry.” The process provides different perspectives for managing an activity, but also can “provide comparative data needed to make metrics more meaningful.” Benchmarks also help establish “achievable targets for driving improvements in existing practices” (Payne, 2006, p. 6).

Chief Information Security Officers (CISO) also called the Chief Security officer or CSO, Director of Information Security, or Information Security Manager, is responsible for the assessment, management, and implementation of the security program that secures the organization’s information (Whitman & Mattord, 2008).

Clinger-Cohen Act of 1996 provides that the government information technology shop be operated exactly as an efficient and profitable business would be operated. The intention of the law is to "reform acquisition laws and information technology management of the Federal Government”. CCA emphasizes an integrated framework of technology aimed at efficiently performing the business of the Department. http://www.ed.gov/policy/gen/leg/cca.html

Component is defined as a constituent part or element. A component is any smaller, self-contained part of a larger entity. (Component, n.d.)

Federal Information Security Management Act (FISMA) requires federal agencies to provide appropriate protection of their resources through implementing a comprehensive information security program that is commensurate with the sensitivity of the information being processed, transmitted, and stored by agency information systems. It also requires agencies to assess and report their performance in implementing and managing their information security programs (Chew et al., 2008).

Government Paperwork Elimination Act (GPEA) requires Federal agencies, by October 21, 2003, to allow individuals or entities that deal with the agencies the option to submit information or transact with the agency electronically, when practicable, and to maintain records electronically, when practicable. The Act specifically states that electronic records and their related electronic signatures are not to be denied legal effect, validity, or enforceability merely because they are in electronic form, and encourages Federal government use of a range of electronic signature alternatives. http://www.whitehouse.gov/omb/fedreg/gpea2.html

Government Performance and Results Act (GPRA) focuses on improving security program effectiveness and efficiency by adequately articulating program goals and providing information on program performance (Chew et al., 2008).

Information Security is the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information, through the application of policy, training and awareness programs, and technology (Whitman & Mattord, 2008).

Information Security Metrics are used to facilitate decision making and improve performance and accountability through the collection, analysis, and reporting of relevant performance-related data (Chew et al., 2008)

Information Security Program, also referred to as security program or program, describes the structure and organization of the effort that strives to contain the risks to the information assets of the organization (Whitman & Mattord, 2008).

InfoSec is an abbreviation for "information security" and was primarily used in the military (INFOSEC) and migrated to commercial parlance. See Information Security (InfoSec, n.d.).

Inventory refers to an itemized catalog or list of tangible goods or property, or the intangible attributes or qualities (Inventory, n.d.).

Keywords are words or short phrases summarizing your research topic that can point you toward potentially useful resources (Leedy & Ormrod, 2005).

Metrics are tools designed to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data (Swanson et al., 2003).

Prominent is defined as widely and popularly known or readily noticeable (Prominent, n.d.).

Risk Management is the process of determining an acceptable level of risk, assessing the current level of risk, taking steps to reduce risk to the acceptable level, and maintaining that level of risk (Geer, 2006).

Security Consultant is typically an independent expert in some aspect of information security (Whitman & Mattord, 2008).

Security Manager is a member of an organization accountable for the day-to-day operation of the information security program, accomplishing the objectives identified by the CISO (Whitman & Mattord, 2008).

Security Posture is an organization's overall security plan, which protects from internal and external threats; it is comprised of technical and non-technical policies, procedures and controls (Shinn, n.d.).

Research Parameters

This section of the document provides an overview of the methods used to develop the literature review. This section reports on the strategies used in locating and selecting literature for this literature review and the results of those efforts; explains the reference selection criteria; describes the documentation approach; and presents the full data analysis and writing plans.

Research Questions and Sub-questions

Main Question. What are the key components of an information security metrics program plan?

Sub-questions.

- What is an Information security program?
- What are the components of an information security metrics program plan, as reported in four pre-selected options?
- What is an information security metric?
- How are effective information security metrics developed?
- Why is it important to measure the performance of an information security program and why has information security been a "notoriously difficult area to measure" (Hinson, 2006, p. 2)?
- What aspects of an information security program can be measured?
- What are the most effective ways to report information security metrics?

Search Strategy Report

Search terms. The process of creating keywords involved three stages (Hewitt, 2002):

1. Identify the key concepts in your research area.

2. Analyze the concepts; extend their scope to find broader terms; define them with increasing precision to produce narrower terms; produce a list of synonyms; produce a list of related terms.

3. Map the list of key words or terms to the subject headings of each index to be used in the search.

After examining an initial set of resources related to the topic, the researcher identified an initial set of keywords and then prepared a refined set of words (Leedy & Ormrod, 2005). The following set of search terms developed:

Security and Metrics

Security and Management

Security and Statistics

Information Security and Metrics

Information Security and Measurement

Information Security and Management

Information Security and Statistics

Information Security and Key Performance Indicator (KPI)

Information Security and Strategic

Information Security and Reporting

Initial search details. Appendix A documents the details of the search strategy used to date for this topic.

Literature resources. Keywords and controlled vocabulary are used for inquiries in this literature review. The tools and information sources used are outlined below.

Search engines. The primary search engines used for this literature review are Clusty, Google, Google Scholar, and Yahoo. These search engines have had the most consistent and relevant results.

Databases. Literature review resources are collected using these databases: WorldCat, Summit, ACM Digital Library. ACM Digital Library produced the highest number of results that had relevant content.

Additional literature resources. Private research from Forrester was used for the literature review. Information from Forrester was accessed was accessed through a private subscription**.** Journals from the ISSA (Information Systems Security Association) were used as a resource the literature review. The following professional Websites were also used as resources:

IEEE (Institute of Electrical and Electronics Engineers) found at www.ieee.org,

Securitymetrics.org found at www.securitymetrics.org

ISECOM (Institute for Security and Open Methodologies) found at www.isecom.org

SANS Institute (SysAdmin, Audit, Networking, and Security) found at www.sans.org

Data Analysis Plan

According to Busch et al. (2005), conceptual analysis begins with identifying research questions, choosing a sample or samples, and then coding the text into manageable content categories. Busch et al. (2005) describes the process of coding as a process of "selective reduction" (Busch et al., 2005, para. 1). The goal of coding the text in relation to selected words or phrases is that the researcher can collect a body of information related to the research question under investigation (Busch et al., 2005).

Key elements, supporting ideas, and successful case studies in information security metric programs are obtained by coding a set of twenty references, collected from an academic, government, professional, and association literature including, including books, information security journals, and articles. This set of references includes four preselected prominent plans, identified during the preliminary review of the literature. Plans include those by (a) Campbell and Blades (2009), (b) Kark and Stamp (2007), (c) Payne (2006), and (d) Whitman and Mattord (2008).

The goal of the coding process is to reveal of a set of key components necessary to the development of an information security metrics program. The coding process is framed with criteria provided by Chew et al. (2008): (a) increase accountability, (b) improve information security effectiveness, and (c) demonstrate compliance. Detailed below are eight coding steps Busch et al. (2005) outlined for conducting conceptual analysis:

1. **Level of analysis –** A single word, such as "reporting", or for sets of words of phrases, such as "metric development" or "development of metrics" are coded.

2. **Number of concepts to code for –** The following pre-defined or interactive set of concepts and categories have been developed:

- Accountability
- Compliance
- Security effectiveness
- Program initiation
- Metric development
- Metrics program
- Reporting
- Maintaining

Words are coded if determined relevant to information security metrics. Relevant words discovered in the coding process that are relevant to the Literature Review are included in the coding process.

3. **Code for existence or frequency of a concept** - Coding is done for the existence of a concept, rather than for frequency.

4. **How to distinguish among concepts** – Concepts are coded even when they appear in different form. For example, "program planning" might also appear as "program initiation".

5. **Rules for coding your texts -** Translation rules protect against invalid interpretation and give the coding process a crucial level of consistency and coherence. For example, "Information security" is coded under "Security", and "Reporting" and "Maintaining" are coded under "Security program", which is under "Information security".

6. **Decide what to do with "irrelevant" information** – Information that is determined irrelevant information is ignored as long as it does not impact the outcome of the coding.

7. **Code the texts** – The coding method this literature review is coding by hand. Coding by hand is a manual process of reading each resource and documenting the concept occurrences. Coding by hand is more time consuming than software that automates the process, but a researcher can recognize context and errors far more easily. The results of the hand coding can be reviewed in Appendix B: Manual-Coding Results.

8. **Analyze the results** – In this phase that data is examined and attempts to draw conclusions and generalizations are made. See the Writing Plan below, for further description.

Writing Plan

The Writing Plan for the Review of Literature section of this paper adopts a "thematic" approach. (Literature review, 2007, para. 27). Results of the coding process are analyzed and synthesized in relation to a set of four preselected themes, derived from preliminary review of four prominent plans. Plans include those by: (a) Campbell and Blades (2009), (b) Kark and Stamp (2007), (c) Payne (2006), and (d) Whitman and Mattord (2008).

An outline of the expected development of these four pre-selected themes into security metrics program plan components follows, however additional themes, resulting in a potential reconfiguration of final components, may be added once the data analysis is completed.

1. **Program Initiation:** This component "identifies relevant stakeholders" (Chew et al., 2008, p. 25), determines who receives the metrics, and "what information they require to discharge their responsibility" (Brotby, 2009, p. 10). In this component, the importance to "develop milestones and goals" is also addressed (Kark & Stamp, 2007, p. 5).

2. **Developing information security metrics:** This component analyzes and synthesizes how others in the industry are developing security metrics within their organizations. Lennon (2003) states that the IT security metrics development process consists of two major activities: identification and definition of the current IT security program and development and selection of specific metrics to measure implementation, efficiency, effectiveness, and the impact of the security controls (p.1).

3. **Reporting information security metrics:** This component analyzes how information security metrics can be used to demonstrate "compliance with security requirements (e.g., policy and procedures), gauge the effectiveness of security controls and manage risk, provide a basis for trend analysis, and identify specific areas for improvement" (Jansen, 2009, p. 1).

4. **Maintaining an information security metrics program:** Once an information security metrics program is deployed, the process is not over. Kark and Stamp (2007) state that "It can take years before you have a mature security metrics program" (p. 4) and Payne (2006) states that "maintaining a security metrics program could take considerable effort" (p. 3). This component addresses what must be done to successfully maintain and benefit from an information security metrics program.

Annotated Bibliography

This section provides the annotated bibliography of twenty references selected for use in development of the Review of the Literature section of the document. This list of twenty references forms the data set for coding during data analysis. Each entry includes a bibliographic citation, a summary of the content, a description of the credibility of the source and an explanation of how the reference supports this study.

Brotby, W. K. (2008). *Information security metrics: A definitive guide to effective security monitoring and measurement*. Boca Raton, FL: Auerbach.

Abstract: Book offers approaches to developing and implementing relevant security metrics that are essential for effective security management. This book offers practical guidance for implementing metrics across an entire organization, thereby improving budget and resource allocation, and reducing the possibility that unanticipated events will have catastrophic impacts. The book presents metrics that complement those used by IT managers, and demonstrates how to make adjustments to metrics without interrupting business processes.

Comments: This book emphasizes the importance information security metrics management, and as such, supports all sections of the paper. This book also includes case studies and tools for monitoring specific items. The author holds the CISM certification from reputable technology industry organizations ISACA.

Bryant, A. R. (2007). *Developing a framework for evaluating organizational information assurance metrics programs*. Ft. Belvoir: Defense Technical Information Center. Retrieved April 5, 2009, from http://handle.dtic.mil/100.2/ADA467367

Abstract: 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. These case studies illustrate 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.

Comments: 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. The authors take the position that security metrics should be used to identify security weaknesses, determine trends to better utilize security resources, and measure the success or failure of implemented security solutions (The National Science and Technology Council, 2006). This resource supports all sections of the paper. This paper is of a scholarly nature and deemed credible as it was written by the author as a partial requirement for the fulfillment of the requirements for the degree of Master of Science in Information Resource Management at the Air Force Institute of Technology Air University.

Chapin, D. A., & Akridge, S. (2005). How can security be measured? *Information Systems Control Journal. 2,* 43-47. Retrieved April 5, 2009, from http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=24173

Abstract: Traditional security metrics are haphazard at best; at worst they give a false impression of security that leads to inefficient or unsafe implementation of security measures. This paper presents an approach whereby maturity and quality are combined to provide a more complete and orderly picture of an organization's security posture. The approach will be referred to as the Security Program Maturity Model. Security metrics—the measurement of the effectiveness of the organization's security efforts over time—have always been difficult to evaluate. How can an organization determine whether it is secure? The measure of the quality of the security program can be truly tested only when the organization is stressed by a crisis. Yet, this situation is exactly what the security effort is designed to prevent.

Comments: This article outlines the need for the measurement of information security and focuses on quantifying an organization's security posture and a security program's maturity. Aspects of the article are used to , supports discussion of how information security metrics management can in increase accountability and improve information security effectiveness, referenced in the Outcome and Focus sections of the paper. This article is considered credible since both authors hold certifications from reputable technology industry organizations including ISACA and (ISC)^2 as well as the article's publication in a peer-reviewed journal.

Chew, E., Clay, A., Hash, J., Bartol, N., & Brown, A. (2006). *Guide for developing performance metrics for information security: Recommendations of the National Institute of Standards and Technology.* Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology. Retrieved April 8, 2009, from http://purl.access.gpo.gov/GPO/LPS72067

Abstract: This publication focuses on developing and implementing information security metrics for an information security program. The processes and methodologies described in this guidance link information security performance to agency performance by leveraging agency-level strategic planning processes. The performance metrics developed according to this guide will enhance the ability of agencies to respond to a variety of federal government mandates and initiatives, including the Federal Information Security Management Act (FISMA) and the President's Management Agenda (PMA).

Comments: This guidance document is a companion guide to *Security Metrics for Information Technology Systems*. This paper was published by the National Institute of Standards and Technology (NIST) which gives it credibility. NIST is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce which is responsible for developing standards and guidelines, including minimum requirements that enhance economic security. This paper provides a set of overarching criteria used to frame basic themes of an information security metrics program plan, presented in the program initiation and program development sections. This paper also provides a list of key components needed in an information security metrics program plan, and is thus selected as one item in the data set for conceptual analysis.

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance measurement guide for information security*. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology. Retrieved April 8, 2009, from http://purl.access.gpo.gov/GPO/LPS96650

Abstract: This document is a guide to assist in the development, selection, and implementation of measures to be used at the information system and program levels. This guide indicates the effectiveness of security controls applied to information systems and supporting information security programs. Such measures are used to facilitate decision making, improve performance, and increase accountability through the collection, analysis, and reporting of relevant performance-related data—providing a way to tie the implementation, efficiency, and effectiveness of information system and program security controls to an agency's success in its mission-critical activities. The performance measures development process described in this guide will assist agency information security practitioners in establishing a relationship between information system and program security activities under their purview and the agency mission, helping to demonstrate the value of information security to their organization.

Comments: This paper is credible since the National Institute of Standards and Technology (NIST) published it. NIST is a measurement standards laboratory which is a non-regulatory agency of the United States Department of Commerce which is responsible for developing standards and guidelines, including minimum requirements that enhance economic security. Chew provides the three overarching criteria used to frame the initial presentation of themes, in the Review of Literature section of this paper.

Corporate Information Security Working Group. (2005). *Report of the best practices and metrics teams*. Retrieved April, 20, 2009 from http://www.cisecurity.org/Documents/BPMetricsTeamReportFinal111704Rev11005.pdf

Abstract: The Corporate Information Security Working Group (CISWG) was originally convened in November 2003. The Best Practices team surveyed available information security guidance. It concluded in its March 2004 report that much of this guidance is expressed at a relatively high level of abstraction and is therefore not immediately useful as actionable guidance without significant and often costly elaboration. In a subsequent phase convened in June 2004, the Best Practices and Metrics teams was charged with refining Information Security Program Elements and developing recommended metrics supporting each of the elements.

Comments: This report is designed as a resource for those who want to establish their own comprehensive structure of principles, policies, processes, controls, and performance metrics to support the people, process, and technology aspects of information security. This resource is reviewed as a guide and report of key components for an information security metrics program plan, and is included as one item in the data set for conceptual analysis.

Herrmann, D. S. (2007). *Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI*. Boca Raton, FL: Auerbach Publications.

Abstract: This book provides a practical foundation for establishing an effective and efficient security metrics program. It serves as a guide for how to measure compliance with security and privacy laws and regulations, the operational resilience of a system or network, and the effectiveness of physical, personnel, or operational security. It also covers how to determine the return on investment for security investments. This book is ideal for corporate officers, security managers, internal and independent auditors, and system developers and integrators.

Comments: This book supports the identification of the key components for information security metrics program plan and is part of the data set selected for conceptual analysis. This resource is considered credible since the author has over 20 years experience in the field and holds a M.S. degree in Computer Science. The author has also published numerous papers and three books in the Information technology field.

Hinson, G. (2006). Seven myths about information security metrics. *The Information Systems Security Association (ISSA) Journal, July 2006*. Retrieved April 11, 2009, from https://www.issa.org/Library/Journals/2006/July/Hinson%20-%20Seven%20Myths.pdf

Abstract: This paper discusses the requirements and design constraints for a practical system to measure, report and improve information security. While managing a substantial ISO 17799 implementation program for a financial services client, Dr. Hinson observed a need of a way to gauge and report progress towards the goal of achieving ISO

17799 compliance. Senior management also needed a way to track the 17799 program, ensuring that the expense of the program would be justified by the benefits achieved.

Comments: This resource supports the analysis process to determine which components of an information security metrics management plan can increase accountability and improve information security effectiveness. As such, it is used to elaborate details of the presentation of themes in the Review of Literature section of this study. This article is considered credible since the author hold certifications from reputable technology industry organizations including ISACA and (ISC)² as well as the article's publication in a peer-reviewed journal.

Jansen, W. (2009, March). *Directions in security metrics research* (National Institute of Standards and Technology Rep. NISTIR 7564). Retrieved April 22, 2009 from http://csrc.nist.gov/publications/drafts/nistir-7564/Draft-NISTIR-7564.pdf

Abstract: Information security metrics are seen as an important factor in making sound decisions about various aspects of security, ranging from the design of security architectures and controls to the effectiveness and efficiency of security operations. During the last few decades, researchers have made various attempts to develop measures and systems of measurement for computer security with varying degrees of success. This paper provides an overview of the security metrics area and looks at possible avenues of research that could be pursued to advance the state of the art.

Comments: This resource supports this review with key elements to consider when designing security metrics for an organization and discusses possible areas of research in the information security metrics field. This paper is credible since the Information Technology Laboratory (ITL) created it and the National Institute of Standards and Technology (NIST) published it. The ITL at the NIST promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analysis to advance the development and productive use of information technology.

Jaquith, A. (2007). *Security metrics: replacing fear, uncertainty, and doubt.* Upper Saddle River, NJ: Addison-Wesley.

Abstract: Security Metrics is a guide to defining, creating, and utilizing security metrics in the enterprise. Using sample charts, graphics, and case studies, The author demonstrates exactly how to establish effective metrics based on your organization's unique requirements. You will discover how to quantify hard-to-measure security activities, compile and analyze all relevant data, identify strengths and weaknesses, set cost-effective priorities for improvement, and create compelling messages for senior management.

Comments: This book illustrates both the management quantitative viewpoint and the approach typically taken by security professionals in the field and ties them together. This book is used to support the development and reporting of information security metrics sections of the paper. The author has extensive consulting work in the software, aerospace and financial services industries. Others also cite the author and text in the field including Brotby (2009), Bryant (2007), Geer (2006), and Patriciu (2006).

Kahraman, E. (2005). *Evaluating IT security performance with quantifiable metrics*. Retrieved March 20, 2009 from Stockholm University, Department of Computer and Systems Science Website: http://www.dsv.su.se/en/seclab/pages/pdf-files/2005-x-245.pdf

Abstract: The growing attention of organizations' towards information security has risen from the need for protection of their most valuable assets and companies started to invest more on information security. But security, as it has always been, still is seen as a cost center since the return on security investments (including the budget, hiring professionals, education programs) could not be calculated effectively. IT security is an activity that is in need for a tool to be measured. Managerial, but also financial and regulatory tools do not only drive this requirement. When preparing the tool, a holistic approach to system science and system theory would help to understand the security performance goals and objectives better by combining all technical, organizational and ethical assets of information systems.

Comments: This paper identifies the steps of IT Security Officers/ Auditors to measure IT Security Performance and the adequacy of security policies and protocols by setting up a Metrics Scorecard evaluated with quantifiable metrics, designed to continuously validate the security level. This paper supports the developing information security metrics, reporting information security metrics portions of the paper referenced in the Focus section of this paper. This is a master's thesis of a scholarly nature and deemed credible.

Kark, K. (2008, July 22). *Best practices: security metrics.* Retrieved March 12, 2009 from Forrester database: http://www.forrester.com/Research/Document/Excerpt/0,7211,45787,00.html

Abstract: Security metrics are a key initiative for many organization today, but many struggle with picking the right security metrics to provide meaningful information regarding information security. Forrester interviewed more than 20 companies in various stages of their security metrics programs, and some that have successfully implemented them, to glean best practices and lessons learned from those efforts.

Comments: The three main themes that came out of this research are: (a) be very selective in picking your security metrics, (b) think beyond the security organization, and (c) focus on reporting and presentation. Khalid holds a master's degree in telecommunications management from University of Pennsylvania and a bachelor's degree in business and economics from University of Texas at Austin. Khalid is also a Certified Information Systems Security Professional (CISSP), a Certified Information Security Manager (CISM), and a Certified Information Security Auditor (CISA). This paper is part of the data set analyzed to identify the needed key components of and information security metrics program plan, presented in the Review of Literature section of this study.

Kark, K., & Stamp, P. (2007, May 16). *Defining an effective security metrics program*. Retrieved March 12, 2009 from Forrester database: http://www.forrester.com/Research/Document/Excerpt/0,7211,42354,00.html

Abstract: In a recent survey, Forrester found that the majority of security metrics programs are still in their infancy or planning phases. The respondents cited two main challenges in developing their metrics programs: finding the right metrics and translating the security metrics into business language. Many security managers are focused on gathering and reporting tactical and status update information. To develop a successful security metrics program, CISOs need to identify, prioritize, monitor, and measure security based on business goals and objectives. They should then focus on translating those measurements into business language to help executive management in strategic business decisions.

Comments: This article lists and describes the seven steps to a successful security metrics program. This paper provides support in identifying the key components of an information security metrics program, and is part of the data set selected for conceptual analysis. Khalid holds a master's degree in telecommunications management from University of Pennsylvania and a bachelor's degree in business and economics from University of Texas at Austin. Khalid is also a Certified Information Systems Security Professional (CISSP), a Certified Information Security Manager (CISM), and a Certified Information Security Auditor (CISA).

Patriciu, V., Rriescu, I., & Nicolaescu, S. (2006). Security metrics for enterprise information systems. *Journal of Applied Quantitative Methods,* 1(2). Retrieved April 8, 2009, from http://jaqm.ro/issues/volume-1,issue-2/pdfs/patriciu_priescu_nicolaescu.pdf

Abstract: Managing the security of enterprise information systems has become a critical issue in the era of Internet economy. As any other process, security cannot be managed if it cannot be measured. The need for metrics is important for assessing the current security posture, to develop operational best practices and for guiding future security research. The topic is important at a time when companies are coming under increasing compliance pressures that require them to demonstrate due diligence when protecting their data assets. Metrics give companies a way to prioritize threats and vulnerabilities and the risks they pose to enterprise information assets based on either quantitative or qualitative measures.

Comments: This paper presents a framework for ranking vulnerabilities in a consistent fashion, and some operational metrics used by large enterprises in managing their information systems security process. This paper supports all key component portions of the paper. This paper provides bibliographic citations to previous publications, which indicates that it is a scholarly resource. The article is also published in a peer-reviewed journal. All three contributors of the paper hold doctoral degrees in a field relevant to the topic.

Payne, S. C. (2006, June 19). *A guide to security metrics.* SANS Institute. Retrieved April 7, 2009, from http://www.sans.org/reading_room/whitepapers/auditing/a_guide_to_security_metrics_55?show=55.php&cat=auditing

Abstract: Various surveys indicate that over the past several years computer security has risen in priority for many organizations. Spending on IT security has increased significantly in certain sectors. As with most concerns that achieve high priority status with executives, computer security is increasingly becoming a focal point not only for investment, but also for scrutiny of return on that investment. In the face of regular, high-profile news reports of serious security breaches, security managers are more than ever before being held accountable for demonstrating effectiveness of their security programs. What means should managers be using to meet this challenge? Some experts believe that key among these should be security metrics.

Comments: This guide provides a definition of security metrics, explains their value, discusses the difficulties in generating them, and suggests a methodology for building a security metrics program. This paper is considered a reliable resource because it was written as partial requirement for the SysAdmin, Audit, Network, Security's (SANS) GIAC Security Essentials Certification (GSEC) certification. The Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals around the world. The guide is also developed within the tradition of scholarly publications, and includes traditional research categories and citations.

Pironti, J. P. (2007). Developing metrics for effective information security governance. *Information Systems Control Journal. 2,* 33-38. Retrieved April 7, 2009, from http://www.isaca.org/AMTemplate.cfm?Section=20075&Template=/ContentManagement/ContentDisplay.cfm&ContentID=40248

Abstract: Key performance indicators (KPIs) are one of the most effective tools that can be implemented to measure the effectiveness of an organization's information security business processes and capabilities. When designed and implemented properly, they provide business-aligned quantitative measures of the success or failure of business processes, personnel, technology and organizational effectiveness.

Comments: This paper supports two identified key components: the development information security metrics and the reporting information security metrics. This article is considered credible since the author holds certifications from reputable technology industry organizations including ISACA and (ISC)^2 as well as the article's publication in a peer-reviewed journal.

Schechter, S. E. (2004). *Computer security strength & risk: A quantitative approach.* Unpublished doctoral dissertation, Harvard University. Retrieved May 6, 2009, from http://www.eecs.harvard.edu/~stuart/papers/thesis.pdf

Abstract: The importance of quantifying security strength and risk continues to grow as individuals, businesses, and governments become increasingly reliant on software systems. The security of software deployed to date has suffered because these systems are

developed and released without any meaningful measures of security, causing consumers to be unable to differentiate stronger software products from weaker ones. Even if we knew that we could make systems measurably stronger, the lack of accurate security risk models has blurred our ability to forecast the value to be gained by strengthening these systems. Without the tools introduced in this dissertation, those of us tasked with making security decisions have been forced to rely on expert opinion, anecdotal evidence, and other unproven heuristics.

Comments: The paper supports the metrics development key component and reporting development portions of the paper. This resource supports all sections of the paper. This paper is of a dissertation, written as a partial requirement for the degree of Doctor of Philosophy in the subject of Computer Science at Harvard University.

Swanson, M., Bartol, N., Sabato, J., Hash, J., & Graffo, L. (2003). *Security metrics guide for information technology systems*. Gaithersburg, MD: National Institute of Standards and Technology, Technology Administration, U.S. Dept. of Commerce. Retrieved April 8, 2009, from http://purl.access.gpo.gov/GPO/LPS35202.

Abstract: This document provides guidance on how an organization, through the use of metrics, identifies the adequacy of in-place security controls, policies, and procedures. It provides an approach to help management decide where to invest in additional security protection resources or identify and evaluate nonproductive controls. The results of an effective metric program can provide useful data for directing the allocation of information security resources and should simplify the preparation of performance-related reports.

Comments: This document proceeded *Performance Measurement Guide for Information Security* (Chew et al., 2008). This resource supports all key component portions of the paper. This paper was published by the National Institute of Standards and Technology (NIST) which gives it credibility. NIST is a measurement standards laboratory that is a non-regulatory agency of the United States Department of Commerce, which is responsible for developing standards and guidelines, including minimum requirements that enhance economic security.

Wang, J. A., Xia, M. & Zhang, F. (2007). Metrics for information security vulnerabilities. *Proceedings of Intellectbase International Consortium*, USA, 1, 284-294. Retrieved April 17, 2009, from http://www.intellectbase.org/ProceedingsFall2007.pdf

Abstract: It is widely recognized that metrics are important to information security because metrics can be an effective tool for information security professionals to measure, control, and improve their security mechanisms. However, the term "security metrics" is often ambiguous and confusing in many contexts of discussion. Common security metrics are often qualitative, subjective, without a formal model, or too naïve to be applied in real world. This paper introduces the criteria for good security metrics and how to establish quantitative and objective information security metrics with the recently released CVSS 2.0 (Common Vulnerability Scoring System), which provides a tool to quantify the severity and risk of a vulnerability to an information asset in a computing environment.

Comments: This resource focuses on security metrics and their applications in security automation and standardization. This resource provides support for the discussion of what criteria are needed for creating effective information security metrics, referenced in the Problem and Significance sections. This resource is considered credible because it is published in a peer-reviewed journal and cites experts within the field of information security metrics.

Whitman, M. E., & Mattord, H. J. (2004). *Management of information security*. Boston: Course Technology.

Abstract: Management of Information Security provides an overview of information security from a management perspective, as well as a thorough understanding of the administration of information security.

Comments: Written by two Certified Information Systems Security Professionals (CISSP), this book has the added credibility of incorporating the CISSP Common Body of Knowledge (CBK), especially in the area of information security management. The second edition has been updated to maintain the industry currency and academic relevance that made the previous edition so popular, and case studies and examples continue to populate the book, providing real-life applications for the topics covered. This resource is used to provide a high level list of components needed in an information security metrics program (and as such is part of the data set selected for conceptual analysis) and as reference to provide definitions of key terms.

Review of the Literature

The purpose of the Review of Literature section of this paper is to organize and synthesize what others have written in the information security metrics field in relation to the purpose of the study (Leedy & Ormrod, 2005). Information is presented within a "thematic" approach (Literature review, 2007, para. 27). In this case, themes are defined as "key components" of an information security metrics program plan. The goal is to provide an ordered guide of components necessary to develop an information security metrics program plan. Identified components are extrapolated from multiple sources and categorized as themes in relation to three overarching criteria provided by Chew et al. (2008): (a) increase accountability, (b) improve information security effectiveness, and (c) demonstrate compliance.

The Review of the Literature first provides a detailed discussion on the identification of the key components of an information security metrics program. Four preselected prominent plans are examined, which include: five steps in building a responsive security metrics program (Campbell & Blades, 2009), seven steps to a successful metric program (Kark & Stamp, 2007), tasks of an information security program (Whitman & Mattord, 2008), and seven key steps of establishing a security metrics program (Payne, 2006).

Next, based on an analysis of the results derived from these four prominent plans, the Review of the Literature presents an integrated set of key components necessary for an information security metrics program and details what should be included in each of the identified key components.

Key Component Identification

Key components are extrapolated from material emphasized in four preselected prominent plans, specifically by Campbell and Blades (2009), Kark and Stamp (2007), Whitman and Mattord (2008) and Payne (2006). The following set of four tables summarizes each approach.

Campbell and Blades (2009) lists five steps in a security metrics program (p. 3-5)
1. Identify the business drivers and objectives for the security metrics program
2. Determine who your metrics are intended to inform and influence
3. Identify the types and locations of data essential for actionable security metrics
4. Establish relevant metrics
5. Establish internal controls to ensure integrity of data and data assessments, and to protect confidentiality

Table 1: Five steps from Campbell & Blades (2006)

Kark and Stamp (2007) Seven steps in a security metrics program (p. 4-5)
1. Make measurements and metrics a key part of the security program
2. Define a security framework
3. Define metrics and thresholds for domains in the framework
4. Identify and document information sources, assumptions, and calculations
5. Develop milestones and goals
6. Respond to monitoring and measurement

7. Report security metrics that help with strategic business decisions

Table 2: Seven steps from Kark and Stamp (2007)

Whitman and Mattord (2008) lists four key activities in a security metrics program (p. 245)
1. Specifying the information security metrics
2. Collecting the information security metrics
3. Interpreting information security metrics
4. Disseminating the information security metrics

Table 3: Four activities from Whitman and Mattord (2008)

Payne (2006) identifies seven key steps in an information security metrics program (p. 3)
1. Define the metrics program goal(s) and objectives
2. Decide what metrics to generate
3. Develop strategies for generating the metrics
4. Establish benchmarks and targets
5. Determine how the metrics will be reported
6. Create an action plan and act on it
7. Establish a formal program review and refinement cycle

Table 4: Seven steps from Payne (2006)

A comparison of the four pre-selected plans reveals that, while experts generally agree on the activities required to develop an information security metrics program, each expert chooses to separate those activities differently. As a way to develop the final integrated set of components for an information security metrics plan, the entries above are reorganized with attention to three overarching criteria provided by Chew et al. (2008). The goal in this process is to design key components that better meet the needs of the indented audience. The set of key components developed with the criteria from Chew et al. (2008) utilized as a framework provides the reader with an information security metric program that can a) increase accountability, b) improve information security effectives and c) demonstrate compliance. Each key component is examined in relation to a set of core elements, as defined in the literature. Elements are described as they pertain to the three criteria from Chew et al (2008). Five components, originally designated as themes, are proposed:

- Initiation of the information security metrics program
- Development of information security metrics
- Analysis of information security metrics
- Reporting information security metrics
- Maintaining an information security metrics program

Component #1: Program Initiation

According to Swanson (2003), this component recognizes that a "foundation of strong upper- level management support" is needed for an information security metrics program to be successful (p. 2). At the outset, the program developer "identifies relevant stakeholders" (Chew et al., 2008, p. 25), determines who receives the metrics, and ". . . what information they require to discharge their responsibility" (Brotby, 2009, p. 10). In this component, the importance to "develop milestones and goals" is also addressed (Kark & Stamp, 2007, p. 5).

Increased accountably and quantifying improvements in securing information systems are addressed in the Program Initiation key component. Swanson (2003) recommends documenting the "audience for the plan" as part of the "Metrics Program Implementation Plan" (p. 24). Brotby (2009) states that without defined objectives for an information security program, it is not possible to develop useful metrics (p. 4).

Secure management support. Chew et al. (2008) lists the number one critical factor for success to an information security metrics program as "strong upper-level management support" (p. 3). Swanson (2003) states "this support establishes a focus on security within the highest levels of the organization" (p. 2). Bryant (2007) identifies executive buy-in as critical to the success of an information security metrics program. "Managing the use of InfoSec metrics requires commitment from the InfoSec management team" (Whitman & Mattord 2008). InfoSec is an abbreviation for "information security" and was primarily used in the military and migrated to commercial parlance (InfoSec, n.d.). Having management support is also required in order to build a culture that is accepting of information security metrics. As noted by Kahraman (2005), "having management commitment is the most important part to generate a measurement culture within the organization" (p. 8).

Define goals, objectives, and business drivers. In order to develop effective metrics it is important to first define goals, objectives, and business drivers. Brotby (2009) reinforces this when stating "Without defined objectives for an information security program it is not possible to develop useful metrics" (p. 4). Determining goals, objectives, and business drivers before implementing an information security metrics program can save resources and assist the program's success. Payne (2006) states that "a security metrics program could take considerable effort and divert resources away from other security activities" so "it is critical that the goal(s) and objectives of the program be well-defined and agreed upon up front" (p. 3). Developing an information security metric program with the goals, objectives, and business drivers of the organization in mind helps ensure the success of the program. It is important to gain support from the individuals whose initiatives are measured. Jaquith (2007) states that when implementing a major initiative in an organization, such as a metrics program, all stakeholders "need to have a tangible reason to buy into the program, or [they] will covertly or overtly resist its implementation" (p. 295-296).

Determining the audience of the information security metrics. Brotby (2009) states that "any discussion of metrics must first and foremost consider the constituency"(p. 10). Swanson (2003) recommends documenting the "audience for the plan" as part of the "Metrics Program Implementation Plan" (p. 24). Pironti (2007) affirms this, "If a measure is communicated to an inappropriate audience, it is ineffective and potentially may cause confusion and unwanted business impacts for the organization that is being measured (p. 1). Herrmann (2007) states "you need to have a good understanding of who are the metric consumers" (chap. 2.5). Pironti (2007) gives the illustration that upper management in most organizations is "typically less interested in technical measures and more in measures of the risks and costs associated with information security activities to business impact" and the operational elements of an organization typically "have more interest in technological measures to understand the effectiveness of their service delivery capabilities" (p. 1).

Component #2: Development of Information Security Metrics

This component analyzes the attributes of a good security metric and how to determine what should be measured. And, as noted by Jaquith (2007), not all metrics are appropriate for all organizations (p. 45).

The Development of Information Security Metrics key component addresses increased accountability and demonstrating compliance with applicable laws. To address increased accountability, Pironti (2007) states "When developing metrics and measures, it is important to align them to the business goals of the organization" (p. 2). To address compliance with applicable laws, rules, and regulations, Payne (2006) states that "any underlying corporate framework for process improvement" such as Six Sigma or ISO 9001, could be used to dictate what security metrics are needed (p. 4).

Determining attributes of a good information security metric. The notion of what constitutes a set of attributes for "good" metrics varies among experts in the field. Jaquith (2007) states that a good metric should meet the following attributes: a) it must be consistently measured, without subjective criteria, b) it must be cheap to gather, preferably in an automated way, c) it must be expressed as a cardinal number or percentage, not with qualitative labels like "high," "medium," and "low", and d) it must be expressed using at least one unit of measure, such as "defects," "hours," or "dollars" (p. 22). Wang (2007) provides another set of attributes for a good metric. He lists objectiveness, repeatability, clarity, and easiness as attributes of a good metric. Patriciu (2006) states that good metrics should be "specific, measurable, comparable, attainable, repeatable, and time dependent" (p. 152).

Although each expert lists slightly different attributes, upon further investigation, there are some obvious commonalities. Both Bryant (2007) and Payne (2006) summarize these common attributes as specific, measurable, attainable, repeatable, and time-dependent or SMART. The origin of SMART is unknown, since both experts cite different resources.

Determining what to measure. When determining what to measure, it is important to include all appropriate stakeholders. Chew et al. (2008) states that appropriate stakeholders must be included in the development of information security measures (p. 151). Pironti (2007) states "When developing metrics and measures, it is important to align them to the business goals of the organization" (p. 2). Using an underlying framework can also be used to determine what needs to be measured within the organization. Payne (2006) suggests that "any underlying corporate framework for process improvement" such as Six Sigma or ISO 9001 could be used to dictate what security metrics are needed (p. 4). Kark and Stamp (2007) reinforce this by suggesting "a framework-based approach" to identify areas to measure and track progress over time (p. 4).

Testing and determining thresholds. Once metrics are aligned to organization goals, Kark and Stamp (2007) recommend testing metrics on a subset of users before implementing them to the entire organization in order to be able to change or adjust metrics based on changing threats in the larger landscape or corporate objectives (p.4). Additionally, Kark and Stamp (2007) suggest identifying the acceptable threshold levels for each metric. Pironti (2007) states "Every measure must have a clearly defined acceptable, unacceptable and excellent range of values that can be easily identified by the audience to which the measure is communicated" (p. 1). For example, "one organization measuring the percentage of employees that completed security awareness training decided that an acceptable threshold was 95%. Setting thresholds will help you quickly identify areas that have unacceptable levels of security controls" (Kark & Stamp, 2007, p. 4).

Component #3: Collect and Analyze Information Security Metrics

This component discusses the collection, analysis and benchmarking activities of an information security metrics program. Swanson (2003) states that after the metrics have been identified, specific implementation steps should be defined on how to collect and analyze the security metrics (p. 24).

Collect information security metrics. Kahraman (2005) states that once data has been collected through information security metrics the information can be "analyzed to create a quantitative understanding of security level in the organization (p. 22). Patriciu (2006) states "metrics should also be easily obtainable" (p. 153). Jaquith (2007) supports this with his "cheap to gather, preferably in an automated way" criteria of what makes a good metric (p. 22). Bryant (2007) states that "automation is also more reliable" when referring to the collection of information security metrics.

Whitman and Mattord (2008) state that once the question of what to measure is decided, the how, when, where, and who questions of metrics collection must be answered (p. 245). Herrmann (2007) supports this with a set of seven steps involved in planning for metric data collection and validation. (chap. 2.3). The seven steps are presented below, in Table 5.

Planning step	**Step detail**
Step 1: What?	Define what information is going to be collected.

Step 2: Why?	Define why this information is being collected and how it will be used.
Step 3: How?	Define how the information will be collected, the constraints and controls on the collection process.
Step 4: When?	Define the time interval and frequency with which the information is to be collected.
Step 5: Where?	Identify the source(s) from which the information will be collected.
Step 6: Ensure data integrity	Define how the information collected will be preserved to prevent accidental or intentional alteration, deletion, addition, other tampering, or loss.
Step 7: Derive true meaning	Define how the information will be analyzed and interpreted.

Table 5: Steps for metric data collection and validation, from Herrmann (2007)

Analyze information security metrics. Once collected, information must be analyzed. Bryant (2007) states that every metrics program should include processes for analyzing and interpreting the data (p. 8). Activities for this component include consolidation of collected data, gap analysis, identifying causes of poor performance and areas that require improvement (Swanson, 2003, p. 25). Chew et al., (2008) gives the following examples (see Table 6) contributing to poor performance and identifying potential areas that may require improvement (p. 37).

Potential issue	**Area for improvement after analysis**
Resources	Insufficient human, monetary, or other resources
Training	Lack of appropriate training for the personnel installing, administering, maintaining, or using the systems
System Upgrades	Security patches that have been removed but not replaced during

	the operating system upgrades
Configuration Management Practices	New or upgraded systems that are not configured with required security settings and patches
Software Compatibility	Security patches or upgrades that are incompatible with software applications supported by the system
Awareness and Commitment	Lack of management awareness and/or commitment to security
Policies and Procedures	Lack of policies and procedures that are required to ensure existence, use, and audit of required security functions
Architectures	Poor system and security architectures that render information systems vulnerable
Inefficient processes	Inefficient planning processes that influence measures including the communication processes necessary to direct organizational actions

Table 6: Metric analysis – Potential issues and areas of improvement, from Chew, et al. (2007).

Establish benchmarks and targets. Payne (2006) describes benchmarking as the "process of comparing one's own performance and practices against peers within the industry or noted 'best practice' organizations outside the industry" (p. 6). Pironti (2007) states that this industry information can be "gathered through publicly available surveys, individual data-gathering activities, or analysts or third-party consultants" (p. 2). Benchmarks can be used, for example, to determine a "minimum essential configuration" for workstations, servers, laptops, routers, firewalls, and other network devices (Corporate Information Security Working Group, 2005, p. 31). Benchmarks also help establish achievable targets for driving improvements in existing practices (Payne, 2006, p. 6).

Component #4: Reporting and Responding to Information Security Metrics

Once data has been analyzed, it can then be reported. Pironti (2007) states meaningful reporting is the key to the success of any information security metrics program (p. 4). This component describes how information security metrics can be used to demonstrate “compliance with security requirements (e.g., policy and procedures), gauge the effectiveness of security controls and manage risk, provide a basis for trend analysis, and identify specific areas for improvement” (Jansen, 2009, p. 1). Bryant (2007) states “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” (p. 112).

Determine how metrics will be reported, frequency, format, etc. Hinson (2006) states “Presentation of your chosen metrics is just as important as the data content” (p. 3). Pironti (2007) states that “different audiences have different interests in the types and frequency” of metrics that are reported (p. 1). “The frequency of reports depends on organizational norms, the volume and gravity of information available, and management requirements. Regular reporting periods may vary from daily or weekly to monthly, quarterly, biannual or annual” (Hinson, 2006, p. 4). Frequency may also depend on a rate of change in a particular control that is being assessed (Chew et al., 2006). Chew et al. (2006) states that ultimately the frequency will be determined by the stakeholder or reporting requirements.

Determine who will receive information security metrics. To whom the results of the metrics program should be disseminated to should also be considered (Whitman & Mattord, 2008). Kark (2008) states “It’s essential to ensure that your security metrics make sense to your audience” (p. 3). Pironti (2007) recognizes that “different audiences have different requirements and varying interests in the measurements that are gathered and reported” (p. 4). To address the issue of different audiences, he recommends a “tiered reporting model” (Pironti, 2007, p. 4). A tiered reporting model separates reports and details for individual groups. An example would be upper management as one tier that would receive a high-level report and server administrators as another tier that would receive low-level technical details. Providing each tier with a separate report helps prevent the “disconnect” that Kark (2008) refers to when, for example, reporting technical details that are “not very useful for the CEO or executive management” (p. 3).

Respond to information security metrics. The reason that metrics are created and reported is so that an action can be taken. Bryant (2007) lists the ability to respond to malicious events as one of the most desirable properties for an information security metrics program and cites that “reaction” is one of the five pillars of information security (p. 14). Kark and Stamp (2007) point out that “if you are measuring your security program but are not responding to those measurements, the organization will catch on very quickly and will stop paying attention to your metrics” (p. 5). Chew et al. (2008) suggests to first determine the range of corrective actions, then prioritize corrective actions based on overall risk mitigation goals, and then select the most appropriate corrective actions.

Component #5: Maintaining an Information Security Metrics Program

Once an information security metrics program is deployed, the process is not over. Kark and Stamp (2007) state that “It can take years before you have a mature security metrics program” (p. 4). Payne (2006) states that “maintaining a security metrics program could take considerable effort” (p. 3). This component addresses what must be done to successfully maintain and benefit from an information security metrics program.

This component, Maintaining an Information Security Metrics Program, addresses increase accountability. Kark (2008) states that maintaining an information security metrics program encourages a “culture of measurement and accountability” (p. 12).

Establishing a formal program for review and refinement of the information security metrics program. Kark (2008) states a metrics program is not a one-time effort but a constantly evolving one that requires continuous support and processes to improve the program. (p. 12). Payne (2006) recommends that a formal, recurring review take place of the entire security metrics program. He suggests the following basic set of questions be applied as part of this review:

1) Is there reason to doubt the accuracy of any of the metrics?

2) Are the metrics useful in determining new courses of action for the overall security program?

3) How much effort is it taking to generate the metrics?

4) Is the value derived worth that effort?

Hinson (2006) believes that “Continuous feedback on the metrics can help to refine the measurement system. It is always worth soliciting feedback from the intended audiences about whether the metrics are both comprehensible and useful” (p. 5). Additionally, as noted by Swanson (2003), the resources required for maintaining the program “are not expected to be as significant” as the investment to implement the program (p. 14).

Assess the organization's culture. Another task identified by Kark (2008) that should be included in maintaining an information security metrics program is the encouragement of a "culture of measurement and accountability" (p. 12). The assessment of an organization's culture can the help refine and develop metrics used within a program. Jaquith (2007) states each organization should "choose measures that best suit its business and are best aligned with its strategy and culture" (p. 262).

If the employees in an organization are not used to metrics and measurement, it may be difficult to develop a culture in which not only management understands the value of metrics, but also the rest of the organization is willing to start measuring its performance (Kark, 2008). Bryant (2007) recognizes that the "culture of an organization has a great deal to do with how well metrics work as decision making tools in an organization" (p. 79). As stated in the Initiation component, "having management commitment is the most important part to generate a measurement culture within the organization" (Kahraman, 2005, p. 8).

Conclusions

Information security metrics provide organizations with a resource to manage, monitor, control, or improve aspects of an information security program. Wang (2007) states, “It is widely recognized that metrics are important to information security because metrics can be an effective tool for information security professionals to measure the security strength and levels of their systems, products, processes, and readiness to address security issues they are facing”(p.284).

An examination of the security metrics landscape reveals a tremendous diversity of approaches and methods employed to achieve some degree of feedback. No definitive, markedly superior approach to security metrics has surfaced, which demonstrates that the entire field is still in a state of flux (Brotby, 2009, p. 21).

This literature review is designed to provide key components of an information security metrics program plan, developed with the criteria from Chew et al. (2008). The table below summarizes the five key components of an information security metrics program plan. Each component includes the literature that is used to support the articulation of the component and a list of the major tasks that should be conducted within each.

KEY COMPONENTS	ASSOCIATED TASKS
Component #1: **Program Initiation**	This component recognizes that a “foundation of strong upper- level management support” is needed for an information security metrics program to be successful (Swanson, 2003, p. 2). “Without defined objectives for an information security program it is not possible to develop useful metrics” (Brotby, 2009, p. 4). Major tasks of the program initiation component are:

KEY COMPONENTS	ASSOCIATED TASKS
	• Secure management support • Define goals, objectives, and business drivers • Determine the audience of the information security metrics
Component #2: **Development of Information Security Metrics**	Good metrics should be "specific, measurable, comparable, attainable, repeatable, and time dependent" (Patriciu, 2006, p. 152). The following tasks are recommended in the development of information security metrics component: • Determine attributes of a good information security metric • Determine what to measure • Test and determine thresholds
Component #3: **Collection and Analysis of Information Security Metrics**	Once metrics have been identified, specific implementation steps should be defined on how to collect and analyze the security metrics (Swanson, 2003, p. 24). Every metrics program should include processes for analyzing and interpreting the data (Bryant, 2007, p. 8). Major tasks of the collect and analyze information security metrics component include: • Collect information security metrics • Analyze information security metrics • Establish benchmarks and targets
Component #4: **Reporting and Responding to Information Security Metrics**	Meaningful reporting is the key to the success of any information security metrics program (Pironti, 2007, p. 4). Major tasks of the reporting and responding to information security metrics component are as follows: • Determine how metrics will be reported, frequency, format, etc. • Determine who will receive information security metrics

KEY COMPONENTS	ASSOCIATED TASKS
	• Respond to information security metrics
Component #5: **Maintaining an Information Security Metrics Program**	A metrics program is not a one-time effort but a constantly evolving one that requires continuous support and processes to improve the program (Kark, 2008, p. 12). The tasks needed for the maintaining an information security metrics program component include: • Establish a formal program for review and refinement of the information security metrics program • Assess the organization's culture

Table 7: Key components of an information security metrics program

The criteria from Chew et al. (2008), when used as a framework within which to consider these components and the associated tasks, offers a way to view the entire an information security metric program from the standpoint of increased accountability, improved information security effectiveness and demonstrated compliance. Information security measures can ***increase accountability*** for information security by helping to identify specific security controls that are implemented incorrectly, are not implemented, or are ineffective (Chew et al. p. 10). Accountably starts in the first key component, Program Initiation. Swanson (2003) recommends documenting the "audience for the plan" as part of the "Metrics Program Implementation Plan" (p. 24). In the second component, Development of Information Security Metrics, Pironti (2007) states "When developing metrics and measures, it is important to align them to the business goals of the organization" (p. 2). In the fifth component, Maintaining an Information Security Metrics Program, Kark (2008) states that maintaining an information security metrics program encourages a "culture of measurement and accountability" (p. 12).

An information security measurement program can enable organizations to ***quantify improvements in securing information systems*** and demonstrate quantifiable progress in accomplishing agency strategic goals and objectives (Chew et al. p. 10). One of the major tasks of first component, Program Initiation, is to define goals, objectives, and business drivers. Brotby (2009) states that without defined objectives for an information security program, it is not possible to develop useful metrics (p. 4).

Organizations can demonstrate ***compliance with applicable laws*****,** rules, and regulations by implementing and maintaining an information security measurement program (Chew et al. p. 10). In Component #2: Development of Information Security Metrics, the task of determining what to measure addresses compliance demonstration. Payne (2006) suggests that "any underlying corporate framework for process improvement" such as Six Sigma or ISO 9001, could be used to dictate what security metrics are needed (p. 4).

References

Arnason, S. T., & Willett, K. D. (2008). *How to achieve 27001 certification: An example of applied compliance management.* New York: Auerbach Publications.

Brotby, W. K. (2008). *Information security metrics: A definitive guide to effective security monitoring and measurement*. Boca Raton, FL: Auerbach.

Black, P. E., Scarfone, K., & Souppaya, M. (2008). *Cyber security metrics and measures.* National Institute of Standards and Technology. Retrieved May 13, 2009, from http://hissa.nist.gov/~black/Papers/cyberSecurityMetrics2007proof.pdf

Bryant, A. R. (2007). *Developing a framework for evaluating organizational information assurance metrics programs*. Ft. Belvoir: Defense Technical Information Center. Retrieved April 5, 2009, from http://handle.dtic.mil/100.2/ADA467367

Busch, C. De Maret, P. S., Flynn, T. Kellum, R., Le, S., Meyers, B., et al. (2005). *Content analysis. Writing@CSU.* Colorado State University Department of English. Retrieved May 6, 2009 from http://writing.colostate.edu/guides/research/content/

Campbell, G. & Blades, M. (2009). Building a metrics program that matters. *Security Technology Executive. February 2009*. Retrieved May 4, 2009 from http://www.securityinfowatch.com/node/1310623/pdf

Chapin, D. A., & Akridge, S. (2005). How can security be measured? *Information Systems Control Journal. 2,* 43-47. Retrieved April 5, 2009, from http://www.isaca.org/Template.cfm?Section=Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=24173

Chaula, A., Yngstrom, L., & Kowalski, S. (2004). *Security metrics and evaluation of information systems security.* Retrieved April 8, 2009, from http://icsa.cs.up.ac.za/issa/2004/Proceedings/Research/048.pdf

Chew, E., Clay, A., Hash, J., Bartol, N., & Brown, A. (2006). *Guide for developing performance metrics for information security: Recommendations of the National Institute of Standards and Technology.* Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology. Retrieved April 8, 2009, from http://purl.access.gpo.gov/GPO/LPS72067

Chew, E., Swanson, M., Stine, K., Bartol, N., Brown, A., & Robinson, W. (2008). *Performance measurement guide for information security*. Gaithersburg, MD: U.S. Dept. of Commerce, National Institute of Standards and Technology. Retrieved April 8, 2009, from http://purl.access.gpo.gov/GPO/LPS96650

Component. (n.d.). *Merriam-Webster's Online Dictionary*. Retrieved May, 2, 2009, from: http://www.merriam-webster.com/dictionary/component

Corporate Information Security Working Group. (2005). *Report of the best practices and metrics teams.* Retrieved April, 20, 2009 from http://www.cisecurity.org/Documents/BPMetricsTeamReportFinal111704Rev11005.pdf

Dorofee, A., Killcrece, G., Ruefle, R., & Zajicek, M. (2007). *Incident management capability metrics version 0.1*. Retrieved April 22, 2009, from Software Engineering Institute, Carnegie Mellon Website: http://www.sei.cmu.edu/pub/documents/07.reports/07tr008.pdf

Fischer, E. A. (2005). *Creating a national framework for cybersecurity: An analysis of issues and options.* Ft. Belvoir: Defense Technical Information Center. Retrieved May, 6, 2009 from http://handle.dtic.mil/100.2/ADA463076

Garigue, R., & Stefaniu, M. (2003). Information security governance reporting. *Information Systems Security*. 12 (4), 36-40. Retrieved April 8, 2009, from http://publications.ksu.edu.sa/IT%20Papers/CISM/CISM-Security/ISG-Reporting.pdf

Gattiker, U. E. (2007). Merger and acquisition: Effective information security depends on strategic security metrics. *Information Systems Control Journal. 5*, 51-56. Retrieved April 7, 2009, from http://www.isaca.org/AMTemplate.cfm?Section=20075&Template=/ContentManagement/ContentDisplay.cfm&ContentID=44803

Geer, D. (2007). *Measuring security.* Paper presented at the Metricon 2.0 Conference. Retrieved April 22, 2009, from all.net/Metricon/measuringsecurity.tutorial.pdf

Gollmann, D., Massacci, F., & Yautsiukhin, A. (2006). *Quality of protection: Security measurements and metrics.* Advances in information security. New York: Springer.

InfoSec. (n.d.). *PCMAG.COM encyclopedia.* Retrieved June 15, 2009, from: http://www.pcmag.com/encyclopedia_term/0,2542,t=infosec&i=44973,00.asp

Inventory. (n.d.). *BusinessDictionary*. Retrieved April 23, 2009, from: BusinessDictionary.com Web site: http://www.businessdictionary.com/inventory

Herrmann, D. S. (2007). *Complete guide to security and privacy metrics: Measuring regulatory compliance, operational resilience, and ROI*. Boca Raton, FL: Auerbach Publications. Available from http://skillport.books24x7.com/toc.asp?bookid=26407

Hewitt, M. (2002). *Carrying out a literature review*. Retrieved March 31, 2000, from http://ce.uoregon.edu/aim/Capstone07/HewittLitReview.pdf

Hinson, G. (2006). Seven myths about information security metrics. *The Information Systems Security Association (ISSA) Journal, July 2006*. Retrieved April 11, 2009, from https://www.issa.org/Library/Journals/2006/July/Hinson%20-%20Seven%20Myths.pdf

Jansen, W. (2009, March). *Directions in security metrics research* (National Institute of Standards and Technology Rep. NISTIR 7564). Retrieved April 22, 2009 from http://csrc.nist.gov/publications/drafts/nistir-7564/Draft-NISTIR-7564.pdf

Jaquith, A. (2007). *Security metrics: replacing fear, uncertainty, and doubt*. Upper Saddle River, NJ: Addison-Wesley.

Kahraman, E. (2005). *Evaluating IT security performance with quantifiable metrics*. Retrieved March 20, 2009 from Stockholm University, Department of Computer and Systems Science Website: http://www.dsv.su.se/en/seclab/pages/pdf-files/2005-x-245.pdf

Kark, K. (2008, July 22). *Best practices: security metrics.* Retrieved March 12, 2009 from Forrester database: http://www.forrester.com/Research/Document/Excerpt/0,7211,45787,00.html

Kark, K., & Stamp, P. (2007, May 16). *Defining an effective security program*. Retrieved March 12, 2009 from Forrester database: http://www.forrester.com/Research/Document/Excerpt/0,7211,42354,00.html

Koot, M. (2006). *Towards KPIs for enterprise security governance*. Retrieved March 20, 2009 from University of Amsterdam Website: https://alumni.os3.nl/~mrkoot/courses/ICP/ICP-paper_metrics.pdf

Kovacich, G. L., & Halibozek, E. P. (2006). *Security metrics management: How to measure the costs and benefits of security*. Burlington, MA: Butterworth-Heinemann.

Leedy, P., & Ormrod, J. (2005). *Practical research: Planning and design.* New Jersey: Pearson/Prentice Hall.

Lennon, E. B. (2003). IT security metrics*. iTL Bulletin, August 2003*. Retrieved May 5, 2009, from: http://csrc.nist.gov/publications/nistbul/bulletin08-03.pdf

Lester, J. and Lester, J. Jr. (2007). *Writing research papers: A complete guide.* New York: Pearson Education, Inc.

Literature review. (2007). University of North Carolina. Retrieved May 6, 2009, from: http://www.unc.edu/depts/wcweb/handouts/literature_review.html

Lyons, K. B. *How to write a literature review.* Santa Cruz, Calif: University Library, University of California, Santa Cruz. Retrieved April 2, 2009, from http://library.ucsc.edu/ref/howto/literaturereview.html

Mayer, N., Dubois, E., Maulevicius, R., & Heymans, P. (2008). *Towards a measurement framework for security risk management.* Paper presented at Modeling Security 2008 Workshop. Retrieved April 17, 2009, from http://nmayer.eu/publis/MODSEC08_Mayer-Dubois-Matulevicius-Heymans_metrics-risk-management.pdf

The National Science and Technology Council. (2006). *Federal plan for cybersecurity and information assurance research and development*. Retrieved April 6, 2009, from http://nitrd.gov/pubs/csia/csia_federal_plan.pdf

Obenzinger, H. (2005). "*What can a literature review do for me?": How to research, write, and survive a literature review.* Retrieved April 3, 2009, from http://128.223.179.107/aim/Capstone07/LiteratureReviewHandout.pdf

Patriciu, V., Rriescu, I., & Nicolaescu, S. (2006). Security metrics for enterprise information systems. *Journal of Applied Quantitative Methods,* 1(2). Retrieved April 8, 2009, from http://jaqm.ro/issues/volume-1,issue-2/pdfs/patriciu_priescu_nicolaescu.pdf

Payne, S. C. (2006, June 19). *A guide to security metrics.* SANS Institute. Retrieved April 7, 2009, from http://www.sans.org/reading_room/whitepapers/auditing/a_guide_to_security_metrics_55?show=55.php&cat=auditing

Pironti, J. P. (2007). Developing metrics for effective information security governance. *Information Systems Control Journal. 2,* 33-38. Retrieved April 7, 2009, from http://www.isaca.org/AMTemplate.cfm?Section=20075&Template=/ContentManagement/ContentDisplay.cfm&ContentID=40248

Prominent. (n.d.). *Merriam-Webster's Online Dictionary*. Retrieved May, 2, 2009, from: http://www.merriam-webster.com/dictionary/prominent

Rapple, B. (2005). *How do I write a literature review?* Retrieved April 3, 2009, from Boston College Web site: http://libguides.bc.edu/print_content.php?pid=1194&sid=4957&mode=g

Ravenel, P. J. (2006). Effective operational security metrics. *The Information Systems Security Association (ISSA) Journal, February 2006.* Retrieved April 12, 2009, from *https://www.issa.org/Library/Journals/2006/February/Ravenel%20-%20Effective%20Operational%20Security%20Metrics.pdf*

Rosenblatt, J. (2008). Security metrics: A solution in search of a problem. *EDUCAUSE Quarterly.* 31 (3), 8-11. Retrieved April 22, 2009, from http://net.educause.edu/ir/library/pdf/EQM0832.pdf

Sademies, A. (2004). *Process approach to information security metrics in Finnish industry and state institutions.* Espoo [Finland]: VTT Technical Research Centre of Finland. Retrieved April 6, 2009, from http://www.vtt.fi/inf/pdf/publications/2004/P544.pdf

Schechter, S. E. (2004). *Computer security strength & risk: A quantitative approach.* Unpublished doctoral dissertation, Harvard University. Retrieved May 6, 2009, from http://www.eecs.harvard.edu/~stuart/papers/thesis.pdf

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world*. New York: John Wiley.

Shinn, L. (n.d.). *Slouching? Measure your security posture.* Retrieved April 23, 2009, from Inc. Technology Website: http://technology.inc.com/security/articles/200805/posture.html

Sonnenreich, W., Albanese, J., & Stout, B. (2006). Return on security investment (ROSI): A practical quantitative model. *Journal of Research and Practice in Information Technology.* 38 (1), 45. Retrieved April 20, 2009, from http://www.jrpit.acs.org.au/jrpit/JRPITVolumes/JRPIT38/JRPIT38.1.45.pdf

Stevens, J. F. & Willke, B. (2005). *Enterprise security metrics: Taking a measure of what matters*. Paper presented at the Secure IT 2005 Conference. Retrieved April 20, 2009, from http://www.secureitconf.com/OLD/2005/presentations/Enterprise%20Security.pdf

Sundaram, A. (2008) Security metrics: Hype, reality, and value demonstration. *The Information Systems Security Association (ISSA) Journal, May 2008.* Retrieved April 12, 2009, from https://www.issa.org/Library/Journals/2008/May/Sundaram-Security%20Metrics-Hype%20reality%20and%20value%20demonstration.pdf

Swanson, M., Bartol, N., Sabato, J., Hash, J., & Graffo, L. (2003). *Security metrics guide for information technology systems*. Gaithersburg, MD: National Institute of Standards and Technology, Technology Administration, U.S. Dept. of Commerce. Retrieved April 8, 2009, from http://purl.access.gpo.gov/GPO/LPS35202.

Tipton, H. F., & Krause, M. (2007). *Information security management handbook*, sixth edition. Boca Raton, Fla: Auerbach Publications.

Vaughn, R. B., Henning, R., & Siraj, A. (2003). *Information assurance measures and metrics - state of practice and proposed taxonomy*. Presented at the Annual Hawaii International Conference on System Sciences. Retrieved April 20, 2009, from http://www2.computer.org/portal/web/csdl/doi/10.1109/HICSS.2003.1174904 von Solms, B. (2000). Information security: The third wave? *Computers and Security. 19* (7), 615-620. Retrieved April 8, 2009, from http://adam.rau.ac.za/~basie/PDF/sdarticle10.pdf

Wang, C.& Wulf, W.A. (1997). *Towards a framework for security measurement*. Paper presented at the proceedings of the Twentieth National Information Systems. Retrieved April 17, 2009, from http://csrc.nist.gov/nissc/1997/proceedings/522.pdf

Wang, J. A., Xia, M. & Zhang, F. (2007). Metrics for information security vulnerabilities. *Proceedings of Intellectbase International Consortium*, USA, 1, 284-294. Retrieved April 17, 2009, from http://www.intellectbase.org/ProceedingsFall2007.pdf

Whitman, M. E., & Mattord, H. J. (2004). *Management of information security*. Boston: Course Technology.

Appendix A: Search Strategy Details

Search Engine / Database	**Search Terms**	**Results**	**Quality of Results**
ACM Digital Library	Security & Metrics	3,482	Good – Several relevant articles
	Information Security & Metrics	3,333	Good – Several relevant articles
	Information Security & Measurement	5,566	Poor – No relevant material
	Information Security & Statistics	4,283	Poor – No relevant material
CiteSeer.IST	Security & Metrics	12	Poor – No relevant material
	Information Security & Metrics	0	Poor – No relevant material
	Information Security & Measurement	0	Poor – No relevant material
	Information Security & Statistics	0	Poor – No relevant material
Clusty	Security & Metrics	894,300	Fair – Use clusters option on lf hand site for better results
	Information Security	750,300	Fair – Limited

Search Engine / Database	**Search Terms**	**Results**	**Quality of Results**
	& Metrics		applicable articles
	Information Security & Measurement	1,388,000	Fair – Limited applicable articles
	Information Security & Statistics	4,090,000	Fair – Limited applicable articles
CompletePlanet (Computing & Internet Tree)	Security & Metrics	6	Poor – No relevant material
	Information Security & Metrics	4	Poor – No relevant material
	Information Security & Measurement	1	Poor – No relevant material
	Information Security & Statistics	19	Poor – No relevant material
Google Scholar	Security & Metrics	109,000	Fair – Limited applicable articles
	Information Security & Metrics	105,000	Fair – Limited applicable articles
	Information Security & Measurement	1,480,000	Fair – Limited applicable articles
	Information Security & Statistics	1,190,000	Fair – Limited applicable articles
	Approaches to	73,100	Fair – Limited

Search Engine / Database	**Search Terms**	**Results**	**Quality of Results**
	Security Metrics		applicable articles
	Defining Security Metrics	52,300	Fair – Limited applicable articles
	Information security & Key Performance Indicator	162,000	Poor – No relevant material
	Information security & metrics & KPI & Measurement	4,190	Good – Several relevant articles
Summit	Security & Metrics	99	Good – Several relevant articles
	Information Security & Metrics	28	Good – Several relevant articles
	Information Security & Measurement	56	Fair – Limited applicable articles
	Information Security & Statistics	395	Poor – No relevant material
UO Library Catalog EBSCO HOST Research Databases – Academic Search	Security & Metrics	5	Fair – Limited relevant articles
	Security & Management	2002	Poor – No relevant material

Search Engine / Database	**Search Terms**	**Results**	**Quality of Results**
Premier Database	Security & Statistics	334	Poor – No relevant material
	Information Security & Metrics	3	Fair – Limited applicable articles
	Information Security & Measurement	5	Fair – Limited applicable articles
	Information Security & Management	563	Poor - Too broad
	Information Security & Statistics	22	Poor – No relevant material
WorldCat	Security & Metrics	401	Good – Several relevant articles
	Information Security & Metrics	239	Good – Several relevant articles
	Information Security & Measurement	439	Fair – Limited applicable articles
	Information Security & Statistics	4,739	Poor – No relevant material
	Information Security & Key Performance Indicator	6	Poor – No relevant material

Search Engine / Database	**Search Terms**	**Results**	**Quality of Results**
	Information Security & Reporting	1,001	Fair – Limited applicable articles
Yahoo	Security & Metrics	31,200,000	Good – Several relevant articles
	Information Security & Metrics	25,200,000	Good – Several relevant articles
	Information Security & Measurement	292,000,000	Good – Several relevant articles
	Information Security & Statistics	158,000,000	Poor – No relevant material

Appendix B: Manual-Coding Results

Author	Concept or Category Coded	Manual Search	Relevant	Notes
Brotby (2008)	Accountability	5	Yes	chap. 13.3.2
	Compliance	33	Yes	chap. 1.4, 5.2, 9.3.1, 13.1, 13.3.2
	Security effectiveness	22	Yes	chap. 13
	Program initiation	7	Yes	chap. 1
	Metric development	77	Yes	chap. 4-13
	Metrics program	12	Yes	chap. 2, 12.1
	Reporting	22	Yes	chap. 1, 11.3, 13.3.2,
	Maintaining	4	Yes	chap. 5,
Bryant (2007)	Accountability	13	Yes	p.7, 48, 55, 65, 79, 135, 149, App III
	Compliance	25	Yes	p. 48, 74, 117, 126, 144, 147, 150, 154, 167, 168
	Security effectiveness	1	Yes	p. 69
	Program initiation	0		
	Metric development	0		
	Metrics program	83	Yes	p. iv, 7-9, 11, 13-14, 69, 84, 88, 91-92, 104, 136, 154, 165
	Reporting	42	Yes	p. 7, 9, 13, 50, 87, 111-112, 126, 131, 153, 155
	Maintaining	2	Yes	85
Chapin (2005)	Accountability	0		
	Compliance	8	Yes	p. 2-4
	Security effectiveness	0		
	Program initiation	0		
	Metric development	0		
	Metrics program	0		
	Reporting	1	No	
	Maintaining	0		
Chew (2006)	Accountability	8	Yes	p. 1, 6, 12, 40

Author	**Concept or Category Coded**	**Manual Search**	**Relevant**	**Notes**
	Compliance	7	Yes	p. 1, 3, 36
	Security effectiveness	0		
	Program initiation	0		
	Metric development	0		
	Metrics program	7	Yes	p. 17, 21-22
	Reporting	46	Yes	p. 1, 3-10, 12, 18, 24
	Maintaining	0		
Chew (2008)	Accountability	6	Yes	p. 1, 10
	Compliance	7	Yes	p. 10, 17, 22, 37
	Security effectiveness	2	Yes	p. 10, 30
	Program initiation	0		
	Metric development	0		
	Metrics program	0		
	Reporting	52	Yes	p. 1, 2, 8-9, 16, 20-22, 33, 36
	Maintaining	2	Yes	p. 39
CISWG (2005)	Accountability	2	Yes	p. 16
	Compliance	34	Yes	p. 4, 9, 12-13, 15-23
	Security effectiveness	0		
	Program initiation	0		
	Metric development	0		
	Metrics program	0		
	Reporting	12	No	
	Maintaining	0		
Herrmann (2007)	Accountability	44	Yes	chap. 1, 3
	Compliance	32	Yes	chap. 3.1, 3.4, 3.9
	Security (effectiveness)	37	Yes	chap. 3
	Program initiation	0		
	Metric development	45	Yes	chap. 2

Author	**Concept or Category Coded**	**Manual Search**	**Relevant**	**Notes**
	Metrics program	47	Yes	chap. 1.2, 2.6, 2.7, 2.8
	Reporting	34	Yes	chap. 1.1, 2.9, 3.3, 3.13
	Maintaining	16	Yes	chap. 1.1, 2.9, 3.1, 4.2
Hinson (2006)	Accountability	0		
	Compliance	2	Yes	p. 33, 36
	Security effectiveness	0		
	Program initiation	0		
	Metric development	0		
	Metrics program	0		
	Reporting	13	Yes	p. 35-37
	Maintaining	0		
Jaquith (2007)	Accountability	23	Yes	p. 11, 51, 90, 91, 93-94, 119, 263, 283, 295
	Compliance	66	Yes	p. 24, 29, 31, 81, 93, 98, 126-130, 207, 241, 255, 264-265
	Security effectiveness	11	Yes	p. xxii, xxiv, 22-23, 90, 127, 149, 250, 255, 288
	Program initiation	0		
	Metric development	0		
	Metrics program	16	Yes	p. xxi, 29, 37, 45, 95, 220-224, 230, 244-247, 249
	Reporting	32		p. 16, 91, 115, 120, 134, chap. 6, 226
	Maintaining	9		p. 111
Kahraman (2005)	Accountability	6	Yes	p. 1-3, 42
	Compliance	8	Yes	p. 2-3, 12-13
	Security effectiveness	0		
	Program initiation	0		
	Metric development	0		
	Metrics program	9	Yes	p. 6-7, 9, 41, 43
	Reporting	4	Yes	p. 2
	Maintaining	1	No	

Author	**Concept or Category Coded**	**Manual Search**	**Relevant**	**Notes**
Kark & Stamp (2007)	Accountability	1	Yes	p. 8
	Compliance	11	Yes	p. 2, 4, 6, 8
	Security effectiveness	0		
	Program initiation	0		
	Metric development	0		
	Metrics program	24	Yes	p. 2, 4-6
	Reporting	12	Yes	p. 1-5, 7
	Maintaining	0		
Kark (2008)	Accountability	3	Yes	p. 12
	Compliance	7	Yes	p. 2, 4-5, 9
	Security effectiveness	0		
	Program initiation	0		
	Metric development	0		
	Metrics program	32	Yes	p. 2-4, 6-12
	Reporting	20	Yes	p. 2-4, 6-7, 10-13
	Maintaining	1	Yes	p. 7
Jansen (2009)	Accountability	1	Yes	p. 3
	Compliance	1	Yes	p. 1
	Security (effectiveness)	14	Yes	p.1, 5-6
	Program initiation	0		
	Metric development	0		
	Metrics program	0		
	Reporting	3	Yes	p. 1
	Maintaining	1	Yes	p. 1
Patriciu (2006)	Accountability	1	No	
	Compliance	4	Yes	p. 151, 157-158
	Security effectiveness	0		
	Program initiation	0		
	Metric	0		

Author	Concept or Category Coded	Manual Search	Relevant	Notes
	development			
	Metrics program	0		
	Reporting	0		
	Maintaining	0		
Payne (2006)	Accountability	0		
	Compliance	5	Yes	p. 3-4
	Security effectiveness	0		
	Program initiation	0		
	Metric development	0		
	Metrics program	17	Yes	p. 1-4, 6-7
	Reporting	4	Yes	p. 6
	Maintaining	1	Yes	p. 3
Pironti (2007)	Accountability	0		
	Compliance	10	Yes	p. 1-4
	Security effectiveness	0		
	Program initiation	0		
	Metric development	1	Yes	p. 2
	Metrics program	0		
	Reporting	13	Yes	p. 1-4
	Maintaining	0		
Schechter (2004)	Accountability			
	Compliance	1	No	
	Security (effectiveness)	8	Yes	p. 1, 23, 27, 33, 96, 106
	Program initiation	0		
	Metric development	0		
	Metrics program	0		
	Reporting	26	Yes	p. 72, 82-83
	Maintaining	0		
Swanson et al. (2003)	Accountability	12	Yes	p. 1, 9-10, A54, A61
	Compliance	31	Yes	p. 2, 10-11, 22, 25, A7-A60

Author	**Concept or Category Coded**	**Manual Search**	**Relevant**	**Notes**
	Security effectiveness	2	Yes	p. 19, 21
	Program initiation	0		
	Metric development	1	Yes	p. vii
	Metrics program	49	Yes	p. 1-10, 13-15, 24-25, 27
	Reporting	51	Yes	p. 1-2, 7-10, 12-13, 24-25, 28
	Maintaining	6	Yes	p. 10, 14
Wang (2007)	Accountability	1	Yes	p. 283
	Compliance	0		
	Security effectiveness	0		
	Program initiation	0		
	Metric development	0		
	Metrics program	0		
	Reporting	0		
	Maintaining	0		
Whitman & Mattord (2004)	Accountability	0		
	Compliance	0		
	Security effectiveness	0		
	Program initiation	1	Yes	p. 245
	Metric development	3	Yes	p. 244-245
	Metrics program	1	Yes	p. 244
	Reporting	1	Yes	p. 245
	Maintaining	0		