MEASURING SYSTEMS SECURITY:

AN INITIAL SECURITY THEORETICAL CONSTRUCT FRAMEWORK

By

Jennifer L. Bayuk

A DISSERTATION

Submitted to the Faculty of the Stevens Institute of Technology
in partial fulfillment of the requirements for the degree of

DOCTOR OF PHILOSOPHY

Jennifer L Bayuk, Candidate	12/01/11 Date

ADVISORY COMMITTEE

Ali Mostashari, Chairman	12/01/11 Date
Barry Horowitz	12/1/11 Date
Paul Rohmeyer	12/01/11 Date
Brian Sauser	12/1/11 Date

STEVENS INSTITUTE OF TECHNOLOGY
Castle Point on Hudson
Hoboken, NJ 07030
2011

MEASURING SYSTEMS SECURITY:

AN INITIAL SECURITY THEORETICAL CONSTRUCT FRAMEWORK

ABSTRACT

System security metrics have evolved side by side with the advent of cyber security tools and techniques. They have been derived from the techniques rather than specified as system requirements. This dissertation surveys the evolution and state of the practice of system security metrics from both a technical and historical perspective. The survey leads to the conclusion that currently accepted methodology for measuring system security has no empirical basis. This research provides new criterion with which to evaluate security metrics, and proposes a new methodology for *security theory attribute construction* ("STAC"). The STAC framework has been applied to case studies in Cloud Computing and Mobile Communications. Specific research in a variety of system security topics is recommended to reinforce these results, and provide theoretical foundation for more effective tools and techniques for systems security engineering.

Author: Jennifer L. Bayuk

Advisor: Ali Mostashari

Date: December 1, 2011

Department: School of Systems and Enterprises

Degree: Doctor of Philosophy

ACKNOWLEDGMENTS

This has truly been a journey into uncharted territory for which every available navigation aid assumes a different set of environmental conditions. I am fully indebted to my committee members who lent every available methodology within their grasp of expertise to my cause. Ali Mostashari led this team of diverse adventurers with a rigorous scientific approach, iteratively measuring the extent to which each endeavor brought us closer to our destination. Barry Horowitz maintained our focus on the community goal of security improvement by consistently framing successive attempts at security problem resolution in terms of efficacy against an adversary. Paul Rohmeyer repeatedly quantified this research in terms of its contribution to the field of system security, and ensured that no stone was left unturned to strengthen our bonds with scientific thinkers in the security community. Brian Sauser intuitively drew parallels between systems security problems and other complex problems that benefit from applied systems thinking, which ultimately led to the development of the STAC framework. In addition, though not an official member of the committee, Stevens adjunct professor Bill Miller provided valuable insight on how to connect the research hypothesis to survey results. Thank you all for your efforts to bring this journey to fruition.

I also acknowledge my husband for his support throughout this journey, though support is far too meek a word to describe the sustenance he provides. Thank you Michael.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. Introduction and Problem Setting

The topic of this dissertation is System Security Architecture Metrics.

1.1. Introduction

Steady escalation of threats to both cyberspace and cyber-supported infrastructure has prompted recognition that security cannot be assumed to be provided by physical isolation [1]. Vast sums of money have been directed toward systems security solutions[2-4]. However, there is no theoretically proven method of deciding on what that money should be spent. Recent history of data breach cases and industrial control system incidents has called attention to the inadequacy of our current approaches to systems security [5-9], but no new paradigms have evolved to guide management decisions toward practical security solutions. This research is intended to introduce a new paradigm in the form of a system security engineering framework that promotes recognition of strong security by emphasizing security validation metrics. Due to the possibility of threats that are unknown [10], no system will ever be 100% secure. Nevertheless, the framework is expected to provide value to executive decision-makers through its ability to measure the security of a given system compared to other systems.

1.2. Overview of the Problem

Any attempt to depict systems security necessarily relies on some metric that identifies security as a systems attribute. Metrics rely on measures. Measurement is the process of

mapping from the empirical world to the formal, relational world. The measure that results characterizes an attribute of the object under scrutiny. Metrics are frameworks that are used in measuring, for example, the metric system. Security is not the object of measurement, nor a well-enough-understood attribute of a system to easily define metrics. Nevertheless, the field of security metrics is rich and fertile. This dissertation surveys that field and suggests a new framework approach to understanding and appreciating both current and potential future security metrics.

A foundation for any metrics framework is a shared understanding of its target. The dictionary defines security as a feeling of safety, and there is no other authoritative definition to which security researchers agree. However, a recent research roadmap for systems security engineering prepared by the Systems Engineering University Affiliated Research Center offered this definition: *Something that thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value [11]*.

The definition has all the elements of multiple industry, national, and international security standards [12-14], as well as face validity in that it can be understood in layman's terms [15]. However, there is no generally accepted method of directly measuring security in terms of achievement in thwarting threats. So those engaged in security metrics must measure other things and draw conclusions about security goal achievement from them. Moreover, though the definition sufficed for its purpose in motivating security research, it is not precise enough to be a target for metrics. In order to

test the definition, we must specify that security is a system attribute. Hence, for the purposes of this study, we define system security as a *system attribute that that thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value.*

1.3. Problem Statement

Executive decision makers, typically system owners and operators, have requirements for secure systems. Systems engineers are charged with proposing alternative options for implementing secure solutions. Yet there is no shared understanding of the problem domain and no common concept of a correct solution. This is not a disconnect unique to decision makers and engineers, but a general lack of a recognizably correct articulation of the concept of system security. Decision-makers and systems engineers need to collaborate on the overall systems engineering trade space. To achieve this collaboration with respect to security, they need some common way to evaluate the security benefit that may be expected from each of multiple alternative security features presented by systems engineers. Simply put, the problem to be solved is:

How can system security be measured?

In order to provide precise articulation for an intangible concept, the definition of system security is presented as a theory of security using formal logic. In this chapter, the formal logic presentation uses some English words to make the reasoning easy-to-follow. The pure propositional logic expressions for the lettered statements in this section are included in Appendix A.

Premise:

(A) "System X is secure" if and only if "X thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value"

Definitions:

(B) S(X) equals by definition "X is a system"

(C) "S" equals by definition the attribute "Security"

(D) "E(X,A)" equals by definition "Attribute A is a property of system X, that is, X exhibits property, or attribute, A"

(E) "V(A)" equals by definition "Attribute A is an exploitable vulnerability that permits system disruption"

(F) "T(B,P)" equals by definition "Attribute B thwarts perpetrator P"

(G) "P(Y,A) " equals by definition "Y is a perpetrator who exploits attribute A"

Putting these definitions together, we can construct the hypothesis with a few statements of formal logic.

First, it is possible that there is a system vulnerability that no perpetrator exploits:

(H) ~Exists(Y)(P(Y,V(A)))

Second, where a system has an exploitable vulnerability as an attribute as in statement H, it may be that the system has another attribute that thwarts the perpetrator from that exploit:

(I) For all A (E(X,V(A)) (Exists(B)(E(X,B) AND T(B,P(Y,V(A)))))

If every system vulnerability meets conditions of either statement H or I, then the system itself would be secure, given premise A. Formally stated, the attribution of security is:

(J) E(X,S) ←→For all A, (E(X,V(A)) ➔ (~Exist(Y)(P(Y,A) OR Exists(B)(E(X,B) AND T(B,P(Y,A)))

In words, a system is secure if and only if, for all of its attributes, if any one of them is a vulnerability, then either there are no perpetrators who exploit that vulnerability, or the system also exhibits an attribute that thwarts any perpetrator who exploits that vulnerability.

If the problem statement is now considered, "How do you measure E(X,S)?" then the formal definition creates at least two vectors for providing an answer: as the absence of vulnerabilities and/or the means to thwart exploits. Both of these factors are inherently uncertain. As both vulnerabilities and exploits cannot be defined without reference to the mission or purpose of the system, these concepts must also be explored to frame any problem solution. Nevertheless, the problem statement does provide enough guidance to clarify the objectives for recognizing system security via system security metrics. The metrics could then be used by executive decision makers and systems engineers engaged in trade space discussions concerning the value of system security features.

1.4. Research Objectives

Building on our problem statement, we assume that there are perpetrators who seek to exploit vulnerabilities, that is, statement H is not universally true, which is stated as:

(K) For some A (Exists(Y)(P(Y,A)))

This leaves the security attributes to be measured as those corresponding to the second half of the OR clause in statement J, that is, statement I:

(I) For all A (E(X,V(A)) (Exists(B)(E(X,B) AND T(B,P(Y,A))))

That is, that to attribute security to a system, none of its other attributes (with the exception of those corresponding to H) should be vulnerabilities, unless there is also a system attribute that thwarts perpetrators who would exploit the vulnerability.

The objective of this research is to provide two contributions to security engineering:

- An authoritative methodology for planning security and creating associated metrics at the system level through identification of attributes corresponding to B in statements I and J.
- An explanatory and descriptive framework for systems security that executive decision makers and systems engineers may use to understand the security implications of system design alternatives.

1.4.1. *Research Hypothesis and Implications*

The research hypothesis, based on the problem statement, research question, and research objectives, is:

(L) System security can be measured if and only if the system-level attributes of

- *mission and purpose,*
- *validated input, and*
- *incident detection and response*

contribute to that measurement.

To make this hypothesis consistent with the problem statement requires a few more definitions:

(M) "M" equals by definition the attribute "mission and purpose"

(N) "I" equals by definition the attribute "validated input"

(O) "R" equals by definition the attribute "incident detection and response"

(P) E(X,S) ←→ S includes M AND I AND R

Note that M and I and R are all system-level attributes. A system attribute is a generic term to refer to a property of a system. A system attribute refers to component parts of a system or to the system as a whole. A *system-level* attribute is one that can *only* be observed at the top level of a hierarchical structure forming a system comprised of organized people, process, and technology. Changes in components may affect a system level attribute but the effect will not be a straightforward measurement resulting from the component change, it would be a result of reorganization of the set of parts that comprise the system. Inter-component interaction as well as system interaction with the environment is a key characteristic of system-level attributes. Following Bar-Yam's definition of system-level properties as *emergent*, system-level attributes are defined as those that reside in the ensemble and can only be observed in the state of a system as a whole rather than in any subset of components [16]. In the case of security, the hypothesis that these three security attributes are at the *system level* requires that at least three attributes corresponding to B in statement J are a system-level attribute rather than an attributes of a component.

To formally state the hypothesis in the context of the definition of security in the problem statement now requires a definition of a system-level, rather than a component-level security attribute. For an example of the contrast, a system-level attribute may be observed at the system boundary such as a periphery defense posture, while a component-level attribute may be the technical configuration of a component, such as a firewall's rule set. The system-level posture may be affected by changes in a component attribute, but they are not the same and the system-level posture cannot be derived from the composition of the technical configurations of its parts without attention to structure and other system-level attributes.

A formal definition of a system component is:

(Q) "C(X,T)" equals by definition "T is a component of system X"

Using the definition of a component, the definition of E(X,S) may be refined to refer to the three hypothesis-identified system-level attributes of X, not attributes that may be attributed to a subsystem composed of some system components but not others. This clarification is formalized with a statement that systems composed of an incomplete subset of components of X do not have system-level attributes. That is, any system that has component overlap with X but does not have all components of X does not have X's system-level attributes.

(R) For all A (E(X,A) ←→ For all Y ((S(Y) AND

(For all T, (C(Y,T) → (C(X,T)) AND (Exists U (C(X,U) AND ~C(Y,U))))

→ ~E(Y,A))))

So to be perfectly clear, the hypothesis encompasses statements P, R, and J, and may be rewritten as:

(S) E(X,S) ←→ (Exists E(X,M) AND E(X,I) AND E(X,R)) AND

((For all Y ((S(Y) AND (For all T, (C(Y,T) → (C(X,T)) AND (Exists U (C(X,U) AND ~C(Y,U)))) → (~(M = U) AND ~(I = U) AND ~(R = U)))) AND

(For all A, (E(X,V(A)) ➔ (~Exist(Y)(P(Y,A) OR Exists(B)(E(X,B) AND T(B,P(Y,A)))

Statement S clarifies the definition in the context of the hypothesis that a system-level attribute either applies equally to all components or applies to no components as it emerges from their combination. The validation of this hypothesis will imply that system security architecture should always include requirements analysis with respect to system-level attributes. This is nothing less than a paradigm shift for the field of system security metrics because system security is typically measured as adherence to component requirements specifications which are typically aggregated to form measures of overall system security. This issue will be more thoroughly covered in Chapter 2. Although security metrics using systems-level attributes appear in the literature, these are typically deemed too difficult to measure and no standard methods exist to measure them. However, there are many standards that rely on metrics based on component measurement aggregation.

If the hypothesis is correct, it implies that systems security metrics should not be limited to component attributes, but should instead be examined at the system level. A framework that is used to measure system security would be extensible to facilitate security measurement for systems of different origin and composition. An example of such a framework would provide a proof of concept to support the feasibility of hypothesis implications.

1.4.2. *Hypothesis Validation*

Given that there is no deductive logic that will allow us to deduce security metrics from premises, validation of the hypothesis proceeds by induction. The research hypothesis is restated as a *null hypothesis*:

(T) System security can be measured by measuring attributes of components.

To test the null hypothesis, systems security experts were surveyed and asked to identify the relative importance of system security attributes. The role of these experts was to provide an independent and authoritative opinion on the relative efficacy of candidates for measurable dimensions of system security that have so far been identified from the security metrics literature. Because there were no project or policy goals involved in the process of gathering opinions from these experts, their views were expected to reflect a technical expert's approach to reasoning about uncertainty in their own field of expertise while providing an anonymous, and therefore conflict-free, communication vehicle for their collective opinion.

To ensure that the security metrics literature is not missing any important attributes, experts were encouraged to contribute additional attributes that were not identified in the survey. The security attributes that were agreed upon by experts were deemed most important to measure when creating security metrics. The research method was to survey the experts as described, and to identify if any of the three identified system-level security attributes are identified by the experts as most important to measure in order to measure system security. Where this occurs, it is taken as evidence to reject statement T,

the null hypothesis that all important dimensions of system security are attributes that can be measured at the component level.

1.4.3. *Research Approach*

Building on our definition of security and the above formal arguments, key questions were formed to provide evidence that security experts would reject or support the null hypothesis. They were asked to identify system attributes that contribute to system security as well as the utility of various system security measurement techniques for the purpose of establishing system security metrics. Sets of questions were combined to provide evidence to support a conclusion that system security dimensions are considered by security subject matter experts to be measures of security. Multiple other questions in the survey were included to create “noise” for the purposes of ensuring that survey participants were not limited in their responses by expected conclusions. Where relevant, respondents were also given the choice of “other” to ensure that ideas about security metrics not present in the survey may be collected as well.

The plan for the survey was documented for the Stevens Institute of Technology Institutional Review Board (IRB). The IRB’s major concerns were the source of research material, plans for recruitment of subjects, as well as potential risks and procedures for protecting against or minimizing any potential risks. The extent to which the survey responses are valid will depend on the level of expertise and experience of the respondents, so security industry standard demographic questions were used as a filter

with which to analyze all results. The logic behind the survey design is included in Chapter 2.

The survey provided enough evidence to reject the null hypothesis. Hence, the research hypothesis is supported because the three systems-level security attributes identified in statement (L) were identified by the experts as most important to the attribution of security. Moreover, these three attributes may be measured using techniques that are (1) available and (2) capable of providing reliable measurement. These and other measures identified by the experts were combined into criteria for system security metrics and used to develop a security metrics framework by which to map measurable security attributes to systems architecture. All of the measures identified as "most important" were system-level, emergent attributes rather than attributes of components. The resulting security metrics framework is expected to facilitate the activities of system owners and operators who wish to secure their systems.

1.5. Uniqueness of this Research

Security research has to date mostly concentrated on technology issues involved in implementing security features as opposed to the measure of systems security as a whole. Although one textbook attempted to model enterprise security using the Zachman framework [17], that attempt did not result in any comprehensive way to model or measure the security of any given system. Even textbooks that combine security and engineering principals emphasize the mindset of the security engineer rather than suggest any standard methods, tools, and procedures with which to approach systems security

engineering [18-20]. This research will be the first attempt to prove that one approach to systems security is demonstrably better than another.

1.6. Dissertation Organization and Structure

This dissertation is composed of six chapters. This introductory chapter discusses the security measurement problem in terms of a theory of system attributes that contribute to security. The other five chapters describe subsequent steps of the research process, specifically:

- Chapter 2 examines and classifies currently available literature on system security metrics.
- Chapter 3 describes data collection and analysis via a survey of security experts.
- Chapter 4 utilizes the judgment of those experts in proposing the security measurement strategy.
- Chapter 5 applies the proposed measurement strategy to real world system security engineering problems.
- Chapter 6 draws conclusions concerning the validity of the research hypothesis.

Each of these other five chapters is described in a single paragraph below. Following these chapters is a list of publications or planned publications that were based on this research. This dissertation also includes several appendices related to the survey construction, administration, and analysis.

Chapter 2 is a review of the literature on security metrics. It covers industry standards, academic analysis, and practitioner materials. It provides a foundation for understanding how security may be productively measured by examining how systems security may be scrutinized within the context of scientific validity, and describes the potential contribution of various types of measurements to an evaluation of system security capability. The chapter concludes with a discussion of the research problem and hypothesis in the context of the literature review.

Chapter 3 chronicles the development of a list of system-level security metrics in the context of the survey process. It describes the statistics used to analyze the survey results. The chapter ends with examples of subject matter expert comments on system-level security measures.

Chapter 4 applies the survey results identified in Chapter 3 to systems engineering. It introduces a security metrics framework that integrates the security metrics taxonomy introduced in Chapter 2 with systems security engineering lifecycle activities. It shows how the framework may be applied in analysis of requirements, concepts of operations, verification and validation planning, and ongoing evaluation procedures.

Chapter 5 applies the framework described in Chapter 4 to two case studies. Both of the cases describe actual enterprise architecture initiatives in major global corporations that have significant security requirements. One is the enterprise infrastructure for management control over application lifecycle for cloud computing. The other is

enterprise infrastructure to support and control remote access to internal computing facilities via mobile communications.

Chapter 6 discusses the contribution of this research to the field of systems security metrics. It emphasizes the uniqueness of this research, and summarizes why the framework is a more comprehensive approach to security metrics than other currently available guides. The chapter concludes with a description of future research in the area of systems security metrics.

2. Security Metrics Literature Review

Systems security measurement presents a problem of *wicked* proportion, where *wicked* refers to the nature of a problem for which there is no ultimate right solution, but merely a goal of situational improvement for which the planner has solemn accountability [21]. This makes it difficult to arrive at a concept of security that will allow it to be understood as a tangible systems attribute and to validate its measurement according to these scientific standards. As Dan Geer, a founding member of securitymetrics.org, put it:

"Speaking as a once-upon-a-time statistician, one has to ask if we are at the hypothesis testing stage or still at the hypothesis generation stage. I know that I am at the latter which is more or less why I am always looking for data on which I can do some exploratory analysis. People who have data can do hypothesis testing, of course, but as with the rest of science, once someone has generated and tested an hypothesis, then

reporting it with sufficient attention to the "Methods" section is so important -- others can then do the verification step with their own data / apparatus / analysis."[22]

Geer illustrated his view with this example:

"*Josh Corman, 451 Group, presciently looked closely at the Verizon Data Breach Report(s) and noticed that the share of significant breaches that involved vulnerabilities for which a patch was available at the time of exploit declined from 100% to 30% to 6% to 0% over four successive years. In other words, and I have heard Peter Tippett say this in plain English, the implication is that it is not worth patching if you are a prime target as the opposition no longer needs to look for unpatched vulns (sic) since with the series of 100>30>6>0 we have quantitative evidence that patchability no longer matters.*

Once we have 'enough' examples of test/re-test reliability, then comes the meta-analysis stage, i.e., where N studies are combined to decide whether, say, Red Dye #2 should or should not be banned. Here in cybersecurity, that will be a long time yet in coming."[22]

Today's security metrics have evolved via consensus and not scientific endeavor, and have not been subject to Geer's recommended level of scientific scrutiny. This study is unique in that standards for scientific measurement in security metrics will be explicitly observed. There are four major types of validity used in scientific evaluation:

Face: a measurement technique is valid with respect to "face" or has "face value" when an unsophisticated judge determines that employing the

technique is suitable or unsuitable for its expected use, that is, a layman would accept it [15]

Content: a measurement of an elusive attribute may employ the technique of measuring things that are both measurable in themselves and may be composed in such a way that the elusive attribute predictably emerges [23]

Criterion: a measurement of behavior via a technique of measuring things that are predictive of the behavior, and is valid to the extent it can be shown that measurement results correspond to the criterion [23]

Construct: a theoretical construct that includes a set of hypothetical correlations that, if shown to be consistent with an initial definition, could serve to make the theory even stronger, and is valid to the extent each measure relates to the other measures consistent with theoretically derived hypotheses concerning the concepts [23]

This chapter compares these concepts of scientific validity to current literature in security metrics. It uses these concepts to classify security metrics.

2.1. Face Valid

The concept of face validity in security metrics has been widely denounced as *security theatre* [24, p.38]. Security theatre is something that looks like it increases security, but in fact affords no more safeguards than if it did not exist at all. A security-receptionist is one example of security theatre. The average layman may regard the fact that a door is

monitored by a person as an indication that the person will challenge those who are not authorized to access the building. However, in many cases, the security-receptionist has no ability to prevent adversaries from entering, and it is not even part of their job function to do so. For example, the person may be stationed at the door merely to assist customers of building tenants who cannot find an office. In these cases, the existence of a security-receptionist should not be considered a measure of security. In another example, the person may be charged with preventing unauthorized access, but given no means by which to determine who is authorized to enter the building, and so defaults on the side of allowing access. This is the case where a guard is charged with checking that each person entering the building has a certain format of a picture ID, but not with any way of determining whether the ID was forged. This is also security theatre.

However, within the security profession, there is some consensus on what is commonly meant by security, and this reflects a layman's view of what the professional practice of security should entail. The definition of security offered in Section 1.2 has face validity in that it can be understood and generally accepted in layman's terms:

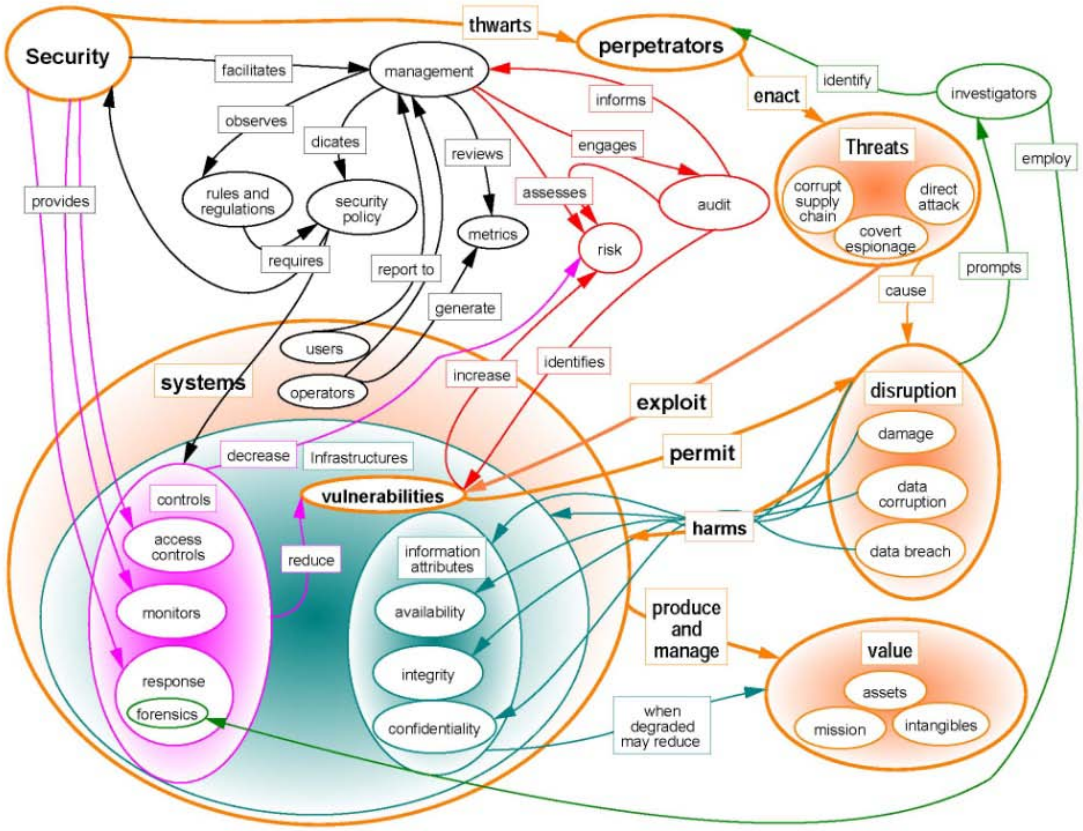
Security: Something that thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value.

The concept has been further developed to include multiple perspectives on security that appear in the literature. In order to clarify the multiple perspectives security, the creators of this definition modeled them via a systemigram, which is pictured in Figure 1. The word systemigram was coined by as a convergence of "system" and "diagram" [25]. It is

a tool to assist systems engineers in succinctly describing a topic without sacrificing detail required to accomplish clarity. A systemigram is composed of nodes and links. Nodes are nouns. Links are verbs. A systemigram is read by focusing on a noun as a concept, and following the links from it, reading the verbs to understand the relationships between concepts. A systemigram has a "mainstay" thread, which starts with the most upper-left node and ends with the most bottom-right. In Figure 1, the mainstay is the definition of security that has the most face validity.

Other sets of noun-verb combinations link the main concept defined to other contexts which are also face-valid, though to a lesser degree. A complex system will typically be understood in specialized contexts, and the systemigram demonstrates that. The detail under the link label “harm” demonstrates that those who work in information processing tend to conceptualize security in terms of information attributes that are subject to similar types of threats and disruptions. The depiction of security measures on the left adopts the point of view of a network engineer, who typically views security in terms of preventive, detective, and corrective controls designed to minimize vulnerabilities and reduce risk. The management nodes and links adopt a perspective on security from the point of view of technology governance. Other nodes and links adopt an audit and investigator view, respectively. The full systemigram provides a holistic view of security that depicts it as having multiple stakeholders.

Figure 1: Security Systemigram



2.2. Content Valid

As there is no direct way to measure whether something *thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value*, systems security is considered an elusive attribute that may be measured only by the presence of defining characteristics that require expertise to understand and thus are outside the realm of face validity.

The history of this type of security metrics begins with the first attempts to standardize a scale for measuring computer security. The first such system security standards body was established in the late 1970s by the US Department of Defense (DoD) Directive 5200.28 [26]. In early 1980s, it produced the *Trusted Computer System Evaluation Criteria* (TCSEC), also known as the *Orange Book* due to the color of its cover. Using formal models to describe logical access controls, the Orange Book set requirements in the form of a hierarchical structure of security features. A was the highest score afforded by the hierarchical labeling system and D was the lowest. For a system to be labeled secure, it had to verifiably exhibit all of the security features at some level in the hierarchy. Its security metric was the highest alphabetical label for the corresponding level. At the lowest level there was no security. In the middle there was password authentication and *discretionary* access control, which allowed users with access to files to share them with other users. At the top level was *mandatory* access control expected to be configured by administrators, accountability tracing for every operation in the system, and verified design. A security testing process was set up whereby vendors could have their systems rated by a team using the Orange Book levels as a security metric. This is a content metric as the system had to contain a set of security features, and the requirements to receive a label could be verified by examining the system itself.

In the mid-1980s, most of the products being rated using Orange book metrics were computer operating systems and many could not achieve very high ratings. The TCSEC was a countermeasure to the threat surface of 1980, and system threat surface had evolved to include network connectivity. The Orange Book standard could only be

applied to a single system, and was operating-system centric, so a new set of systems security criteria was devised that was intended to provide more flexibility to designers of security tests. This is called the *Common Criteria* [27]. First published in the mid-1990s, the Common Criteria allowed the owner of a targeted system to specify what security features the system is supposed to have, and the testers are supposed to design customized tests to verify that those features work as advertised. The term *Target of Assessment*, or *Technical Target of Assessment*, or TTOA, became the label for the system as configured and tested, no matter how many technical components it may comprise (note that TTOA has become a generic term for the technical scope of an assessment). As in the Orange Book, the Common Criteria specifies hierarchical levels of validation, and the resulting security rating reflects the level of testing that was successful. The lowest level is functional, followed by structural, and then methodical. Higher ratings may be obtained if it can be demonstrated that the product was methodically designed, and even higher by being semiformally or formally verified. The Common Criteria has evolved into an international standard [28].

Both the Orange Book and Common Criteria are effective verification measures only of systems that are designed to include a specified set of features that are assumed to provide system security. However, in practice, these security features did not always work correctly, especially in systems that did not received the highest ratings, those corresponding to verified design. System security vulnerabilities in the form of software bugs and design flaws are common. This recognition led to the establishment of security content metrics that could certify that a system was free of known vulnerabilities. To this

end, the US National Security Agency (NSA) and the National Institute of Standards and Technology (NIST) introduced a new type of content metrics based on system security configuration, the security configuration automation protocol (SCAP) [29]. This program created a set of specifications for software vulnerabilities testing that required tests to be defined in terms of configuration on specific systems platforms as the target of a vulnerability scan. These tests are called Common Vulnerability Enumerations and Common Configuration Enumerations (CVE and CCE). A language has been created for defining enumerations and technical specifications for its implementation have been developed. Though many vendors cooperated, others found the framework too constraining. The first target for SCAP tests was the Microsoft XP operating system, which has so many security design flaws that no amount of configuration would ever protect it from vulnerabilities.

Nevertheless, SCAP is a good example of a content metric because it uses the same methodology that many enterprise security products use to verify that security has been configured to some documented standard [30]. One such product has even become a generic name for alerting on any system configuration that deviates from an enterprise standard: *tripwire* [31]. The products allow an enterprise to set and maintain technical configuration variables that are expected to enforce security mechanisms on individual machines. The products centrally report security metrics based on the content of those machines.

Security with respect to a given TTOA is measured by its ability to conform to specifications, given the values in a set of variable configurations that make the operating systems and network software difficult to penetrate. Without sacrificing our definition of security, a content validity test would be to compare the variables in the configuration files to a set of values for those variables that have been previously determined to thwart perpetrators who enact threats to exploit vulnerabilities that permit system disruption. Those systems whose configuration files contain the expected content would be validated to warrant a label of "secure," given this definition. One of the issues complicating the application of measurement to the property of security is a question of scope. Technical and process metrics are concerned with components rather than the system as a whole. Aggregation is used to make claims for security at the system level. If the TTOA is just a component of a larger system, it may then be a subject of debate as to whether the security content of this one target, in combination with other system components, may contribute to an assessment that the system as a whole is secure. This debate has a long history and shows no signs of being resolved soon [32, 33]. Even if simple aggregation of content metrics were sufficient to measure security, content valid security metrics present difficulty because it requires enumeration of the complete domain of the content required to accomplish security [23]. Again, security is an elusive concept.

Another complication for TTOA metrics is that systems generally include operators who have the ability to accomplish configuration changes. It is hard to assess content validity with respect to our definition of security in an environment where changes are frequent on both the threat and the configuration front. For example, the configuration variables

may be set so that only authorized software is running on the machine. But if authorized software has security bugs or flaws due to either a mistake in a software update or an emerging threat technology, then the content validation will pass but will not accurately measure security. Also, there may be situations where one organization is exposed to threats that are not faced by another organization. In these cases, TTOA configuration metrics may only be *internally valid*, that is, they might be completely applicable in the sample of systems under examination, but not extensible to the domain to which conclusions might reasonably be extended [34].

Even if methods for preserving security through TTOA composability and operator integrity were available, in most systems of any significant level of size and complexity, in order to be assured that the system can withstand perpetrator attacks, content validity alone would not be sufficient. This is because systems in operation are constantly exposed to new threats, and content validity as we have described it with respect to a TTOA requires reuse of a configuration known to thwart previous attacks. Therefore, though content validity may be a security metric, it cannot be assumed to satisfy (H) for the purposed of affirming statement (J). However, it is possible that, in combination with other system attributes, a security content metric may satisfy (I).

2.3. Criterion Valid

Criterion validity relies on the ability to predict future behavior based on the results of a test process that produces a test score. To devise a test for secure behavior requires both knowledge of system attributes that drive secure system behavior as well as the ability to

devise a test score that corresponds to those attributes. An intuitive example often used to illustrate the concept of criterion validity is the test that one takes to obtain a driver's license, because it relies on a written test of knowledge about how to handle a car in given environment, but tests by observation are only a small subset of the potential situations a driver will face. In the field of security metrics, the most common example of this type of metric is a security audit.

There are two types of systems security audits: compliance and substantive [35]. Compliance audits begin with a documented process for achieving a security goal and tests that the process has been implemented with no relevant exceptions. Substantive audits begin with a content description of secure system configuration and tests to ensure that the configuration is correctly implemented. Substantive audits are reducible to content validity, so the type of audit that tests for criterion validity is a compliance audit. However, tests for compliance may contain elements of both content and behavioral testing.

An example of criterion that is expected to predict secure behavior is the Payment Card Industry Data Security Standard (PCI-DSS) [36] . The scope of the standard is data that is used to process credit card payments. The criteria for security attribution range from building a secure network to maintaining an information security policy. The tests range from sampling system components as TTOAs to observing systems operators executing incident response procedures. The test result is a worksheet completed by the assessor indicating the extent of system compliance with the PCIS-DSS standard.

Another example of criterion that is expected to predict secure behavior is a vulnerability score based on a penetration test. Vulnerability scoring has its roots in the physical security concept of design basis threat (DBT) [37]. A DBT describes characteristics of the most powerful and innovative adversary that it is realistic to expect security to protect against. In New York City, it may be a terrorist cell equipped with sophisticated communications and explosive devices. In Idaho, it may be a 20-strong posse of vigilantes carrying machine guns on motorcycles. Adopting a DBT approach to security implies that the strength of security protection required by a system should be calculated with respect to a technical specification of how it is likely to be attacked. In physical security, this process is straightforward. If the DBT is a force of 20 people with access to explosives of a given type, then the strength of the physical barriers to unauthorized entry must withstand the ton of force that these twenty people could physically bring into system contact. Barrier protection materials are specified, threat delay and response systems are designed, and validation tests are conducted accordingly. In cyber security, potential attacks are the aggregated set of all publicly documented cyber attacks to date.

Tests for systems-level DBTs are typically referred to as *penetration tests* or *pentests*, for short. They rely on publicly available databases of known exploited vulnerabilities such as the National Vulnerability Databse (NVD) [38]. An automated scan for these vulnerabilities is designed to imitate the behavior of a malicious perpetrator, and the test's criterion validity is based on its ability to predict how a system will withstand an attack. Vulnerability test scores are assigned based on scan results. Security software that tests for such vulnerabilities usually use a traffic light metric, where a system is typically

rated red if it has any vulnerabilities that may be exploited to gain administrative access to the system, yellow if an exploit allows unauthorized access, and green if the system does not have any of the vulnerabilities included in the scan [39]. However, some vulnerability scanning procedures use more sophisticated of these scoring methods, such as the Common Vulnerability Scoring System (CVSS) [40]. CVSS evaluation produces a numeric score based on how easy it is for a perpetrator to accomplish significant damage by exploiting a vulnerability. Systems that score high have vulnerabilities that are easily exploited, and those exploits results in total system compromise. Regardless of the scoring system, each vulnerability is scored independently, and someone must in advance decide which vulnerabilities will be tested for in a given system. There are as of this writing 48607 vulnerabilities and 886 software weaknesses in the National Vulnerability Database. No system can be tested for all known vulnerabilities. Even if there was a practical way to test a system for all of them, studies show that such vulnerability tests are fraught with both false positives and negatives due to the difficulty of designing and executing tests in multiple environments [41].

Even if pentests were 100% accurate, they only test for vulnerabilities that are known. Yet the discovery of previously unknown threats is so routine that security professionals have a term for them: zero-day threats. As explained by Acohido and Swartz, a zero-day threat is a hazard so new that no viable protection against it yet exists [42]. No vulnerability scans exists for a zero-day threat either. The only recourse for measuring security at this point is an after-the-fact classification for post-mortem comparison of similar events [43]. While a vulnerability metric may be useful to a security practitioner

that believes the organization is protected against commonly known attacks, as McGraw put it, they are a *badness-ometer* [44]. If a complete inventory test for all the known vulnerabilities was passed with flying colors, this would not mean that the system was secure, it could simply mean that *if* the system had security bugs, those bugs were not yet identified.

Although there is criterion validity in the theory that there *should* be a constant correlation between the ability to pass an audit or a pentest and the ability to withstand an attack, actual evidence to support that claim is lacking, and plenty of evidence exists to the contrary. For example, in a recent cybersecurity court case, it was revealed that a credit card processing company passed a PCIS-DSS audit designed to ensure confidentiality of information, and a short while later, they experienced one of the largest data breaches in history [5, 45]. Virtually all global international banks methodically pentest all of their Internet applications, yet they still experience security breaches. So, in practice, tests have not yet been devised that withstand scrutiny with respect to criterion validity for security. This does not mean that there is no hope for criterion validity in security metrics, just that the theory and associated evidence that would be required to support criterion validity has not yet been developed.

2.4. Construct Valid

This leaves us with construct validity, which involves identifying relationships between theories of security and measurable things that correlate with those theories. As Carmines and Zeller put it, we correlate “the extent to which a particular measure relates to the

other measures consistent with theoretically derived hypotheses concerning the concepts" [23]. Security is an abstract concept, but it may be described by means of a theory. Given a theory of security, it should be possible to derive testable hypotheses that, if true, would provide evidence to support the theory. A hypothesis on what it means to be secure, and whether a system that corresponds to a theoretical description of security can confirm that hypothesis, would serve to test validity of a theory of security. Such descriptions and tests would also provide a comprehensible framework through which to evolve a more thorough understanding of security itself.

There is no lack of motivation behind publication of a theory of security. Regardless of the fact that full-fledged validity tests are unavailable, requirements for security assessment have long driven responsible assessors to adopt theoretical constructs for security attribution. Both public and private sector organizations charged with security assessment on behalf of those stakeholders have adopted and endorsed various systems security control practices published in the form of *system security standards* (for example: [13, 46-49]). These constructs are based on the assessor's collective belief that some enterprises are better at security than others, and the practices of those organizations should be a model that others can use to make significant leaps forward (the most straightforward application of this reasoning is found in the ITPI standard [50]). These practices are not limited to standards in the sense of the documented content of technical variables, as described in Section 2.1. They mostly reflect consensus around security management practices that are widely believed to result in superior system security. By incorporating these standards into their systems security assessment

processes, many audit and regulatory organizations have tacitly characterized systems security as a state of system owner-operator compliance with these standards.

The basic theoretical construct behind a security standard involves a process and a set of security controls. Figure 2 illustrates the structure of today's security standards [51]. As in the systemigram of Figure 1, the mainstay of Figure 2 reflects a statement that is uncontroversial: *security standards dictate process that recommends controls that reduce the vulnerability of assets*. Note that standards do not actually recommend controls themselves, but are presented as methods for system owners and operators to evaluate their own systems and use the results of their evaluation to identify a set of security control mechanisms that suit their requirements. These standards typically contain little guidance by way of methods, processes, or tools with which to analyze systems or system components in order to identify the relevant security requirements. The processes they dictate assume rather than analyze the root causes of security issues.

Another type of theoretical construct for security is a security model. Like management standards, these reflect consensus among security subject matter expert practitioners as to best practice in systems security, though at the technical configuration rather than the management level. They include network-centric defense-in-depth layered controls, data-centric digital rights management, system and device security services, and software security patterns [52]. Figure 3 illustrates some common security models.

Figure 2: Security Standards as a Theoretical Construct

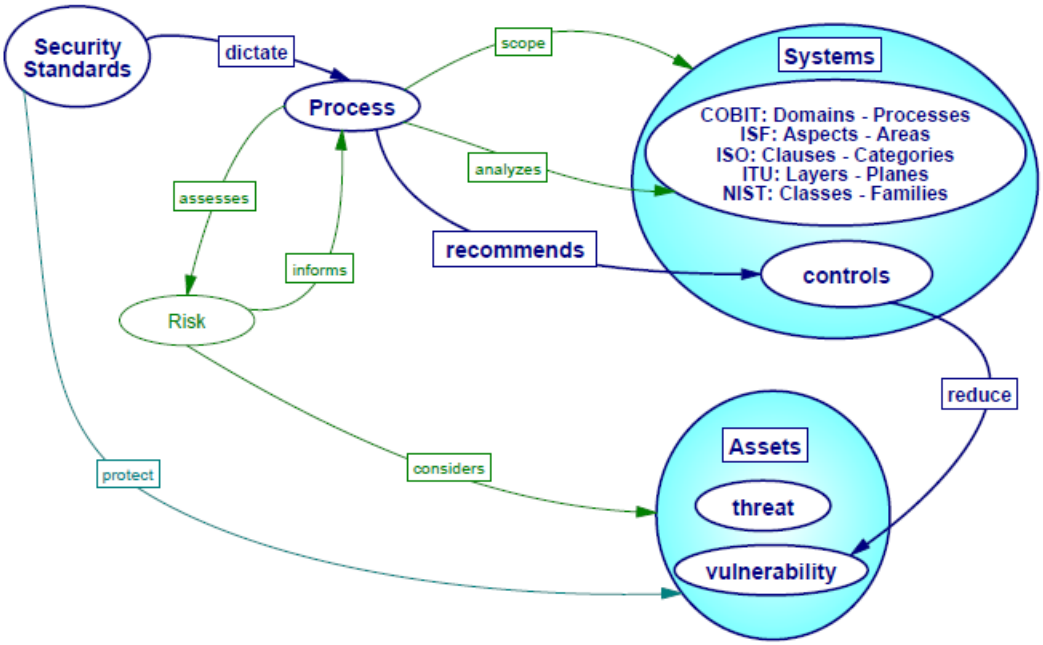
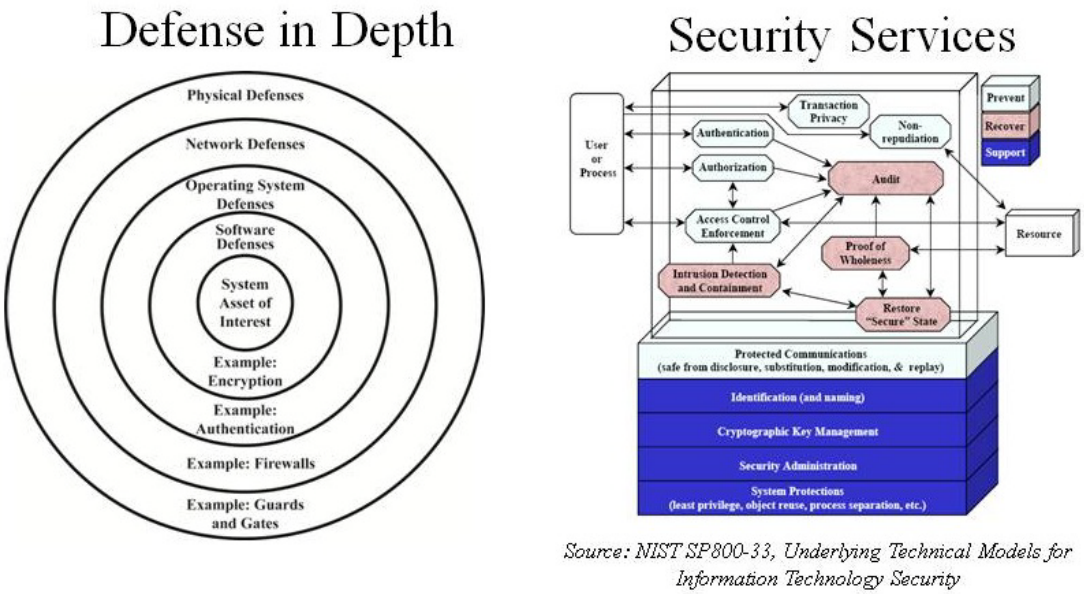


Figure 3: Security Models



Source: NIST SP800-33, Underlying Technical Models for Information Technology Security

Though security models are useful in formulating technical security requirements, they still leave the choice of components to the risk-judgment of management, and they have not as yet come up with measurement methods that would be of utility for security metrics. As different systems have different security requirements, a theory of security cannot be reducible to a generic model, but must somehow incorporate a system-specific version of the model to demonstrate how security may be supposed to be accomplished for a given system. The theoretical construct could be used to make an hypothesis about whether the model would render effective security if all elements described by it were functioning correctly. Verification tests could be devised for key controls identified by the model to see if they are working. Advances in content and criterion metrics are typically employed to demonstrate compliance with both standards and models. Although external verification that standards are met are difficult due to the nature of point-in-time assessment, where content and criterion tests are performed continuously by the system owner-operator, adherence to a standard should be verifiable.

If the theoretical construct underlying a given security standard or model is valid, it is possible to identify a close correlation with successful implementation of the standard or model and effective system security. That is, there would be no counterexample of a system that implemented the standards or model but nevertheless had bad security. However, neither a security management standard nor a security model can stand alone in supplying a full theory of security. The more secure management may be rendered weak by vulnerable technology and visa versa. Note that some of today's standards approximate a customized approach to technology better than others, but they still fall

short when it comes to validating that the planned technology design achieves security goals [53]. Moreover, while there are currently no recommended positive measures that would validate the theory that a standard or model achieves security, any one security breach or badness-ometer test result is taken as counterevidence that the standard or model actually achieves security. As in any theoretical construct, a theory of security is easier to disprove than to prove. Despite the heavy burden of regulatory security standards that every bank must follow, the financial services literature is jam-packed with stories of successful security breaches [54]. In some cases, standards advocates are even hard-pressed to find an example of the standard as implemented. For example, every US Government Accounting Office (GAO) audit has found some flaw in security standards implementation, even the audit of GAO itself [55]. As any indication that security is absent while the construct holds is proof that the concept does not work, there is no validity as yet in standards or models-based information security.

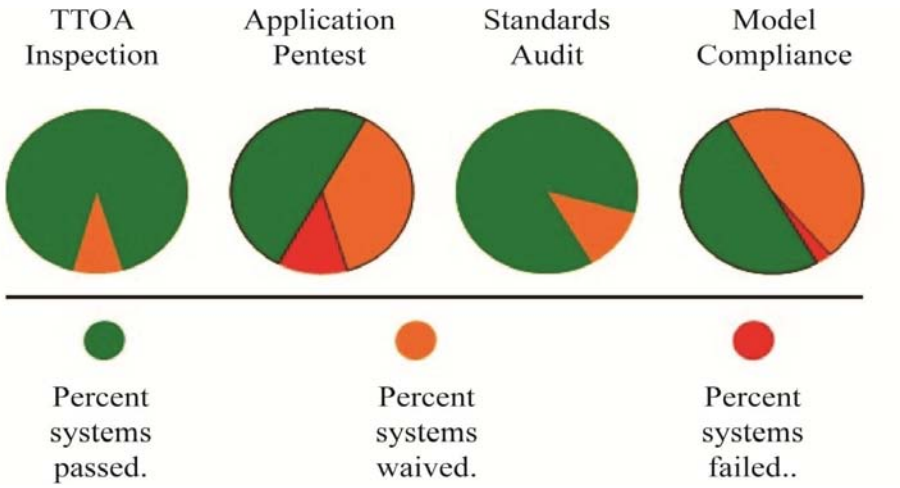
2.5. Taxonomy

From the forgoing, it is clear that there are a plethora of innovative approaches to security metrics. What passes for the state-of-the-art in security metrics is not a standardized way to measure security. In fact, there is not even a standard taxonomy for security metrics. Principals to be used in such classification have been explored by different researchers, and these explorations have produced different results. A survey of security metrics taxonomy efforts was recently summarized by Savola [56], who reported a common theme in security metrics literature, that taxonomies of security metrics tended to address

technical configuration and operational process from the point of view of security management rather than to directly described business goals for security. Even taxonomies that include *governance* in addition to management tend to focus on the security management tasks that are evidence of governance, and those metrics could easily be considered part of the management category [57]. Moreover, as there is currently no convergence around a *single* organizational management structure for security, no corresponding authoritative security metrics taxonomy has emerged.

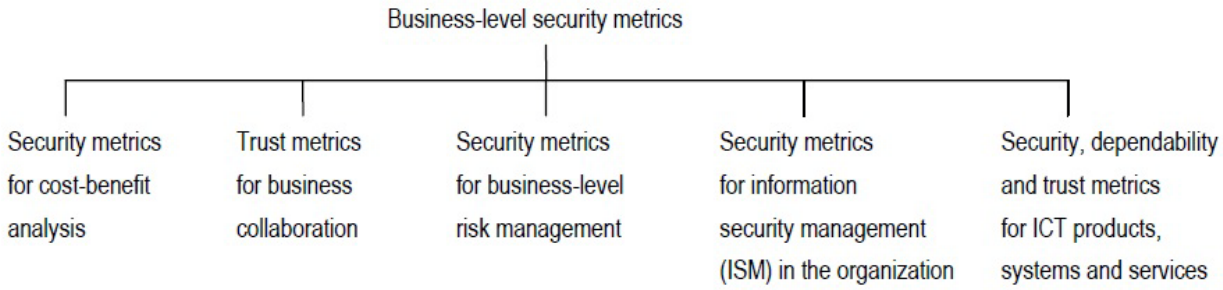
In practice, the combination of content, criterion, and standards-based constructs is combined into dashboard and scorecard presentations such as the one in Figure 4 [58, 59]. As Figure 4 illustrates, content and criterion are verified by TTOA inspection and test results and are presented to management as a percentage of technology environment's inspection and test results, as well as compliance with security standards and models [60]. The slice of the pie chart that is orange in Figure 4 refers to the common practice of risk acceptance in security compliance activities. Where a system owner/operator is willing to tolerate the risk of non-compliance with security standards, security practitioners typically do not count non-compliant systems as test failures, but as waivers [61]. In Figure 4, such waivers are identified, but often they are not, and this makes it hard to use security metrics reports as evidence that security constructs are implemented.

Figure 4: Example Security Metrics



Note that the security metrics dashboard of Figure 4 does not include any validation criteria, simply verification that different types of security measures have been applied. In an attempt to correct this focus on simple verification as opposed to security goal validation, security researchers have proposed that business-level security metrics take precedence over others. For example, Savola suggests a hierarchical metrics structure where business process security metrics are at the top, and the next level includes information security management, trust in business collaboration, cost-benefit analysis, business risk management, and technology products and services [56]. As illustrated in Figure 5, he then expands the taxonomy a few levels lower to include security information management and the technology products and services. However, Savola's taxonomy is still subject to a wide variety of interpretation by security practitioners and he provides no examples of what metrics should go in each category.

Figure 5: Example Business-Oriented Security Metrics Taxonomy [56]



The assumption that there are many more security metrics to be incorporated in some taxonomy than are currently documented in literature is not unique to Savola. The academic study of system security has resulted in a plethora of security metrics candidates for potential inclusion in as-yet-to-be-defined constructs. These include security metrics for mathematical modeling of security management processes [62], weighting network forensics evidence to increase probabilities of conviction [63], quantifying network threat surface using hidden Markov models [64], comparing attack outcomes to different configurations of the same technical variables[65], creating trust models with ant-based stigmergy [66], using game theory to determine security investment strategies [67], complex mathematical models for assessing software security [68, 69], and tracking a "honeymoon period" between the first release of a program and the disclosure of its first vulnerability [70]. Most of these are the subject of one or two papers by the same group of authors, and rely on data that is not completely described, and also usually includes subjective measures of probability. However, it is possible that this literature does contain a few potentially useful metrics that are not incorporated into any content, criteria, or construct theory as yet. That is, although none of these candidates

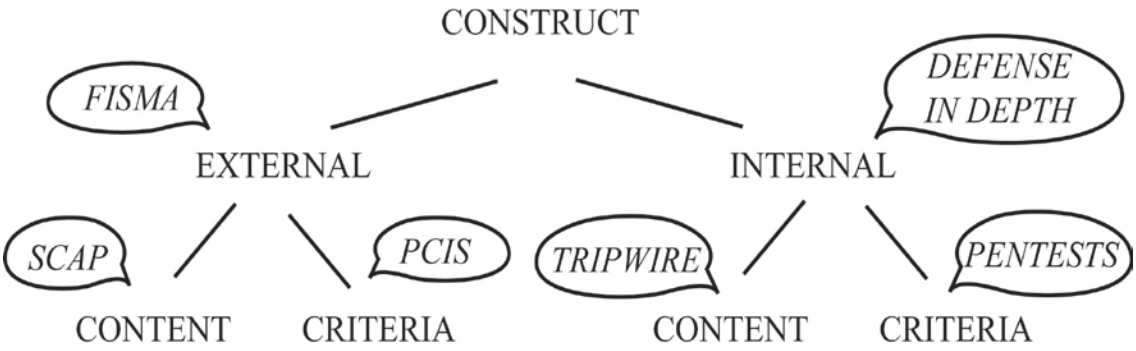
is currently considered a measureable security attribute, some may feasibly be incorporated into a theory of systems security.

At this point in time, there are at least 900 metrics that exist in the systems security literature. They range from the percentage of machines in inventory with up-to-date anti-virus programs to the percentage of executives who go to jail for compromising information. This we know is true, because they are listed in a 2007 book, *A Complete Guide to Security and Privacy Metrics* by Herrmann [71]. Despite this large number of metrics, Herrmann claims only to have included metrics that she considered appropriate for use in decision-making by practicing auditors, engineers, and managers. Herrmann's intent was to create a useful menu for security practitioners, and so she purposely excluded metrics that were abstruse or that relied heavily on an intuitive understanding of complex mathematical models. This idea is echoed in security literature: that metrics which form the basis for decisions should be well understood. As Jaquith put it, "transparency facilitates adoption by management" [58 , p.20]. As Pironti put it, "keep it simple" [72].

Figure 6 shows the taxonomy of security metrics so far described. At the lowest level, metrics are equivalent to measures of content or criteria. Both content and criterion tests may be manual or automated. Content tests are performed by inspection and criteria test by observation of behavior. At the highest level, security metrics are complex sets of measures combined into constructs. The construct components may be set by a source

external or internal to the system being measured. Examples of metrics in each taxonomy category appear in balloons pointing to their corresponding placement in the figure.

Figure 6: Taxonomy of Security Metrics



2.6. Outlook

Though the Section headings 2.1 through 2.4 that outline the taxonomy of security metrics end in the word "valid," from the content of those sections, it is clear that none of the types of metrics discussed are valid from either a scientific perspective or engineering perspective. Not even the simple and transparent dashboards used to facilitate security decision making provide conclusive evidence that the given system has an attribute called security. At best, these metrics provide verification that plans for security measures have been accomplished. In recognition of the need for research in security metrics, NIST characterizes this distinction as *correctness versus effectiveness* [73]. It has even been acknowledged in security metrics texts that the state of the art in security metrics is to design metrics to manage security processes rather than attribute or identify security [74]. From an architecture perspective, verification is the determination that a system is "built

right" while validation determines that the "right system was built" [75]. Hence, before any claim can be made for the validity of security metrics, we must have some idea of what we are actually trying to build.

In the field of systems engineering, the terms *correctness* and *effectiveness* may properly be translated as *verification* and *validation (V&V)* [52]. *Verification* and *correctness* criteria ask, "*Did we build the system according to specifications?*" *Effectiveness* and *validation* ask, "*Did we specify the right system?*" Yet the systems engineering approach to security has yielded no better outcome than security standards bodies. Although one systems engineering textbook attempted to model enterprise security using an enterprise architecture framework [17], that attempt did not result in a comprehensive way to validate enterprise security, and the book is now out of print. Even textbooks that combine security and engineering principals emphasize the mindset of the security engineer rather than suggest any standard methods, tools, and procedures with which to approach systems security engineering [18, 19].

Moreover, organizational focus on risk management as a key responsibility for security management has decoupled the presentation of security itself from the security metrics presented to executive management. Management reporting with respect to systems security now focuses almost exclusively on risk analysis as measured by standards and best practices rather than progress with respect to the organization's goals and objectives for security. None of these supposed systems-level measures, however, attempts to quantify whether a system actually achieves security goals. Instead, they view a system

through a small lens of security indicators, and use the indicators to make claims about system security as a whole.

Nevertheless, this literature review is not intended to dismiss current literature in security metrics, but to be informed by it. From the content of today's security standards, it has evidently been the experience of the security professionals who wrote the standards that effective security requires a coordinated effort in management, operations, and technology. There is also agreement in security metrics literature that security metrics should facilitate decision-making and improve organizational performance with respect to security [58, 59, 71, 74]. Each system attribute cited as important to maintenance of security goals and objectives is a candidate for inclusion in the set of system attributes referred to in statement (J). As described at the end of Section 2.2 in the context of content metrics, criterion and construct metrics are possible system attributes that, in combination with other system attributes, may satisfy (I). Any set of system attributes that does this may be considered to be a construct valid indicator of system security. Such attributes would be considered important aspects of system security. This study claims that such attributes are system-level rather than component-level attributes.

3. Security Survey

A scientific perspective on the realm of security metrics evokes an image of a system attribute called *security* that can be measured in various indirect ways, where some measures provide more information than others. Like some natural and visible yet little understood attribute of the planet such as the weather, we are completely engulfed by

security attributes, good or bad, and have multiple methodologies with which to attribute properties to them. Nevertheless, the definition of the thing as a whole escapes us, and there is the constant reminder that the unknowable aspects of it may render our current theories untenable. If the current set of security metrics is considered a sample from which to draw observations on security in order to strengthen a theory of what security is, then we must measure those system characteristics that will provide the most significant correlations with the properties that define our core concept of this elusive attribute.

The fact that security metrics seem so elusive has led some security subject matter experts to declare that security is more of an art than a science [19]. A validation method of an artist as opposed to a scientist may be described as something like, "*I know it when I see it*." One reason security seems to fall into that category may be that there is something of a mystique around the ability to practice security in the context of alternative systems environments. Security architects tend to be jacks-of-all-trades when it comes to technology, and cannot explain how they know to do what they do when they design secure systems. Debates among researchers and practitioners on the topic of qualifications for the professional practice of security often center on this distinction of art versus science and pseudo-science [76, 77]. But technical verification does not seem to require the talents of an artist, and validation that security goals are met does not seem to be the forte of an artist. So those on the art side of the debate are comfortable with the void in the current state of the practice around validation, and this leaves us with simple verification that systems are configured or operating as intended, as opposed to validation that systems are secure [for example, 29]. From an architecture perspective, *verification*

is the determination that a system is “built right” but does not provide information on whether the “right system was built” [75]. Any claim to be made for the *validity* of security metrics must reference some preconception of what achieving security goals means in the context of the system mission or purpose.

As noted in Section 2, there is currently agreement in security metrics literature that security metrics should facilitate decision-making and improve organizational performance with respect to security. But there are no attempts on record to directly measure the elusive attribute of security itself. Security metrics cannot directly measure security, but they can be designed to measure system attributes that *strengthen* the system against vulnerability to threat. In the formal language of our statements (F) and (G), “T(B,P(Y,A))” that equals by definition “Attribute B thwarts a perpetrator who exploits attribute A),” the fact that B is an attribute that compensates for vulnerability A makes B an important dimension of system security. This study is meant to settle the “*art or science*” debate firmly on the side of science. To provide evidence in support of a scientific conclusion that something can be known about properties like B, and to support the hypothesis that attributes like B are system-level attributes, a survey of system security experts was conducted.

3.1. Survey Design

The purpose of the survey was to elicit expert opinions on the properties (and associated measures) of a system that could be used to attribute security to it. The objective was to have systems security experts rank systems attributes according to their importance in

comprising overall system security. A complete description of the survey, including its design, construction, results, analysis, is in Appendix C.

The survey was facilitated by a team of security expert reviewers, who immediately commented that security experts are busy, and tend to get distracted by changes in the threat environments for systems for which they are responsible. For this reason, they advised that the survey questions be streamlined and easy to answer quickly. This led to changes in questions that asked for rankings and weightings of security attributes in favor of a simple Likert-scale approach to registering opinions about security attributes. An important design criteria for the survey was that it had to take the minimum amount of time required to deliver opinions on the entire field of study that currently constitutes security metrics.

The change in approach was not viewed as a total setback due to known issues with similar studies which solicited rankings and weights. In a similar study with respect to multi-attribute utility measurement in the domain of nuclear power plant planning, Borcherding et.al, used four weighting methods: the ratio method, the swing weighting method, the tradeoff method and the pricing out method [78]. The comparison of results showed significant consistency and validity problems of these methods to the extent to which they persist in a carefully designed interactive elicitation process. Speculated reasons for this inconsistency ranged from participant boredom with the information elicitation process to lack of true expertise on the part of the respondents. The study recommended using carefully designed interactive procedures for elicitation. For this

reason, the security survey respondents were requested to provide contact information if they would be willing to participate in interactive follow-up if necessary.

The Boercherding study used an Analytic Hierarchy Process (AHP) approach, wherein one assumes that the problem space can be fully described in a way that priorities, allocations, weights, and preference ratios are judgments that can be represented with meaningful numbers which represent the importance of and dependencies between alternative and competing system attributes [79]. This approach was not used in the security survey because decision analysis in security is not as mature as it is the domain of nuclear power plant planning. Security outcomes cannot yet be quantified in as clear terms, such as lost lives and environmental damage. The literature review of Chapter 2 makes it evident that there is no starting hierarchy that is agreed upon, and yet there is a wealth of candidate attributes for ranking.

Another approach to structuring this type of problem is described by Thurstone, where participants initially are provided with a blank slate, and iterative ranking exercises reduce the population of the overall attribute list [80]. Unfortunately in this study, the time constraints of potential survey respondents made it improbable that many would participate if they had to start with a blank slate. The properties that professionals currently use are readily apparent from the literature survey in Chapter 2, and these were used as a starting point.

Both the Boercherding and the Thurstone studies acknowledge that it is necessary to analyze sensitivity to ambiguous questions, as well as any potential environmental

changes in criteria that may result in changes in judgments. Decision theory as applied to security has typically concentrated on only one aspect of the security problem, which is investments in a single technology [81]. Thus the security problem, in contrast to that performed by Boercherding and the Thurstone, does not have a framework waiting to be articulated. Rather, this research is necessary *due* to the fact that system security is not yet well understood enough to place a framework around the problem for others to refine with weights. Yet neither do we begin with a blank slate. This situation is typical in any theory construction for attributes that are not well understood. As observed by Wrenn, "We must subject our constructs to measurement if we are to test our theories, but if we were to insist that theory tests wait until we have a fully axiomatic theoretical model, scientific inquiry would virtually halt" [82]. Hence, in addition to the security attribute criteria, the survey contained other questions of multiple types which were designed to provide background "noise" in order to ensure that bias in attribute select choices was minimized. It also allow respondents to clarify their responses with open ended questions and selections of "other".

To answer prior studies' concerns related to ambiguity and environment, attribute-related questions were ranked using three methods: Thurstone's method post-initial ranking, where the positioning of items on the Thurstone scale can be found by averaging the percentiles of the standard normal distribution corresponding to the proportions of the respondents preferring one item over each of the others [80], the One Number Method, which was designed to register strong opinions [83], and a simple survey rating system based on proportionate number of respondent selections. These rankings were separated

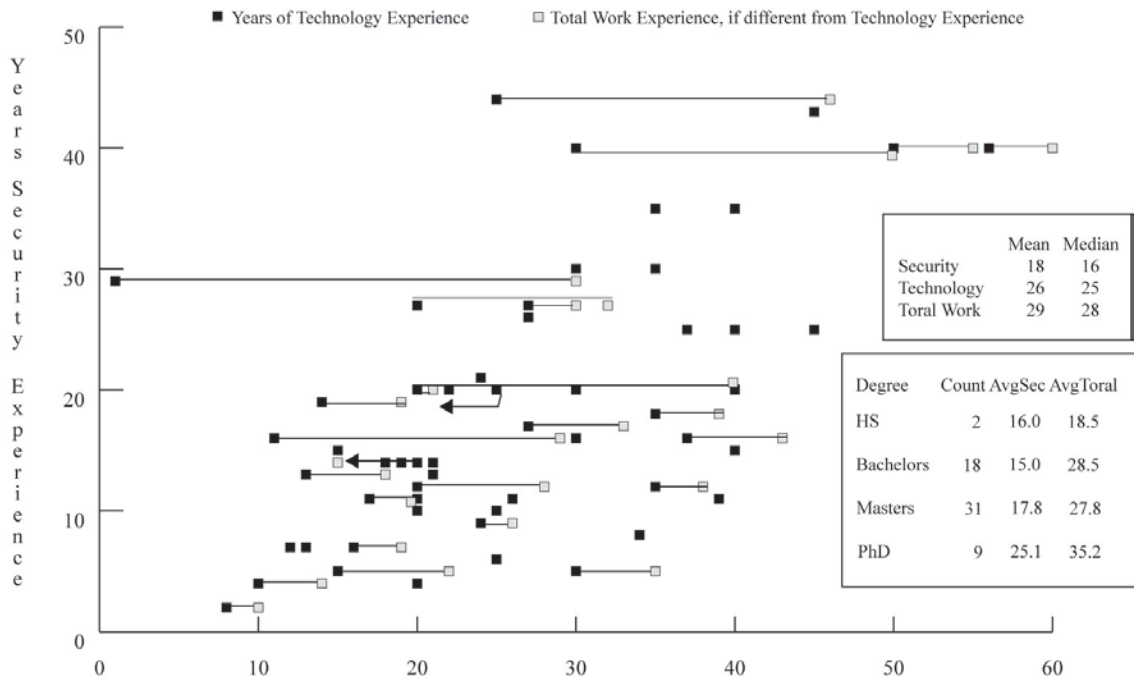
into four levels and sent to the CISO-level survey respondents who volunteered to be asked follow-up questions. Of the respondents who provided an email address for follow-up questions, a significant number were either CISOs or consultants with CISO experience.

3.2. Survey Results

3.2.1. *Qualifications*

Though 109 out of 224 solicited took the survey, after scrutiny of responses, there were 60 qualified respondents. The qualifications of those experts are illustrated in Figure 7. Where technology experience and work experience were not the same, they are connected by a line on the graph. Two people reported having a few more years of technology experience than total work experience, and this result is depicted by an arrow pointing to the left in the line which connects them on the graph. The graph shows less than 60 points because a few respondents had exactly the same number of years experience in all three dimensions. Figure 7 also shows the highest level of education for the individuals. Following the count is the average years in security of the individuals at that degree level, and the average total work experience at that level. Two thirds of the participants were active in security professional organizations and over two-thirds had some form of security certification. Seventy-eight percent of the participants were either active or certified.

Figure 7: Survey Respondent Demographics



In the survey, four questions asked respondents to rate system attributes relationship to security metrics on a Likert scale. These constituted a 44 independent multinomial trial of 5 possible outcomes of the same probabilities. A normal distribution of results would indicate that respondent answers were the equivalent of random selections. This would be the case if the respondents as a whole had ambiguous attitudes toward a given question. By contrast, a positive kurtosis or significant skewness would indicate that the observations are more clustered about an attitude on which respondents agree. Collective responses to any question that approximated a normal distribution or a flat curve were judged too ambiguous to merit inclusion as a security attribute. Appendix F includes descriptive statistics for all attributes. Seven of the forty-four attributes were removed

due to ambiguity have a skew value below 0.3 and also a central mean (flat) or kurtosis near zero (normal).

3.2.2. *Rank Results*

The resulting rank order of security attributes reflects the attitudes of the respondents on all questions which merit positive attribution of security. As expected, the three statistical methods used to rank expert opinions of system security attributes yielded slightly different results. These are listed in Table 1.

Table 1: Attribute Rank Order for Survey Responses

Orig Order	Question Label	Thurstone	One Number	Survey Rating
20	Q21-20-IDAuth	1	1	1
27	Q24-4-PassPenTest	2	2	3
11	Q21-11-Incident	3	4	4
36	Q26-4-VaInput	4	3	2
1	Q21-1-Mission	5	7	13
8	Q21-8-Awareness	6	5	5
23	Q21-25-ThreatProtProb	7	6	9
14	Q21-14-PhysEnv	8	14	22
15	Q21-15-Personnel	9	12	19
10	Q21-10-Recovery	10	10	7
17	Q21-17-Interfaces	11	11	15
9	Q21-9-SWChange	12	18	10
37	Q26-5-DefOutput	13	8	8
26	Q24-3-PassSecRev	14	20	18
19	Q21-19-AuditTrails	15	15	23
4	Q21-4-Risk	16	9	6
18	Q21-18-Segregate	17	17	17
16	Q21-16-SWIntegrity	18	19	16
7	Q21-7-Acquisition	19	21	24
5	Q21-5-Infrast	20	13	12

Table 1: Attribute Rank Order for Survey Responses				
6	Q21-6-Features	21	25	21
13	Q21-13-Media	22	26	30
33	Q25-4-Logs	23	16	11
2	Q21-2-Certif	24	32	34
22	Q21-22-AssetValue	25	24	29
32	Q25-3-Mgmt	26	28	25
3	Q21-3-Standards	27	30	26
34	Q25-5-BCP	28	23	14
29	Q24-8-FailSafe	29	35	35
28	Q24-7-Interfaces	30	31	33
25	Q24-2-SecAudit	31	29	27
35	Q26-2-Pattern	32	22	20
31	Q25-2-Config	33	27	28
24	Q24-1-RegAudit	34	36	36
12	Q21-12-VendorOver	35	34	32
21	Q21-21-TechCfg	36	33	31
30	Q25-1-Resources	37	37	37

3.2.3. *Subsequent Analysis and Feedback*

Rank order centroid analysis was performed to determine whether deviations between three types of ranks in Table1 were large enough to be investigated, and further investigation was deemed unnecessary. However, it was determined that responses were clustered within ranks. Table 2 shows that 4 sets of values maintained their general order outside of the more detailed sub-ordering within the clusters. All three of the security attributes identified by the research hypothesis are in the top tier of importance to security measurement, and indeed, all of the security attributes in the top tier are system-level attributes. So the null hypothesis that all important dimensions of system security are attributes that can be measured at the component level is not true, and the hypothesis that

security measurement requires the contribution of the system-level attributes: articulated mission and purpose, validated input, and incident detection and response cannot be rejected.

Of course, like most theories, its ultimate confirmation lies in its utility, and requires continual study. Although some of the subject matter experts who engaged in follow-up analysis did shuffle a few of the attributes from tier to tier, the research hypothesis as well as the more general finding that the most important attributes of security are at the system rather than component level was also generally supported by these subject matter experts. Specific subject matter expert follow-up comments included general disappointment that any security attribute would be considered "not important" as component security could of course be a weak link in a chain or armor. They also commented that responses to the survey were subjective, and complained about the "noise" level of the questions, both of which were, as noted in Section 3.1, intentional.

Table 2: Clusters of Ranked Attributes

1	User identification and authentication
	Withstand targeted penetration attacks by skilled attack teams
	Incident detection and response
	System interfaces accept only valid input
	Articulate, maintain, and monitor system mission
	Security awareness
	Evaluate the extent to which systems are protected from known threats
	Physical and environmental protection
	Personnel screening and supervision
2	System recovery planning
	Security features required to maintain integrity over system interfaces
	System and software change control

	Table 2: Clusters of Ranked Attributes
	System output conforms to well-defined specifications
	Pass internal security review
	Maintain audit trails on use of system functions
	System-level risk assessment
3	Segregate users into groups or roles for access control
	Software integrity preservation
	Due diligence in system and services acquisition
	Infrastructure Risk Assessment
	Security features that correspond to system functions
	Control over removable media
	Logs that verify that process designed to secure system is followed
	Certification, accreditation, and security assessments
	Quantify the value of assets at risk in system operation
4	Progress in a management plan to secure system
	Use security standards as system requirements
	Successful execution of business continuity procedures
	Fail in denial of service mode
	Maintain integrity of interfaces through system development lifecycle
	Pass security audit
	System follows a commonly used architecture pattern
	Percentage of systems or components that have passed security configuration tests
	Pass regulatory audit
	Oversight of vendor maintenance
	Maintain values of standard security variables in system technical configuration
	Number of resources consumed in system security-related tasks

The full set of survey results in Appendix D includes all comments from all participants. Notable comments emphasizing the importance of a system-level approach to security attribution are:

- The environment requires easy to understand system documentation from inception to production with security being an identifiable component at all levels. As much detail as is needed to fully describe security related elements/functions is required and development phases are reviewed and accepted or rejected based on completeness and ease of understanding.
- System security verification requires an assessment of how the integrated security components combine to defend against, discover or respond to attacks.
- Security is an epiphenomenon, a second-order effect of a business process as implemented in a cultural context. As such it is difficult to define repeatable, comparable, quantifiable objective measures of security.
- The best security metrics are those that have business correlation, and can be collected analyzed and communicated to support decisions (I assume your context implies that this capability exists, but in truth most organizations struggle reaching a minimal level of maturity) Your question brought to mind a similar question: "What is the best language?" My response to that has always been similar to the one above. Those with the ability to communicate in multiple languages have strong opinions in this area, but if you ask a language professor they will often slap their foreheads and wish that their students knew how to communicate in any language. (My 2 cents from the soapbox)

4. Security Theory Attribute Construction

The results of the subject matter expert survey map to the formulation of the hypothesis in statement S of Section 1.4.2. The following list is a decomposition of statement S into statements that correspond to our experiment, and allow a derivation of a formal conclusion.

1. System contains an hypothesis attribute
2. Attribute is at component level
3. Component attribute is not an hypothesis attribute
4. System exhibits security attribute

These numbered statements allow the following simplification of statement S:

System is Secure ←→ { 1 } AND { 2 → 3 } AND { 4 }

Given that our subject matter experts were asked to opine on a plethora of attributes and that they identified all three hypothesis attributes as important security attributes, and they did not identify any components as most important security attributes, it is feasible to use these opinions to designate statement 1 and 4 as true, and statement 2 as false. These values allow us to conclude that the hypothesis is logically correct. Although such surveys cannot confirm our hypothesis, they do provide enough evidence to reject the null hypothesis that all system security attributes are at the component level. The survey provides a basis for the claim that the three security attributes in the hypothesis provide a foundation for a construct theory of security.

We also know from the comments provided both in the survey and via subject matter expert feedback that the attribution of security will differ with system purpose. This issue

was also discussed in Section 2.4 as a reason for rejecting most current candidates for a construct theory of security. So any newly posited theory must be careful to avoid the same pitfall. Hence, this section does not draw on our survey result to describe a construct theory of security, but instead describes a *framework* with which to create construct security theories for a given system of interest.

"Framework" has become a generic term for standards and guidelines, process improvement models, and assessment methods in various disciplines within systems and software engineering [84]. The term, "Security Framework" is typically used to refer to an enterprise security methodology of the sort depicted in Figure 8 that allows management to see the relationship between security process, technology, and risk [17, 85, 86].

Figure 8: Example Security Architecture Framework [17]

	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Contextual	The Business	Business Risk Model	Business Process Model	Business Organisation and Relationships	Business Geography	Business Time Dependencies
Conceptual	Business Attributes Profile	Control Objectives	Security Strategies and Architectural Layering	Security Entity Model and Trust Framework	Security Domain Model	Security-Related Lifetimes and Deadlines
Logical	Business Information Model	Security Policies	Security Services	Entity Schema and Privilege Profiles	Security Domain Definitions and Associations	Security Processing Cycle
Physical	Business Data Model	Security Rules, Practices and Procedures	Security Mechanisms	Users, Applications and the User Interface	Platform and Network Infrastructure	Control Structure Execution
Component	Detailed Data Structures	Security Standards	Security Products and Tools	Identities, Functions, Actions and ACLs	Processes, Modes, Addresses and Protocols	Security Step Timing and Sequencing
Operational	Assurance of Operational Continuity	Operational Risk Management	Security Service Management and Support	Application and User Management Support	Security of Sites, networks and Platforms	Security Operations Schedule

Though security management frameworks aimed at producing security metrics are readily available [87, 88], there are not many examples of using frameworks to construct security metrics. Without such construct foundations, these management frameworks are assuming, rather than demonstrating, that the measured activities will produce the desired results. Amoroso described a similar situation when he pointed out that the US Department of Homeland Security's attempt to portray threat levels as colors was intended to mimic the fire threat level of the Smokey the Bear signs. But because it lacks the same theoretical underpinning (which in the forest fire case is based on environmental measures), has instead left a wake of confusion [89].

The difference between these traditional security frameworks and the approach that is used herein is the focus on system mission and purpose as opposed to the more generic goal of security. Figure 9 illustrates this approach using the systems security engineering research roadmap from which the definition of security was derived in Section 1.2. The roadmap approach begins with the requirements specific to the system of interest, whereas traditional security architecture frameworks begin with generically-phrased systems security requirements. An example of the traditional approach is articulated by Fabian, "A **goal** is a **security property** of an asset, in which the stakeholder is interested. Goals get more detailed by transforming them into **requirements**. Those get more concrete by the conjunction of **specification** and **assumptions** (supported by **facts**)" [90]. Another example as articulated by Mead states that the security engineering process starts by "identifying **security** goals" [86]. In a roadmap-driven security framework, the only goal is that of system functionality. Security attributes gain credence by contributing to

that goal, not by identifying a separate set of security goals that align with it.

Figure 9: Roadmap Path for Security

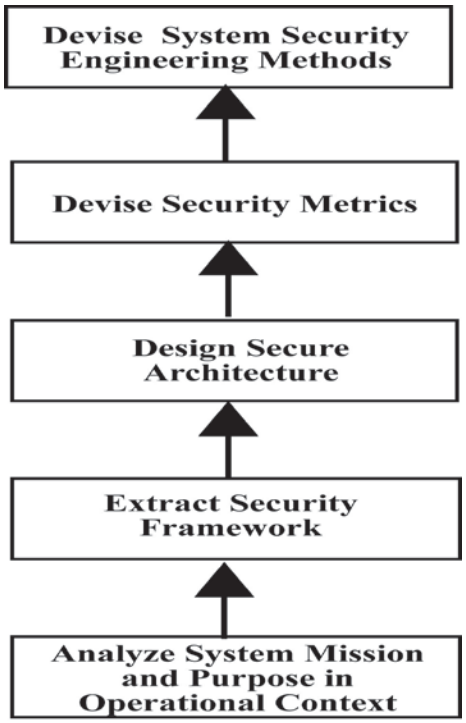
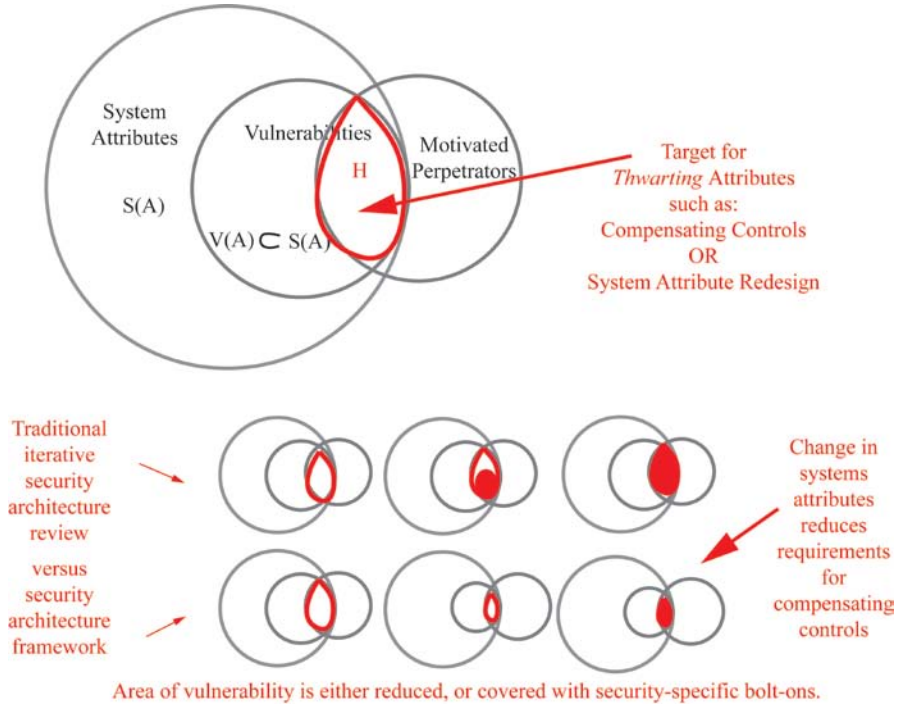


Figure 10 is a set-theoretic view that illustrates the difference between the traditional approach to security architecture and the new, system level, approach. Statement J says that, for each system attribute which presents a vulnerability, either there is no perpetrator who will exploit the vulnerability, or there should be another system attribute that compensates for the vulnerability. Figure 10 shows the vulnerable attributes as a subset of system attributes, and perpetrator targets as a subset of the vulnerable attributes. These also become targets for security engineering. Traditionally, security engineering has attacked this problem with *compensating controls*, which is a technical term in the security profession that refers to controls that are devised because the system itself has no

controls that will minimize damage were the vulnerability to be exploited. Compensating controls are by definition work-arounds that are not part of the system itself, but security-specific components, derogatorily referred to as *bolt-ons*. The history of security technology is the story of the development of one of these bolt-ons after another, all motivated by a specific exploit, and most have been incorporated into the various security standards described in Section 2.4 [91]. By contrast, a security engineering framework that recommends construct security theory based on system level security attributes would be expected to alter system-level attributes to eliminate or reduce vulnerability. If this approach is tried first, the number of security-specific compensating controls should be minimal. The progression of the set-theoretic constructs at the bottom of Figure 10 illustrate this difference.

Figure 10: Set-Theoretic Illustration of the system Level Approach



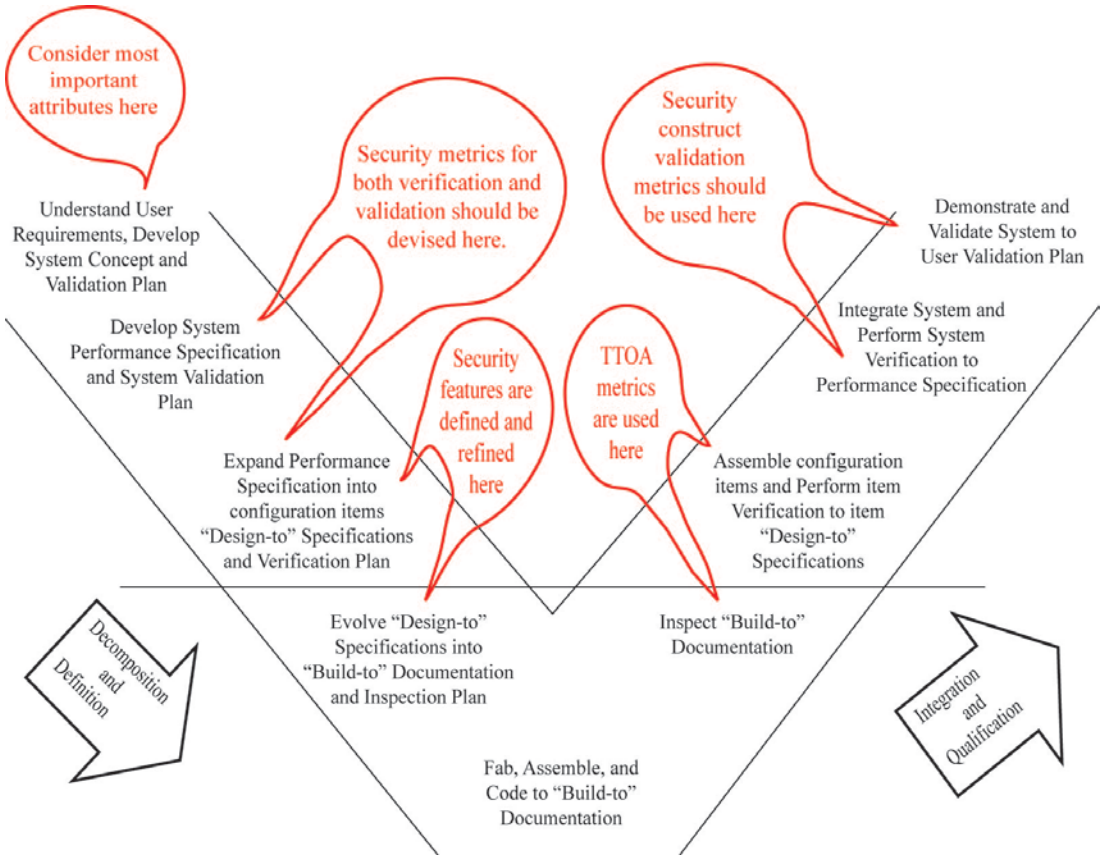
A clear understanding of required security attributes in the context of a given system mission should allow the design of effective security features, as well as metrics to determine their effectiveness in maintaining system security. Armed with a clear definition of security, and with the most important systems attributes that indicate security effectiveness, it is possible to construct a framework with which to apply those survey results.

For a security engineer to follow the advice of the experts as described in Chapter 3, the list of the most important systems security attributes would be included in the first stage of system analysis depicted in Figure 9, and would take place early in the systems engineering process rather than in a separate security-specific process. These include the three system-level attributes in the hypothesis, and also others that made the security experts' most important list:

1. Articulate, maintain, and monitor system mission
2. System interfaces accept only valid input
3. Incident detection and response
4. User identification and authentication
5. Withstand targeted penetration attacks by skilled attack teams
6. Security awareness
7. Evaluate the extent to which systems are protected from known threats
8. Physical and environmental protection
9. Personnel screening and supervision

As these are all system-level rather than component-level requirements, any systems engineering process following the standard “Vee” model as illustrated in Figure 11 should consider them prior to formulation of a concept of operations (Note: the standard systems engineering Vee in both Figure 11 and Figure 12 is adopted from[75]). Figure 11 also illustrates in which stage of the systems engineering process systems security metrics should be devised for both verification and validation.

Figure 11: Security Metrics Framework Overlay on the Vee Model



The two research objectives as described in section 1.4 are *to contribute a methodology for planning security that includes metrics* and *to provide an explanatory framework that is helpful in understanding decisions about security*. The framework just described achieves both objectives by providing a method for both engineers and system owners/operators to:

- Identify system security support features and the system functions and components that instantiate them.
- Evaluate the extent to which security features enable a system to *thwart perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value* (using definition A from Section 1.2).
- Devise verification and validation metrics at the system level that demonstrate the presence of security attributes.
- Consider design alternatives in terms of their effects on system security.

The framework uses the most important systems-level security attributes as a systems-thinking springboard to extract a set of desired security attributes, or features, from the mission and purpose of the system in the context within which it operates. Security architecture can then be integrated into systems architecture, customized rather than bolted-on in response to the latest threat. Metrics may be devised that measure whether security functional requirements are met by security features. Design alternatives may be evaluated using these metrics. Where systems exhibit similar architecture patterns, it

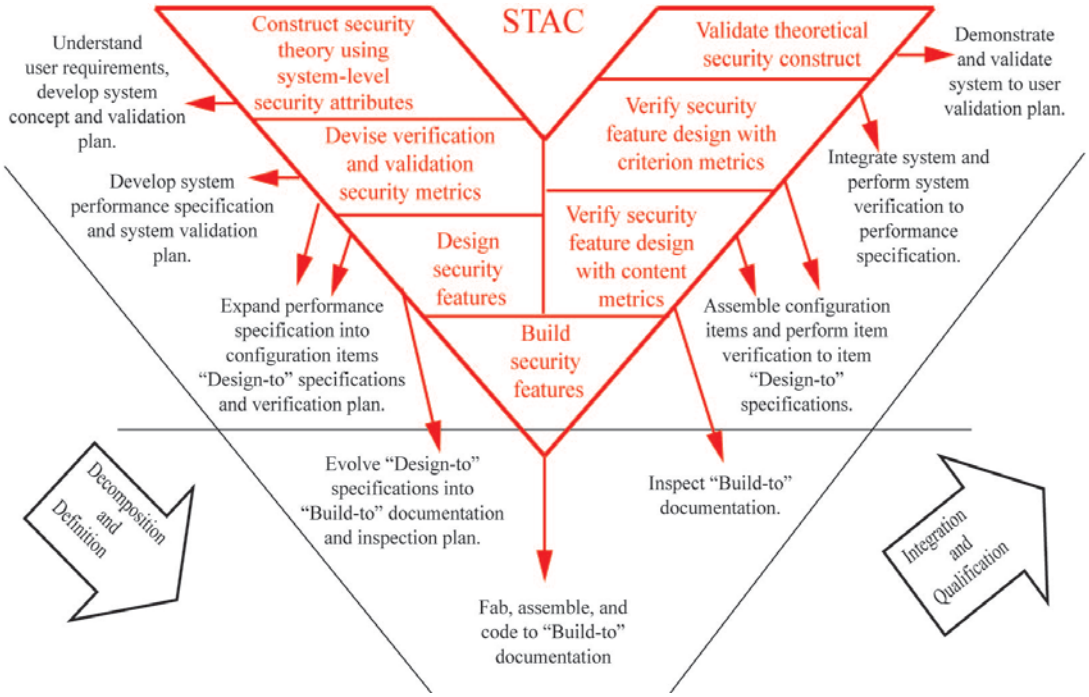
makes sense that they make use of common security architecture models [92]. The existence of system-level security metrics for common security architecture models should make it possible to develop tools that guide future engineering efforts toward more secure solutions.

Note that the research objective is not to provide a tool for a specialty security engineering group, rather to equip systems engineers with security dimensions of thinking as they develop an initial concept of operations and subsequent system design goals. Therefore, the security metrics framework does not come with a security-specific guide such as that in Figure 8. Rather it is meant to be understood as a Vee model overlay based on Figure 11. As illustrated in Figure 12, the overlay facilitates the ability of systems engineers to construct a theory of security as composed of important security attributes that must be systemic properties of the resulting system. In Figure 12, the framework is labeled “STAC,” an acronym that stands for *security theory attribute construction*. It suggests that systems engineers include seven security activities in the system architecture process, but stops short of being a separate, seven-step process itself because the steps must be integrated into the existing Vee model, not performed separately. The seven activities are:

1. Construct security theory using system-level security attributes
2. Devise verification and validation security metrics
3. Design security features
4. Build security features

5. Verify security feature design with content metrics
6. Verify security feature design with criterion metrics
7. Validate theoretical security construct

Figure 12: Security Theory Attribute Construction Framework



Security at the system level starts with a STAC-framework suggestion for how security is supposed to be accomplished. As in any other systems engineering requirements analysis, the engineer may then evaluate whether the STAC *would* be effective if all system elements proscribed by it were functioning *correctly*. Systems engineers employing such methods should be able to build on prior results by citing successful security verification and validation results in similar architecture patterns. The challenge is to devise metrics that show that the security that was the design objective was accomplished for the given system of interest, and employ measurements that reflect the design objectives in addition

to the verification that the design was implemented correctly. In the next Chapter, two case studies provide examples of how such frameworks and metrics may be integrated into the systems engineering process.

5. System Security Engineering Case Studies

In this chapter, the STAC framework introduced in Chapter 4 is applied to case studies in *Cloud Computing* and *Mobile Communications*. The case studies follow Checkland's soft systems engineering methodology. Each section describes the problem situation unstructured, expresses it in a structured manner, defines the system, develops a conceptual model, compares that model with the structured problem, identifies feasible changes in structure, procedure, and attitude, and recommends action to improve the situation [93]. The soft systems engineering component of each case study provides a descriptive rationale for applying the STAC framework to meet the security requirements of the system of interest. The remainder of each case study addresses implementation issues.

5.1. Cloud Computing

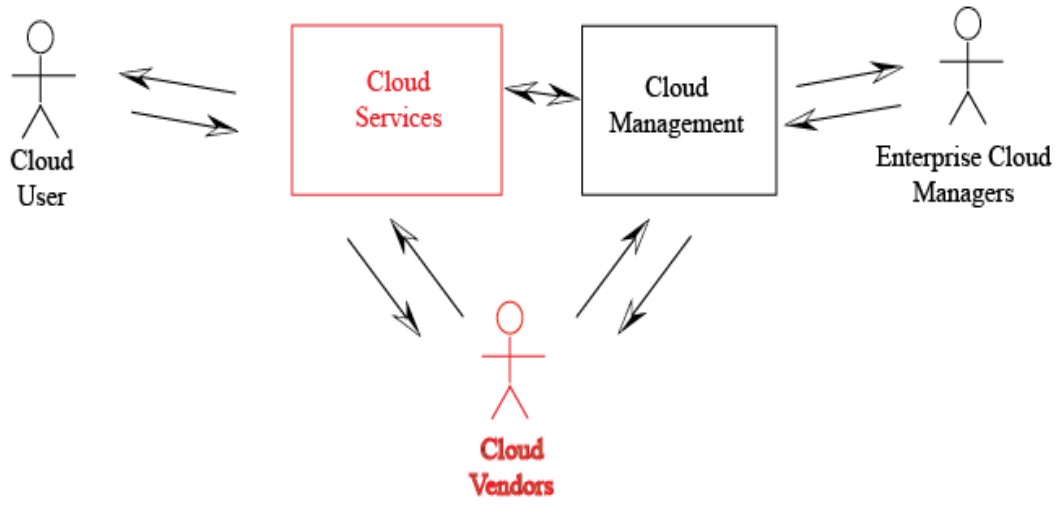
5.1.1. *Cloud Computing Security Problem*

The Cloud Computing case study is an enterprise cloud management system ("Cloud System") meant to allow business technology units to both deploy internal applications into cloud services and to allow safe use of commercial cloud-hosted platforms and applications. As illustrated in the use case diagram of Figure 13, the purpose of that system is to facilitate the ability of an enterprise customer to procure technology services

which may be dependent on multiple clouds. Because the security challenges are obvious from the use case diagram, it may also serve as an initial *trust model*, which is a security engineering technique to illustrate reliance on security-related claims [17]. The red components in Figure 13 indicate inherently untrusted components of the system of interest. The problem is how the enterprise can control its information confidentiality, integrity, and availability while the actual operation of its technology services is performed by a variety of cloud operators.

In the context of Cloud Computing, trust relationships between an enterprise cloud customer and counterparties are typically decided by working committees of cloud security professionals who have published cloud-specific security standards, and they may place significant emphasis on legal vendor service level agreements in order to resolve such trust issues [94]. However, the STAC framework does not consider recommendations for contractual assurances or risk tolerance as security measures, but instead concentrates on cloud customer system goals and the sociotechnical context in which the Cloud System of systems operates. Hence, the use case diagram of Figure 13 illustrates that system functions that are typically controlled or influenced only by the cloud vendor must also be capable of being managed by the enterprise cloud customer, referred to in the diagram as the “Enterprise Cloud Managers.”

Figure 13: Cloud Computing Problem



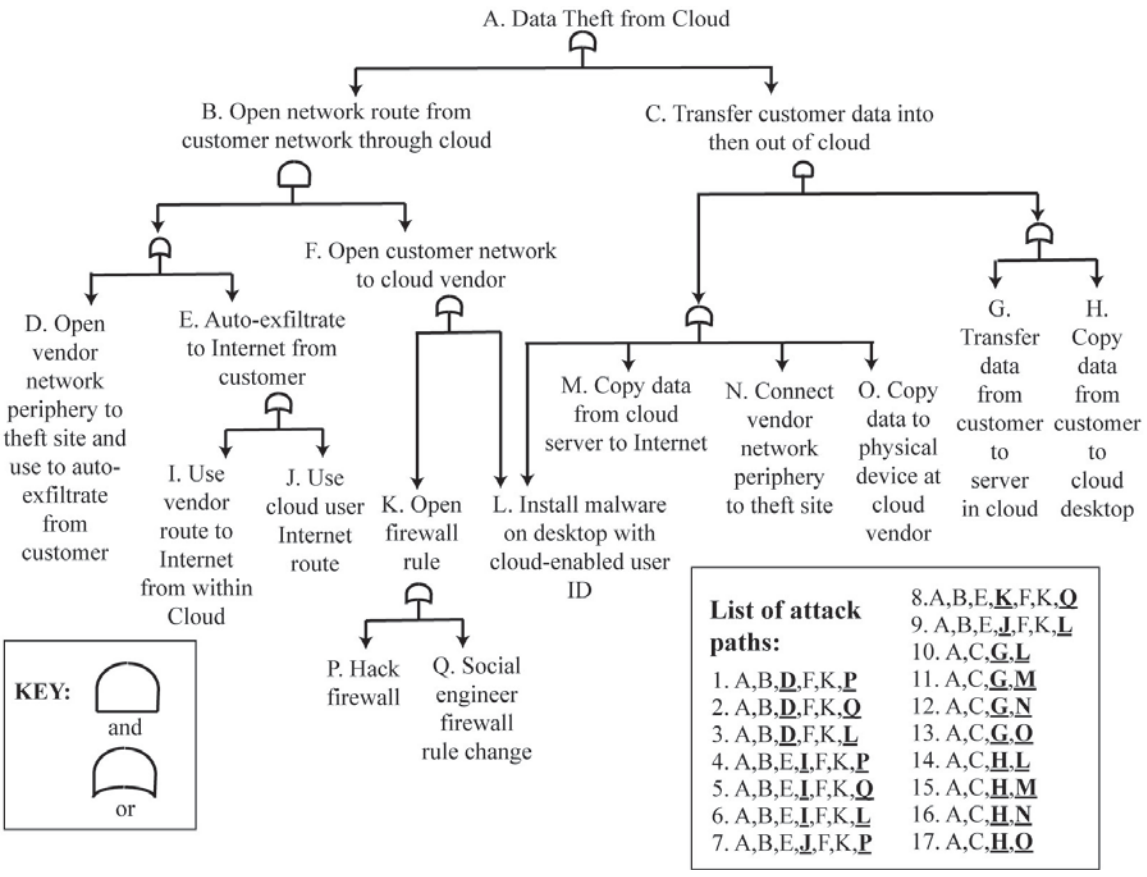
5.1.2. *A Structured Expression*

Systems security engineering typically facilitates structured expression of security problems via threat analysis. The experts in our survey highlighted this capability as an important security attribute, which in the survey was labeled: “the extent to which systems are protected from known threats.” In the case of Cloud Computing, any Internet security vulnerability is considered a potential point of threat exploit. In addition to these ubiquitous and common threats, any given system will have its unique set of adversaries who are both knowledgeable and capable of gaining advantage through disrupting productive system operation. These include, but are not limited to competitors, disgruntled customers and employees, individual and organized criminals, hostile nation-states, and terrorists. Hence, it is possible to structure the problem in terms of potential attack from these adversaries. Security requirement analysis tools available to structure the problem include attack trees, adversary sequence interruption models, and

connectivity diagrams [37]. If security requirements are to be proposed prior to completion of system design, then the problem must be structured at a high level that does not assume a specific system architecture. Attack trees are distinguished from other security-requirement-gathering tools in that they model only adversary behavior in the absence of a representation of the system itself. Therefore they are the most appropriate tool with which to structure a problem without foreshadowing its solution.

Figure 14 is an attack tree where the goal is to steal information trusted to the cloud, and that event may be used as an example of cloud failure to achieve its mission or purpose. In Figure 14, the attack goal is decomposed into sub-goals that would have to be combined according to an identified logical structure in order to accomplish the goal identified in a higher layer. It identifies seventeen (17) distinct attack paths. Each attack path relies on some combination of eleven (11) possible activities that, if possible, would contribute to a situation in which customer data may be exfiltrated from the customer either through the cloud network or to the cloud network and then on to an external site. These activities are underlined in the attack paths in Figure 14. They are referred to as *leaves*, because they are at the lowest level of a branch of an attack tree, become the basis for specifying security features to thwart anticipated attacks. Together, they establish the design basis threat (DBT) for the Cloud Computing System.

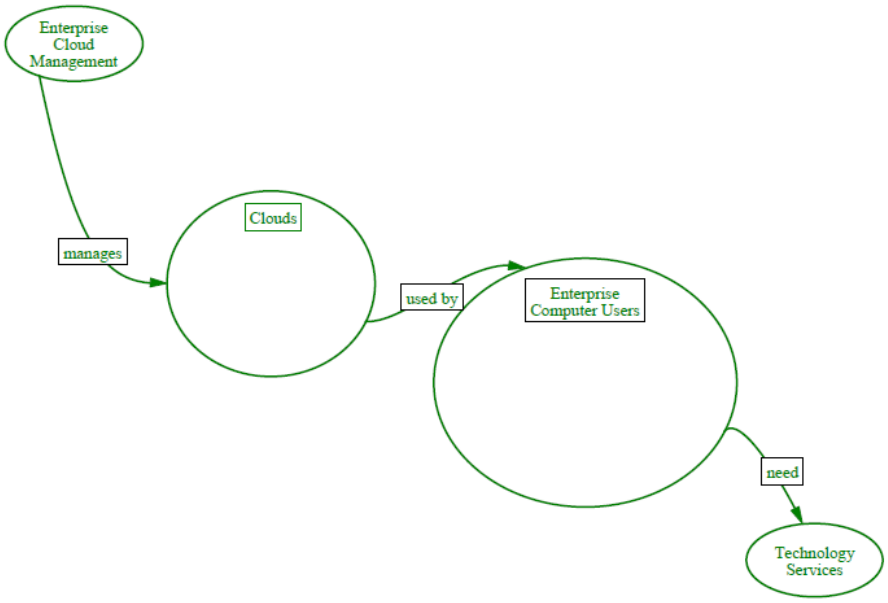
Figure 14: Structured Cloud Problem [95]



5.1.3. *System Definition*

The root definition of the relevant system is expressed in the systemigram of Figure 15. It draws on the use cases wherein the system of interest is an *Enterprise Cloud Management* system, and that system manages *Clouds* that are used by *Enterprise Cloud Users* that need *Technology Services*.

Figure 15: Cloud System Definition



5.1.4. *Conceptual Model*

To apply the STAC framework to the problem of cloud security management, important system-level security requirements shall be considered part of the system model at the initiation stage of system analysis, and incorporated in system security engineering methods that are used to gather functional requirements.

STAC Step 1: Construct security theory using system-level security attributes

While a traditional security engineering process would flow directly from the potential vulnerabilities identified in an attack tree to security requirements to technology controls designed to limit these activities, the STAC framework suggests that a systems engineer should examine these potential exploits in the context of system attributes as a whole and system level security in particular, while simultaneously considering the system mission to allow technology service use by authorized cloud users. Table 3 maps the requirements

introduced by the leaves of the attack tree to the important dimensions of system level security identified in the survey analysis:

Table 3: Cloud Computing Requirements

leaf	*Attribute from Section 1 of Table 2:*	*1. Mis-sion*	*2. In-put*	*3. Inci-dent*	*4. ID-Auth*	*5. Pen-Test*	*6. Awr-ness*	*7. Eval Thrt*	*8. Phys -Env*	*9. Per-son*
D	All network connections that allow automated data transfer external to the cloud shall permit only customer-authorized data transfers	X								
G H	All movement of data into the cloud shall follow well-defined business processes and shall be filtered to ensure content conforms to the purpose of the authorized access path.	X	X		X					
I	Internet access from the cloud shall be used only for customer specified communications, and shall not be configured to allow any ad hoc or personal use of the Internet	X								
J	There shall be no route from the cloud to the customer network that does not terminate medication within the customer network	X								

Table 3: Cloud Computing Requirements

leaf	*Attribute from Section 1 of Table 2:*	*1. Mis-sion*	*2. In-put*	*3. Inci-dent*	*4. ID-Auth*	*5. Pen-Test*	*6. Awr-ness*	*7. Eval Thrt*	*8. Phys -Env*	*9. Per-son*
P	Customer network connection to cloud should show control changes to network access via an authorized system lifecycle process, wherein all actual changes are compared to records of authorization and authorized purpose		X	X			X			X
Q	Changes to network access shall require the collaboration of at least two skilled engineers responsible for following system lifecycle process		X	X	X	X	X	X		X
L	Cloud users who do not have up-to-date security patches and desktop images shall be prevented from connecting to the cloud		X	X	X	X	X			X
M	All Cloud outbound Internet connectivity shall be filtered to prevent exfiltration of sensitive data	X								
N	Cloud vendor shall not allow changes to network access unless supported by controlled system lifecycle process	X	X	X			X	X		X
O	Physical access to equipment at cloud vendor shall not allow data access				X	X			X	

The requirements in Table 3 may also be viewed as potential vulnerabilities in the systems security attributes listed in the numbered columns, or in other systems functions that support the activities referred to in the first column. At this high-level stage in a requirements analysis process, it is important for a systems engineer to keep in mind the difference between statement H in the hypothesis derivation process:

it is possible that there is a system vulnerability that no perpetrator exploits

and statement I:

given there is a perpetrator who exploits an attribute, it is possible that the system has another attribute that thwarts the perpetrator from that exploit

The effort should attempt to identify if there are any systems functions whose vulnerability would not be a perpetrator target. As long as none of the important system security dimensions were placed in this category, risk-based exclusions may make security analysis and thus the overall systems engineering process more efficient. An example of such an exclusion in the case of Cloud Computing might be the system attribute of *Internet Connectivity*. Though critical to the mission and purpose of the system, a cloud vendor would virtually be put out of business if it was not connected to the Internet. So setting customer-specific security requirements or features to reduce potential vulnerability due to Internet unavailability in this area may be waived as overly redundant with the cloud service provider's security responsibilities.

With the high level security requirements documented, a systems engineer should introduce features and functionality designed to thwart perpetrators who would exploit systems vulnerabilities that allow the leaf activities in the attack tree to occur. Combining

these security features and functions with the security attributes of Table 3 in the context of the set-theoretic process at the bottom of Figure 10 provides the scope of system attributes to be scrutinized for possible modification to reduce vulnerability. Each important security attribute in the numbered columns of Table 3 should be supported by systemic security features that cover the requirements in the corresponding rows. Some of the security attributes correspond to the same subset of security requirements, and this suggests that security features may be developed that cover more than one important security attribute.

For example, the security attribute, *Articulate, maintain, and monitor system mission,* should be addressed with system functionality expected to control data flow through network connectivity. While network level security features are traditionally restricted to communications protocols at the host level, this analysis suggests that data-centric security models be utilized at the system level [96].

For an example of the situation where multiple security attributes correspond to the same subset of security requirements, consider that both *User identification and authentication* and *Withstand targeted penetration attacks by skilled attack teams* cover requirements for access controls at both the network engineering, servers, desktop, and physical levels. This wide range of narrowly defined user job functions to be covered by user identification and protected from pentests suggests that enterprise-level identification repositories will be required to coordinate authorization for various cloud-enabled

technology services, and that any concept of operations must ensure that user communities are appropriately segregated.

Another example where multiple security attributes correspond to the same subset of security requirements includes systemic lifecycle attributes. This finding is of notable importance because it indicates that incident detection and response is closely associated with other systems lifecycle attributes that are typically considered quality-driven, such as software and network change control. Creating systemic security features that would meet a combined set of software, network, and security incident response and change control requirements is a significant contribution to the efficiency of the systems engineering security process.

Note that one important system attribute contributing to these features is the “extent to which systems are protected from known threats.” This indicates that continuous improvement of the attack model should be incorporated into the system lifecycle process. This type of security requirement will come as no surprise to any system security engineer familiar with the observe, orient, decide, act loop prevalent in military security operations, in which security depends on one's ability to assess the current environment in the context of the mission and be able to alter mission strategy based on the result of that evaluation [97].

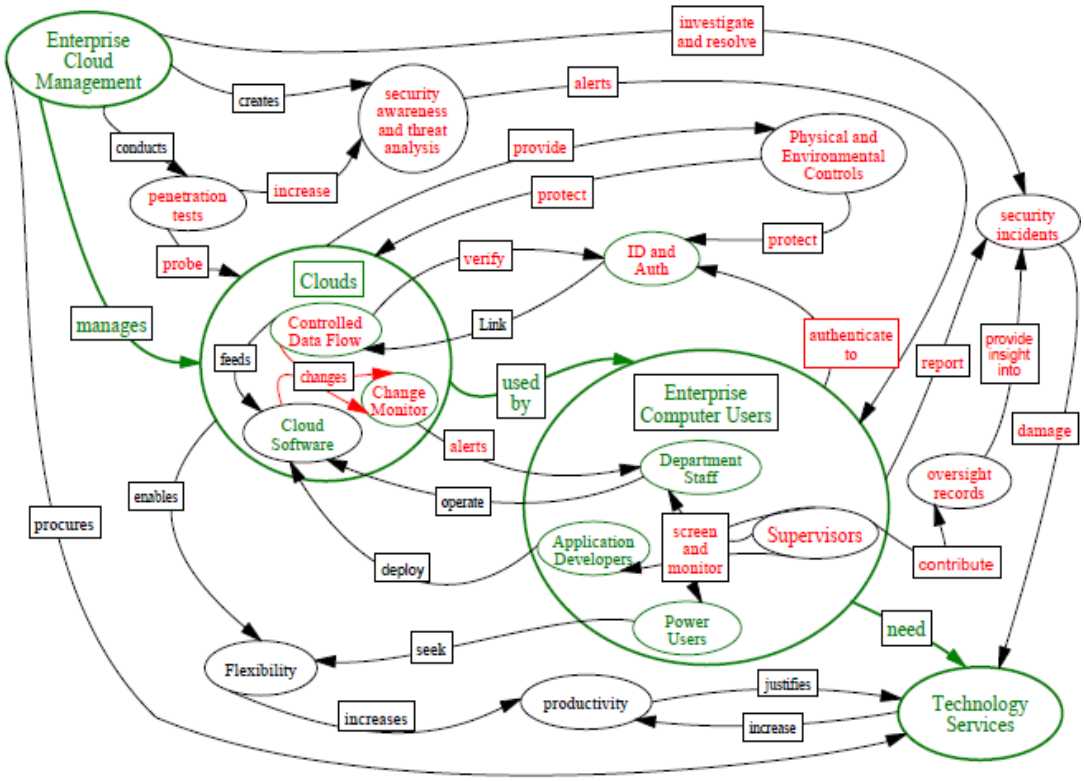
The security requirements suggest a revision of the systemigram for the Cloud Management System, which is illustrated in Figure 16. Given the above discussion, which is meant to emulate the security system thinking undertaken by a systems engineer,

controlled data flow and change detection become core features within the system mission and purpose. Other security features suggested by Table 3 are also incorporated in the systemigram. They appear in red. This integration of key security features with system mission and purpose becomes the initial security model for Cloud Computing, and ultimately the Concept of Operations for the Enterprise Cloud Management System.

5.1.5. *Comparison of the Model to the Structured Problem*

To facilitate comparison of the security model to the structured problem, it is helpful to envision a scenario in which the Cloud system is in use while under attack.

Figure 16: Cloud Security Model



STAC Step 2: Devise verification and validation security metrics

For the purposes of the case study, it is assumed that a full set of security features corresponding to the systemigram of Figure 16 are available to be integrated with the system of interest. In this section, we compare the model to the attack tree in Section 5.1.2. One system-level measurement approach to this comparison is a Security Work Factor Ratio (“SWFR”) between "time to protect" and “time to attack” [98]. A SWFR is a product of two measurements, defined as:

- The time to protect (TTP) is the average interval between when a target is first aware of the existence of a new threat and when it successfully deflects it. This measure depends mainly on the speed and effectiveness of a target's response capability.
- The time to attack (TTA) is measured as the median lifetime of malicious activity emanating from a specific source. This is useful to measure in situations where attackers must constantly create and abandon original points to evade detection. The shorter this median lifetime, the heavier is the burden on the attacker to continuously change its location to evade detection.
- To the extent the ratio TTP/TTA is minimized, the defenders are successfully thwarting attacks. To the extent it increases, the attackers are more successful. The goal of absolute security would be measured with a TTP/TTA metric that is better as the ratio approached zero.

To measure whether the goal of preventing data theft is met in a Cloud environment, the TTP may be derived from a combination of the vulnerable components that need to be compromised for the data to be stolen and the existence (or not) of security controls that compensate for the vulnerable components. This requires modeling of attack paths and identification of defenses in place to delay or stop each path. For example, attack path 1 in Figure 14 indicates that activities on leaves D and P set the stage for the attack path to be utilized. The vendor network periphery must be opened to an attacker site and the customer firewall must be hacked in order for the exploit to occur via attack path 1.

To assign a time to attack value to the path, the length of time that an attack is available to the attacker would be calculated for each leaf activity. Assume that there is no control against the vendor periphery connecting to the attacker site (such would be the case if outbound Internet access was allowed from within the vendor network, which is common). Then the time assigned to the leaf is infinity (INF). The time to attack is then bounded only by the time an attacker determines there is opportunity to hack a customer firewall to gain administrative access. The opportunity determination will depend on what vulnerabilities are known to exist in firewalls in general at the time, and the prevalence of hacker tools that efficiently execute that firewall attack. Such measures can be estimated using publicly available historical data concerning similar attacks [39]. As Clouds are subject to the same attacks as any network on the public Internet, comparative attack data may also be captured using the time that URLs used to distribute malicious software and/or collect data from infected hosts are active before they are detected by

security services companies that investigation and filter such URLs (“web reputation services”).

To assign a time to protect (TTP), available corrective controls must be reviewed. For a firewall whose rules and configurations are checked daily via automated mechanisms and response is immediate configuration correction, this attack may be available for one day. For environments where firewall rules are checked once annually by external auditors, this time period is one year. For firewalls with known exploitable vulnerabilities due to software flaws, this time period is the average time between firewall software vulnerability announcements, and the time customers install patches. Consideration of more detailed alternatives may prompt a systems engineer to add levels to the attack tree in an iterative requirements process.

Where there is a single point of security failure on any one attack path, then the time to defend is the time to correct that situation. Assume that the control failure that allows a firewall hack is a software vulnerability in firewall access control. In this case, the time to fix that component includes not only the time the firewall vendor takes to offer a patch for the component, but also the time the Cloud vendor takes to apply the patch. Although the vendor may have signed a service level agreement to apply patches “as soon as possible,” the vendor’s historical time to repair can only be measured by monitoring the system in operation. If another mechanism may compensate for that failure, but is a detection rather than a prevention mechanism, then the time to protect is the interval between the detection and the response that thwarts the threat. Hence, the time to protect

a given path will depend on the controls preventing exploit on that path, and is measured as the minimum time required to establish compensating or corrective controls.

If each attack path can be assigned a SWFR based on the minimum TTP/TTA for attack recovery, then the security of any given Cloud System C may be measured by the time to protect against all identified threats to the Cloud. Assume P_1 through P_n are the paths on a rigorously devised attack tree for Cloud System C, and P_{1SWFR} through P_{nSWFR} are the corresponding SWFR ratios that an attack of depth d would take on each path. CSWFR is the longest of those minimum values, calculated as:

$$CSWFR = \max (P_{1SWFR} \ldots P_{nSWFR})$$

Using SWFR, the median of a Cloud attack is measured using a moving historical sample of active attacks. Trends will of course change continuously, so any cloud security validation metric based on it will have to be continuously monitored to ensure that any validation that stakeholder expectations for security are met evolve in conjunction with changes in the threat environment. But in general, assuming equivalently thorough attack trees, the lower the CSWFR, the stronger the security metric. Given two Cloud environments with roughly equivalent threat services, a Cloud with a lower CSWFR will be more secure than one in which it is higher.

In this metric calculation, the time to thwart the attack is taken as a constant. In practice, however, customers should insist that there be multiple controls layered on each attack path to ensure that there is no single point of failure that would allow attacks to be successful. This is a “defense in depth” approach. In such cases, each path’s SWFR

would not be a single number, but an upper and lower bound. Different combinations of controls may be compared to achieve the longest time period as the upper bound, while minimizing the range between the upper and lower bound. Where redundant protective controls have been designed into a path, the path is said to have defense in depth, and, unless the same vulnerability applies to both controls, the TTP for redundant controls is zero. This suggests that another metric may be the percentage of attack paths for which the TTP is zero due to the presence of compensating controls of diverse technology.

If the structure of the problem is assumed to include Table 3's map of structured problem requirements to system-level security features, other system-wide security functionality may be validated with different techniques that also demonstrate how the systemigram security model maps to real life situations. A design goal derived from Figure 16 is that users are to be identified and authenticated to clouds. This can be validated with a security inclusion test wherein an active login in any electronic component of the cloud is sampled and compared with a centralized *Identification and Authentication* function to ensure that it is represented and a random sample of identities is made from the centralized repository and compared with access that it has recorded. Another example would be to actually insert an unauthorized login into a cloud electronic component and observe to ensure that a security incident was detected and reported, and the incident response process resulted in its removal. This observation could also be used to validate the design goal of incident response. The security awareness goal can be validated by having all cloud users participate in planned exercises such as the unauthorized login one,

and observe that they all follow the procedures in which they need to participate in for the security features to work.

The system mission of providing technology services will presumably be validated with service metrics that are not specific to security, but should be also capable of confirming that the system-level attribute of *Identification and Authentication* supports the system mission by allowing authorized login. However, because there exist perpetrators who seek to exploit that attribute, it may also present a system vulnerability. This vulnerability is tested for via pentests, which is also a system-level attribute, but not one that thwarts a perpetrator seeking to exploit vulnerabilities in *Identification and Authentication.* To thwart any perpetrator seeking unauthorized access, there must be a deterrent or negative consequences resulting from exploiting the vulnerability. Such a deterrent or consequence becomes a requirement for a security feature. The Cloud Computing security model supports multiple possibilities for such a feature. One is a monitoring mechanism supporting a system-level attribute of *Incident Detection and Response*, where response may include some way to identify and punish the perpetrator, such as disabling further access from its source device. However, even if incident detection is not possible, the system can be designed to provide minimal data of value to a perpetrator, a technique known to security professionals as *avoidance*. Such a feature may allow data to be accessible only when encrypted. It may also be possible to introduce *deception* features that deliberately provide perpetrators with easy access to falsified data that would, if used by a perpetrator, arouse suspicions that may lead to arrest. These candidates for avoidance features have the common element that they reduce the value of

the attack goal, such as the bank automatic teller machine feature that leaks ink onto money if tampering occurs. Design considerations in this iterative manner should serve to reduce system level vulnerabilities rather than to immediately resort to bolt-on security technologies.

The outcome of the STAC step of devising verification and validation metrics may also feed back into the security requirements process, as the process of verification and validation itself may introduce the need for additional or refinement of already specified security features.

5.1.6. *Identify Feasible Changes in Structure, Procedure, and Attitude*

The current standards for measuring cloud security dictate that cloud users should query the cloud vendor on the extent to which they have establish best practices in security management [94]. When and if the vendors disclose their security model, it is compared with the customer security model and discrepancies prompt negotiations with the vendor for additional security controls. In the best of all possible situations, the vendor will agree to a 3rd Party audit and provide the results to customers [99]. Using this process, customers rarely if ever gain insight into a vendor's capability to thwart attacks. Using a system-level metric such as CSWFR provides that missing insight.

Systems security engineering has traditionally presented quantification of potential impact in combination with a suggestion for bolt-on security technology. A decision-maker would decide whether the cost of the technology was a feasible way to minimize the possibility of exploit to a level where risk of damage could be tolerated. However,

neither the attribute of *System-level risk assessment* (Q21-4) nor the *Quantify the value of assets at risk in system operation* (Q21-22) made it to the top tier of system security attributes, and so in this analysis is considered less important at this initial concept of operations stage. This is intuitively true because the STAC framework proposes tightly integrated rather than bolt-on security features and the costs of these cannot be quantified until the design is more thoroughly understood. Moreover, no quantification of assets at risk in system operations is possible prior to a development of a concept of operations.

STAC Step 3: Design security features

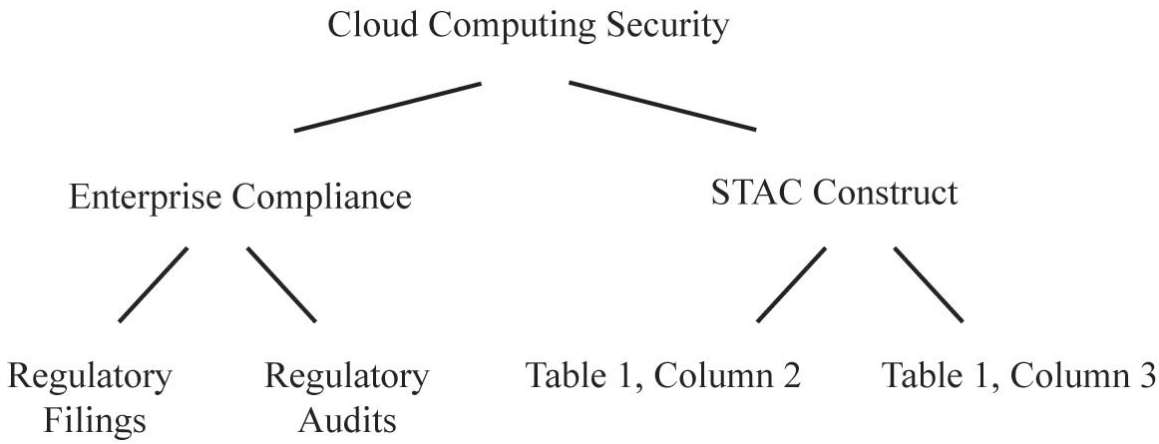
Section 5.1.5 discussed how the STAC framework is applied to construct a theory of security for the Cloud Computing system. If the theory holds, is should be possible to design a system with the security features implied in Figure 16 and subsequent discussion, and verify that each security feature is able to control the functionality and data flow depicted in the diagram. It should also be possible to devise verification metrics that show the system as a whole has important security attributes in the combination necessary to support the security construct. Although great care must be taken to specify each security feature in order to achieve its purpose, and a similar level of diligence to specify verification metrics for each feature, these tasks are well within the range of today's security engineering methodology. Table 4 provides an example of security metrics that correspond to the security features, as labeled in the systemigram.

Table 4: Example Verification Metrics		
Security Features	**Example Verification Metrics**	
	Content	**Criterion**
controlled data flow	Software ports and network traffic filters configured as per specifications.	Pattern-based analysis of network traffic for data outside of control flow should yield no results.
change monitor	All devices and data files may be traced to an authorized purpose.	Exercises in recovering earlier versions of software should be successful.
penetration tests	The set of vulnerabilities tested corresponds to current threat analysis results.	Tests for known vulnerabilities should yield no results.
security awareness and threat analysis	Current threat trees exist for commonly known vulnerabilities.	Simulated security incidents should yield behavior according to pre-established process and procedure.
physical and environmental controls	Manual and automated monitoring the physical premises should not reveal exceptions specifications.	Physical security drills should yield behavior according to pre-established process and procedure.
identification and authentication	All active system users should correspond to authorized staff.	Simulated social engineering tests should not result in unapproved access.
security incidents	Security incident documentation should reveal conformance to procedure.	Simulated security incidents should yield behavior according to pre-established process and procedure.
supervisors	All employees have a designated supervisor responsible for screening and monitoring their activity.	Supervisors should be able to pass test demonstrating knowledge of security process and procedure.
oversight records	Employee personnel records should include evidence of required screening and monitoring.	Random selections of oversight records should be immediately available.

Note that these are just examples. There may be many moving parts to each security feature and all would require some level of ongoing verification to ensure that the feature continues to reliably perform its function. Figure 17 illustrates how verification metrics

for the Cloud Computing theory construct may be modeled using the taxonomy depicted in Figure 6.

Figure 17: Cloud Computing Metrics Taxonomy



The security features should be tested for correctness and these verification tests will use content and criterion validity to show that the features are composed as expected, and that their behavior conforms to specified functionality. As described in the literature review of Chapter 2, the challenge is not to find reliable ways to implement verification metrics, but to *validate* that design goals have been met. Feasible responses to this challenge have been introduced in the previous section. Note that the validation metrics such as SWFR do not directly correspond to the security features, nor should they. Only validation tests derived independently of the features can show that the right features were specified.

5.1.7. *Recommend Action to Improve the Situation*

To validate the security of the system as a whole, it must be possible to observe the emergent system level property of security. This can be straightforward now that security

has been defined as the combination of system-level attributes that comprise the theory of security. These attributes include both the validation criteria developed in Section 5.1.5 and this security feature functionality specified in Section 5.1.6. The first identifies the goal of security and the second provides the guidance to achieve it. Together, they form a theory of security, which of course should be continuously validated.

The set of individual validation of system security features in the custom definition of system security must all be individually validated for security to be attributed to the system itself. It should be possible to normalize these metrics in such a way that demonstrates their relative contribution to systems security measurement as a whole. The outcome of the STAC step *design security features* includes not just the features themselves, but their validation mechanisms, and any supporting functionality required to conduct both verification and validation tests. These would be included in the recommendations to improve the situation, as per the methodology described as the start of Section 5 as dictated by Checkland.

5.1.8. *Cloud Computing Security Validation*

The soft systems engineering methodology, in combination with the first three steps of the STAC framework, should produce the build-to specifications with which to execute the cloud security model described in Section 5.1.4.

STAC Step 4: Build security features

This step of the STAC framework is not itself innovative, except that security features would be incorporated into the mainstream systems development process, as opposed to

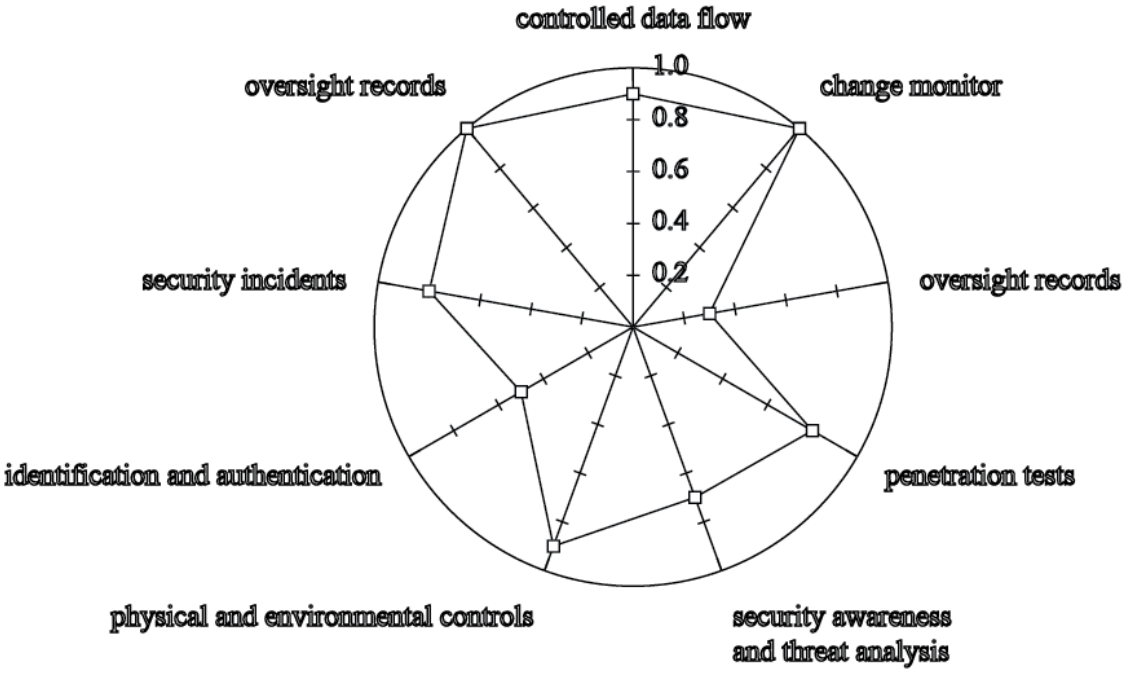
being specified and tracked by a separate security review process, a situation which is common today.

STAC Step 5: Verify security feature design with content metrics

STAC Step 6: Verify security feature design with criterion metrics

As described in Sections 2.2 and 2.3, specifying how security features can be verified with content and criterion metrics is well within the capability of today's security engineers using existing methodology. Such verification of carefully derived content and criterion metrics are essential to demonstrably adhere to the STAC-created security theory. Figure 18 is an example graphical illustration of the verification approach for the Cloud Computing case study. This figure demonstrates how the major security features in the Cloud Computing security model may be combined in multivariate analysis using a radar graph. Each feature labels a spoke on the graph, and the measurement reflects the extent to which verification tests for that feature are successful. The aggregate representation of the extent to which verification tests for each feature are met is a system-level security verification metric. This representation allows for easy comparison of the security of two different clouds, as one radar graph can overlay and other in the same diagram.

Figure 18: Cloud Computing STAC Metrics Report



STAC Step 7: Validate theoretical security construct

Validation of a STAC-produced theoretical security construct is equivalent to validating that the construct secures the system of interest. The validation tests envisioned in Step 2 of the framework are performed and results recorded. Validation tests such as SWFR provide a baseline, which becomes a numeric measure. Whether or not the numeric measure is adequate for securing the system may change over time as changes occur in the system's threat environment. Other validation tests, such as the identity management, record inclusion and exclusion tests described in Section 5.1.5, will have nominal measures such as pass or fail. It may not be immediately evident whether the root cause of failure is an issue with verification or with design, but any failures and validation

should be immediately investigated and remediated. As any one validation test failure may indicate systemic vulnerability, it does not make sense to display validation test results using normalized scales, as may be appropriate for verification test results. Rather, validation test results should be individually reported, as depicted in Table 5.

Table 5: Cloud Computing Validation Results	
Test	**Result**
CSWFR	35 minutes
Random identification sample	Pass
Intrusion simulation response	Fail
Authorized access provisioning	5 minutes
Unauthorized access deterrents	Pass

5.2. Mobile Communications

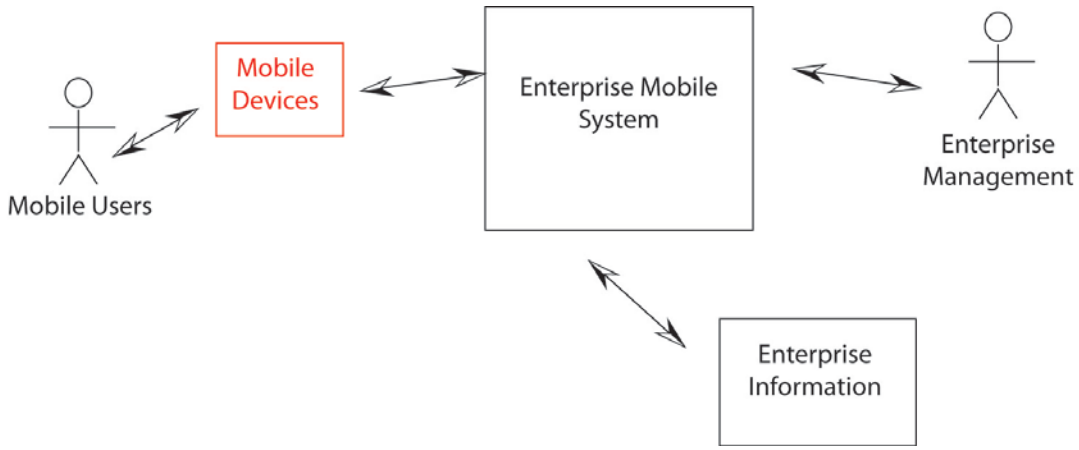
5.2.1. *Mobile Communications Security Problem*

The mobile communications case study is an enterprise mobile communications system ("Mobile System"), wherein a mobile device that is personally owned and operated by an employee of a company is used to access a communications infrastructure that is supported by the company. The purpose of the Mobile System is to provide confidential communications between internal users while allowing them access to information via external devices.

As in the Cloud Computing case study, the use case diagram becomes a trust model. In the context of mobile communications, trust relationships exist between enterprise management and users, but the enterprise has no control over the security of the mobile device, and even the user who owns a mobile device does not have adequate means to control its configuration [100, 101]. Hence, the use case diagram of Figure 19 illustrates

that the enterprise mobile communications system interacts with its users via untrusted external systems: the mobile devices. The untrusted devices appear in red in the diagram. This represents the mobile communications security problem.

Figure 19: Mobile Communications Problem



5.2.2. *A Structured Expression*

The Mobile System use case diagram reveals an obvious threat in that any adversary with a reason to attack the system has the opportunity to engineer an attack through the mobile device with little fear of detection or repercussion from the user, and even less from the enterprise. Moreover, as the mobile applications provided to the users face the Internet as a way to communicate with mobile devices, the system is also subject to common and ubiquitous Internet threats. As in the Cloud Computing case, potential threats include, but are not limited to competitors, disgruntled customers and employees, individual and organized criminals, hostile nation-states, and terrorists.

Figure 20 illustrates an attack tree for mining the Mobile System for data, which would defeat the Mobile System security goal for confidential communications. Note that the attack tree assumes that the target architecture will use at least two factors of authentication and refers to the second factor as a hard or soft token. This assumption is due to regulatory requirements which constrain the design. The attack tree observes that the mobile communications infrastructure itself may be a target of attack independent of its device support operations. The tree identifies twenty-four (24) distinct attack paths that may be executed against the Mobile System, with various combinations of eighteen (18) possible leaf activities (again, these are underlined in the attack path listing in the diagram). When combined according to the logical constructs which dictate whether they must be used in combination (the *and* gates in the diagrams), between one and three activities could result in successful adversary goal achievement. The full set of these activities form the basis for security requirements.

5.2.3. *System Definition*

The root definition of the Mobile System is expressed in the systemigram of Figure 21. As in the case of Cloud, it draws on the use case for the system of interest. In this case, the system of interest is an *Enterprise Mobile System*, and that system allows users to access *Information* via *Mobile Devices* for the purpose of increasing productivity.

Figure 20: Structured Mobile Communications Problem

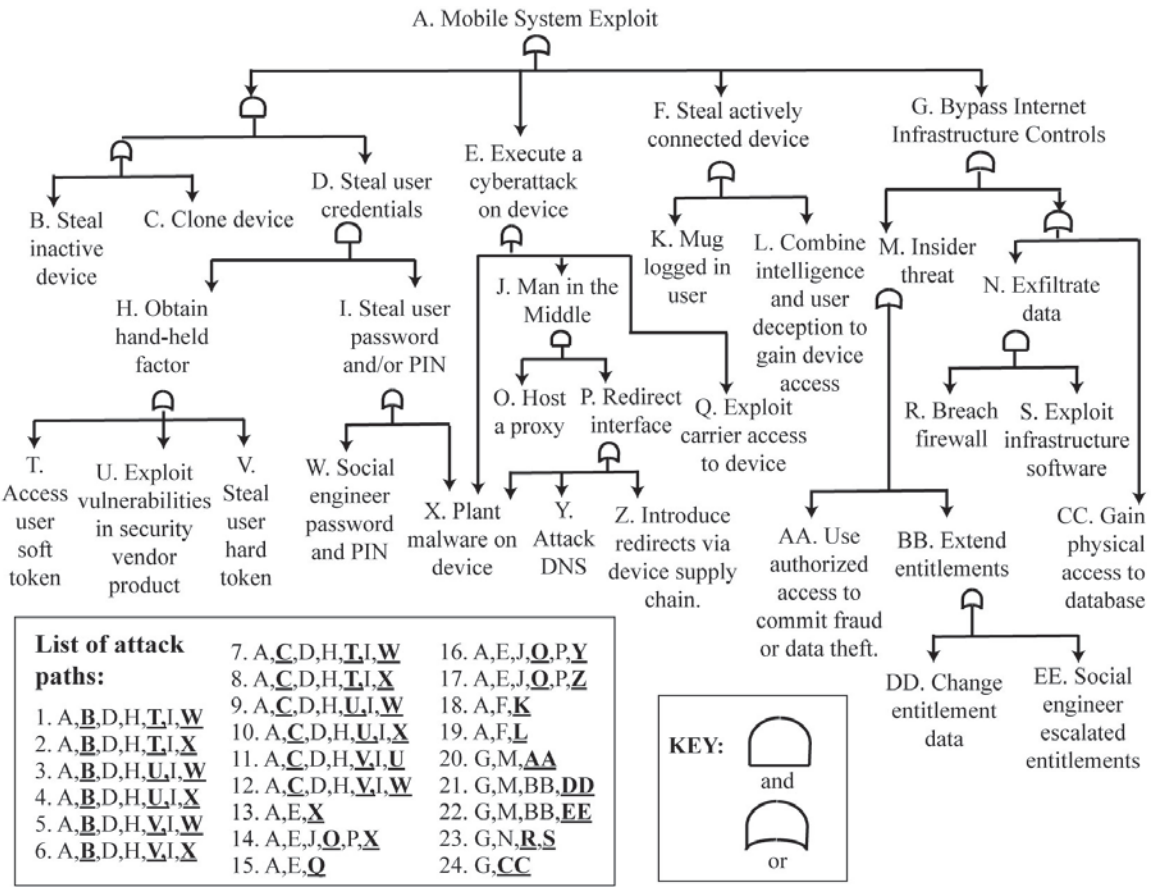
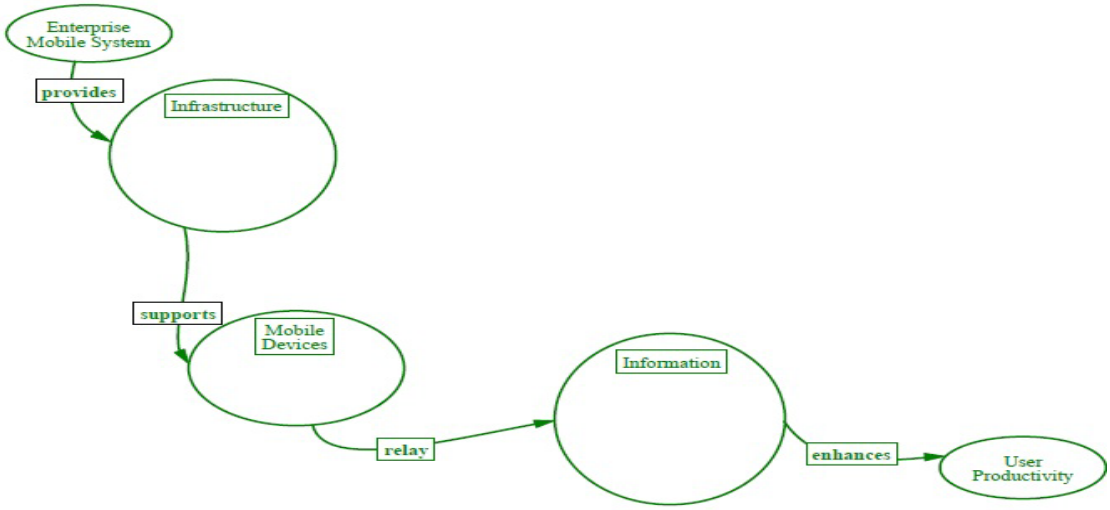


Figure 21: Mobile System Definition



5.2.4. *Conceptual Model*

Following the STAC framework, attacker activities are analyzed in conjunction with system-level security attributes that are considered most important based on the survey results.

STAC Step 1: Construct security theory using important security attribute

Table 6 maps the requirements introduced by the leaves of the attack tree to the important dimensions of system level security identified in the survey analysis:

Table 6: Mobile Communications Requirements

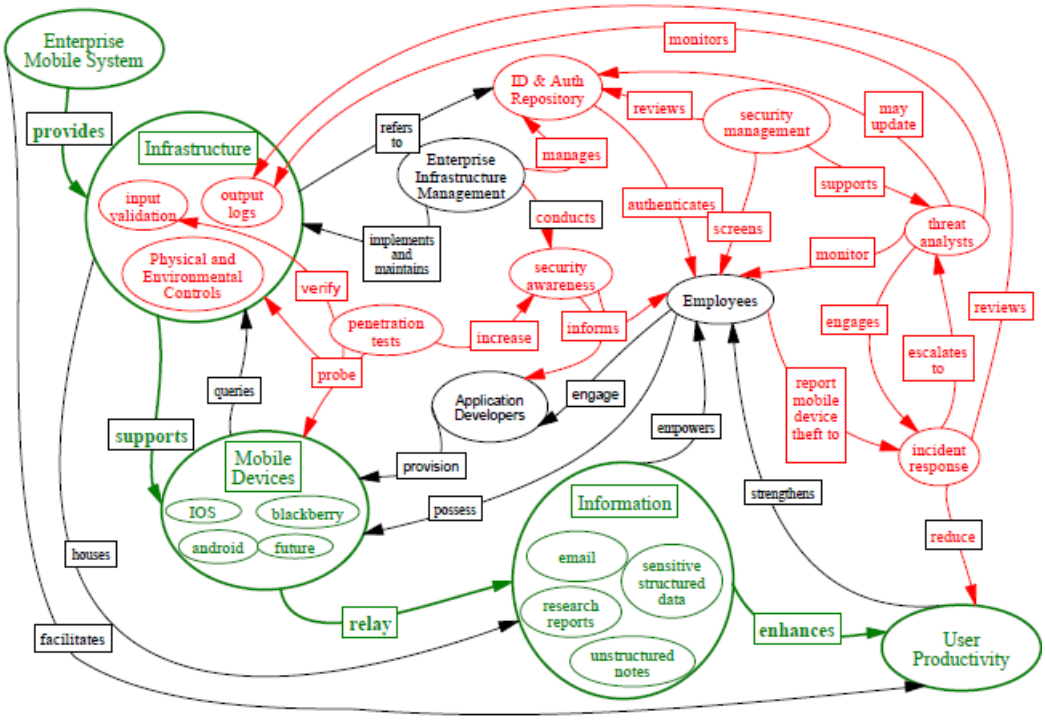
Leaf	*Attribute from Section 1 of Table 2:*	*1. Mis-sion*	*2. In-put*	*3. Inci-dent*	*4. ID-Auth*	*5. Pen-Test*	*6. Awr-ness*	*7. Eval Thrt*	*8. Phys -Env*	*9. Per-son*
B C K L	Train users and report device control loss, terminate device access		X				X		X	X
	Detect anomalies in device usage						X	X		
	Initiate fraud investigation, and incident response			X				X		
O	Conceal data on mobile devices, detect device tampering	X	X			X				
R	Mobile system infrastructure lifecycle assurance, including change control, and corresponding change and anomaly detection	X	X	X				X	X	
S	Software development lifecycle assurance, including internal and external security testing	X	X			X				
T	Multifactor authentication, device switch detection		X	X	X					
U	Supply chain vulnerability detection			X		X	X	X		
V	Multifactor authentication, device switch detection		X	X	X					

Table 6: Mobile Communications Requirements

Leaf	*Attribute from Section 1 of Table 2:*	*1. Mis-sion*	*2. In-put*	*3. Inci-dent*	*4. ID-Auth*	*5. Pen-Test*	*6. Awr-ness*	*7. Eval Thrt*	*8. Phys -Env*	*9. Per-son*
W X	Train users to avoid both physical and cyber social engineering techniques						X			X
	Change device authentication, software and data configuration		X	X	X					
Y	Device tamper detection, multifactor authentication, user behavior anomaly detection		X	X	X			X		
AA	Fraud incident detection and response	X	X	X	X			X		
CC	Mobile system change control and anomaly detection	X	X						X	
DD	Maintain least privilege entitlements, monitor client accounts		X	X	X		X	X		X
EE	Entitlements administrator procedures and training		X		X		X			X

As discussed in Section 5.1.4, the requirements in Table 6 may also be viewed as potential vulnerabilities in the systems security attributes listed in the numbered columns, as well as system functionality that enables the leaf activity itself. This should prompt a systems engineer to introduce security features designed to deter perpetrators who would exploit systems vulnerabilities that allow the activities listed. Following this method , the requirements of Table 6, in conjunction with consideration of system-level security attributes, led to the development of the security model illustrated in the systemigram of Figure 22.

Figure 22: Mobile Communications Security Model



The figure shows how the system definition has been enhanced by the consideration of security requirements. Input validation, output logs, and physical and environmental controls are key to achieving mission, these security features are included as core components of the infrastructure. This emphasis is due to the reliance on these controls for avoiding the most obvious threats. The emphasis on output logs is especially necessary for attack scenarios wherein few preventive controls exist to thwart a threat, hence the threat analysis and incident response processes will depend heavily on the mobile infrastructure's ability to provide accurate audit trails of inputs and outputs from/to any given user and/or mobile device.

5.2.5. *Comparison of the Model to the Structured Problem*

To facilitate comparison of the security model to the structured problem, the attack tree of Figure 21 is used to envision a scenario in which the Mobile System is under attack. As in the Cloud Computing case, it is assumed that a full set of security features corresponding to the systemigram of Figure 22 are available to be integrated with the system of interest.

STAC Step 2: Devise verification and validation security metrics

The Security Work Factor Ratio ("SWFR") metric applies to the Mobile System in the same way it applies to the Cloud. Each attack path is assigned a SWFR based on the minimum TTP/TTA for attack recovery, then for any given Mobile System M, the security may be measured by the time to protect against all identified threats to the Mobile System. Assume P_1 through P_n are the paths on a rigorously devised attack tree for Mobile System M, and P_{1SWFR} through P_{nSWFR} are the corresponding SWFR ratios that an attack of depth d would take on each path. MSWFR is the longest of those minimum values, calculated as:

$$MSWFR = \max (P_{1SWFR} \ldots P_{nSWFR})$$

As in the case of cloud, assuming equivalently thorough attack trees, the lower the MSWFR, the stronger the security metric. Given two Mobile System environments with roughly equivalent threat services, a Mobile System with a lower MSWFR will be more secure than one in which it is higher. The assumption of equivalency in attack tree "thoroughness" is of course a candidate for continued refinement. If structured

methodology could be devised for this type of exercise, it may even be possible to use the SWFR to compare the security of systems of different types.

As in the case of Cloud Computing, the structure of the problem is assumed to include Table 6's map of structured problem requirements to system-level security features, which resulted in the model in Figure 22. Other methods of comparing the model to the structured problem definition include validation of security features working within the system in operation. Such validation tests could include taking samples of data available for investigation for randomly chosen users and devices. Successful execution of these tests could provide assurance that incident response could be done quickly enough to contain potential fraudulent device usage. Such random data samples could also be compared to the data on the actual device to validate that both input and output security features have resulted in the achievement of stakeholder security objectives. A third type of validation test that could be conducted using both output logs and actual device data would be to compare those data sets to authorization repository records to ensure that the user accessing the Mobile System via the device was actually authorized to receive the data in the sample.

5.2.6. *Identify Feasible Changes in Structure, Procedure, and Attitude*

The current standards for measuring mobile security specify the extent to which mobile users or mobile carriers can control the content on a mobile device [101]. Content is typically divided into software applications, device configuration, and user data. Mobile system security metrics typically focus at the mobile telecommunication system level, in

which mobile carrier architecture evolution generally includes enhanced mechanisms to defeat theft of service [102]. In the security literature, not much attention is paid to the enterprise mobile communications problem as defined in Section 5.2.1, and there are no off the shelf metrics ready to be applied to the problem.

STAC Step 3: Design security features

The MSWFR approach to mobile security metrics, and the validation test approaches described in Section 5.2.5 suggest that it is feasible to identify and develop security features to strengthen systems that are built using technology for which no security had previously been planned. Although it would be theoretically possible to use native phone functionality with off-the-shelf security bolt-ons like authentication and firewalls, investigation of a security incident would be time-consuming and drive the MSWFR upward. Without careful planning, it is improbable that the enterprise would be able to determine what data information had been accessed by any given user or device, in which case, the SWFR for any path requiring incident response would be infinity. By contrast, the STAC framework suggests a theory of Mobile Communications security that allows for a more efficient and effective Concept of Security Operations via readily available and easily implemented technology such as input validation and audit trails. These security features, as labeled in the systemigram, are:

- input validation
- output logs
- physical and environmental controls

- penetration tests
- identification and authentication
- security awareness
- security management
- threat analysts
- incident response

Note that some of these security features seem very similar to the security features in the Cloud Computing system. However, the relationship between these features and the system of interest is different, as is evident from the systemigram. Although they are labeled with the same words, it is not the case that an identification and authentication feature that works for Cloud Computing could be assumed to work for Mobile Communications. Similarly, penetration test designed for one environment will not be adequate for the other. These differences are not in levels or strength of security, but in feature design. The verification metrics corresponding to these features must be customized for the specific purpose of the feature in the mobile computing environment. However, at the high level verification metrics must be presented outside of a technical specification, the examples are similar enough not to repeat the exercise of creating a Mobile Communications specific set of verification metrics and corresponding taxonomy diagram herein.

5.2.7. *Recommend Action to Improve the Situation*

Once all security features have been specified, and the verification and validation requirements specified, for the Mobile System STAC construct, specification of the security of the Mobile System as a whole is defined as the combination of security features that are required to instantiate the construct theory of security. These comprise the set of specifications that becomes the security contribution to a systems engineering build-to documentation and inspection plan.

5.2.8. *Mobile Communications Security Validation*

STAC Step 4: Build security features

As described in the case of Cloud Computing, this step of the STAC framework is not itself innovative, except that security features would be incorporated into the mainstream systems development process, as opposed to being specified and tracked by a separate security review process, a situation which is common today.

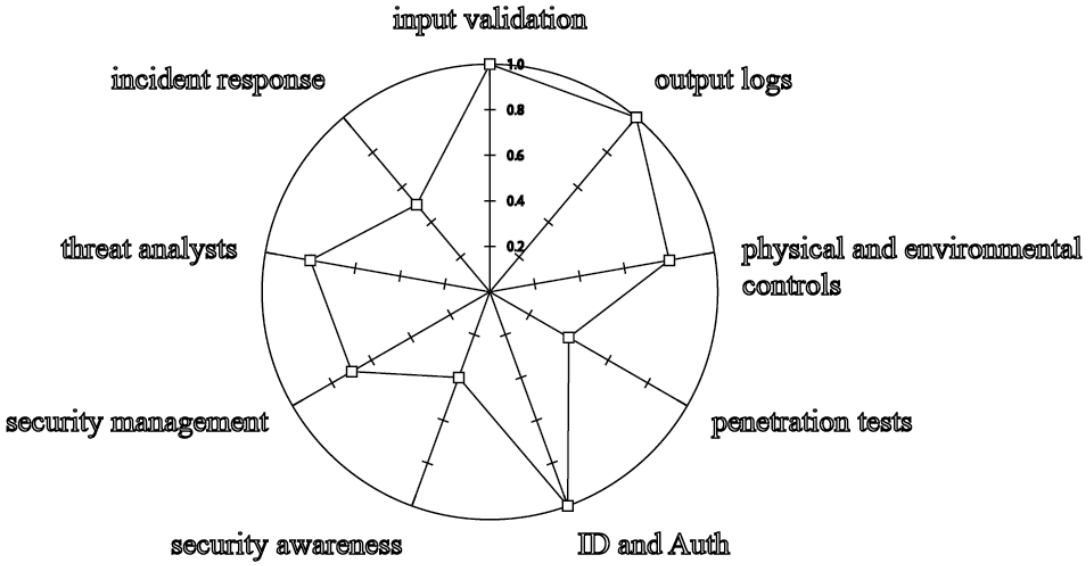
STAC Step 5: Verify security feature design with content metrics

STAC Step 6: Verify security feature design with criterion metrics

As in the Cloud Computing case, it should be possible to normalize verification metrics in such a way that demonstrates each feature's relative contribution to systems security verification measurement as a whole. Figure 23 is an example graphical illustration of one such approach for the Mobile System case study. As in the Cloud Computing case study, the main security features identified in the Mobile Communications security model

are independently verified. The verification measures are normalized, and represented in aggregate format on a radar graph. Note that in both cases, these metrics would not make sense without the context of the security model. The STAC framework provides the link from security requirements to a set of security metrics that may be appropriately applied to the system of interest. Where system architecture and security goals are similar, it is reasonable to expect that security models and metrics are transferable.

Figure 23: Mobile Communications STAC Metrics Report



STAC Step 7: Validate theoretical security construct

Validation of the Mobile Communications security construct theory employs the validation tests envisioned in Step 2 of the STAC framework. Examples of such validation results derived from the test described in Section 5.2.5 are listed in Table 7.

Table 7: Mobile Communications Validation Results	
Test	**Result**
MSWFR	23 minutes
Investigation data availability	Fail
Investigation data integrity	Pass
Unauthorized data download	Pass
Unauthorized access deterrents	Pass

5.3. Case Study Conclusions

Case studies provide anecdotal but not scientific validation for STAC. The case studies clearly demonstrate that the framework is useful in constructing a theory of security. STAC itself is not a theory but a method. The systems engineering process of defining any system function in terms of components provides the way to test STAC-suggested security features using both content and criterion validity. These methods exploit existing security content and criterion metrics such as targeting 100% standards compliance and vulnerability testing. These are a necessary, though not sufficient, part of the overall construct theory testing process.

Further application of the STAC theory is required to accumulate more test results and ensure that they correspond to the expert criterion. If they do not exactly match up, these results may instead be used to refine the criterion. Overall, this research result has face validity in that “system security should be measured at system-level” appears tautological. Nevertheless, it may be expected to be resisted, given today’s emphasis on measuring security using generics standards. This attitude will only be overcome by repeated and documented successful application of the STAC framework.

6. Summary and Conclusions

To date, systems security engineering has typically been a process of applying the same set of predefined security solutions to all systems. The situation is that system-specific security vulnerabilities are not identified in the systems engineering process. This research shows that it is possible to identify a set of system security features that minimize overall system vulnerability by examining system-level security attributes in the context of system mission and purpose. The process by which these security features are identified has been codified as a system engineering security metrics framework utilizing security theory attribute construction, or STAC.

The STAC framework equips a systems engineer to construct a theory of security for a given system of interest that can be tested for validity. STAC theoretical constructs focus on system security validation and so are comprehensible to executive decision-makers faced with trade-space decisions that affect system security. That is, where the STAC framework is correctly applied, resulting theories of system security are both construct and face valid. This research thereby provides a new theoretical foundation for approaches to system security engineering.

Although the STAC framework could have been created based on any set of system-level security attributes, it derives criterion validity by using security attributes identified by a survey of system security experts. That is, security experts may be expected to provide the criteria required for something to be called secure. Among the security attributes that security experts considered *Most Important* were the three system-level attributes in the

research hypothesis: articulated mission and purpose, validated input, and incident detection and response.

The research hypothesis is also an application of construct theory, requiring identification of relationships between security and measurable things that correlate with it. As no agreed-upon security metrics yet exist, this led to the nonparametric statistical approach of attitude measurement. The measured attitudes supported the hypothesis. The full set of statistically relevant subject matter expert opinions on important dimensions of security included only system-level attributes.

Rejection of the null hypothesis does not prove the research hypothesis but it does indicate that it may not be rejected. Further confirmation of the hypothesis could result from scrutiny by a wider community of those engaged in security analysis. Note that, in the systemigram of Figure 1, there are several different communities of security-related professionals who may be presumed to have opinions on security metrics: auditors, investigators, and technology managers. Hence, one avenue for future research would be to repeat the survey on security metrics using subjects from these other professions. Perspectives from these professions may provide additional insight into the systems security attributes that contribute to security audit, forensics and management capabilities, respectively. It may also be possible to identify what characteristics of systems (via STAC comparison) would most benefit from the analysis techniques, or scrutiny, associated with respective focus of each profession.

This dissertation's contribution to the field of security metrics has at least four dimensions. First, the literature review in Chapter 2 is the first to use scientific validity as criteria for creating a security metrics taxonomy. Second, this research empirically tested a theory about security metrics, whereas prior research based conclusions about security on metrics without prerequisite foundational theoretical constructs. Third, the concept of requiring system-level security measurement for security validation provides the field of security metrics with a sorely-needed shift toward systems thinking. Finally, the STAC framework for success-oriented security validation encompasses and leverages existing security engineering tools and techniques, and provides a method to compare security among similar systems. Overall, this research heralds a paradigm shift for systems security engineering, which to date has relied almost exclusively on unscientific best-practice declarations as the basis for security requirements.

Parallel research exploring this paradigm has already been spawned by this study. It includes, but is not limited to:

- Enlisting practicing systems engineers to incorporate the STAC method of security requirements and metrics into their mainstream requirements process and compare resulting sets of security verification and validation metrics [103, 104].
- The classification of research in security decision support and implications of recommended security decision support models with respect to system security requirements [81].

- Comparison of systems security education curriculum at the component versus system level, and its corresponding evaluation as appropriate for educational goals and/or training objectives [105].
- Systems engineering guidance for turning system-level security requirements into concepts of operations [106].
- Measuring cyber security in intelligent urban infrastructure systems [107].

The more of these studies that are completed, the more sets of security features will be available to apply to systems of similar mission and purpose. As such security architecture patterns become available, future studies may be able to compare the security efficacy of systems using these patterns to those which do not. Such studies could be expected to provide more comprehensive sets of systems engineering methods, processes, and tools based on system level security attributes and associated metrics.

The ultimate goal of such research would be to dispel the belief that compliance with security standards provides assurance that system security goals are met. This research would not make today's certification and accreditation programs obsolete, but it would raise awareness within the engineering profession of the relative contribution of standards compliance in the context of systems security goals and objective. The research may be expected to ultimately result in a pattern catalogue of systems security models suitable for a given type of system of interest. This catalogue would not compete with security standards, but provide an alternative view on system security requirements that would enhance stakeholder appreciation for systemic security features.

Publication Summary:

Bayuk, J.L. and B.M. Horowitz, An Architectural Systems Engineering Methodology for Addressing Cyber Security. Journal of Systems Engineering, 2011. 14(3).

Bayuk, J., A. Mostashari, and B. Sauser, Security Verification and Validation, in Conference on Systems Engineering Research (CSER), 2011.

Bayuk, J. and A. Mostashari, Measuring Cyber Security in Intelligent Urban Infrastructure Systems, in International IEEE Conference & Expo on Emerging Technologies for a Smarter World (CEWIT), 2011.

Bayuk, J.L. The Utility of Security Standards, in Security Technology, IEEE International Carnahan Conference on Security Technology (ICCST), 2010.

Bayuk, J. (2011). "On the Horizon - Systems Security Engineering." IEEE Security & Privacy 9(2): 72-74.

Bayuk, J., Cloud Security Metrics, in IEEE International Conference on System of Systems Engineering. 2011.

Bayuk, J. and A. Mostashari, Security Metrics for Systems Engineers – A Survey, Accepted by Systems Engineering, TBD 2012.

Appendix A – Hypothesis Derivation Logic

The lettered statements included in the derivation of the hypothesis in Sections 1.3 and 1.4 are represented using pseudo-code rather than pure logical form in order to make the document more accessible to a wide variety of readers. This appendix repeats the statements in pure propositional logic.

(A) "System X is secure" if and only if "X thwarts perpetrators who enact threats that exploit system vulnerabilities to cause damage that adversely impacts system value"

The definitions (B) through (I) decompose (A) so that its ultimate translation is statement (J).

(B) S(X) equals by definition "X is a system"

S(X)

(C) "S" equals by definition the attribute "Security"

S

(D) "E(X,A)" equals by definition "Attribute A is a property of system X, that is, X exhibits property, or attribute, A"

E(X,A)

(E) "V(A)" equals by definition "Attribute A is an exploitable vulnerability that permits system disruption"

V(A)

(F) "T(B,P)" equals by definition "Attribute B thwarts perpetrator P"

T(B,P)

(G) "P(Y,A) " equals by definition "Y is a perpetrator who exploits attribute A"

P(Y,A)

(H) ~Exists(Y)(P(Y,A))

∃ (A) !∃ (Y)(P(Y,A))

(I) For all A (E(X,V(A)) (Exists(B)(E(X,B) AND T(B,P(Y,V(A)))))

∀ (E(X,V(A)) ∃(B)(E(X,B) & T(B,P(Y,V(A))))

(J) E(X,S) ←→For all (A) (E(X,V(A)) ➔ (~Exist(Y)(P(Y,A) OR Exists(B)(E(X,B) AND T(B,P(Y,A)))

∃ (X,S) (E(X,S) ←→∀ (A) (E(X,V(A)) ➔ (!∃(Y)(P(Y,A) | ∃(B)(E(X,B) & T(B,P(Y,A))))

(K) For some A (Exists(Y)(P(Y,A)))

∃(A)(∃(Y)(P(Y,A)))

(L) *System security can be measured if and only if the system-level attributes of*

- *mission and purpose,*
- *validated input, and*
- *incident detection and response*

contribute to that measurement.

(M) "M" equals by definition the attribute "mission and purpose"

M

(N) "I" equals by definition the attribute "validated input"

I

(O) "R" equals by definition the attribute "incident detection and response"

R

(P) E(X,S) ←→ S includes M AND I AND R

E(X,S) ←→ Exists (M,I,R) ((E(X,M) AND E(X,I) AND E(X,R))

(Q) “C(X,T)” equals by definition “T is a component of system X”

C(X,T)

The definition of a system-level attribute:

(R) For all A (E(X,A) ←→ For all Y ((S(Y) AND (For all T, (C(Y,T) → (C(X,T)) AND

(Exists U (C(X,U) AND ~C(Y,U)))) → ~E(Y,S)))

∀ (X,A) (E(X,A) ←→ (∀(Y) (S(Y) & (∀(T) (C(Y,T) → (C(X,T)) & (∃(U) (C(X,U)

& !C(Y,U)))) & !E(Y,A)))))

(S) E(X,S) ←→ Exists (M,I,R) ((E(X,M) AND E(X,I) AND E(X,R)) AND

(For all Y ((S(Y) AND (For all T, (C(Y,T) → (C(X,T)) AND (Exists U (C(X,U) AND

~C(Y,U)))) → (~(M = U) AND ~(I = U) AND ~(R = U))) AND

(For all A, (E(X,V(A)) ➔ (~Exist(Y)(P(Y,A) OR Exists(B)(E(X,B) AND T(B,P(Y,A)))

The following list is a decomposition of statement S into statements that correspond to our experiment, and allow a derivation of a formal conclusion.

1. System contain a hypothesis attribute
2. Attribute is at component level
3. Component attribute is not hypothesis attribute
4. System exhibits security attribute
5. System X is Secure ←→ { 1 } AND { 2 → 3 } AND { 4 }

As subject matter experts were asked to consider only secure systems and their attributes, we assume statement 4 is true and evaluate our hypothesis given subject matter expert opinion that system-level attributes are important measuring security. These values are

highlighted in red in the truth table below. The logical result of applying these values to the hypothesis is also highlighted in red.

Truth table demonstrating experimental results effect on the hypothesis				
1	2	3	4	5
T	T	T	T	T
T	T	F	T	F
T	F	T	T	T
T	F	F	T	T
F	T	T	T	F
F	T	F	T	F
F	F	T	T	F
F	F	F	T	F

Appendix B – Survey Design

The survey was designed to validate claims that system-level security metrics are better indicators of overall system security than component-level security metrics.

The survey has four distinct sections: demographic, contact information, security metrics experience, and opinions of the efficacy of various security assessment and implementation techniques.

Demographic information included background on information security metrics experiences, industry affiliation, and education level. Contact information was optional and requested only if it was necessary to clarify answers.

Information security metrics experience was elicited via open ended questions designed to separate experts in security metrics from average security professionals. These questions included defining what is meant by security metrics and commenting on standard information security metrics publications.

The survey was composed of questions in five categories.

- **ISACA Demographic Questions:** Demographic baseline questions are the same as those asked the Information Systems Audit and Control Association, the international organization certification authority for information systems auditors and security managers (ISACA, www.isaca.org).
- **Non-ISACA Demographic Questions:** Demographic baseline questions that are not the same as one that are asked by ISACA. Note ISACA uses these types of demographic categories too, but the choice of answered to these ISACA questions are different than those listed below. In most cases, they have been enhanced to

provide more detail. In some cases, categories have been condensed or ranges expanded to reflect relevance to security architecture questions. For example, ISACA distinguished between organizations that have 150-300 employees, but its largest organization size range is greater than 13,000. The same question below has an answer for 150-500 employees and include an organization size of 75,000 or more. This reflects an expectation that organizational size influences security metrics choices at less granular levels in smaller organizations, but in more granular levels in very large organizations.

- **Security Metrics Baseline Questions:** These questions were designed to assess the respondent's familiarity with the field of metrics and measurement as applied to security.
- **Security Questions:** These questions mapped to the requirements for evidence gathering to support the inductive reasoning about system security attributes. They included questions corresponding to each of the three dimensions of security identified in the *Research Hypothesis.* System-level security metrics were defined as those which supported the research hypothesis that system security can only be measured using system-level attributes of support for mission and purpose, validated input, and incident detection and response. The survey included metrics that corresponded to these three dimensions of security, and it also included every other type of metric identified in the literature of security professional practice. It purposely rephrased similar questions from different perspectives (e.g. security measurement, security utility, security management). Security metrics were

presented in the form of attributes of secure systems as well as methods of security measurement. This questions set was meant to be a large set of options from which consistent security opinions could be extracted.

- **Contact Questions:** These requested a survey recipient to identify themselves for the purpose of ongoing communication, should it be required to evaluate survey results.

Note that Survey Recipients saw only three categories: *Demographics, Security,* and *Contact*. *ISACA, non-ISACA,* and *Security Metrics Baseline* questions were merged into one category called *Demographics*.

The survey was vetted by a team of consulting subject matter experts, two of these were Chief Information Security Officers, one was a retired Chief Information Security Officer, and two were highly respected security architects, one from a financial firm and one from a defense industrial base firm. This review team identified language issues that may interfere with accurate responses and also suggested some additions to the categories of metrics to be included. Their suggestions were incorporated into the survey prior to it being released to participants.

As the survey was intended for completion by human participants, it fell within the domain of scrutiny by survey the Stevens Institute of Technology Institutional Review Board. Topics of interest to the review board and corresponding details were:

- Characteristics of the subject population.

  The population is comprised of security subject matter experts. Security professionals are qualifies as experts by being invited to invitation-only security metrics workshops

run by well-qualified program committees. A return rate of about 25% is anticipated. The population is comprised of both male and female adults of average health and of unknown ethnical diversity. There is no intention to target special classes of subjects or those that may be vulnerable.

- The source of research material.

  All data collected is self-reported data collected through an online survey. Identifiable data is data about which industry the security professional works in, and security profession demographic information (e.g. level of education, number of years experience), as well as an option to provide an e-mail for volunteering to explain survey answers in more detail and/or to obtain survey results. The survey system uses a unique code in the survey link in order to allow the survey taker to quit the survey midway through completion and then return and complete later, from the same computer.

- Plans for recruitment of subjects.

  Those invited to take the survey were qualified in two ways. One set of experts was the group of people invited to an invite-only workshop of security metrics experts. The other was drawn from a database of contacts from our set of consulting experts, and so were prequalified based on personal experience. Each recommended expert will be vetted via biography-checking as well as asked to provide demographic information on security expertise in the survey itself. Consent is given by simply choosing to participate.

- Potential risks and procedures for protecting against or minimizing any potential risks.

  Little to no stress is anticipated, as participation is voluntary, and any stress experienced will most likely be due to inexperience with the survey tool (as is typical in online activity) itself rather than any content contained therein. The data collected is not personal in nature and the respondents may choose at any time to discontinue the survey. The survey population is security professionals who are already motivated to share their opinions about security metrics in forums such as workshops. Professional curiosity motivates security professionals to participate in these surveys because they expect to learn from the results.

Based on the above responses to Review Board concerns, approval for the survey was granted.

Appendix C – Survey Analysis Detail

Survey Method

The purpose of the survey was to elicit expert opinions on the properties and measures that are productively used to attribute security to a system. Five top tier security experts, a group comprised two security architects and three CISOs with strong technical background, were provided with a draft survey and asked to identify any ambiguities in it, or other potential difficulties a security expert may have in responding to it. This review team identified language issues that may interfere with accurate responses and also suggested some additions to the categories of metrics to be included. Their suggestions were incorporated into the survey prior to it being released to participants. These CISOs are also known for their participation in industry committees and other professional activities, and they were also requested to provide contact information for security subject matter experts that they felt would be qualified to opine on the survey content. As security experts are not easy to come by, the sample can only be considered a sample of convenience. Additional respondents were solicited from an invitation-only workshop on security metrics and a highly specialized technical security website blog. It is not known how many security experts may have viewed the survey participation request on the blog, so the percent response in this category is not meaningful. Table 1 summarizes the survey sample.

Table 1: Survey Response				
Survey Participant Source:	Total Solicited	Reminders Sent	Total Response	Percent Response
Security SME CISO Contacts	146	8	62	42.47%
Security SME Workshop	58	7	27	46.55%
SubTotal:	204		89	43.63%
Security SME Blog	20	0	20	100%
Total:	224		109	48.66%

The original survey questions asked respondents to assign ranks and weights to metrics. For example, to assign percentage weights to a list of security attributes, and to ensure that the sum of the weights totaled 100%. All of the expert survey reviewers commented that security experts are busy, and tend to get distracted by changes in the threat environments for systems for which they are responsible. For this reason, they advised that the survey questions would have to be more streamlined and easy to answer quickly. This led to changes in questions that asked for rankings and weightings of security attributes in favor of a simple Likert-scale approach to registering opinions about security attributes. An important design criteria for the survey was that it had to take the minimum amount of time required to deliver opinions on the entire field of study that currently constitutes security metrics.

The change in approach was not viewed as a total setback due to known issues with similar studies which solicited rankings and weights. In a similar study with respect to multi-attribute utility measurement in the domain of nuclear power plant planning, Borcherding et.al, used four weighting methods: the ratio method, the swing weighting method, the tradeoff method and the pricing out method [78]. The comparison of results

showed significant consistency and validity problems in the extent to which the results persist in a carefully designed interactive elicitation process. Speculated reasons for this inconsistency ranged from boredom with the information elicitation process to lack of true expertise on the part of the respondents. The study recommended using carefully designed interactive procedures for elicitation. For this reason, the security survey respondents were requested to provide contact information if they would be willing to participate in interactive follow-up if necessary.

The Boercherding study used an Analytic Hierarchy Process (AHP) approach, wherein one assumes that the problem space can be fully described in a way that priorities, allocations, weights, and preference ratios are judgments that can be represented with meaningful numbers which represent the importance of and dependencies between alternative and competing system attributes [79]. This approach was not used in the security survey because decision analysis in security is not as mature as it is in the domain of nuclear power plant planning. Security outcomes cannot yet be quantified in as clear terms, such as lost lives and environmental damage. The literature review of Chapter 2 makes it evident that there is no starting hierarchy that is agreed upon, and yet there is a wealth of candidate attributes for ranking.

Another approach to structuring this type of problem is described by Thurstone, where participants initially are provided with a blank slate, and iterative ranking exercises reduce the population of the overall attribute list [80]. Unfortunately in this study, the time constraints of potential survey respondents made it improbable that many would participate if they had to start with a blank slate. Moreover, an initial set of properties that

professionals currently use are readily apparent from the literature survey in Chapter 2, and so these were used as a starting point.

Both the Boercherding and the Thurstone studies acknowledge that it is necessary to analyze sensitivity to ambiguous questions, as well as any potential environmental changes in criteria that may result in changes in judgments. Decision theory as applied to security has typically concentrated on one aspect of the security problem, which is investments in a single security technology [81]. Thus the security problem, in contrast to that performed by Boercherding and the Thurstone, does not have a framework waiting to be articulated. Rather, this research is necessary *due* to the fact that system security is not yet well understood enough to place a framework around the problem for others to refine with weights. Yet neither do we begin with a blank slate. This situation is typical in any theory construction for attributes that are not well understood. As observed by Wrenn, "We must subject our constructs to measurement if we are to test our theories, but if we were to insist that theory tests wait until we have a fully axiomatic theoretical model, scientific inquiry would virtually halt" [82]. Hence, in addition to the security attribute criteria gleaned from the hypothesis and literature review, the survey contained other questions of multiple types which were designed to provide background "noise" in order to ensure that bias in attribute select choices was minimized. It also allow respondents to clarify their responses with open ended questions and selections of "other".

To answer prior studies' concerns related to ambiguity and environment, attribute-related questions were ranked using three methods: Thurstone's method [80], the One Number

Method [83], and the Survey Rating System based on proportionate number of respondent selections. These calculations are performed as follows:

- Thurstone's Method

  Post-initial ranking, the positioning of items on the Thurstone scale can be found by averaging the percentiles of the standard normal distribution corresponding to the proportions of the respondents preferring one item over each of the others.

- The One Number Method

  The One Number Method focuses on participant registration of strong opinion, and ignores responses that simply agree with a selection presented. Hence, it is calculated by summing the number of "5s" in a rating response, and subtracting the sum of the "1s", "2s" and "3s" from it, then dividing by the total responses. Where this calculation produced equal values, the number of "4s" was used to disambiguate the responses to allow a basis for selecting the order of the final ranking.

- Survey Rating Method

  Each of the 37 relevant questions on the survey received a rating based on a multiple of the number of respondents who selected a given value multiplied by that value. A straightforward calculation of the rating for a question wherein 5 people selected 1, 10 people selected 2, 15 people selected 3, 20 people selected 4 and the remaining 10 selected 5 was computed as:

  $$(5*1 + 10*2 + 15*3 + 20*4 + 10*5) / 60 = 3.33$$

  These ratings were disambiguated by a second order sort by the number of 5s, then 4s, and so on.

This three-part overall ranking was separated into four groups based on convergence of average rankings. The groups were further analyzed using a *Rank Order Centroid* method [108]. This showed that the differences between the weights in some of the Survey Rating System attributes that ended up in different order were small. The resultant rankings were compared and sent to the CISO-level survey respondents who volunteered to be asked follow-up questions.

Survey Results

Qualifications

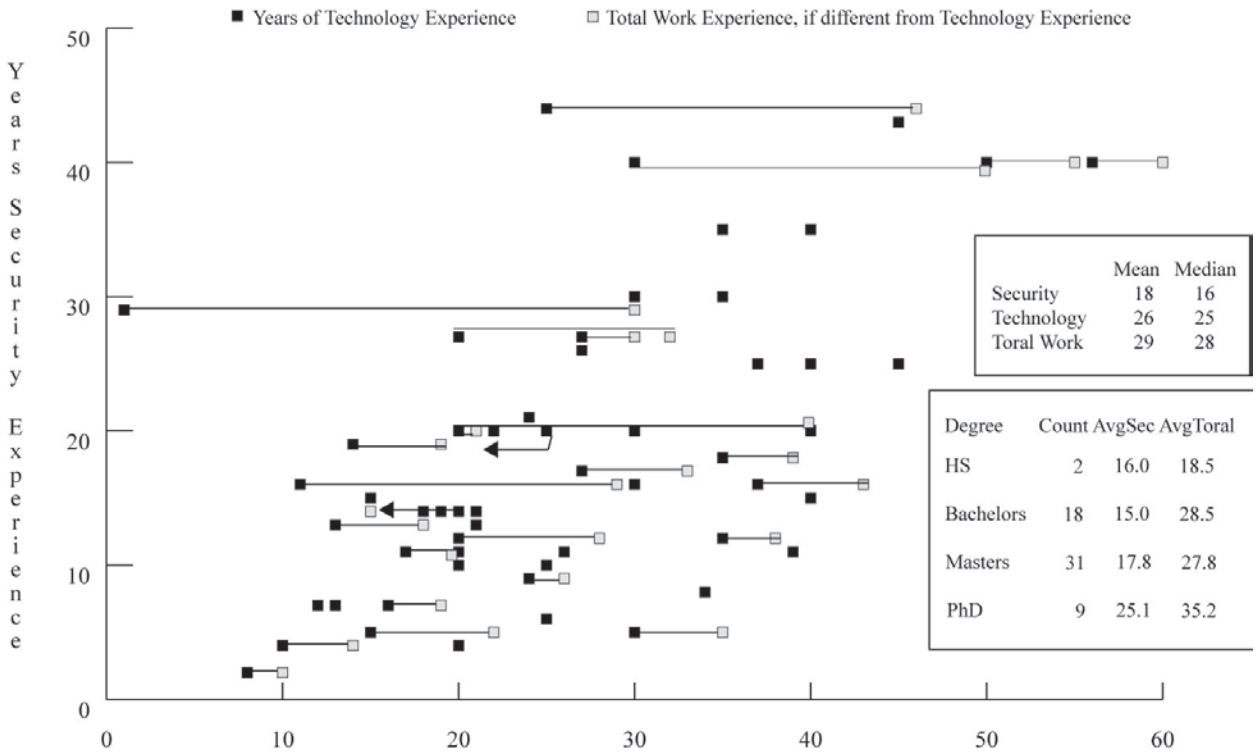
The supposition by the survey reviewers that security experts would get distracted while taking the survey and not finish it was correct. 13 of these had found the survey via the security expert blog site. Therefore, criteria were required to qualify partial respondents for inclusion in results analysis. The criteria were based upon the necessity to include questions on metrics identified in the research hypothesis, as well as a sufficient number of noise questions. This necessity suggested that the criteria include completion of the survey question that contained the widest variety of metrics alternative responses, which was question 21 on the survey. Only 62 respondents of the 109 who started the survey actually completed this question. An additional two respondents were removed from the results because they wrote that they had zero years of security experience. One was a student and another was a network administrator. A few others also missed putting in their years of security experience, but did fill in technology and work experience and were later determined to have been working in security for at least 15 year or more. Some of those who self-selected out of the survey by not reaching question 21 would also have

been removed based on lack of expert qualifications. For example, in response to a question about metrics types, two selected the option, “These terms are unfamiliar to me,” which was purposely included in order to weed out inexpert responses. Three others wrote that their job function was to build, operate or provide project management for security, and these professions are not typically sophisticated in security metrics. However, the ranks of the drop-outs did include at least 10 CISOs, 5 security architects, and a few reknowned security researchers. One researcher complained that the request for assistance with follow-up was improper, given that there was no statement given in advance of taking the survey that identification with the requested. One CISO was from the software industry and did not see a connection between the survey questions and her job function, which was not enterprise but product security. The final count for analysis was 60.

The minimum number of years in the security profession among the 60 was two, but that person had ten years of work experience, and eight years of that experience was in technology. This was also the minimum technology and work experience of the group, no one among the respondents has less than ten years of total work experience. The most experienced in security had 44 years of security experience, 25 years in technology, and 46 years total work experience. The qualifications of the experts are illustrated in Figure 1. Where technology experience and work experience were not the same, they are connected by a line on the graph. Two people reported having a few more years for technology experience than total work experience, and this result is depicted by an arrow pointing to the left in the line which connects them on the graph. The graph shows less

than 60 points because a few respondents had exactly the same number of years experience in all three dimensions. Figure 1 also shows the highest level of education for the individuals. Following the count is the average years in security of individual of that degree level, and the average total work experience at that level.

Figure 1: Survey Respondent Demographics



Two thirds of the participants were active in security professional organizations and over two-thirds had some form of security certification. Seventy-eight percent of the participants were either active or certified. Forty percent of the participants were from the financial industry. This demographic factor was considered large enough to potentially skew the results as financial industry-specific, so a hypothesis was formulated that the distribution of results was the same in this population as compared to the non-financial participants. The Mann-Whitney (Wilcoxon) test was performed on all of the questions

that led to our security attribute ranking, and only one attribute registered a level of significance required to reject that hypothesis. This was the attribute of being able to pass a penetration test. A cross tabulation of industry group with that attribute revealed that financial industry background was strongly correlated with a high rating for penetration testing. This is likely due to the financial industry's relatively higher budgets for hiring outside consultants, and resulting experience that such measures often identify previously unknown vulnerabilities. As this recognition is a sign of experience with a specific tool, rather than being related to financial industry systems, the observation was not sufficiently financial-industry specific to omit either the participants or the question from the sample data. As the Mann-Whitney tests for change in median, an additional test for a more general change of shape, the Kolmogorov-Smirnov test, was performed. The results of both independence tests, and the cross-tabulation results for the question on penetration studies, are included in Appendix E. Given the results, there is no reason to believe that our sample, though skewed toward financial services representation, is not representative of the more general population of security experts sampled.

Rank Results

In the survey, security attributes were rated by experts in six questions, though two of those were confined to systems of a given type, and had lower participation levels. Combining the other four questions provided the general set of opinions on security attributes required for comparison (Questions 21, 24, 25, 26). The three rating methods were compared and disambiguated on this subset of four questions.

The four general questions combined constitute a 44 independent multinomial trial of 5 possible outcomes of the same probabilities. A normal distribution of results would indicate that respondent answers were the equivalent of random selections. This would be the case if the respondents as a whole had ambiguous attitudes toward a given question. By contrast, a positive kurtosis or significant skewness would indicate that the observations are more clustered about an attitude on which respondents agree.

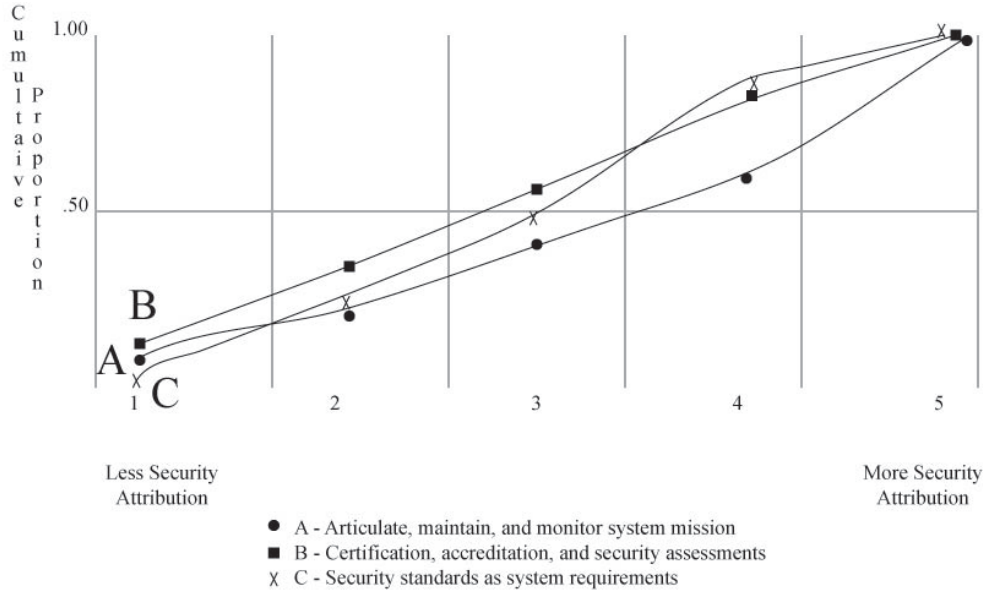
Sorting the statements requires the collected opinions to be compared. As in [80], this was done via a phi-gamma curve as illustrated in Figure 2. The diagram plots the respondent's answers to the first three statements on which they were asked to opine. The steeper the curve associated with a set of opinions concerning the corresponding security attribute, the smaller is the degree of disagreement in the scale by which it was classified by the respondents, so it is a more precise statement. The gentler the slope of the curve, the more ambiguous is the statement. In the example of Figure 2, item C is a less controversial a statement than A or B. Those which are both skewed to the right and have positive kurtosis ranked higher than those with a larger area of the curve in the lower quadrants. Collective responses to any question that approximates a normal distribution or a flat curve are judged too ambiguous to merit inclusion as a security attribute.

Appendix F includes descriptive statistics for all attributes. Those removed due to ambiguity have a skew value below 0.3 and also a central mean (flat) or kurtosis near zero (normal). These were:

- Q21-23-ThreatProb
- Q21-24-DamageProb

- Q24-5-Deliver
- Q24-6-Provenance
- Q25-6-Perform
- Q26-1-IndepComp
- Q26-3-COTS

Figure 2: Example Diagram of Opinions on Security Attribution



The results of the rankings of all three methods are listed in Table 2.:

Table 2: Attribute Rank Order for Survey Responses

Orig Order	Question Label	Thurstone	One Number	Survey Rating
20	Q21-20-IDAuth	1	1	1
27	Q24-4-PassPenTest	2	2	3
11	Q21-11-Incident	3	4	4
36	Q26-4-VaInput	4	3	2

Table 2: Attribute Rank Order for Survey Responses				
Orig Order	**Question Label**	**Thurstone**	**One Number**	**Survey Rating**
1	Q21-1-Mission	5	7	13
8	Q21-8-Awareness	6	5	5
23	Q21-25-ThreatProtProb	7	6	9
14	Q21-14-PhysEnv	8	14	22
15	Q21-15-Personnel	9	12	19
10	Q21-10-Recovery	10	10	7
17	Q21-17-Interfaces	11	11	15
9	Q21-9-SWChange	12	18	10
37	Q26-5-DefOutput	13	8	8
26	Q24-3-PassSecRev	14	20	18
19	Q21-19-AuditTrails	15	15	23
4	Q21-4-Risk	16	9	6
18	Q21-18-Segregate	17	17	17
16	Q21-16-SWIntegrity	18	19	16
7	Q21-7-Acquisition	19	21	24
5	Q21-5-Infrast	20	13	12
6	Q21-6-Features	21	25	21
13	Q21-13-Media	22	26	30
33	Q25-4-Logs	23	16	11
2	Q21-2-Certif	24	32	34

Table 2: Attribute Rank Order for Survey Responses				
Orig Order	**Question Label**	**Thurstone**	**One Number**	**Survey Rating**
22	Q21-22-AssetValue	25	24	29
32	Q25-3-Mgmt	26	28	25
3	Q21-3-Standards	27	30	26
34	Q25-5-BCP	28	23	14
29	Q24-8-FailSafe	29	35	35
28	Q24-7-Interfaces	30	31	33
25	Q24-2-SecAudit	31	29	27
35	Q26-2-Pattern	32	22	20
31	Q25-2-Config	33	27	28
24	Q24-1-RegAudit	34	36	36
12	Q21-12-VendorOver	35	34	32
21	Q21-21-TechCfg	36	33	31
30	Q25-1-Resources	37	37	37

Subsequent Analysis

The result is three ordered lists. Although the rank order of systems properties that merit positive attribution of security are the three types of ranks in Table 2 were different in order, they periodically converged. There were clusters of responses wherein the averaging of responses within ranks show that several sets of values maintained their general order within the more detailed sub-ordering within the clusters. That is, holding

one ordering constant, the sum the ranks for all three of the methods for the corresponding survey question was divided by the rank within the corresponding order. Where these values converged, the ranks within groups were roughly equal. This overall ranking was separated into four groups based on convergence of average rankings holding the Thurstone order constant. The choice of Thurston was based on the scientific validity of that study compared to the other methods. A further test was performed to ensure that the ordering did not overlook the differences in each interval between the ordered ratings. For example, a rank order of 1,2,3 has a different meaning than a rank order of 1, 3.4, 4.6. The groups were further analyzed using a *Rank Order Centroid* method [108]. This showed that the differences between the weights in some of the Survey Rating System attributes that ended up in different order were small. Table 3 shows the four clusters of attributes that resulted from this analysis.

Table 3: Clusters of Ranked Attributes

1	User identification and authentication
	Withstand targeted penetration attacks by skilled attack teams
	Incident detection and response
	System interfaces accept only valid input
	Articulate, maintain, and monitor system mission
	Security awareness
	Evaluate the extent to which systems are protected from known threats
	Physical and environmental protection
	Personnel screening and supervision

Table 3: Clusters of Ranked Attributes	
2	System recovery planning
	Security features required to maintain integrity over system interfaces
	System and software change control
	System output conforms to well-defined specifications
	Pass internal security review
	Maintain audit trails on use of system functions
	System-level risk assessment
3	Segregate users into groups or roles for access control
	Software integrity preservation
	Due diligence in system and services acquisition
	Infrastructure risk assessment
	Security features that correspond to system functions
	Control over removable media
	Logs that verify that process designed to secure system is followed
	Certification, accreditation, and security assessments
	Quantify the value of assets at risk in system operation
4	Progress in a management plan to secure system
	Use security standards as system requirements
	Successful execution of business continuity procedures
	Fail in denial of service mode
	Maintain integrity of interfaces through system development lifecycle
	Pass security audit

Table 3: Clusters of Ranked Attributes
System follows a commonly used architecture pattern
Percentage of systems or components that have passed security configuration tests
Pass regulatory audit
Oversight of vendor maintenance
Maintain values of standard security variables in system technical configuration
Number of resources consumed in system security-related tasks

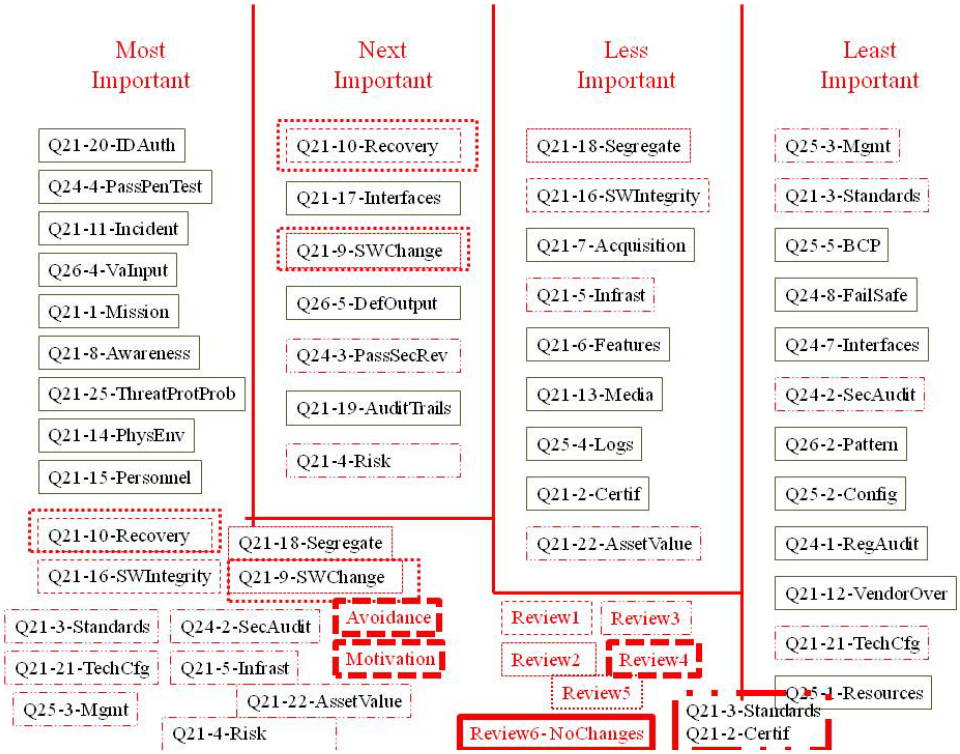
Final Analysis

Of the 29 people who provided an email address for follow-up questions, 19 were either CISOs or consultants with CISO experience. The CISO-level follow-up participants were instructed to review the rankings in the lists attached and make any corrections or comments they thought may be necessary to ensure that this study emphasizes the most important attributes of system security in proper order. Six of these individuals provided detailed feedback. Of those who completed the request for corrections and comments, all but one suggested minor changes in the four categories of groupings, and these are displayed in Figure 3. Only one of the participants suggested that a component level measure (technical configuration) be elevated to “Most Important” status. This person had considerable experience in the component certification and accreditation process, and even had authored a book on the subject [109]. This confirmed some of the other reviewers’ comments that bias will of course affect professional judgment. None of the

suggested changes affected the conclusion that the three systems level attributes identified in the research hypothesis are among the most important.

Specific subject matter expert follow-up comments included general disappointment that any security attribute would be considered “not important” as component security could of course be a weak link in a chain or armor. They also commented that responses to the survey were subjective, and complained about the “noise” level of the questions, both of which were, as noted in Section 3.1, intentional.

Figure 3: Rank Shifts Suggested by Survey Follow-Up Respondents



A few respondents that did not provide detailed feedback instead commented either that it was an onerous exercise, or superfluous given the natural bias of participants and inherent limitations of surveys as tools to compare dissimilar concepts.

The full set of survey results in Appendix C includes all comments from all participants. Notable comments supporting this tiered approach to security requirements are:

- *The environment requires easy to understand system documentation from inception to production with security being an identifiable component at all levels. As much detail as is needed to fully describe security related elements/functions is required and development phases are reviewed and accepted or rejected based on completeness and ease of understanding.*
- *System security verification requires an assessment of how the integrated security components combine to defend against, discover or respond to attacks.*
- *Security is an epiphenomenon, a second-order effect of a business process as implemented in a cultural context. As such it is difficult to define repeatable, comparable, quantifiable objective measures of security.*
- *The best security metrics are those that have business correlation, and can be collected analyzed and communicated to support decisions (I assume your context implies that this capability exists, but in truth most organizations struggle reaching a minimal level of maturity) Your question brought to mind a similar question: "What is the best language?" My response to that has always been similar to the one above. Those with the ability to communicate in multiple languages have strong opinions in this area, but if you ask a language professor they will often slap their foreheads and wish that their students knew how to communicate in any language. (My 2 cents from the soapbox)*

Comments also echoed some remarks from Chapter 1 that emphasized the need for reliable security metrics. For example:

- *My use of metrics is not particularly mature or consistent. I rely a great deal on the judgment and consensus of SMEs.*
- *Security Metrics should be used as transitory - they are not true representation of performance or status, but more a convenient means to define targets, benchmarks, status for the temporary time they remain relevant and are not gamed*
- *Like all metrics they become gamed unless reality is more difficult to achieve than the metric itself.*
- *The phrase security metrics means: a migrane.*

The STAC framework provided by this dissertation attempts to answer these concerns and provide some utility to these security experts.

Appendix D – Survey Questions and Answers

Security SME Metrics

SurveyMonkey

1. Please use the following drop-down list to select your current field of employment:

	Response Percent	Response Count
Financial/Banking	**33.0%**	**36**
Insurance	3.7%	4
Public Accounting	1.8%	2
Transportation	0.0%	0
Aerospace	0.0%	0
Retail/Wholesale/Distribution	1.8%	2
Government/Military – National/State/Local	6.4%	7
Technology Service/Consulting	18.3%	20
Manufacturing/Engineering	2.8%	3
Telecommunications/Communications	5.5%	6
Mining/Construction/Petroleum/Agriculture	0.9%	1
Utilities	0.0%	0
Legal/Law/Real Estate	0.0%	0
Health Care/Medical	1.8%	2
Pharmaceutical	0.0%	0
Advertising/Marketing/Media	0.9%	1
Education/Student	14.7%	16
Other	8.3%	9
	If you chose OTHER, please specify:	8
	answered question	**109**

skipped question	0

2. Please use the following drop-down list to select your current professional activity:

		Response Percent	Response Count
CEO, President, Owner, General/Executive Manager		5.5%	6
CAE, General Auditor, Partner, Audit Head/VP/EVP		0.0%	0
CISO/CSO, Security Executive/VP/EVP		**23.9%**	**26**
CIO/CTO, Security Executive/VP/EVP		0.0%	0
CIO/CTO, Info Systems/Technology Executive/VP/EVP		5.5%	6
CFO/Controller, Treasurer, Finance Executive/VP/EVP		0.9%	1
Chief Compliance/Risk/Privacy officer, VP/EVP		0.9%	1
IT Audit Director/Manager/Consultant		3.7%	4
Security Director/Manager/Consultant		18.3%	20
IT Director/Manager/Consultant		2.8%	3
Compliance/Risk/Privacy Director/Manager/Consultant		2.8%	3
IT Senior Auditor (External/Internal)		0.0%	0
IT Auditor (External/Internal Staff)		0.0%	0
Non-IT Auditor (External/Internal)		0.0%	0
Security Staff		2.8%	3
IT Staff		5.5%	6

IT/IS Compliance/Risk/Control Staff		3.7%	4
Professor/Teacher		6.4%	7
Student		4.6%	5
Security Architect		4.6%	5
Other		8.3%	9
		If you chose OTHER, please specify:	10
		answered question	109
		skipped question	0

3. and 4. If you selected 'Security Architect' in response to question 2, please answer questions 3 and 4. Otherwise, please select the 'NEXT' button below. 3. On roughly how many projects did you have security architecture responsibilities?

Response Count
12
answered question 12
skipped question 97

4. What was the budget of the largest one?

Response Count
9
answered question 9
skipped question 100

5. Please use the following drop-down list to describe the size of your organization:

	Response Percent	Response Count
Not applicable	6.1%	6
Fewer than 50 employees	17.3%	17
50-499 employees	11.2%	11
500-4,999 employees	16.3%	16
5000-19,999 employees	13.3%	13
20,000-74,999 employees	13.3%	13
Over 75,000 employees	**22.4%**	**22**
	answered question	**98**
	skipped question	**11**

6. Please use the following drop-down list to describe the size of the IT audit staff:

	Response Percent	Response Count
Not applicable	22.4%	22
0 individuals	9.2%	9
1-10 individuals	26.5%	26
11-25 individuals	7.1%	7
Over 25 individuals	**34.7%**	**34**
	answered question	**98**
	skipped question	**11**

7. Please use the following drop-down list to describe the size of the security staff:

	Response Percent	Response Count
Not applicable	18.4%	18
0 individuals	3.1%	3
1-5 individuals	19.4%	19
6-10 individuals	10.2%	10
11-25 individuals	8.2%	8
Over 25 individuals	**40.8%**	**40**
	answered question	**98**
	skipped question	**11**

8. Please use the following drop-down list to describe the area of your professional interest:

	Response Percent	Response Count
Assurance/Audit	2.0%	2
Governance of Enterprise IT	4.1%	4
Information Security	**66.3%**	**65**
IT Compliance	1.0%	1
IT Control	1.0%	1
IT Value Delivery	5.1%	5
Risk Management	20.4%	20
	answered question	**98**
	skipped question	**11**

9. Please check all Professional Certifications you currently hold:

	Response Percent	Response Count
CISSP from ISC2	**61.7%**	**37**
CISM from ISACA	43.3%	26
CISA from ISACA	21.7%	13
GSEC from SANS	5.0%	3
GIAC from SANS	3.3%	2
Other, please specify certification and organization in the box below	40.0%	24
	answered question	**60**
	skipped question	**49**

10. Which of these or other professional security associations are you a member or officer?

	Member	Officer	Response Count
ASIS	**100.0% (3)**	0.0% (0)	3
CSI	**100.0% (5)**	0.0% (0)	5
ISACA	**91.4% (32)**	8.6% (3)	35
ICS2	**96.4% (27)**	3.6% (1)	28
ISF	**100.0% (7)**	0.0% (0)	7
ISSA	**86.4% (19)**	13.6% (3)	22
SANS	**75.0% (3)**	25.0% (1)	4
	Other, please specify membership and officer status		13
		answered question	**54**
		skipped question	**55**

11. Education (select all that apply):

	Response Percent	Response Count
High School	**51.1%**	**46**
Bachelor's Degree in Science or Engineering	43.3%	39
Bachelor's Degree Social Science or Humanities	12.2%	11
Other Bachelor's Degree	13.3%	12
Masters Degree in Science or Engineering	33.3%	30
Masters Degree Social Science or Humanities	6.7%	6
Masters Degree not in Science, Engineering, Social Science or Humanities	20.0%	18
PhD in technical field	11.1%	10
PhD non-technical field	2.2%	2
	answered question	**90**
	skipped question	**19**

12. Enter the number of years in security (if any):

	Response Count
	86
answered question	**86**
skipped question	**23**

13. Number of years in a technology-related field (if any):	
	Response Count
	87
answered question	87
skipped question	22

14. Enter the total number of years of work experience:	
	Response Count
	91
answered question	91
skipped question	18

15. If you have current responsibilities with respect to security architecture, how would you describe them (please check all that apply and add any significant others):

	Response Percent	Response Count
Consulting	**65.8%**	**50**
Requirements	55.3%	42
Design	42.1%	32
Manufacture	1.3%	1
Implementation	28.9%	22
Integration	21.1%	16
Test	22.4%	17
Operate	14.5%	11
Evaluate	44.7%	34
Recommend	55.3%	42
Approve	38.2%	29
Purchase	22.4%	17
Sell	9.2%	7
Management Oversight	44.7%	34
Audit	17.1%	13
Sign-off on requirements	31.6%	24
Sign-off on design	26.3%	20
Sign-off on implementation strategy	26.3%	20
Sign-off on production operation	15.8%	12
Other (please specify in the box below)	11.8%	9
	answered question	**76**

skipped question	33

16. Please provide your definitions of the word "measurement," the word "metrics," and the phrase "security metrics" in general, without reference to security, by completing the following sentences: The word "measurement" means:

Response Count
71

answered question	71
skipped question	38

17. The word "metrics" means:

Response Count
71

answered question	71
skipped question	38

18. The phrase "security metrics" means:

Response Count
71

answered question	71
skipped question	38

19. In your opinion, are the best security metrics (please choose from the following drop-down list):

	Response Percent	Response Count
Nominal	5.6%	4
Ordinal	11.3%	8
Interval	2.8%	2
Ratio	16.9%	12
These terms are unfamiliar to me	25.4%	18
Other	**38.0%**	**27**
If you chose OTHER, please describe and explain why in the box below.		29
	answered question	**71**
	skipped question	**38**

20. Please explain the reasoning behind your answer to Question 19:

	Response Count
	71
answered question	**71**
skipped question	**38**

21. Please rate the following list of activities on a scale from 0 to 5, where the number indicates the contribution of the activity to an organization's ability to maintain its security. Each activity must be assigned its own number, but the number can be zero:

	0	1	2	3	4	5	Rating Average	Response Count
Articulate, maintain, and monitor system mission	0.0% (0)	8.1% (5)	11.3% (7)	22.6% (14)	16.1% (10)	**41.9% (26)**	3.73	62
Certification, accreditation, and security assessments	3.2% (2)	9.7% (6)	17.7% (11)	**30.6% (19)**	19.4% (12)	19.4% (12)	3.11	62
Use security standards as system requirements	4.8% (3)	4.8% (3)	14.5% (9)	**29.0% (18)**	**29.0% (18)**	17.7% (11)	3.26	62
System-level risk assessment	1.6% (1)	0.0% (0)	8.1% (5)	21.0% (13)	**43.5% (27)**	25.8% (16)	3.82	62
Infrastructure risk assessment	1.6% (1)	4.8% (3)	8.1% (5)	19.4% (12)	**43.5% (27)**	22.6% (14)	3.66	62
Identify security features that correspond to system functions	1.6% (1)	4.8% (3)	8.1% (5)	**32.3% (20)**	30.6% (19)	22.6% (14)	3.53	62
Due diligence in system and services acquisition	1.6% (1)	1.6% (1)	16.1% (10)	**29.0% (18)**	27.4% (17)	24.2% (15)	3.52	62
Security awareness	1.6% (1)	1.6% (1)	11.3% (7)	19.4% (12)	25.8% (16)	**40.3% (25)**	3.87	62
System and software change control	4.8% (3)	0.0% (0)	11.3% (7)	27.4% (17)	**29.0% (18)**	27.4% (17)	3.58	62
System recovery planning	4.8% (3)	0.0% (0)	9.7% (6)	21.0% (13)	**33.9% (21)**	30.6% (19)	3.71	62
Incident detection and response	3.2% (2)	3.2% (2)	4.8% (3)	14.5% (9)	29.0% (18)	**45.2% (28)**	3.98	62
Oversight of vendor maintenance	0.0% (0)	8.1% (5)	12.9% (8)	30.6% (19)	**35.5% (22)**	12.9% (8)	3.32	62
Control over removable media	4.8% (3)	9.7% (6)	12.9% (8)	19.4% (12)	**30.6% (19)**	22.6% (14)	3.29	62
Physical and environmental protection	3.2% (2)	8.1% (5)	9.7% (6)	24.2% (15)	21.0% (13)	**33.9% (21)**	3.53	62

Personnel screening and supervision	3.2% (2)	6.5% (4)	12.9% (8)	17.7% (11)	27.4% (17)	**32.3% (20)**	3.56	62
Software integrity preservation	3.2% (2)	0.0% (0)	16.1% (10)	24.2% (15)	**30.6% (19)**	25.8% (16)	3.56	62
Identify security features required to maintain integrity over system interfaces	1.6% (1)	8.1% (5)	8.1% (5)	17.7% (11)	**35.5% (22)**	29.0% (18)	3.65	62
Segregate users into groups or roles for access control	1.6% (1)	8.1% (5)	6.5% (4)	24.2% (15)	**33.9% (21)**	25.8% (16)	3.58	62
Maintain audit trails on use of system functions	1.6% (1)	3.3% (2)	16.4% (10)	18.0% (11)	**36.1% (22)**	24.6% (15)	3.57	61
User identification and authentication	3.2% (2)	0.0% (0)	3.2% (2)	4.8% (3)	29.0% (18)	**59.7% (37)**	4.35	62
Maintain values of standard security variables in system technical configuration	6.5% (4)	1.6% (1)	19.4% (12)	22.6% (14)	**38.7% (24)**	11.3% (7)	3.19	62
Quantify the value of assets at risk in system operation	1.6% (1)	4.8% (3)	17.7% (11)	21.0% (13)	**35.5% (22)**	19.4% (12)	3.42	62
Quantify probability of system security threats	4.8% (3)	8.1% (5)	19.4% (12)	**30.6% (19)**	17.7% (11)	19.4% (12)	3.06	62
Quantify potential organizational damage from system security threats	1.6% (1)	1.6% (1)	19.4% (12)	**30.6% (19)**	21.0% (13)	25.8% (16)	3.45	62
Evaluate the extent to which systems are protected from known threats	0.0% (0)	3.2% (2)	11.3% (7)	16.1% (10)	33.9% (21)	**35.5% (22)**	3.87	62
Other, if applicable	38.9% (7)	0.0% (0)	5.6% (1)	0.0% (0)	5.6% (1)	**50.0% (9)**	2.83	18
						If you chose OTHER, please specify:		13
						answered question		**62**
						skipped question		**47**

22. Please answer this question from the perspective of the highest level of management in your organization (e.g. CEO or President), as you perceive them to think about security. That is, how would your management rate, on a scale of 1 to 5, where 5 is the highest indicator that an organization which performs these activities is secure and is the lowest or least significant indicator of organizational security: (If not applicable please skip to the next question)

	1	2	3	4	5	Rating Average	Response Count
Articulate, maintain, and monitor system mission	2.2% (1)	13.0% (6)	21.7% (10)	28.3% (13)	**34.8% (16)**	3.80	46
Certification, accreditation, and security assessments	8.5% (4)	23.4% (11)	25.5% (12)	**31.9% (15)**	10.6% (5)	3.13	47
Use security standards as system requirements	8.5% (4)	19.1% (9)	25.5% (12)	**34.0% (16)**	12.8% (6)	3.23	47
System-level risk assessment	2.1% (1)	25.5% (12)	29.8% (14)	**36.2% (17)**	6.4% (3)	3.19	47
Identify security features that correspond to system functions	6.5% (3)	28.3% (13)	**45.7% (21)**	15.2% (7)	4.3% (2)	2.83	46
Due diligence in system and services acquisition	2.1% (1)	14.9% (7)	27.7% (13)	**36.2% (17)**	19.1% (9)	3.55	47
Security awareness	4.3% (2)	6.4% (3)	**31.9% (15)**	29.8% (14)	27.7% (13)	3.70	47
System and software change control	0.0% (0)	25.5% (12)	**29.8% (14)**	23.4% (11)	21.3% (10)	3.40	47
System recovery planning	2.1% (1)	17.0% (8)	21.3% (10)	**40.4% (19)**	19.1% (9)	3.57	47
Incident detection and response	0.0% (0)	19.1% (9)	19.1% (9)	**36.2% (17)**	25.5% (12)	3.68	47
Oversight of vendor maintenance	4.3% (2)	21.3% (10)	**34.0% (16)**	27.7% (13)	12.8% (6)	3.23	47
Control over removable media	17.0% (8)	**29.8% (14)**	14.9% (7)	**29.8% (14)**	8.5% (4)	2.83	47
Physical and environmental protection	0.0% (0)	23.4% (11)	17.0% (8)	**38.3% (18)**	21.3% (10)	3.57	47

Personnel screening and supervision	0.0% (0)	14.9% (7)	19.1% (9)	**42.6% (20)**	23.4% (11)	3.74	47
Software integrity preservation	8.5% (4)	27.7% (13)	**29.8% (14)**	25.5% (12)	8.5% (4)	2.98	47
Identify security features required to maintain integrity over system interfaces	10.6% (5)	**38.3% (18)**	23.4% (11)	23.4% (11)	4.3% (2)	2.72	47
Segregate users into groups or roles for access control	10.9% (5)	15.2% (7)	28.3% (13)	**30.4% (14)**	15.2% (7)	3.24	46
Maintain audit trails on use of system functions	4.3% (2)	27.7% (13)	21.3% (10)	**34.0% (16)**	12.8% (6)	3.23	47
User identification and authentication	0.0% (0)	8.5% (4)	27.7% (13)	**34.0% (16)**	29.8% (14)	3.85	47
Maintain standard security variables in system technical configuration	10.6% (5)	**34.0% (16)**	31.9% (15)	17.0% (8)	6.4% (3)	2.74	47
Quantify the value of assets at risk in system operation	4.3% (2)	12.8% (6)	**38.3% (18)**	17.0% (8)	27.7% (13)	3.51	47
Quantify probability of system security threats	4.3% (2)	21.3% (10)	**34.0% (16)**	23.4% (11)	17.0% (8)	3.28	47
Quantify potential organizational damage from system security threats	2.1% (1)	17.0% (8)	27.7% (13)	**29.8% (14)**	23.4% (11)	3.55	47
Evaluate the extent to which systems are protected from known threats	2.1% (1)	14.9% (7)	27.7% (13)	**31.9% (15)**	23.4% (11)	3.60	47
Other, if applicable	**30.8% (4)**	0.0% (0)	15.4% (2)	23.1% (3)	**30.8% (4)**	3.23	13
					If you chose OTHER, please specify:		6

answered question	**47**
skipped question	**62**

23. Please select the sentence fragments that complete the stem sentence and make it true (select all that apply): System security verification requires

	Response Percent	Response Count
... finite, cost-effective verification techniques	52.5%	32
... clear articulation of system mission and/or purpose	67.2%	41
... quantification of system assets	42.6%	26
... quantification of system threat environment	47.5%	29
... quantification of impact of system vulnerability exploit	52.5%	32
... technical analysis of security features	70.5%	43
... specification of security functional requirements	**72.1%**	**44**
Other (please specify in the box below)	8.2%	5
	answered question	**61**
	skipped question	**48**

24. Please rate the following system abilities on a scale of 1 to 5, where 5 is the highest indicator that a system which exhibits these attributes is secure and 1 is the lowest or least significant indicator that the system exhibits security.

	1	2	3	4	5	Rating Average	Response Count
pass regulatory audit	26.2% (16)	23.0% (14)	**31.1% (19)**	8.2% (5)	11.5% (7)	2.56	61
pass security audit	6.6% (4)	11.5% (7)	32.8% (20)	**34.4% (21)**	14.8% (9)	3.39	61
pass internal security review	4.9% (3)	8.2% (5)	**36.1% (22)**	26.2% (16)	24.6% (15)	3.57	61
withstand targeted penetration attacks by skilled attack teams	1.6% (1)	6.6% (4)	9.8% (6)	37.7% (23)	**44.3% (27)**	4.16	61
deliver on service level agreements despite damage to functional components	8.2% (5)	21.3% (13)	24.6% (15)	**36.1% (22)**	9.8% (6)	3.18	61
trace software provenance	9.8% (6)	21.3% (13)	**49.2% (30)**	11.5% (7)	8.2% (5)	2.87	61
maintain integrity of interfaces through system development lifecycle	9.8% (6)	14.8% (9)	**31.1% (19)**	29.5% (18)	14.8% (9)	3.25	61
fail in denial of service mode	21.3% (13)	**27.9% (17)**	23.0% (14)	13.1% (8)	14.8% (9)	2.72	61
Other, if applicable	25.0% (2)	0.0% (0)	12.5% (1)	0.0% (0)	**62.5% (5)**	3.75	8
					If you chose OTHER, please specify:		7

answered question	**61**
skipped question	**48**

25. Please rate the following types of measurement on a scale of 1 to 5, where 5 is the highest indicator that a measurement of the given type is useful in measuring system security and 1 is the lowest or least significant indicator that measurement of the given type is useful in measuring system security.

	1	2	3	4	5	Rating Average	Response Count
Number of resources consumed in system security-related tasks	**30.4% (17)**	23.2% (13)	28.6% (16)	14.3% (8)	3.6% (2)	2.38	56
Percentage of systems or components that have passed security configuration tests	3.6% (2)	19.6% (11)	21.4% (12)	**42.9% (24)**	12.5% (7)	3.41	56
Progress in a management plan to secure system	3.6% (2)	12.5% (7)	**35.7% (20)**	30.4% (17)	17.9% (10)	3.46	56
Logs that verify that process designed to secure system is followed	3.6% (2)	5.4% (3)	28.6% (16)	**42.9% (24)**	19.6% (11)	3.70	56
Successful execution of business continuity procedures	1.8% (1)	7.1% (4)	32.1% (18)	**42.9% (24)**	16.1% (9)	3.64	56
System performance measures in changing threat environment	1.8% (1)	21.4% (12)	23.2% (13)	**33.9% (19)**	19.6% (11)	3.48	56
Other, if applicable	22.2% (2)	0.0% (0)	11.1% (1)	11.1% (1)	**55.6% (5)**	3.78	9
					If you chose OTHER, please specify:		6
						answered question	**56**
						skipped question	**53**

26. Please rate following system characteristics on a scale of 1 to 5, where 5 is the highest indicator that system security requirements should be easy to identify and gather, and 1 is the lowest or least significant indicator that system security requirements should be easy to identify and gather.

	1	2	3	4	5	Rating Average	Response Count
System is comprised of independently operating functional components	10.7% (6)	19.6% (11)	23.2% (13)	**33.9% (19)**	12.5% (7)	3.18	56
System follows a commonly used architecture pattern	1.8% (1)	12.5% (7)	25.0% (14)	**46.4% (26)**	14.3% (8)	3.59	56
System uses off-the-shelf security software	14.3% (8)	21.4% (12)	**35.7% (20)**	12.5% (7)	16.1% (9)	2.95	56
System interfaces accept only valid input	1.8% (1)	5.4% (3)	16.1% (9)	33.9% (19)	**42.9% (24)**	4.11	56
System output conforms to well-defined specifications	5.4% (3)	5.4% (3)	21.4% (12)	**42.9% (24)**	25.0% (14)	3.77	56
Other, if applicable	33.3% (2)	0.0% (0)	16.7% (1)	0.0% (0)	**50.0% (3)**	3.33	6
					If you chose OTHER, please specify:		4
					answered question		**56**
					skipped question		**53**

27. Assume you are using a system to maintain critical industrial control operations. Please rate following security features on a scale of 1 to 5, where 5 is the highest indicator that the critical industrial control operation system requires implementation of this feature to be considered secure, and 1 is the lowest or least significant indicator that including of this item as a system security feature is required to be considered secure

	1	2	3	4	5	Rating Average	Response Count
Role-based identification	5.5% (3)	3.6% (2)	23.6% (13)	29.1% (16)	**38.2% (21)**	3.91	55
Access control	0.0% (0)	0.0% (0)	9.1% (5)	18.2% (10)	**72.7% (40)**	4.64	55
Non-repudiation	5.5% (3)	12.7% (7)	21.8% (12)	**30.9% (17)**	29.1% (16)	3.65	55
Data confidentiality	10.9% (6)	7.3% (4)	12.7% (7)	27.3% (15)	**41.8% (23)**	3.82	55
Data integrity	0.0% (0)	0.0% (0)	3.6% (2)	27.3% (15)	**69.1% (38)**	4.65	55
Communication security	1.8% (1)	1.8% (1)	10.9% (6)	25.5% (14)	**60.0% (33)**	4.40	55
Software integrity	0.0% (0)	1.8% (1)	7.3% (4)	21.8% (12)	**69.1% (38)**	4.58	55
Interface integrity	0.0% (0)	1.8% (1)	14.5% (8)	23.6% (13)	**60.0% (33)**	4.42	55
Compartmentalization	1.8% (1)	7.3% (4)	29.1% (16)	**30.9% (17)**	**30.9% (17)**	3.82	55
Resistance to DDOS	1.8% (1)	9.1% (5)	20.0% (11)	**36.4% (20)**	32.7% (18)	3.89	55
Resistance to Botnet activities	3.6% (2)	7.3% (4)	18.2% (10)	30.9% (17)	**40.0% (22)**	3.96	55
					answered question		**55**
					skipped question		**54**

28. Assume you are using a system to maintain a corporate network. Please rate following security features on a scale of 1 to 5, where 5 is the highest indicator that a corporate network requires implementation of this feature to be considered secure, and 1 is the lowest or least significant indicator that this corporate network security feature is required to be considered secure.

	1	2	3	4	5	Rating Average	Response Count
Role-based identification	5.5% (3)	5.5% (3)	16.4% (9)	32.7% (18)	**40.0% (22)**	3.96	55
Access control	0.0% (0)	0.0% (0)	5.5% (3)	23.6% (13)	**70.9% (39)**	4.65	55
Non-repudiation	7.3% (4)	12.7% (7)	18.2% (10)	**36.4% (20)**	25.5% (14)	3.60	55
Data confidentiality	0.0% (0)	1.8% (1)	18.2% (10)	25.5% (14)	**54.5% (30)**	4.33	55
Data integrity	0.0% (0)	0.0% (0)	14.5% (8)	29.1% (16)	**56.4% (31)**	4.42	55
Communication security	0.0% (0)	0.0% (0)	9.1% (5)	32.7% (18)	**58.2% (32)**	4.49	55
Interface integrity	1.8% (1)	3.6% (2)	25.5% (14)	27.3% (15)	**41.8% (23)**	4.04	55
Compartmentalization	3.6% (2)	3.6% (2)	**34.5% (19)**	30.9% (17)	27.3% (15)	3.75	55
System availability	0.0% (0)	7.3% (4)	21.8% (12)	34.5% (19)	**36.4% (20)**	4.00	55
Resistance to DDOS	1.8% (1)	3.6% (2)	27.3% (15)	**40.0% (22)**	27.3% (15)	3.87	55
Resistance to Botnet activities	1.8% (1)	3.6% (2)	18.2% (10)	32.7% (18)	**43.6% (24)**	4.13	55
					answered question		**55**
					skipped question		**54**

29. Please rate the following attributes of metrics data on a scale of 1 to 5, where 5 is the highest indicator that metrics data which exhibits these attributes provides a good measure of security and 1 is the lowest or least significant indicator of metrics data that contributes to good security metrics.

	1	2	3	4	5	Rating Average	Response Count
Valid: data supports a hypothesis that system is secure	3.8% (2)	5.7% (3)	22.6% (12)	32.1% (17)	**35.8% (19)**	3.91	53
Accurate: data reflects the content of measurement as it was envisioned	1.9% (1)	1.9% (1)	13.2% (7)	**56.6% (30)**	26.4% (14)	4.04	53
Numeric: data can be precisely quantified	9.4% (5)	13.2% (7)	20.8% (11)	**37.7% (20)**	18.9% (10)	3.43	53
Verifiable: data can be verified to conform to a given syntax	1.9% (1)	7.5% (4)	26.4% (14)	**39.6% (21)**	24.5% (13)	3.77	53
Correct: data is collected according to specifications	3.8% (2)	3.8% (2)	30.2% (16)	26.4% (14)	**35.8% (19)**	3.87	53
Consistent: measure is independent of measurer	1.9% (1)	1.9% (1)	17.0% (9)	30.2% (16)	**49.1% (26)**	4.23	53
Time-based: there is a fixed reference point of data collection	1.9% (1)	13.2% (7)	24.5% (13)	**30.2% (16)**	**30.2% (16)**	3.74	53
Replicable: measurement repeated in same manner in same environment yields same result	1.9% (1)	3.8% (2)	24.5% (13)	24.5% (13)	**45.3% (24)**	4.08	53
Unit-based: data may be expressed in terms of a unit	7.5% (4)	17.0% (9)	22.6% (12)	**26.4% (14)**	**26.4% (14)**	3.47	53
Informative: data provides information without reference to a specific situation or incident	11.3% (6)	3.8% (2)	22.6% (12)	**35.8% (19)**	26.4% (14)	3.62	53
					answered question		**53**
					skipped question		**56**

30. Please rate the following attributes of metrics on a scale of 1 to 5, where 5 is the highest indicator that metrics which exhibit these attributes provide a valid measure of security and 1 is the lowest or least significant indicator of metrics that provide a valid measure of security.

	1	2	3	4	5	Rating Average	Response Count
easy to connect to concept of security	1.9% (1)	3.8% (2)	26.4% (14)	30.2% (16)	**37.7% (20)**	3.98	53
transparent data gathering process	1.9% (1)	7.5% (4)	32.1% (17)	**39.6% (21)**	18.9% (10)	3.66	53
supports security decision-making	1.9% (1)	1.9% (1)	11.3% (6)	28.3% (15)	**56.6% (30)**	4.36	53
mathematical modeling of security management processes	11.3% (6)	26.4% (14)	**43.4% (23)**	13.2% (7)	5.7% (3)	2.75	53
weighting network forensics evidence to increase probabilities of conviction	22.6% (12)	24.5% (13)	**32.1% (17)**	17.0% (9)	3.8% (2)	2.55	53
quantifies threat surface	9.4% (5)	5.7% (3)	**43.4% (23)**	26.4% (14)	15.1% (8)	3.32	53
usies game theory to determine security investment strategies	32.1% (17)	22.6% (12)	**34.0% (18)**	11.3% (6)	0.0% (0)	2.25	53
complex mathematical models for assessing software security	**37.7% (20)**	24.5% (13)	28.3% (15)	7.5% (4)	1.9% (1)	2.11	53
					answered question		**53**
					skipped question		**56**

31. The following standards have been used as a basis for security metrics. Please rate the extent to which you are familiar with each standard, on a scale of 1 to 5, where 5 indicates that you are very experienced with the standard and 1 indicates that you have never heard of the standard.

	1	2	3	4	5	Rating Average	Response Count
Common Criteria for Information Technology Security Evaluation	20.8% (11)	15.1% (8)	**34.0% (18)**	18.9% (10)	11.3% (6)	2.85	53
ISO 27001, 27002 on Security Management (heritage BS7799 and ISO17799)	13.2% (7)	7.5% (4)	24.5% (13)	22.6% (12)	**32.1% (17)**	3.53	53
National Vulnerability Database Common Vulnerability Enumerations (CVE)	11.3% (6)	9.4% (5)	28.3% (15)	**32.1% (17)**	18.9% (10)	3.38	53
National Vulnerability Database Common Weakness Enumerations (CWE, which includes OWASP top 25)	15.1% (8)	13.2% (7)	22.6% (12)	**24.5% (13)**	**24.5% (13)**	3.30	53
Payment Card Industry Data Security Standard (PCI DSS)	11.3% (6)	9.4% (5)	28.3% (15)	20.8% (11)	**30.2% (16)**	3.49	53
Recommended Security Controls for Federal Information Systems (NIST SP800-53)	11.3% (6)	13.2% (7)	**30.2% (16)**	**30.2% (16)**	15.1% (8)	3.25	53
Systems Security Engineering Capability Maturity Model®, Version 3.0, SSE-CMM®, 2003.	30.2% (16)	13.2% (7)	**32.1% (17)**	15.1% (8)	9.4% (5)	2.60	53
Technical Specification for the Security Content Automation Protocol (SCAP - NIST SP800-126)	**32.1% (17)**	20.8% (11)	30.2% (16)	9.4% (5)	7.5% (4)	2.40	53
ISACA Control Objectives for Information Technology (COBIT)	9.4% (5)	17.0% (9)	26.4% (14)	18.9% (10)	**28.3% (15)**	3.40	53
Trusted Computer System Evaluation Criteria (The Orange Book)	18.9% (10)	17.0% (9)	**24.5% (13)**	20.8% (11)	18.9% (10)	3.04	53
Underlying Technical Models for Information Technology Security (NIST SP800-33)	**32.1% (17)**	15.1% (8)	30.2% (16)	17.0% (9)	5.7% (3)	2.49	53

answered question	53
skipped question	56

32. The following standards have been used as a basis for security metrics. For each standard on the list for which you answered 2 or higher in the previous question, please rate its utility in providing good security metrics, on a scale of 1 to 5, where 5 indicates that metrics based on the standard provide a good measure of security and 1 indicates that metrics based on the standard do not provide any measurement of security.

	1	2	3	4	5	Rating Average	Response Count
Common Criteria for Information Technology Security Evaluation	22.6% (12)	24.5% (13)	**41.5% (22)**	9.4% (5)	1.9% (1)	2.43	53
ISO 27001, 27002 on Security Management (heritage BS7799 and ISO17799)	13.2% (7)	11.3% (6)	**34.0% (18)**	28.3% (15)	13.2% (7)	3.17	53
National Vulnerability Database Common Vulnerability Enumerations (CVE)	18.9% (10)	9.4% (5)	**37.7% (20)**	17.0% (9)	17.0% (9)	3.04	53
National Vulnerability Database Common Weakness Enumerations (CWE, which includes OWASP top 25)	18.9% (10)	11.3% (6)	**34.0% (18)**	17.0% (9)	18.9% (10)	3.06	53
Payment Card Industry Data Security Standard (PCI DSS)	11.3% (6)	15.1% (8)	**39.6% (21)**	24.5% (13)	9.4% (5)	3.06	53
Recommended Security Controls for Federal Information Systems (NIST SP800-53)	17.0% (9)	5.7% (3)	**45.3% (24)**	20.8% (11)	11.3% (6)	3.04	53
Systems Security Engineering Capability Maturity Model®, Version 3.0, SSE-CMM®, 2003.	**32.1% (17)**	15.1% (8)	**32.1% (17)**	18.9% (10)	1.9% (1)	2.43	53
Technical Specification for the Security Content Automation Protocol (SCAP - NIST SP800-126)	30.2% (16)	11.3% (6)	**34.0% (18)**	15.1% (8)	9.4% (5)	2.62	53
ISACA Control Objectives for Information Technology (COBIT)	7.5% (4)	13.2% (7)	**45.3% (24)**	18.9% (10)	15.1% (8)	3.21	53

Trusted Computer System Evaluation Criteria (The Orange Book)	26.4% (14)	15.1% (8)	**41.5% (22)**	13.2% (7)	3.8% (2)	2.53	53
Underlying Technical Models for Information Technology Security (NIST SP800-33)	34.0% (18)	9.4% (5)	**43.4% (23)**	13.2% (7)	0.0% (0)	2.36	53
					answered question		**53**
					skipped question		**56**

33. The National Institute of Standards and Technology has published Performance Measurement Guide for Information Security (NIST SP800-55, original 2003 updated 2008). Please select the response from the following drop-down list that most closely describes your experience with that document:

	Response Percent	Response Count
I am not familiar with NIST SP800-55	26.4%	14
I am familiar with NIST SP800-55 but I have not read it	18.9%	10
I have read NIST SP800-55 but I do not recall details	**32.1%**	**17**
I have read NIST SP800-55 and I agree with most of what it recommends	11.3%	6
I have read NIST SP800-55 and I do not agree with most of what it recommends	1.9%	1
I have read NIST SP 800-55, but neither agree nor disagree with what it recommends	5.7%	3
Please provide an explanation of your response, and/or comments on NIST SP800-55.	3.8%	2

Please provide an explanation of your response, and/or comments on NIST SP800-55.	15
answered question	**53**

skipped question	56

34. We ask you to identify yourself for three reasons: • Someone may one day want to verify the integrity of the data collected by this survey. • We may wish to interview you on the topic of your answers. • You might be interested in receiving a copy of the survey results. If you agree to be identified for the purposes of potential follow up questions, please provide your name, affiliation, and email address:

	Response Percent	Response Count
Name	100.0%	37
Affiliation	83.8%	31
Address	70.3%	26
City	73.0%	27
State	75.7%	28
Email	100.0%	37
answered question		37
skipped question		72

35. Please indicate whether you would be willing to be interviewed, or just to verify the results, check all that apply: If you would rather not be identified but would like to get a copy of the survey results, you may do so by registering at securitymetrics.org, as the results will be posted to that mail list.

	Response Percent	Response Count
Verify	48.8%	20
Interview	46.3%	19
Receive results	**90.2%**	**37**
	answered question	**41**
	skipped question	**68**

Page 1, Q1. Please use the following drop-down list to select your current field of employment:

1	Federal Research Contractor	May 18, 2011 1:52 PM
2	eCommerce	May 13, 2011 5:07 PM
3	Computer industry	Mar 23, 2011 12:45 PM
4	not for profit	Mar 22, 2011 4:28 PM
5	Consumer products	Mar 21, 2011 12:18 AM
6	Security Consulting	Mar 19, 2011 5:52 PM
7	Consultant	Feb 14, 2011 10:45 PM
8	Research institute	Feb 14, 2011 1:01 PM

Page 1, Q2. Please use the following drop-down list to select your current professional activity:		
1	Director of Research and Development	May 18, 2011 1:52 PM
2	Digital Forensic Analyst	May 16, 2011 10:36 AM
3	Forensic Analyst/Investigator	May 16, 2011 12:15 AM
4	security consultant	May 15, 2011 4:47 PM
5	Title is Director of Security and Compliance. Department of one. Have full range of tactical, operational, and strategic responsibilities; including architecture.	May 14, 2011 4:14 PM
6	Principal investigator, security R&D	May 13, 2011 9:29 AM
7	Applied Research	Mar 31, 2011 11:51 AM
8	Retired security consultant	Mar 20, 2011 9:51 PM
9	Researcher	Feb 14, 2011 1:01 PM
10	Product Manager for online banking security	Feb 14, 2011 9:54 AM

Page 1, Q3. and 4. If you selected 'Security Architect' in response to question 2, please answer questions 3 and 4. Otherwise, please select the 'NEXT' button below. 3. On roughly how many projects did you have security architecture responsibilities?		
1	6	May 14, 2011 8:50 PM
2	100	May 14, 2011 4:14 PM
3	3	May 13, 2011 1:40 PM
4	5	Apr 25, 2011 6:01 AM
5	10	Apr 22, 2011 8:39 AM
6	0	Apr 22, 2011 8:39 AM
7	5	Mar 21, 2011 2:01 PM
8	2	Mar 21, 2011 5:34 AM
9	2	Mar 19, 2011 5:03 PM
10	10	Mar 9, 2011 6:45 AM
11	20	Feb 14, 2011 10:45 PM
12	1	Feb 14, 2011 1:15 PM

Page 1, Q4. What was the budget of the largest one?		
1	1000000	May 14, 2011 8:50 PM
2	1000000	May 14, 2011 4:14 PM
3	1000000	May 13, 2011 1:40 PM
4	4000000	Apr 25, 2011 6:01 AM
5	40000000	Apr 22, 2011 8:39 AM
6	1500000	Mar 19, 2011 5:03 PM
7	2000000	Mar 9, 2011 6:45 AM
8	10000000	Feb 14, 2011 10:45 PM
9	100000	Feb 14, 2011 1:15 PM

Page 3, Q9. Please check all Professional Certifications you currently hold:		
1	EnCE, CEH, CHFI	May 16, 2011 10:42 AM
2	EnCE, SCERS, CEH	May 16, 2011 12:20 AM
3	MCSE	May 14, 2011 4:19 PM
4	cgeit, cpa	May 13, 2011 10:03 AM
5	CCM from AFP; AAP from NACHA	May 13, 2011 9:26 AM
6	CGEIT	May 13, 2011 9:23 AM
7	CGEIT	May 3, 2011 8:12 AM
8	CGEIT	Apr 27, 2011 6:50 PM
9	CSSLP	Apr 22, 2011 11:12 PM
10	In process of getting CISSP	Apr 22, 2011 9:14 AM
11	CGEIT	Apr 22, 2011 8:56 AM
12	CISSLP	Apr 22, 2011 8:55 AM
13	CSSLP from ISC2	Apr 14, 2011 7:26 AM
14	Other real qualifications e.g. C.Eng, C.Sci, FBCS	Mar 23, 2011 12:54 PM
15	CCM - NSA; CEE - NSA	Mar 21, 2011 8:37 AM
16	CIPP, CGEIT	Mar 21, 2011 12:20 AM
17	CSSLP - ISC2	Mar 20, 2011 7:45 PM
18	CRISC from ISACA, Professional Engineer - State of CA	Mar 19, 2011 10:10 PM
19	GCIH from SANS	Mar 19, 2011 7:04 PM
20	PMP from PMI	Mar 14, 2011 8:35 PM
21	Security+	Mar 10, 2011 11:49 PM
22	CGEIT	Mar 9, 2011 6:56 AM
23	Technical Diploma	Mar 9, 2011 6:48 AM
24	ITIL Foundation, FAIR Analyst	Feb 14, 2011 8:13 PM

Page 3, Q10. Which of these or other professional security associations are you a member or officer?		
1	IIA member	Jun 6, 2011 9:23 PM
2	ACM and IEEE	May 16, 2011 4:27 PM
3	Member IEEE, ACM	May 13, 2011 12:10 PM
4	LOMA CISO Council, currently chairman	May 13, 2011 10:05 AM
5	OWASP	Apr 25, 2011 6:36 AM
6	none	Apr 23, 2011 6:40 PM
7	FSSCC Financial Services Sector	Apr 1, 2011 8:29 AM
8	Center for Internet Security - Board	Mar 23, 2011 12:54 PM
9	InfraGard, former Board of Directors	Mar 22, 2011 9:25 AM
10	IAPP	Mar 21, 2011 12:20 AM
11	ISA, IEEE, CIGRE, NERC	Mar 19, 2011 10:10 PM
12	Gesellschaft für Informatik	Mar 10, 2011 11:49 PM
13	IEEE	Feb 14, 2011 10:47 PM

Page 3, Q12. Enter the number of years in security (if any):		
1	20	Jun 6, 2011 9:23 PM
2	15	Jun 2, 2011 6:21 AM
3	26	May 20, 2011 10:58 AM
4	10	May 18, 2011 1:54 PM
5	11	May 16, 2011 10:58 PM
6	12	May 16, 2011 4:27 PM
7	4	May 16, 2011 12:38 PM
8	4	May 16, 2011 10:42 AM
9	14	May 16, 2011 7:09 AM
10	2	May 16, 2011 1:10 AM
11	25	May 16, 2011 12:49 AM
12	2	May 16, 2011 12:20 AM
13	5	May 15, 2011 7:33 PM
14	20	May 15, 2011 6:12 PM
15	4	May 15, 2011 4:56 PM
16	30	May 15, 2011 1:17 PM
17	16	May 14, 2011 8:50 PM
18	14	May 14, 2011 4:19 PM
19	40	May 13, 2011 5:17 PM
20	4	May 13, 2011 1:43 PM
21	15	May 13, 2011 12:10 PM
22	8	May 13, 2011 10:05 AM
23	17	May 13, 2011 9:45 AM
24	19	May 13, 2011 9:31 AM
25	5	May 13, 2011 9:26 AM
26	12	May 13, 2011 9:23 AM
27	27	May 3, 2011 8:12 AM
28	20	Apr 27, 2011 6:50 PM
29	11	Apr 25, 2011 10:13 AM

Page 3, Q12. Enter the number of years in security (if any):		
30	20	Apr 25, 2011 8:34 AM
31	7	Apr 25, 2011 6:36 AM
32	10	Apr 25, 2011 6:03 AM
33	11	Apr 23, 2011 6:40 PM
34	25	Apr 23, 2011 4:38 AM
35	44	Apr 22, 2011 11:12 PM
36	30	Apr 22, 2011 9:16 AM
37	15	Apr 22, 2011 9:14 AM
38	21	Apr 22, 2011 8:56 AM
39	9	Apr 22, 2011 8:55 AM
40	19	Apr 22, 2011 8:44 AM
41	16	Apr 22, 2011 8:42 AM
42	20	Apr 22, 2011 8:41 AM
43	20	Apr 19, 2011 4:42 AM
44	6	Apr 18, 2011 5:34 PM
45	29	Apr 14, 2011 7:26 AM
46	25	Apr 7, 2011 1:23 PM
47	16	Apr 5, 2011 8:39 AM
48	7	Apr 3, 2011 10:31 AM
49	20	Apr 1, 2011 8:29 AM
50	14	Mar 27, 2011 4:22 AM
51	20	Mar 23, 2011 12:54 PM
52	27	Mar 22, 2011 4:30 PM
53	14	Mar 22, 2011 9:25 AM
54	12	Mar 21, 2011 2:23 PM
55	20	Mar 21, 2011 2:03 PM
56	30	Mar 21, 2011 11:38 AM
57	13	Mar 21, 2011 10:37 AM
58	43	Mar 21, 2011 8:37 AM

Page 3, Q12. Enter the number of years in security (if any):		
59	7	Mar 21, 2011 6:16 AM
60	13	Mar 21, 2011 6:00 AM
61	15	Mar 21, 2011 5:43 AM
62	13	Mar 21, 2011 12:20 AM
63	40	Mar 20, 2011 9:54 PM
64	16	Mar 20, 2011 7:45 PM
65	25	Mar 20, 2011 7:56 AM
66	11	Mar 19, 2011 10:10 PM
67	10	Mar 19, 2011 7:04 PM
68	11	Mar 19, 2011 6:45 PM
69	40	Mar 19, 2011 5:55 PM
70	10	Mar 19, 2011 5:04 PM
71	5	Mar 14, 2011 8:35 PM
72	13	Mar 11, 2011 11:31 AM
73	11	Mar 10, 2011 11:49 PM
74	10	Mar 10, 2011 7:24 AM
75	18	Mar 9, 2011 3:27 PM
76	10	Mar 9, 2011 6:56 AM
77	10	Mar 9, 2011 6:48 AM
78	19	Feb 22, 2011 3:55 PM
79	3	Feb 17, 2011 1:07 PM
80	19	Feb 15, 2011 9:46 AM
81	35	Feb 14, 2011 10:47 PM
82	20	Feb 14, 2011 8:13 PM
83	5	Feb 14, 2011 5:16 PM
84	4	Feb 14, 2011 1:17 PM
85	3	Feb 14, 2011 9:58 AM
86	10	Feb 14, 2011 8:33 AM

Page 3, Q13. Number of years in a technology-related field (if any):		
1	25	Jun 6, 2011 9:23 PM
2	15	Jun 2, 2011 6:21 AM
3	27	May 20, 2011 10:58 AM
4	12	May 18, 2011 1:54 PM
5	17	May 16, 2011 10:58 PM
6	15	May 16, 2011 4:27 PM
7	20	May 16, 2011 12:38 PM
8	10	May 16, 2011 10:42 AM
9	21	May 16, 2011 7:09 AM
10	2	May 16, 2011 1:10 AM
11	30	May 16, 2011 12:49 AM
12	8	May 16, 2011 12:20 AM
13	25	May 15, 2011 7:33 PM
14	30	May 15, 2011 6:12 PM
15	20	May 15, 2011 5:53 PM
16	10	May 15, 2011 4:56 PM
17	35	May 15, 2011 1:17 PM
18	19	May 14, 2011 8:50 PM
19	19	May 14, 2011 4:19 PM
20	30	May 13, 2011 5:17 PM
21	15	May 13, 2011 1:43 PM
22	40	May 13, 2011 12:10 PM
23	34	May 13, 2011 10:05 AM
24	20	May 13, 2011 10:03 AM
25	27	May 13, 2011 9:45 AM
26	19	May 13, 2011 9:31 AM
27	30	May 13, 2011 9:26 AM
28	20	May 13, 2011 9:23 AM
29	20	May 3, 2011 8:12 AM

Page 3, Q13. Number of years in a technology-related field (if any):		
30	25	Apr 27, 2011 6:50 PM
31	26	Apr 25, 2011 10:13 AM
32	30	Apr 25, 2011 8:34 AM
33	16	Apr 25, 2011 6:36 AM
34	15	Apr 25, 2011 6:03 AM
35	20	Apr 23, 2011 6:40 PM
36	40	Apr 23, 2011 4:38 AM
37	25	Apr 22, 2011 11:12 PM
38	30	Apr 22, 2011 9:16 AM
39	29	Apr 22, 2011 9:14 AM
40	24	Apr 22, 2011 8:56 AM
41	24	Apr 22, 2011 8:55 AM
42	20	Apr 22, 2011 8:44 AM
43	30	Apr 22, 2011 8:42 AM
44	25	Apr 22, 2011 8:41 AM
45	24	Apr 19, 2011 4:42 AM
46	25	Apr 18, 2011 5:34 PM
47	1	Apr 14, 2011 7:26 AM
48	45	Apr 7, 2011 1:23 PM
49	11	Apr 5, 2011 8:39 AM
50	12	Apr 3, 2011 10:31 AM
51	22	Apr 1, 2011 8:29 AM
52	20	Mar 27, 2011 4:22 AM
53	25	Mar 23, 2011 12:54 PM
54	18	Mar 22, 2011 9:25 AM
55	35	Mar 21, 2011 2:23 PM
56	40	Mar 21, 2011 2:03 PM
57	10	Mar 21, 2011 11:38 AM
58	16	Mar 21, 2011 10:37 AM

Page 3, Q13. Number of years in a technology-related field (if any):		
59	45	Mar 21, 2011 8:37 AM
60	13	Mar 21, 2011 6:16 AM
61	21	Mar 21, 2011 6:00 AM
62	23	Mar 21, 2011 5:43 AM
63	56	Mar 20, 2011 9:54 PM
64	37	Mar 20, 2011 7:45 PM
65	37	Mar 20, 2011 7:56 AM
66	40	Mar 20, 2011 6:35 AM
67	39	Mar 19, 2011 10:10 PM
68	12	Mar 19, 2011 7:04 PM
69	11	Mar 19, 2011 6:45 PM
70	50	Mar 19, 2011 5:55 PM
71	20	Mar 19, 2011 5:04 PM
72	15	Mar 14, 2011 8:35 PM
73	13	Mar 11, 2011 11:31 AM
74	16	Mar 10, 2011 11:49 PM
75	20	Mar 10, 2011 7:24 AM
76	35	Mar 9, 2011 3:27 PM
77	25	Mar 9, 2011 6:56 AM
78	20	Mar 9, 2011 6:48 AM
79	20	Feb 22, 2011 3:55 PM
80	10	Feb 17, 2011 1:07 PM
81	14	Feb 15, 2011 9:46 AM
82	35	Feb 14, 2011 10:47 PM
83	20	Feb 14, 2011 8:13 PM
84	15	Feb 14, 2011 5:16 PM
85	5	Feb 14, 2011 1:17 PM
86	7	Feb 14, 2011 9:58 AM
87	17	Feb 14, 2011 8:33 AM

Page 3, Q14. Enter the total number of years of work experience:		
1	21	Jun 6, 2011 9:23 PM
2	30	Jun 2, 2011 6:21 AM
3	27	May 20, 2011 10:58 AM
4	16	May 18, 2011 1:54 PM
5	20	May 16, 2011 10:58 PM
6	15	May 16, 2011 4:27 PM
7	20	May 16, 2011 12:38 PM
8	14	May 16, 2011 10:42 AM
9	21	May 16, 2011 7:09 AM
10	2	May 16, 2011 1:10 AM
11	30	May 16, 2011 12:49 AM
12	10	May 16, 2011 12:20 AM
13	25	May 15, 2011 7:33 PM
14	30	May 15, 2011 6:12 PM
15	48	May 15, 2011 5:53 PM
16	10	May 15, 2011 4:56 PM
17	2	May 15, 2011 4:53 PM
18	35	May 15, 2011 1:17 PM
19	19	May 14, 2011 8:50 PM
20	19	May 14, 2011 4:19 PM
21	50	May 13, 2011 5:17 PM
22	18	May 13, 2011 1:43 PM
23	40	May 13, 2011 12:10 PM
24	34	May 13, 2011 10:05 AM
25	28	May 13, 2011 10:03 AM
26	33	May 13, 2011 9:45 AM
27	28	May 13, 2011 9:31 AM
28	35	May 13, 2011 9:26 AM
29	28	May 13, 2011 9:23 AM

Page 3, Q14. Enter the total number of years of work experience:		
30	32	May 3, 2011 8:12 AM
31	25	Apr 27, 2011 6:50 PM
32	26	Apr 25, 2011 10:13 AM
33	30	Apr 25, 2011 8:34 AM
34	19	Apr 25, 2011 6:36 AM
35	15	Apr 25, 2011 6:03 AM
36	20	Apr 23, 2011 6:40 PM
37	40	Apr 23, 2011 4:38 AM
38	46	Apr 22, 2011 11:12 PM
39	15	Apr 22, 2011 9:24 AM
40	30	Apr 22, 2011 9:16 AM
41	29	Apr 22, 2011 9:14 AM
42	24	Apr 22, 2011 8:56 AM
43	26	Apr 22, 2011 8:55 AM
44	20	Apr 22, 2011 8:44 AM
45	30	Apr 22, 2011 8:42 AM
46	25	Apr 22, 2011 8:41 AM
47	24	Apr 19, 2011 4:42 AM
48	25	Apr 18, 2011 5:34 PM
49	30	Apr 14, 2011 7:26 AM
50	45	Apr 7, 2011 1:23 PM
51	29	Apr 5, 2011 8:39 AM
52	12	Apr 3, 2011 10:31 AM
53	22	Apr 1, 2011 8:29 AM
54	15	Mar 27, 2011 4:22 AM
55	25	Mar 23, 2011 12:54 PM
56	30	Mar 22, 2011 4:30 PM
57	18	Mar 22, 2011 9:25 AM
58	38	Mar 21, 2011 2:23 PM

Page 3, Q14. Enter the total number of years of work experience:		
59	40	Mar 21, 2011 2:03 PM
60	40	Mar 21, 2011 11:38 AM
61	16	Mar 21, 2011 10:37 AM
62	45	Mar 21, 2011 8:37 AM
63	13	Mar 21, 2011 6:16 AM
64	21	Mar 21, 2011 6:00 AM
65	23	Mar 21, 2011 5:43 AM
66	18	Mar 21, 2011 12:20 AM
67	60	Mar 20, 2011 9:54 PM
68	43	Mar 20, 2011 7:45 PM
69	37	Mar 20, 2011 7:56 AM
70	40	Mar 20, 2011 6:35 AM
71	39	Mar 19, 2011 10:10 PM
72	12	Mar 19, 2011 7:04 PM
73	11	Mar 19, 2011 6:45 PM
74	55	Mar 19, 2011 5:55 PM
75	20	Mar 19, 2011 5:04 PM
76	22	Mar 14, 2011 8:35 PM
77	18	Mar 11, 2011 11:31 AM
78	16	Mar 10, 2011 11:49 PM
79	20	Mar 10, 2011 7:24 AM
80	39	Mar 9, 2011 3:27 PM
81	25	Mar 9, 2011 6:56 AM
82	20	Mar 9, 2011 6:48 AM
83	20	Feb 22, 2011 3:55 PM
84	18	Feb 17, 2011 1:07 PM
85	19	Feb 15, 2011 9:46 AM
86	35	Feb 14, 2011 10:47 PM
87	40	Feb 14, 2011 8:13 PM

Page 3, Q14. Enter the total number of years of work experience:		
88	15	Feb 14, 2011 5:16 PM
89	7	Feb 14, 2011 1:17 PM
90	0	Feb 14, 2011 9:58 AM
91	17	Feb 14, 2011 8:33 AM

Page 3, Q15. If you have current responsibilities with respect to security architecture, how would you describe them (please check all that apply and add any significant others):		
1	R&D, Education	May 15, 2011 1:17 PM
2	AS CISO, Security Architecture reports to me...	May 13, 2011 5:17 PM
3	Build	May 13, 2011 1:43 PM
4	Project sponsor and business owner	May 13, 2011 10:05 AM
5	M&A due diligence, Vendor/Customer due diligence	Apr 25, 2011 6:36 AM
6	Help the Infrastructure and Application Development/Operate teams to understand corporate and Industry control requirements and policies, and provide recommendations to ensure compliance with these policies and standards.	Apr 23, 2011 6:40 PM
7	Research	Apr 7, 2011 1:23 PM
8	Represent firm in FS Sector Critical Infrastructure Forums	Apr 1, 2011 8:29 AM
9	Project management.	Feb 17, 2011 1:07 PM

Page 4, Q16. Please provide your definitions of the word "measurement," the word "metrics," and the phrase "security metrics" in general, without reference to security, by completing the following sentences:

The word "measurement" means:

1	The data that results from measuring something	Jun 6, 2011 9:57 PM
2	A count of arbitrary units. For example, "Alice is 4'2" tall" is a measurement.	May 21, 2011 10:16 AM
3	numeric assessment	May 20, 2011 10:59 AM
4	A means of determining the size or amount of an item	May 18, 2011 1:57 PM
5	a unit or system of measurement	May 16, 2011 10:59 PM
6	To assess something against an established standard.	May 16, 2011 12:41 PM
7	Single point in time view of a security factor. This is objective and based on raw data.	May 16, 2011 11:03 AM
8	Quantification of state.	May 16, 2011 7:11 AM
9	Quantifying something	May 16, 2011 12:24 AM
10	Both the operation of qualitatively assessing some measurable value, and the result of that assessment.	May 15, 2011 6:17 PM
11	Observing something - counts of events, rates, ...	May 15, 2011 5:57 PM
12	a number or amount obtained from measuring physical, informational, or other processes	May 15, 2011 1:26 PM
13	the process or the result of determining the magnitude of a quantity,	May 14, 2011 8:52 PM
14	The act of measuring.	May 13, 2011 5:43 PM
15	The process of comparing an entity or occurance to a given standard	May 13, 2011 1:49 PM
16	the act of determining or assessing specific characteristics of an object, entity, system or process	May 13, 2011 12:18 PM
17	a quantitative or qualitative attribute to allow comparisons among like things	May 13, 2011 10:17 AM
18	quantication	May 13, 2011 10:05 AM
19	generally a quantifiable assessment of a characteristic	May 13, 2011 10:03 AM
20	Identify control weakness, adherence to regulatory requirements, allow management to monitor individual key performance indicators, demonstrate the continuing value of Information Security and bring transparency to the organization's technology risk posture and the state of information security in the organization.	May 13, 2011 9:54 AM
21	Collecting feedback to determine if policy goals are achieved.	May 13, 2011 9:50 AM
22	Defining a quantity in terms of units.	May 13, 2011 9:34 AM

Page 4, Q16. Please provide your definitions of the word "measurement," the word "metrics," and the phrase "security metrics" in general, without reference to security, by completing the following sentences:

The word "measurement" means:

23	relative to a standard unit of measurement	May 3, 2011 8:23 AM
24	Quantification.	Apr 27, 2011 6:51 PM
25	ascertain size	Apr 25, 2011 10:33 AM
26	the ability to instrument a process	Apr 25, 2011 8:37 AM
27	repeatable objective method of determining the quantity of an object or group of objects at a given point in time	Apr 25, 2011 7:18 AM
28	I default to Hubbard's definition, something like an observable quantity that reduces uncertainty	Apr 25, 2011 6:08 AM
29	amount or size obtained by comparing it to some standard or etalon	Apr 23, 2011 7:18 PM
30	applying a scale to an unknown	Apr 23, 2011 4:41 AM
31	A number that reflects activity based on data with which is collected.	Apr 22, 2011 11:18 PM
32	Extent, quantiity or size	Apr 22, 2011 9:34 AM
33	The quantification of some item's characteristics	Apr 22, 2011 9:25 AM
34	application of a discrete numerical representation of an attribute or characteristic of something	Apr 22, 2011 9:21 AM
35	Map from empirical world to formal, relational world.	Apr 22, 2011 9:00 AM
36	to measure	Apr 22, 2011 8:59 AM
37	a value to describe quantity	Apr 19, 2011 4:47 AM
38	The capture or generation of a value associated with a metric.	Apr 18, 2011 5:41 PM
39	repeatable observations	Apr 14, 2011 7:31 AM
40	Observations of a system or phenomonon that are quantified in a manner that is useful to a community of people with concerns related to the system or phenomenon	Apr 7, 2011 1:53 PM
41	The action of measuring something	Apr 5, 2011 9:14 AM
42	The extent, quantity, amount, or degree of something, as determined by standard	Apr 4, 2011 6:24 AM
43	A set of observations that reduce uncertainty where the result is expressed as a quantity	Apr 1, 2011 9:13 AM
44	A means to assist the organization make informed decisions about the design of systems, selection of controls, and efficiency of security operations	Mar 28, 2011 8:17 AM

Page 4, Q16. Please provide your definitions of the word "measurement," the word "metrics," and the phrase "security metrics" in general, without reference to security, by completing the following sentences:

The word "measurement" means:

45	A scientific count of some factor in comparison to a baseline.	Mar 27, 2011 4:30 AM
46	Objectively quantify.	Mar 23, 2011 12:55 PM
47	determination of the size or extent of something	Mar 22, 2011 4:37 PM
48	Quantification of one or more traits such that they can be tracked, compared, normalized, baselined, etc.	Mar 22, 2011 9:34 AM
49	the process or the result of a process to determine a specific attribute (quantity or quality) of something using a defined standard of measure	Mar 22, 2011 7:05 AM
50	obtaining a quantitative number or defined unambigious, repeatable qualitative term	Mar 21, 2011 2:07 PM
51	The ability to determine a meaning relationship between reality and imagination.	Mar 21, 2011 8:41 AM
52	An objective quantitative value associated with an observation.	Mar 21, 2011 6:18 AM
53	determining the size of something relative to an agreed and acceptable, repeatable, verifiable unit.	Mar 21, 2011 6:03 AM
54	Quantitative depiction.	Mar 21, 2011 12:22 AM
55	specification	Mar 20, 2011 9:56 PM
56	The ability and tools used to collect information about a process	Mar 20, 2011 7:58 PM
57	Establishing a specific, verifiable quantity of something.	Mar 20, 2011 8:13 AM
58	statistic (number or descriptive term such as high, medium, low) used to represent the relative size of something in relation to an established scale or unit of measure	Mar 20, 2011 7:06 AM
59	making an objective observation.	Mar 19, 2011 10:13 PM
60	The method to determine a quantity or magnitude.	Mar 19, 2011 7:15 PM
61	The act or result of measuring.	Mar 19, 2011 6:01 PM
62	n/a	Mar 19, 2011 5:06 PM
63	to compare something to a known standard	Mar 11, 2011 11:39 AM
64	the process of gathering meaningful data about a process or technology in an effort to determine its state, health, etc.	Mar 10, 2011 7:35 AM
65	a point in time representation of the value, size etc of some concept/item	Mar 9, 2011 3:43 PM
66	*	Mar 9, 2011 2:18 PM

Page 4, Q16. Please provide your definitions of the word "measurement," the word "metrics," and the phrase "security metrics" in general, without reference to security, by completing the following sentences:

The word "measurement" means:

67	Being able to numerically determine a value or quantity of something	Mar 9, 2011 6:59 AM
68	Measurement theory incorporates the scale of nominal, ordinal, interval, ratio, and absolute. These scales are used to measure something, with the output being data. In essence, it is something you know.	Feb 15, 2011 9:50 AM
69	the result of an act of measuring	Feb 14, 2011 10:49 PM
70	A measurement is something that "ascertains the dimensions, quantity, or capacity" of something - an object, a process - anything, really. Measurements have at least these three qualities: validity, reproducibility, appropriate level of detail	Feb 14, 2011 8:23 PM
71	Measuring a process using UCL or LCL (or targets, goals and thresholds)	Feb 14, 2011 5:17 PM

Page 4, Q17. The word “metrics” means:		
1	A unit of measure	Jun 6, 2011 9:57 PM
2	The comparison of one or more measurements for the purpose of drawing a conclusion. For example, Alice is 4'2" tall compared to an average height of 5'6" tall allows us to conclude that Alice is short.	May 21, 2011 10:16 AM
3	scale for numeric assessment	May 20, 2011 10:59 AM
4	The general comparison of sizes / amounts of multiple related items	May 18, 2011 1:57 PM
5	a method of measuring something	May 16, 2011 10:59 PM
6	Bullet points in an established standard to be used as guidelines for measurement.	May 16, 2011 12:41 PM
7	Comparing two or more security measurements over time and comparing them to a known standard. This is subjective to sine extent as it involves analysis of a series of measurements.	May 16, 2011 11:03 AM
8	Set of measurements meaningful to tracking success/failure of an activity.	May 16, 2011 7:11 AM
9	The specific units of measurement used to quantify something	May 16, 2011 12:24 AM
10	A set of measurements applied over a domain, such as time, space, or other variable basis.	May 15, 2011 6:17 PM
11	A formally defined analysis of typically a series of measurements - often compared to a standard.	May 15, 2011 5:57 PM
12	recording and analyzing measurements, usually with an eye towards determining system norms or progress towards a goal	May 15, 2011 1:26 PM
13	measure of an organization's activities and performance.	May 14, 2011 8:52 PM
14	the art of measurement	May 13, 2011 5:43 PM
15	a predefined measurement that is usually repeated over time to show how a given process or item is performing (usually over time).	May 13, 2011 1:49 PM
16	the results of measurement exercises	May 13, 2011 12:18 PM
17	quantitative or qualitative grouping or ranking - what you get after you correlate your measurements	May 13, 2011 10:17 AM
18	statistics used to monitor something	May 13, 2011 10:05 AM
19	the dimensions or attributes used to measure	May 13, 2011 10:03 AM
20	Meaningful and balanced measurements aligned with business goals and objective to identify and measure the effectiveness of controls against some meaningful criteria.	May 13, 2011 9:54 AM
21	A discrete and measurable parameter	May 13, 2011 9:50 AM

Page 4, Q17. The word "metrics" means:		
22	Measure of performance	May 13, 2011 9:34 AM
23	relative to a defined set of atributes	May 3, 2011 8:23 AM
24	Measurements.	Apr 27, 2011 6:51 PM
25	measurement of performance or progress	Apr 25, 2011 10:33 AM
26	a set of key processes and systems states to measure	Apr 25, 2011 8:37 AM
27	(my definition for business metric) - measurement of performance	Apr 25, 2011 7:18 AM
28	intuitively I'd say a measurement or set of measurements that provide feedback on previous decisions and therefor inform future decisions	Apr 25, 2011 6:08 AM
29	number of units of specific standard	Apr 23, 2011 7:18 PM
30	an agreed-upon scale	Apr 23, 2011 4:41 AM
31	Metrics is a measurement through which one can take actions based on the data collected that can cause change.	Apr 22, 2011 11:18 PM
32	Quantifiable measurement	Apr 22, 2011 9:34 AM
33	The definition of what is being measured, including the characteristic and the unit of measure	Apr 22, 2011 9:25 AM
34	methodology for measuring and tracking changes in the attributes or characteristics of something	Apr 22, 2011 9:21 AM
35	Measurements used for decision-making.	Apr 22, 2011 9:00 AM
36	results of measuring	Apr 22, 2011 8:59 AM
37	measures of a number of variables to discern information about a system	Apr 19, 2011 4:47 AM
38	A dimension of analysis used to quantify and understand performance of a thing or an activity	Apr 18, 2011 5:41 PM
39	repeatable measurements expressed as numeric values	Apr 14, 2011 7:31 AM
40	A means for converting a set of measurements into a quantity related to criteria that are helpful in decision-making regarding a system or phenomenon.	Apr 7, 2011 1:53 PM
41	Standards of measurement by which efficiency, performance, progress, or quality of a plan, process, or product can be assessed.	Apr 5, 2011 9:14 AM
42	measure scientifically and methodically	Apr 4, 2011 6:24 AM
43	Metrics describe a system of measurement that includes the item being measured, the unit of measurement, and the value of the unit	Apr 1, 2011 9:13 AM
44	Quantifiable measurement	Mar 28, 2011 8:17 AM

Page 4, Q17. The word "metrics" means:		
45	A measure statistic	Mar 27, 2011 4:30 AM
46	A time series of measurement instances.	Mar 23, 2011 12:55 PM
47	the definition what is being measured	Mar 22, 2011 4:37 PM
48	A set of measurements as defined above that together help manage some business process/purpose	Mar 22, 2011 9:34 AM
49	A measure to assess performance using an agreed-upon standard	Mar 22, 2011 7:05 AM
50	define in measurable terms	Mar 21, 2011 2:07 PM
51	The ability to quantify what specific items you are trying to measure in a quantitative or qualitative manner.	Mar 21, 2011 8:41 AM
52	Comparing a measurement against a baseline or trend.	Mar 21, 2011 6:18 AM
53	a set of properties	Mar 21, 2011 6:03 AM
54	Collection of measurements to assist in making management decisions.	Mar 21, 2011 12:22 AM
55	measuring	Mar 20, 2011 9:56 PM
56	Meaningful information that gives insight into how a process is internally operating	Mar 20, 2011 7:58 PM
57	The set of objective, verifiable, repeatable relationships between quantities (larger vs smaller) as opposed to non-quantifiable relationships (better vs. worse).	Mar 20, 2011 8:13 AM
58	use of statistics to inform, educate and clarify useful information about subjects or items of interest in relation to a field of interest	Mar 20, 2011 7:06 AM
59	measurable properties	Mar 19, 2011 10:13 PM
60	A standard measurement.	Mar 19, 2011 7:15 PM
61	The standard by/against which one measures.	Mar 19, 2011 6:01 PM
62	n/a	Mar 19, 2011 5:06 PM
63	the rationalization of a lot measurements	Mar 11, 2011 11:39 AM
64	a unit of measurement deemed meaningful that used to provide feedback on a process or technology.	Mar 10, 2011 7:35 AM
65	A collection of measurements over thime that allow comparison and identification of patterns, changes or outliers	Mar 9, 2011 3:43 PM
66	*	Mar 9, 2011 2:18 PM
67	Metrics are a collection of measurements	Mar 9, 2011 6:59 AM

Page 4, Q17. The word "metrics" means:		
68	Metrics however are about analysis and intelligent decision making. Metrics translate data into meaningful information which will support decision making. Information is something you use to make decisions.	Feb 15, 2011 9:50 AM
69	A set of mechanisms used for measurement	Feb 14, 2011 10:49 PM
70	Could mean the same as measurements. Or could be a specific set or collection of measurements designed or conceived to provide information about an object or a process	Feb 14, 2011 8:23 PM
71	Key Performance Indicators	Feb 14, 2011 5:17 PM

Page 4, Q18. The phrase "security metrics" means:		
1	A measuring system that reflects something related to the achievement of security goals	Jun 6, 2011 9:57 PM
2	A metric that allows one to draw a conclusion of some sort related to security.	May 21, 2011 10:16 AM
3	scale for measuring some protecion element	May 20, 2011 10:59 AM
4	Measurement of the security posture of a system, organization, etc.	May 18, 2011 1:57 PM
5	Metrics based on IT security performance goals and objectives	May 16, 2011 10:59 PM
6	Hybrid of metrics used as guidelines for assessing the baseline best practices with regards to preventing unauthorized access or asset loss.	May 16, 2011 12:41 PM
7	Analyzing measurements of security factors, such as those expressed in the McCumber Cube, and comparing system goals to actual outcomes/reality.	May 16, 2011 11:03 AM
8	Set of measurements meaningful to tracking level of provided security.	May 16, 2011 7:11 AM
9	Aspects of security used to quantify something in the field	May 16, 2011 12:24 AM
10	Metrics associated with security, such as costs or incidents per some period.	May 15, 2011 6:17 PM
11	Metrics applicable to IT security.	May 15, 2011 5:57 PM
12	metrics applied to security features such as confidentiality integrity and availability, or to security strategies for prevention, detection, and response	May 15, 2011 1:26 PM
13	measure of an organization's activities and performance around infosec	May 14, 2011 8:52 PM
14	measurements of security risk and effectiveness	May 13, 2011 5:43 PM
15	a predefined measurement that is usually repeated over time to show how a given security process, or tool is performing (usually over time).	May 13, 2011 1:49 PM
16	the results of measurement exercises that are related to physical and/or logical security	May 13, 2011 12:18 PM
17	applying grouping or ranking to information management practices to assess and improve maturity of practices	May 13, 2011 10:17 AM
18	security related statistics	May 13, 2011 10:05 AM
19	the set of attributes or security practices used to determine how secure something is. Often used in conjunction with an overarching framework like ISO 27002.	May 13, 2011 10:03 AM
20	Meaningful and balanced measures that bring/improve transparency of the organization's security posture, program / assurance / compliance / technology risk that are continuously re-evaluated and rebalanced to ensure effectiveness of risk identification and mitigation.	May 13, 2011 9:54 AM
21	Measurable feedback system related to established security goals.	May 13, 2011 9:50 AM
22	Measure of performance around protecting unauthorized or unintended use of systems.	May 13, 2011 9:34 AM

Page 4, Q18. The phrase “security metrics” means:		
23	those atributes/metrics that demonstrate the efficacy of security controls	May 3, 2011 8:23 AM
24	A migraine.	Apr 27, 2011 6:51 PM
25	measurement of performance, progress, or effectiveness of a variety of security controls or remedial activities	Apr 25, 2011 10:33 AM
26	the key security processses and systems states to measure	Apr 25, 2011 8:37 AM
27	measurement of performance or state in one aspect of security (CIA - or Hexad implied)	Apr 25, 2011 7:18 AM
28	metrics for information security	Apr 25, 2011 6:08 AM
29	threat levels	Apr 23, 2011 7:18 PM
30	decision support	Apr 23, 2011 4:41 AM
31	Metrics that are used to improve the security posture and risk.	Apr 22, 2011 11:18 PM
32	Overall program objectives and measurements	Apr 22, 2011 9:34 AM
33	Once the term "security" is defined, measuring how "secure" something is against some scale	Apr 22, 2011 9:25 AM
34	measuring and tracking changes in security posture.	Apr 22, 2011 9:21 AM
35	Metrics used to make security-related decisions.	Apr 22, 2011 9:00 AM
36	measures specific to security	Apr 22, 2011 8:59 AM
37	measures of values to discern information about the security posture of a system	Apr 19, 2011 4:47 AM
38	Those dimensions of analysis dealing with risk and vulnerability, and also efforts both preventative and reactive to mitigate consequences of exploits.	Apr 18, 2011 5:41 PM
39	repeatable security measurements expressed as numeric values	Apr 14, 2011 7:31 AM
40	A means for converting a set of measurements related to the assurance that a computer-based system can in some manner be disrupted, into a quantity related to criteria that are helpful in decision-making regarding that system.	Apr 7, 2011 1:53 PM
41	Standards of measurement by which efficiency, performance, progress, or quality of a security plan, process, or product can be assessed.	Apr 5, 2011 9:14 AM
42	Methodically measure the security posture of a define system or a set of systems.	Apr 4, 2011 6:24 AM
43	Security metrics are a series of key measurements that help quantify the amount of risk that exists in a given envrionment/situation	Apr 1, 2011 9:13 AM
44	Provide quantitative and objective basis for security operations	Mar 28, 2011 8:17 AM
45	A measure related to an aspect of security performance	Mar 27, 2011 4:30 AM
46	Metrics defined by each entities security program.	Mar 23, 2011 12:55 PM

Page 4, Q18. The phrase "security metrics" means:		
47	The definition of security measures	Mar 22, 2011 4:37 PM
48	A set of metrics as defined above that deal with security/risk/loss related aspects of a business process	Mar 22, 2011 9:34 AM
49	measurs to assess the performance or effectiveness of a security control or process	Mar 22, 2011 7:05 AM
50	define some aspect of security or security investment in measurable terms	Mar 21, 2011 2:07 PM
51	The ability to quantitative or qualitative present a true picture of the security posture of an organization to a variety of responsible parties.	Mar 21, 2011 8:41 AM
52	Comparing the effectiveness of security controls against an established goal in order to assess risk posture.	Mar 21, 2011 6:18 AM
53	whatever you want it to be	Mar 21, 2011 6:03 AM
54	Collection of measurements to assist in making management decisions related to security.	Mar 21, 2011 12:22 AM
55	mesuring security	Mar 20, 2011 9:56 PM
56	Meaningful information that gives insight into how security processes are internally operating	Mar 20, 2011 7:58 PM
57	A set of quantifiable relationships between measurable security attributes.	Mar 20, 2011 8:13 AM
58	use of statistics about security topics and conditions such as threats, security incidents, perpetrators, and controls	Mar 20, 2011 7:06 AM
59	measurable properties relevant to securing systems. In this case, industrial control systems.	Mar 19, 2011 10:13 PM
60	Standard measurements used to determine ranges of security.	Mar 19, 2011 7:15 PM
61	The standards by which one evaluates the state of or improvement in security.	Mar 19, 2011 6:01 PM
62	n/a	Mar 19, 2011 5:06 PM
63	metrics that directly or indirectly tie back to measurements of which there are security implications	Mar 11, 2011 11:39 AM
64	metrics that provides meaningful feedback on a security process or technology.	Mar 10, 2011 7:35 AM
65	applying the use of metrics to the security domain. representing activity, posture, evolution and variability	Mar 9, 2011 3:43 PM
66	*	Mar 9, 2011 2:18 PM
67	Security metrics are security related measurements that assist in highlighting a posture or position	Mar 9, 2011 6:59 AM
68	Security metrics are the meaningful measurements and metrics which support security decisions.	Feb 15, 2011 9:50 AM

Page 4, Q18. The phrase “security metrics” means:		
69	a set of mechanisms used for measuring security-related things	Feb 14, 2011 10:49 PM
70	Metrics that provide measurements about an aspect of security, or, more specifically in this context, information and IT security	Feb 14, 2011 8:23 PM
71	Measuring the success of Security Programs	Feb 14, 2011 5:17 PM

Page 4, Q19. In your opinion, are the best security metrics (please choose from the following drop-down list):		
1	The data set and desired conclusion dictate scale type, not the analyst's choice of favorites.	May 21, 2011 10:16 AM
2	It really depends on what specific factors of security are being measured. Some factors are best expressed in nominal metrics, and some in ordinal, interval or as ratios.	May 16, 2011 11:03 AM
3	The best metrics are domain- and availabiity-dependent.	May 15, 2011 1:26 PM
4	All are valid - just depends on what is trying to be shown.	May 13, 2011 1:49 PM
5	metrics incorporating value and uncertainty	May 13, 2011 12:18 PM
6	I do not think I can pick a "best"	May 13, 2011 10:17 AM
7	This question appears to be at the heart of your survey and I don't expect that you are getting meaningful responses. To do so, you should give the definitions you are using and examples.	May 13, 2011 10:03 AM
8	All those types have value depending on what you are trying to communicate/measure.	May 13, 2011 9:54 AM
9	Combination	May 13, 2011 9:50 AM
10	Security metrics can be expressed in several ways.	Apr 25, 2011 10:33 AM
11	It depends on the metrics, both ordinals and percentages / ratios a good methodologies depending on the specific metric	Apr 25, 2011 8:37 AM
12	those that have business correlation, and can be collected analyzed and communicated to support decisions (I assume your context implies that this capability exists, but in truth most organizations struggle reaching a minimal level of maturity) Your question brought to mind a similar question: "What is the best language?" My response to that has always been similar to the one above. Those with the ability to communicate in multiple languages have strong oppinions in this area, but if you ask a laguage professor they will often slap their foreheads and wish that their students knew how to communicate in any language. (My 2 cents from the soapbox)	Apr 25, 2011 7:18 AM
13	security metrics - should uniquely designed in each case based on some standard methods	Apr 23, 2011 7:18 PM
14	Nominal and actual	Apr 22, 2011 9:34 AM
15	Are of these metrics could be used to either measure specific activities or show how the certain attribues have changed over time.	Apr 22, 2011 9:21 AM
16	The best security metrics are key performance indicators that are defined by process owners used to determine the health of business processes with imbedded controls. The KPIs can be divided into implementation KPIs that represent work effort to implement controls and "run the business" KPIs that represents on-going processes.	Apr 22, 2011 8:59 AM

Page 4, Q19. In your opinion, are the best security metrics (please choose from the following drop-down list):		
17	Other. All can be useful. For example, for categorizing attack types, nominal is useful. For relating risk levels, ordinal can be useful. For evaluating security outcomes, such as number of attacks resulting in financial losses exceeding a specific value, interval can be useful. For evaluating the level of human effort that is spent on SW patching in a company from year to year, ratio can be useful.	Apr 7, 2011 1:53 PM
18	security Metrics should be used as transitory - they are not true representation of performance or status, but more a convenient means to define targets, benchmarks, status for the temporary time they remain relevant and are not gamed	Mar 27, 2011 4:30 AM
19	Depends on the context, the metric and the ultimate use.	Mar 23, 2011 12:55 PM
20	"It Depends": different numeric representations are appropriate for expressing and communicating different concepts. Ratios are extremely useful and well understood in many business contexts (by non-security and non-technical folk), but are often misused (intentionally and unintentionally). Ordinal scales are easy to understand and if used correctly can convey an enormous amount of information in a very compact format (i.e. a Class 1 Cleanroom) if the science is sufficiently mature to have such constructs (i.e. not information security!).	Mar 22, 2011 9:34 AM
21	It depends. I can foresee cases where each of these terms would be appropriate depending on what is being measured and how. Ordinal for how many repeat issues I have identified in a risk assessment. Ratio, for percentage of devices that are in compliance with control standards. Interval, the number of malicious packets detected per unit of time...	Mar 22, 2011 7:05 AM
22	I'm not sure that there is such a thing as a security metric.	Mar 20, 2011 8:13 AM
23	Ordinal is useful in some instances where perception is wanted (ie: asking for opinion on a scale of 1-5) but cardinal (actual count) seems most useful in IT Security (ie: # of intrusions by type; cost to remediate versus severity of threat, etc,	Mar 20, 2011 7:06 AM
24	I do not yet believe they exist for industrial control systems	Mar 19, 2011 10:13 PM
25	visualisations	Mar 19, 2011 5:06 PM
26	interesting question. I would error on the side of ratio but it depends on the purpose of the metric and what it is composed of.	Mar 11, 2011 11:39 AM
27	you need a combination of some, even all, of the above. It will depend on which aspect of security you are attempting to assess measurements from	Mar 9, 2011 3:43 PM
28	All the traditional scale measurement types are applicable in some manner. The key is to use them where they serve the necessary purpose (in support of making good decisions)	Feb 15, 2011 9:50 AM
29	As of today,m these are the best available in most cases.	Feb 14, 2011 10:49 PM

Page 4, Q20. Please explain the reasoning behind your answer to Question 19:		
1	In my work in the IT Controls Benchmarking work that spanned over 1000+ organizations, we were able to use units of measures using ratios, and there was a zero point. E.g., change success rate. But many of the metrics were Intervals e.g., Likert style questions about the perceived value and culture.	Jun 6, 2011 9:57 PM
2	For example, I'm currently using the following metrics in my work: Nominal - From a vulnerabiltiy scan, perform root cause analysis to determine _why_ the vuln was present. Categories include: "Base build design," "bad build execution," "bad configuration management," "bad patch management," and several others. By comparing the counts, we can draw conclusions about which root cause is the most important to address next. Ordinal - But, we might want to weight our nominal counts above based on the High/Medium/Low risk ranking of the vulnerabilities. Though, this becomes a problematic technique precisely because the values are ordinal and we seem to be attempting to use them as interval or ratio scale types. Interval - I might also want to track degree of deviation from a baseline (i.e. how far from the desired configuration is my current configuration) Ratio - and, if I'm ever compromised, how many consumers will I have to purchase identity monitoring for? There certainly is a problematic out there for scale types in security metrics. Mainly the issue is that most plausible risk measurements require the use of one or more metrics where the data only supports a nominal or ordinal data set but we're trying to perform analysis that can only be done with interval or ratio scale types. Unfortunately, you 'can't get there from here' without breaking some analytical rules.	May 21, 2011 10:16 AM
3	Based on operational experiences	May 20, 2011 10:59 AM
4	It's easier to explain a ratio to higher level management.	May 18, 2011 1:57 PM
5	My degree is in business, with another year in computer science courses, but not a lot of math.	May 16, 2011 10:59 PM
6	I am not familiar with the application of 'ordinal' and 'ratio' in the context of security metrics.	May 16, 2011 12:41 PM
7	I know you probably want a more detailed response, but I don't think any one level of measurement is optimal over the others for every security factor.	May 16, 2011 11:03 AM
8	Unfamiliar terms.	May 16, 2011 7:11 AM
9	I don't know	May 16, 2011 12:24 AM
10	I haven't run into those terms in a context that applies here.	May 15, 2011 6:17 PM
11	I'm familiar with "analytics", but not specifically in the security field - and don't recognize those terms.	May 15, 2011 5:57 PM
12	We dislike comparing apples and oranges, but at the same time cannot in the real world distill our measurements down to a common number (such as $). We use what we can gather, then focus on specific project domains where the measurements can still make some useful sense.	May 15, 2011 1:26 PM
13	??	May 14, 2011 8:52 PM

Page 4, Q20. Please explain the reasoning behind your answer to Question 19:		
14	security metrics should reflect risk - particularly residual risk and where possible be measured in dollars so they are most relevant to the business.	May 13, 2011 5:43 PM
15	I think metrics should be flexible to drive behavior in a desired direction. It doesn't so much matter what clothing you dress your data in - it matters that they are accurate enough to show where you are now and the direction you have come.	May 13, 2011 1:49 PM
16	Pure numeric metrics omit value and uncertainty characteristics that are important for decision making. Even ratios are not helpful unless put into an appropriate context expressed as value measures. Value measures are seldom precise so should be expressed in the form of probability distributions.	May 13, 2011 12:18 PM
17	My use of metrics is not particularly mature or consistent. I rely a great deal on the judgement and consensus of SMEs.	May 13, 2011 10:17 AM
18	these are unfamiliar to me	May 13, 2011 10:05 AM
19	see above	May 13, 2011 10:03 AM
20	All the types of metrics have value depending on what variables you are trying to measure and analyse. Patch status for example lends itself to be a ratio metric because you are trying to measure an absolute status. Some metrics require significant amounts of historical data to become meaningful. Nominal metrics, such as heat maps, are used to present high level status data in a visually easy to interpret form. So all metric types are valid depending on the data set and the analytical/audience objective.	May 13, 2011 9:54 AM
21	Depends on nature/purpose of measurement: compliance, comparison to external, comparison to past performance. I prefer nominal (binary) for Compliance issues. For comparative measurements with external models I prefer ordinal. For continuous improvement I prefer ratios, using prior performance as the non-arbitrary zero point.	May 13, 2011 9:50 AM
22	terms unfamiliar.	May 13, 2011 9:34 AM
23	It is all relative. There is no absolute in security.	May 3, 2011 8:23 AM
24	It's complicated.	Apr 27, 2011 6:51 PM
25	Not sure if there are "Best" security metrics. I think the best security metrics are "meaningful" security metrics within the context of the environment or organization.	Apr 25, 2011 10:33 AM
26	practical experience	Apr 25, 2011 8:37 AM

Page 4, Q20. Please explain the reasoning behind your answer to Question 19:		
27	(I assume your context implies that this capability exists, but in truth most organizations struggle reaching a minimal level of maturity) Your question brought to mind a similar question: "What is the best language?" My response to that has always been similar to the one above. Those with the ability to communicate in multiple languages have strong oppinions in this area, but if you ask a laguage professor they will often slap their foreheads and wish that their students knew how to communicate in any language. (My 2 cents from the soapbox)	Apr 25, 2011 7:18 AM
28	provides the most statistical manipulations and maps more to reality than others.	Apr 25, 2011 6:08 AM
29	personal experience	Apr 23, 2011 7:18 PM
30	nothing is stable enough to develop an actuarial tail	Apr 23, 2011 4:41 AM
31	I am not familiar with these terms in this context	Apr 22, 2011 11:18 PM
32	Need to set expectations and measure against achieving them.	Apr 22, 2011 9:34 AM
33	We don't have a number scale for measuring "security" so that rules out Interval and Ratio. But security can be relative (machine A is more secure than machine B based on measurements X and Y). Nominal makes no sense here.	Apr 22, 2011 9:25 AM
34	We may measure specific events, specific attributes or characteristics, specific changes in attributes over time or measurement one attribute with respect to another. Thus, all of the techniques have a place in the metrics behind security.	Apr 22, 2011 9:21 AM
35	The more quantitative, the more exact, the more useful in comparisons and trade-off decisions.	Apr 22, 2011 9:00 AM
36	Metrics are numbers and output- a broad definition. the best security metrics are measures of process health where controls are part of those processes	Apr 22, 2011 8:59 AM
37	Ordinal values based against historical trends to show increasing or decreasing values.	Apr 19, 2011 4:47 AM
38	I relied on Jennifer to answer these questions. LoL!	Apr 18, 2011 5:41 PM
39	Most security issues are best represented in a relative manner instead of absolutes, specific targets, or qualitative statements.	Apr 14, 2011 7:31 AM
40	The "best" metric depends on the questions being asked regarding assurance and the value of assurance, and the best questions are dependent on the issues under evaluation and their relationship to overall system objectives .	Apr 7, 2011 1:53 PM
41	Not sure most technology or security executives understand those terms - could just mean I'm a dork!	Apr 5, 2011 9:14 AM
42	N/A	Apr 4, 2011 6:24 AM
43	Includes an absolute zero point and allows more effective comparison of relative risk values	Apr 1, 2011 9:13 AM

Page 4, Q20. Please explain the reasoning behind your answer to Question 19:		
44	We use metrics to show progression (or lack there of) over time.	Mar 28, 2011 8:17 AM
45	Like all metrics they become gamed unless reality is more difficult to achieve than the metric itself.	Mar 27, 2011 4:30 AM
46	Self explanatory.	Mar 23, 2011 12:55 PM
47	You benefit more from something that at least can be put into an order and not just named	Mar 22, 2011 4:37 PM
48	It's in the Other box.	Mar 22, 2011 9:34 AM
49	See response to 19	Mar 22, 2011 7:05 AM
50	best to measure in relative ranges as it is hard to nail down an absolute for security	Mar 21, 2011 2:07 PM
51	Try to show the good, bad and ugly side of things. Draw from history to show the bad side and tie it to cost and then deterministically show the present posture or potential for future if things are put into place.	Mar 21, 2011 8:41 AM
52	Ratio determines how close you are above/below the goal.	Mar 21, 2011 6:18 AM
53	It is a relatively new and unscientific field.	Mar 21, 2011 6:03 AM
54	We may use different terminology to explain the same things.	Mar 21, 2011 12:22 AM
55	Minimal valid data	Mar 20, 2011 9:56 PM
56	To have the ability to see how information is related to processing steps or rework steps tells us how well controlled a process is operating. Proportions of information that is constantly changing state (e.g. percentage of exceptions coming up for expiry) tells us how the processing related to closing exceptions is operating or not operating as intended.	Mar 20, 2011 7:58 PM
57	Security is an epiphenoninon, a second-order effect of a business process as implemented in a cultural context. As such it is difficult to define repeatable, comparable, quantifiable objective measures of security.	Mar 20, 2011 8:13 AM
58	personal preference when reading statistics in security research	Mar 20, 2011 7:06 AM
59	Relevant metrics unique to control system cyber security have not been established	Mar 19, 2011 10:13 PM
60	It allows for an absolute zero which allows for meaningful interpretation.	Mar 19, 2011 7:15 PM
61	Pass	Mar 19, 2011 6:01 PM
62	aggregation of security metrics is impossible	Mar 19, 2011 5:06 PM
63	e.g. a metric (or indicator) could be something like the amount of risk one has assumed. a ratio is probably a better value to present (ratio of assumed to total, or ration of assumed to establish limits..etc).	Mar 11, 2011 11:39 AM

Page 4, Q20. Please explain the reasoning behind your answer to Question 19:		
64	I do not have a formal background in metrics development	Mar 10, 2011 7:35 AM
65	Some things in security are "countable" but others are only qualitatively assessable.	Mar 9, 2011 3:43 PM
66	*	Mar 9, 2011 2:18 PM
67	They need to be numerical in order to prevent any dispute	Mar 9, 2011 6:59 AM
68	All the traditional scale measurement types are applicable in some manner. The key is to use them where they serve the necessary purpose (in support of making good decisions)	Feb 15, 2011 9:50 AM
69	As of today,m these are the best available in most cases.	Feb 14, 2011 10:49 PM
70	ratio, or cardinal numbers can be manipulated in legitimate ways by arithmetic and statistics. Nominaland ordinal values can only be counted; performing other arithmetic operations on ordinal values is problematic.	Feb 14, 2011 8:23 PM
71	N/A	Feb 14, 2011 5:17 PM

Page 5, Q21. Please rate the following list of activities on a scale from 0 to 5, where the number indicates the contribution of the activity to an organization's ability to maintain its security. Each activity must be assigned its own number, but the number can be zero:

1	I'm assuming that zero means "zero contribution" and 5 means "max contribution"	Jun 6, 2011 10:01 PM
2	Jennifer - a note here. The answers to these questions vary depending on the organization. So, I chose my current org to use as a case study since I think what you are really interested in here is the differential between architect and management.	May 21, 2011 10:16 AM
3	Establish priority of security relative to other business functions.	May 16, 2011 7:17 AM
4	Support from the top. Effective enforcement of policy and standards.	May 13, 2011 12:23 PM
5	Quantify, as used above does not necessarily mean to assign a numeric value, rather, it means to be ale to "reason" about the value. Something can be recognized as critical to an organization without assigning a specific dollar value.	May 13, 2011 10:08 AM
6	analyze data from internal and external sources to understand user behavioral patterns to identify anomalies for trending analysis, new control requirements, incident response and forensic analysis.	Apr 22, 2011 9:19 AM
7	Question 21 was answered to indicate our ability/position to track metrics against each line item, not as a representation of our security health.	Mar 28, 2011 8:32 AM
8	Working with the vendors to understand what they feel is baseline security and what peers are doing to make security a reality. Operational security is significanlty different at times from theoretical. You need to implement and sometimes policy does not match reality.	Mar 21, 2011 8:48 AM
9	Segregation of duties	Mar 20, 2011 10:07 PM
10	Expert IT security staff with expert knowledge of systems, infrastructure, architecture, vendors, and the ability to influence, control, or better yet prevent anything that impacts on security.	Mar 20, 2011 7:59 AM
11	Assignment of duties and responsibility, supervision, variance detection (including incident detection), timely corrective action and remediation, safe defaults,	Mar 19, 2011 6:16 PM
12	Apply and maintain a fluid defense-in-depth strategy across the organization with the goal being 'optimal' security.	Feb 15, 2011 9:56 AM
13	The questions have different answers for different situations	Feb 14, 2011 10:52 PM

Page 5, Q22. Please answer this question from the perspective of the highest level of management in your organization (e.g. CEO or President), as you perceive them to think about security. That is, how would your management rate, on a scale of 1 to 5, where 5 is the highest indicator that an organization whi...		
1	The CEO doesn't care. He hired me to do this for him and provide the security assurance the business needs. He wouldn't understand the implications of half of this. Just expects me to cost effectively assure security for our businesses.	May 13, 2011 5:58 PM
2	Protect company reputation. That is what (my) execs really care about from InfoSec.	May 13, 2011 10:25 AM
3	Ability to "pass" audit	Apr 25, 2011 7:25 AM
4	IT Security expertise, diligence and reliability on the part of employees given responsibility for security	Mar 20, 2011 7:59 AM
5	Express enterprise risk tolerance, assign responsibility for asset protection, require timely measurement and reporting.	Mar 19, 2011 6:16 PM
6	Different for different situations	Feb 14, 2011 10:52 PM

Page 6, Q23. Please select the sentence fragments that complete the stem sentence and make it true (select all that apply): System security verification requires		
1	...qualification of system assets, ...qualification of system threat environment, ...qualification of impact of system vulnerability exploit. (Quantification is not practicable in our real world.)	May 15, 2011 1:34 PM
2	I'm not comfortable with the use of "quantification" in the above. Probability for example is notoriously hard to assign.	May 13, 2011 10:32 AM
3	see previous comment about quantification - need enough information to "reason" about each topic	May 13, 2011 10:11 AM
4	An assessment of how the integrated security components combine to defend against, discover or respond to attacks.	Apr 7, 2011 2:06 PM
5	some verification technique (need not be cost-effective) nor the assets, threats, and vulnerabilities quantified although that would give best results for presentation /communication purposes	Mar 20, 2011 9:10 AM

Page 6, Q24. Please rate the following system abilities on a scale of 1 to 5, where 5 is the highest indicator that a system which exhibits these attributes is secure and 1 is the lowest or least significant indicator that the system exhibits security.		
1	Threat modeling based external security assessment. Audit is this game where you define control objectives, controls, evidence sets, and check things off a list. Security is a different game where an adversary tries to defeat, in the most generic sense, your creativity. That's why you need the assessment to include external threat modeling (i.e. the creativity of other experts applied to your problem) which audit does, in theory, perfectly but, in practice, at best, poorly.	May 21, 2011 10:24 AM
2	We need to continue our mission while under attack, including partially successful attacks. This goes further than SLAs to include unwritten and assumptive mission needs.	May 15, 2011 1:34 PM
3	Assumption is that abilities applie to system confidentiality and integrity and not to availablility.	May 13, 2011 12:29 PM
4	Withstand targeted penetration attacks by skilled attack teams that are similar to expected threat actors: 5	Mar 22, 2011 9:41 AM
5	these generally do not apply to industrial control system cyber security	Mar 19, 2011 10:18 PM
6	Provide reliable control over and relative ease in demonstrating the behavior, use, and content of the system.	Mar 19, 2011 6:25 PM
7	The question is a poor one since the term "security" is poorly defined.	Feb 14, 2011 10:54 PM

Page 7, Q25. Please rate the following types of measurement on a scale of 1 to 5, where 5 is the highest indicator that a measurement of the given type is useful in measuring system security and 1 is the lowest or least significant indicator that measurement of the given type is useful in measuring system sec...		
1	Please disregard score for "other" I had to check something to get the comment box. With regard to "performance" I assume you mean performance of security controls, not transaction throughput which may or may not be relevant.	May 21, 2011 10:39 AM
2	System security compared to what?	May 13, 2011 12:35 PM
3	Completeness of expected inventory vs. reality.	Mar 23, 2011 1:01 PM
4	I believe you need to know what the security, auditability and control basis and features that are part of a system to make an eduacated judgement call... What is the package including compensating controls that can be applied.	Mar 21, 2011 8:53 AM
5	metrics demonstrating most threats are routinely thwarted and anomolies are caught in system security set of controls as well as forward looking controls to handle zero day and other threats that can be anticipated but may not have occurred yet (not all orgs can support this but this is my ideal)	Mar 20, 2011 9:25 AM
6	Time to variance detection and corrective action.	Mar 19, 2011 6:32 PM

Page 7, Q26. Please rate following system characteristics on a scale of 1 to 5, where 5 is the highest indicator that system security requirements should be easy to identify and gather, and 1 is the lowest or least significant indicator that system security requirements should be easy to identify and gather.		
1	Please disregard score for "other" I had to check something to get the comment box. Having seen your presentation at MMC, I know that the last two go to your thesis - which I'm not necessairilly a fan of (you've set up your problematic differently than I would have). But, with regard to this question, the first three are of one type and the last two are of another. They can't be compared this way. If I really want to know if a system is secure, I need to look at its inputs and outputs. To the degree that a system is comprised of other systems (i.e. COTS or functional components) then those become systems with their own I/O. At best these describe scope. In terms of measurement, one would use the concepts of the last two (i.e. I/O) to measure the first three and the first three are descriptive scopes by which you could compare between dispirate systems.	May 21, 2011 10:39 AM
2	Need to have set of best-of-breed, well-proven requirements rather than "commonly used" since the latter don't seem to be working.	May 13, 2011 12:35 PM
3	The environment requires easy to understand system documentation from inception to production with security being an identifiable component at all levels. As much detail as is needed to fully describe security related elements/functions is required and development phases are reviewed and accepted or rejected based on completeness and ease of understanding.	Mar 20, 2011 9:25 AM
4	Audit trail fixes accountability for all significant events.	Mar 19, 2011 6:32 PM

Page 9, Q33. The National Institute of Standards and Technology has published Performance Measurement Guide for Information Security (NIST SP800-55, original 2003 updated 2008). Please select the response from the following drop-down list that most closely describes your experience with that document:		
1	I remember studying NIST 800-55, but could not readily differentiate it from the COBIT framework, so didn't refer to it afterwards. I thought it was valid, but remember thinking it needed more discussion of the context of which info sec operates in (e.g, appdev, IT operations, etc.)	Jun 6, 2011 10:17 PM
2	It is an approach. Certainly a practicioner who implemented it or portions of it would be far ahead of a practicioner that didn't and certainly, for example within the enormous community of federal departments and agencies, using a common standard, rather than rolling one's own, makes sense. But, in practice, I'll probably roll my own metrics based on what I'm trying to accomplish most of the time and I will only look to use a standard like this if I need to compare myself to others and if that comparison will be useful (i.e. they are my peers) and if the data exists where I can get to it. As for question 32, I couldn't proceed without checking something for the standards that I don't know well. So, on all of the ones where I checked "1" in question 31, I also checked "1" in 32. These responses should be translated into null.	May 21, 2011 10:59 AM
3	Seems like a good model, especially the way it develops foundation of management and builds metrics and quantifiable practices on top of this foundation.	May 16, 2011 11:40 AM
4	Not particularly applicable to an agile ecommerce environment	May 13, 2011 6:09 PM
5	SP800-55 categories are useful, but is too overly reliant on percentage measurements.	May 13, 2011 5:54 PM
6	I'm familiar with a number of the NIST SP 800 series and might refer to them from time-to-time, but do not look to them on a regular basis. Nor, do I think, do most infosec practitioners. You hardly eve see them referenced in conferences or in the commonly-used popular infosec press. I think that there is a general perception in the corporate world that NIST publications apply to government, not the private sector.	May 13, 2011 12:51 PM
7	I'm not familiar with this standard	Apr 23, 2011 7:43 PM
8	It's one approach	Apr 22, 2011 11:54 AM
9	It's been quite a few years since I read through it.	Apr 22, 2011 9:57 AM
10	It describe how to go about thinking about metrics in an educational manner.	Apr 22, 2011 9:13 AM
11	I have no reason in using this guide as part of my research, so while I read the guide for general value, I have no basis for sustaining detailed recollections regarding what was presented.	Apr 7, 2011 3:24 PM
12	I believe it needs a serious update in light of the world of mobile and idevices...	Mar 21, 2011 9:00 AM
13	I agree in part but what good is it to measure how many mobile devices use encryption when answers are not captured by sensitivity level /criticality of data? I prefer specific operational statistics to tell the security story rather than adherence to standards. For example: penetrations that result in sec incidents by root cause and severity /cost trended to show actual increase or decrease over time with mitigation/recovery costs also presented.	Mar 20, 2011 11:56 AM

Page 9, Q33. The National Institute of Standards and Technology has published Performance Measurement Guide for Information Security (NIST SP800-55, original 2003 updated 2008). Please select the response from the following drop-down list that most closely describes your experience with that document:		
14	Pass	Mar 19, 2011 6:40 PM
15	n/a	Mar 19, 2011 5:12 PM

THE REMAINDER OF THE SURVEY CONTAINED CONTACT INFORMATION
WHICH HAS BEEN DELETED FROM THIS DOCUMENT.

Appendix E – Group Independence Tests

This appendix includes the results of independence tests for the financial industry segment of the survey participants. These include Mann-Whitney and Kolmogorov-Smirnov tests, as well as the cross-tabulation results for the question on penetration studies.

Mann-Whitney Test Results

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The distribution of Q21-1-Mission is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.776	Retain the null hypothesis.
2	The distribution of Q21-2-Certif is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.425	Retain the null hypothesis.
3	The distribution of Q21-3-Standards is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.455	Retain the null hypothesis.
4	The distribution of Q21-4-Risk is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.277	Retain the null hypothesis.
5	The distribution of Q21-5-Infrast is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.157	Retain the null hypothesis.
6	The distribution of Q21-6-Features is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.875	Retain the null hypothesis.
7	The distribution of Q21-7-Acquisition is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.386	Retain the null hypothesis.
8	The distribution of Q21-8-Awareness is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.268	Retain the null hypothesis.
9	The distribution of Q21-9-SWChange is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.083	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
10	The distribution of Q21-10-Recover is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.330	Retain the null hypothesis.
11	The distribution of Q21-11-Incident is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.383	Retain the null hypothesis.
12	The distribution of Q21-12-VendorOver is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.671	Retain the null hypothesis.
13	The distribution of Q21-13-Media is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.068	Retain the null hypothesis.
14	The distribution of Q21-14-PhysEnv is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.455	Retain the null hypothesis.
15	The distribution of Q21-15-Personnel is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.913	Retain the null hypothesis.
16	The distribution of Q21-16-SWIntegrity is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.809	Retain the null hypothesis.
17	The distribution of Q21-17-Interface is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.719	Retain the null hypothesis.
18	The distribution of Q21-18-Segregate is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.336	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
19	The distribution of Q21-19-AuditTrails is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.672	Retain the null hypothesis.
20	The distribution of Q21-20-IDAuth is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.382	Retain the null hypothesis.
21	The distribution of Q21-21-TechCfg is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.282	Retain the null hypothesis.
22	The distribution of Q21-22-AssetValue is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.761	Retain the null hypothesis.
23	The distribution of Q21-23-ThreatProb is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.551	Retain the null hypothesis.
24	The distribution of Q21-24-DamageProb is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.612	Retain the null hypothesis.
25	The distribution of Q21-25-ThreatProtProb is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.956	Retain the null hypothesis.
26	The distribution of Q24-1-RegAudit is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.441	Retain the null hypothesis.
27	The distribution of Q24-2-SecAudit is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	1.000	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
28	The distribution of Q24-3-PassSecRev is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.279	Retain the null hypothesis.
29	The distribution of Q24-4-PassPenTest is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.008	Reject the null hypothesis.
30	The distribution of Q24-5-Deliver is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.571	Retain the null hypothesis.
31	The distribution of Q24-6-Provenance is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.403	Retain the null hypothesis.
32	The distribution of Q24-7-Interfaces is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.446	Retain the null hypothesis.
33	The distribution of Q24-8-FailSafe is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.949	Retain the null hypothesis.
34	The distribution of Q25-1-Resources is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.883	Retain the null hypothesis.
35	The distribution of Q25-2-Config is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.963	Retain the null hypothesis.
36	The distribution of Q25-3-Mgmt is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.431	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
37	The distribution of Q25-4-Logs is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.168	Retain the null hypothesis.
38	The distribution of Q25-5-BCP is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.735	Retain the null hypothesis.
39	The distribution of Q25-6-Perform is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.339	Retain the null hypothesis.
40	The distribution of Q26-1-IndepComp is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.913	Retain the null hypothesis.
41	The distribution of Q26-2-Pattern is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.707	Retain the null hypothesis.
42	The distribution of Q26-3-COTS is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.527	Retain the null hypothesis.
43	The distribution of Q26-4-ValInput is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.947	Retain the null hypothesis.
44	The distribution of Q26-5-DefOutput is the same across categories of Q1-3-Group.	Independent-Samples Mann-Whitney U Test	.586	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Kolmogorov-Smirnov Test Results

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The distribution of Q21-1-Mission is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	1.000	Retain the null hypothesis.
2	The distribution of Q21-2-Certif is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.398	Retain the null hypothesis.
3	The distribution of Q21-3-Standards is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.978	Retain the null hypothesis.
4	The distribution of Q21-4-Risk is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.944	Retain the null hypothesis.
5	The distribution of Q21-5-Infrast is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.819	Retain the null hypothesis.
6	The distribution of Q21-6-Features is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.736	Retain the null hypothesis.
7	The distribution of Q21-7-Acquisition is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.819	Retain the null hypothesis.
8	The distribution of Q21-8-Awareness is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.819	Retain the null hypothesis.
9	The distribution of Q21-9-SWChange is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.560	Retain the null hypothesis.
10	The distribution of Q21-10-Recovery is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.736	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
11	The distribution of Q21-11-Incident is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.978	Retain the null hypothesis.
12	The distribution of Q21-12-VendorOver is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.476	Retain the null hypothesis.
13	The distribution of Q21-13-Media is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.329	Retain the null hypothesis.
14	The distribution of Q21-14-PhysEnv is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.890	Retain the null hypothesis.
15	The distribution of Q21-15-Personnel is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.994	Retain the null hypothesis.
16	The distribution of Q21-16-SWIntegrity is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	1.000	Retain the null hypothesis.
17	The distribution of Q21-17-Interfaces is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	1.000	Retain the null hypothesis.
18	The distribution of Q21-18-Segregate is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.944	Retain the null hypothesis.
19	The distribution of Q21-19-AuditTrails is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.856	Retain the null hypothesis.
20	The distribution of Q21-20-IDAuth is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.978	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
21	The distribution of Q21-21-TechCfg is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.648	Retain the null hypothesis.
22	The distribution of Q21-22-AssetValue is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.944	Retain the null hypothesis.
23	The distribution of Q21-23-ThreatProb is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.944	Retain the null hypothesis.
24	The distribution of Q21-24-DamageProb is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.648	Retain the null hypothesis.
25	The distribution of Q21-25-ThreatProtProb is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	1.000	Retain the null hypothesis.
26	The distribution of Q24-1-RegAudit is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.956	Retain the null hypothesis.
27	The distribution of Q24-2-SecAudit is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	1.000	Retain the null hypothesis.
28	The distribution of Q24-3-PassSecRev is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.956	Retain the null hypothesis.
29	The distribution of Q24-4-PassPenTest is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.069	Retain the null hypothesis.
30	The distribution of Q24-5-Deliver is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.999	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
31	The distribution of Q24-6-Provenance is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.804	Retain the null hypothesis.
32	The distribution of Q24-7-Interfaces is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.998	Retain the null hypothesis.
33	The distribution of Q24-8-FailSafe is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.953	Retain the null hypothesis.
34	The distribution of Q25-1-Resources is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.966	Retain the null hypothesis.
35	The distribution of Q25-2-Config is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	1.000	Retain the null hypothesis.
36	The distribution of Q25-3-Mgmt is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.995	Retain the null hypothesis.
37	The distribution of Q25-4-Logs is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.966	Retain the null hypothesis.
38	The distribution of Q25-5-BCP is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	1.000	Retain the null hypothesis.
39	The distribution of Q25-6-Perform is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.611	Retain the null hypothesis.
40	The distribution of Q26-1-IndepComp is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.982	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
41	The distribution of Q26-2-Pattern is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.992	Retain the null hypothesis.
42	The distribution of Q26-3-COTS is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.987	Retain the null hypothesis.
43	The distribution of Q26-4-ValInput is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	1.000	Retain the null hypothesis.
44	The distribution of Q26-5-DefOutput is the same across categories of Q1-3-Group.	Independent-Samples Kolmogorov-Smirnov Test	.987	Retain the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

Penetration Question Cross-tabulation

			Q24-4-PassPenTest					
			1	2	3	4	5	Total
Non-FI	1	Count	0	0	2	6	15	23
		%	.0%	.0%	8.7%	26.1%	65.2%	100.0%
FI	2	Count	1	4	4	16	11	36
		%	2.8%	11.1%	11.1%	44.4%	30.6%	100.0%
Total		Count	1	4	6	22	26	59
		%	1.7%	6.8%	10.2%	37.3%	44.1%	100.0%

Appendix F - Descriptive statistics for all security attributes

Red italic and underlined font indicates that distribution is either Flat or Normal, and so attributes were removed from further study.

Descriptive Statistics

	N	Mean	Std. Dev.	Var.	Skewness		Kurtosis	
	Stat	Stat	Stat	Stat	Stat	Std. Error	Stat	Std. Error
Q21-1-Mission	60	3.73	1.326	1.758	-.661	.309	-.720	.608
Q21-2-Certif	60	3.15	1.351	1.825	-.325	.309	-.511	.608
Q21-3-Standards	60	3.28	1.303	1.698	-.694	.309	.274	.608
Q21-4-Risk	60	3.80	1.022	1.044	-1.061	.309	1.962	.608
Q21-5-Infrast	60	3.63	1.164	1.355	-1.035	.309	.949	.608
Q21-6-Features	60	3.50	1.172	1.373	-.687	.309	.433	.608
Q21-7-Acquisition	60	3.52	1.157	1.339	-.517	.309	.094	.608
Q21-8-Awareness	60	3.85	1.219	1.486	-.923	.309	.377	.608
Q21-9-SWChange	60	3.55	1.281	1.642	-.940	.309	.949	.608
Q21-10-Recovery	60	3.67	1.271	1.616	-1.182	.309	1.478	.608
Q21-11-Incident	60	3.95	1.281	1.642	-1.454	.309	1.860	.608
Q21-12-VendorOver	60	3.28	1.106	1.223	-.437	.309	-.350	.608
Q21-13-Media	60	3.25	1.457	2.123	-.623	.309	-.512	.608
Q21-14-PhysEnv	60	3.48	1.420	2.017	-.700	.309	-.317	.608
Q21-15-Personnel	60	3.52	1.396	1.949	-.770	.309	-.207	.608
Q21-16-SWIntegrity	60	3.52	1.214	1.474	-.745	.309	.542	.608
Q21-17-Interfaces	60	3.62	1.303	1.698	-.907	.309	.121	.608
Q21-18-Segregate	60	3.55	1.268	1.608	-.839	.309	.194	.608
Q21-19-AuditTrails	59	3.56	1.236	1.527	-.680	.311	-.110	.613
Q21-20-IDAuth	60	4.33	1.100	1.209	-2.447	.309	6.868	.608
Q21-21-TechCfg	60	3.15	1.287	1.655	-.833	.309	.393	.608
Q21-22-AssetValue	60	3.40	1.238	1.532	-.539	.309	-.305	.608
Q21-23-ThreatProb	*60*	*3.03*	*1.402*	*1.965*	*-.252*	*.309*	*-.532*	*.608*
Q21-24-DamageProb	*60*	*3.43*	*1.226*	*1.504*	*-.268*	*.309*	*-.480*	*.608*
Q21-25-ThreatProtProb	60	3.85	1.132	1.282	-.782	.309	-.238	.608
Q24-1-RegAudit	59	2.59	1.288	1.659	.413	.311	-.708	.613
Q24-2-SecAudit	59	3.42	1.086	1.179	-.508	.311	-.121	.613
Q24-3-PassSecRev	59	3.59	1.116	1.245	-.435	.311	-.332	.613
Q24-4-PassPenTest	59	4.15	.979	.959	-1.229	.311	1.176	.613
Q24-5-Deliver	*59*	*3.22*	*1.115*	*1.244*	*-.300*	*.311*	*-.759*	*.613*
Q24-6-Provenance	*59*	*2.86*	*1.042*	*1.085*	*.185*	*.311*	*.014*	*.613*
Q24-7-Interfaces	59	3.27	1.187	1.408	-.359	.311	-.595	.613
Q24-8-FailSafe	59	2.69	1.355	1.836	.410	.311	-.974	.613

Q25-1-Resources	54	2.39	1.172	1.374	.351	.325	-.841	.639
Q25-2-Config	54	3.44	1.058	1.119	-.494	.325	-.503	.639
Q25-3-Mgmt	54	3.50	1.042	1.085	-.312	.325	-.281	.639
Q25-4-Logs	54	3.70	.983	.967	-.722	.325	.596	.639
Q25-5-BCP	54	3.63	.917	.841	-.399	.325	.136	.639
Q25-6-Perform	*54*	*3.48*	*1.112*	*1.235*	*-.208*	*.325*	*-1.016*	*.639*
Q26-1-IndepComp	*54*	*3.15*	*1.219*	*1.487*	*-.229*	*.325*	*-.902*	*.639*
Q26-2-Pattern	54	3.57	.964	.928	-.481	.325	-.180	.639
Q26-3-COTS	*54*	*2.98*	*1.251*	*1.566*	*.156*	*.325*	*-.799*	*.639*
Q26-4-VaInput	54	4.15	.899	.808	-.788	.325	-.210	.639
Q26-5-DefOutput	54	3.81	1.011	1.022	-.865	.325	.690	.639

References

1. **Kramer, F.D., S.H. Starr, and L. Wentz, eds. *Cyberpower and National Security*. 2009, Potomac Books, Inc.**
2. **Perna, G., Cybersecurity Spending - Importance Will Increase, in International Business Times (*www.ibtimes.com*). 2010.**
3. **Williams, C., Cameron to spend £1bn+ on cyber security, in The Register. 2010.**
4. **Krebs, B., DHS Seeking 1,000 Cyber Security Experts, in Washington Post. 2009, www.**
5. **Mogull, R., An Open Letter to Robert Carr, CEO of Heartland Payment Systems, in Securosis Blog. 2009, Securosis.**
6. **Weiss, Stuxnet Incident Description. 2010.**
7. **Sinclair, G., C. Nunnery, and B.B.H. Kang. The waledac protocol: The how and why. in Malicious and Unwanted Software (MALWARE), 2009 4th International Conference on. 2009.**
8. **Waterman, S., Prisons bureau alerted to hacking into lockup, in The Washington Times. November 6, 2011.**
9. **Gjelten, T., Stuxnet Raises Blowback Risk In Cyberwar, in National Public Radio. November 2, 2011.**
10. **Taleb, N.N., *The Black Swan*. 2007: Random House.**
11. **Bayuk, J., et al., *Systems Security Engineering, A Research Roadmap, Final Technical Report*. 2010, Systems Engineering Research Center (www.sercuarc.org).**
12. **FFIEC, *IT Examination Handbook - Information Security Booklet*. 2006, Federal Financial Institutions Examination Council.**
13. **Ross, R., et al., *Recommended Security Controls for Federal Information Systems, SP 800-53 Rev 2*, National Institute of Standards and Technology, Editor. 2007.**
14. **ISO/IEC, *Information technology — Security techniques — Information security risk management (ISO/IEC 27005)*. 2008, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).**
15. **Nevo, B., *Face Validlity Revisited.* Journal of Educational Measurement, 1985. 22(4): p. 287-293.**
16. **Bar-Yam, Y., A mathematical theory of strong emergence using multiscale variety. Complexity, 2004. 9(6): p. 15-24.**

17. **Sherwood, J., A. Clark, and D. Lynas, *Enterprise Security Architecture*. 2005: CMP Books.**
18. **Anderson, R., Security Engineering, Second Edition. 2008: Wiley.**
19. **Bishop, M., *Computer Security, Art and Science*. 2003: Pearson Education.**
20. **Jacobs, S., Engineering Information Security. 2011: Wiley.**
21. **Rittel, H.W.J. and M.M. Webber, *Dilemmas in a general theory of planning.* Policy Sciences, 1973. 4(2): p. 155-169.**
22. **Geer, D. (2010) *Re: discussion topic for Mini-Metricon 5.5* Metricon Program Committee Communication, 11/1/2010.**
23. **Carmines, E. and R. Zeller, *Reliability and Validity Assessment.* Quantitative Applications in the Social Sciences, ed. M.S. Lewis-Beck. 1979, Thousand Oaks, California: SAGE Publications.**
24. **Schneier, B., *Beyond Fear*. 2003: Springer-Verlag.**
25. **Boardman, J. and B. Sauser, *Systems Thinking: Coping with 21st century problems*. 2008: Taylor & Francis.**
26. **DoD, The Orange Book, Trusted Computer System Evaluation Criteria. 1985, Department of Defense.**
27. **Common Criteria Recognition Agreement, Common Criteria for Information Technology Security Evaluation Version 3.1. 2009.**
28. **ISO/IEC, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model (ISO/IEC 15408). 2009, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).**
29. **Quinn, S., et al. *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1, SP800-126 Rev.1*. National Institute of Standards and Technology (US), Information technology Laboratory; Available from: scap.nist.gov.**
30. **For example, Symantec Enterprise Security Manager, Tripwire Enterprise Security Manager, and Computer Associate etrust Access Control.**
31. **Kim, G. and E.H. Spafford, The design and implementation of tripwire: a file system integrity checker, in Second ACM conference on computer and communications security. 1994, ACM Press.**
32. **Schneider, F.B., ed. *Trust in Cyberspace*. 1999, National Research Council, National Academy Press.**
33. **Neumann, P.G., Principled Assuredly Trustworthy Composable Architectures. 2004, SRI International.**
34. **Altmann, J., *Observational study of behavior: sampling methods.* Behavior, 1974. 49(3): p. 227-67.**

35. **Bayuk, J., Stepping Through the IS Audit, A Guide for Information Systems Managers, Second Edition. 2nd ed. 2005: Information Systems Audit and Control Association.**
36. **PCI, *Payment Card Industry (PCI) Data Security Standard, Version 1.2*. 2008, Payment Card Industry (PCI) Security Standards Council.**
37. **Garcia, M.L., The Design and Analysis of Physical Protection Systems. 2008: Butterworth-Heinemann.**
38. **MITRE. *National Vulnerability Database*. ongoing; Available from: http://nvd.nist.gov/.**
39. **For example, Tenable's Nessus Security Scanner and IBM's Internet Security Scanner (ISS).**
40. **Mell, P., K. Scarfone, and S. Romanosky, *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*. 2007, Forum of Incident Response and Security Teams (FIRST).**
41. **Fernandez, E.B. and N. Delessy. Using Patterns to Understand and Compare Web Services Security Products and Standards. in Proceedings of the Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT/ICIW 2006). 2006: IEEE.**
42. **Acohido, B. and J. Swartz, *Zero Day Threat*. 2008, New York: Sterling Publishing Co., Inc.**
43. **Verizon Business, Verizon Incident Sharing Metrics Framework, http://securityblog.verizonbusiness.com/2010/02/19/veris-framework. 2010.**
44. **McGraw, G., *Software Security*. 2006: Addison-Wesley.**
45. ***United States of America versus Albert Gonzalez*. 2010, United States District Court, District of New Jersey.**
46. **ISO/IEC, *Information technology — Security techniques — Code of practice for information security management (ISO/IEC 27002)*. 2005, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).**
47. **ISACA, *Control Objectives for Information Technology (COBIT)*. 2007, Information Systems Audit and Control Association, IT Governance Institute: Rolling Meadows, IL.**
48. **International Telecommunication Union, Security architecture for systems providing end-to-end communications. 2003.**
49. **ISF, The Standard of Good Practice for Information Security. 2007, Information Security Forum.**

50. Kim, G., P. Love, and G. Spafford, *Visible Ops Security*. 2008: Information Technology Process Institute.
51. Bayuk, J.L. The Utility of Security Standards. in Security Technology (ICCST), 2010 IEEE International Carnahan Conference on. 2010.
52. Bayuk, J., A. Mostashari, and B. Sauser, Security Verification and Validation, in Conference on Systems Engineering Research (CSER). 2011.
53. American Institute of Certified Public Accountants, Auditing Practice Release No. 021056: Implementing SAS No.#70 Reports on the Processing of Transactions by Service Organizations.
54. http://bankinfosecurity.com.
55. US Government Accounting Office, Information Security: Evaluation of GAO's Program and Practices for Fiscal Year 2010 March 4, 2011.
56. Savola, R.M., Towards a Taxonomy for Information Security Metrics, in International Conference on Software Engineering Advances (ICSEA). 2007, ACM: Cap Esterel, France.
57. CISWG, *Report of the Best Practices and Metrics Teams*, Corporate Information Security Working Group, Editor. 2005, US House of Representatives, Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Government Reform Committee.
58. Jaquith, A., *Security Metrics*. 2007, Upper Saddle River, NJ: Pearson Education.
59. Hayden, L., IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data 2010: McGraw-Hill Osborne Media.
60. Bayuk, J. and A. Mostashari, *Security Metrics for Systems Engineers – A Survey.* Submitted to Systems Engineering, 2011.
61. Bayuk, J., Information Security Metrics – Legal and Ethical Issues, in Readings and Cases in the Management of Information Security - Legal and Ethical Issues, M.E. Whitman and H.J. Mattord, Editors. 2010, Thomson Course Technology. p. forthcoming.
62. Beres, Y., et al., Using Security Metrics Coupled with Predictive Modeling and Simulation to Assess Security Processes, in Third International Symposium on Empirical Software Engineering and Measurement. 2009, IEEE.
63. Amran, A.R., R. Phan, and D.J. Parish. Metrics for Network Forensics Conviction Evidence. in International Conference for Internet Technology and Secured Transactions. 2009.

64. **Wang, H., et al., A Framework for Security Quantification of Networked Machines, in 2nd International Conference on COMmunication Systems and NETworks, (COMSNETS). 2010**
65. **Haimes, Y.Y., On the Definition of Vulnerabilities in Measuring Risks to Infrastructures. Risk Analysis, 2006. 26(2): p. 293-296.**
66. **Jiang, T. and J.S. Baras, Ant-based Adaptive Trust Evidence Distribution in MANET, in Proceedings of the 24th International Conference on Distributed Computing Systems Workshops (ICDCSW'04) 2004 IEEE.**
67. **Carin, L., G. Cybenko, and J. Hughes, Quantitative Evaluation of Risk for Investment Efficient Strategies in Cybersecurity: The QuERIES Methodology, in Metricon 3.0. 2008: San Jose, California**
68. **Alshammari, B.F., Colin; Corney, Diane. Security Metrics for Object-Oriented Class Designs. in Ninth International Conference on Quality Software. 2009 IEEE.**
69. **Manadhata, P.K., et al., *An Approach to Measuring a System's Attack Surface*. 2007: Carnegie Mellon University.**
70. **Clark, S., M. Blaze, and J. Smith, *Does Software Quality Matter? ,* in *Metricon 4.0*. 2009, www.securitymetrics.org: Montreal, Canada.**
71. **Herrmann, D., *The Complete Guide to Security and Privacy Metrics*. 2007, Boca Raton, FL: Auerbach Publications.**
72. **Pironti, J.P., *Developing Metrics for Effective Information Security Governance.* Information Systems Control Journal, 2007. 2.**
73. **Jansen, W., *Directions in Security Metrics Research*. 2009, National Institute of Standards and Technology Interagency Report.**
74. **Brotby, W.K., Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement. 2009: Auerbach Publications.**
75. **Buede, D.M., The Engineering Design of Systems, Models and Methods. 2009: Wiley.**
76. **Thomas, R.C. and others (2010) *And now for a non-statistic*. Security Metrics Mail List, 5/16-5/24/2010.**
77. **Schell, R.R. Information security: science, pseudoscience, and flying pigs. in Computer Security Applications Conference, 2001. ACSAC 2001. Proceedings 17th Annual. 2001.**
78. **Borcherding, K., T. Eppel, and D. von Winterfeldt, *Comparison of Weighting Judgments in Multiattribute Utility Measurement.* Management Science, 1991. 37: p. 1603-1619.**

79. Saaty, T.L., *How To Make A Decision: The Analytic Hierarchy Process.* European journal of operational research, 1990. Elsevier.

80. Thurstone, L.L., *Attitudes can be measured.* American Journal of Sociology, 1928. 33(4): p. 529-554.

81. Rohmeyer, P., J. Bayuk, and T.B. Zvi, *Security Decision Theory* 2011, Stevens Institute of Technology.

82. Wrenn, B., *The market orientation construct: Measurement and scaling issues.* Journal of Marketing Theory and Practice, 08/1997. 5(3).

83. Reichheld, F.F., The One Number You Need to Grow, in Harvard Business Review. 2003.

84. Sheard, S.A., *The Frameworks Quagmire - 10 Years Later*. 2007, Systems and Software Consortium, Inc.

85. ISO/IEC, *Information technology — Systems Security Engineering — Capability Maturity Model (SSE-CMM, ISO/IEC 28127)*. 2002, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

86. Mead, N.R., E.D. Hough, and T.R. Stehney, *Security Quality Requirements Engineering (SQUARE) Methodology*. 2005, Carnegie Mellon University Software Engineering Institute.

87. Cohen, F., *IT Security Governance Guidebook*. 2007: Auerbach Publications.

88. ISO/IEC, *Information technology — Security techniques —Information security management — Measurement (ISO/IEC 27004)*. 2009, International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC).

89. Amoroso, E., *Cyber Security*. 2006: Silicon Press.

90. Fabian, B., et al., *A comparison of security requirements engineering methods.* Requirements Engineering, 2010. 15(1): p. 7-40.

91. Bayuk, J., et al., *Cyber Security Policy Guidebook*. forthcoming, 2012: Wiley.

92. Bayuk, J.L. and B.M. Horowitz, *An Architectural Systems Engineering Methodology for Addressing Cyber Security.* Journal of Systems Engineering, 2011. 14(3).

93. Checkland, P., *Soft systems methodology: a thirty year retrospective.* Systems Research and Behavioral Science, 2000. 17(S1).

94. Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V2.1, see http://www.cloudsecurityalliance.org. 2009.

95. Bayuk, J., Cloud Security Metrics, in IEEE International Conference on System of Systems Engineering. 2011.

96. Bilgerm, M., et al., *Data-centric Security*. 2006, IBM.

97. **Boyd, J., *A discourse on winning and losing,* in *Briefing slides*. 1987, Air University Library Document No. M-U 43947: Maxwell Air Force Base, AL.**
98. **Arrott, A., *Work Factor Ratios*. securitymetrics.org. June 9, 2011.**
99. **Bayuk, J.L., *Third Party Data Handling.* Information Systems Control Journal, 2009.**
100. **Botha, R.A., S.M. Furnell, and N.L. Clarke, *From desktop to mobile: Examining the security experience.* Computers & Security. 28(3-4): p. 130-137.**
101. **Barrera, D. and P. Van Oorschot, *Secure Software Installation on Smartphones.* IEEE Security & Privacy, 2011. May/June 2011: p. 42-51.**
102. **Chatzinotas, S., et al., Evaluation of Security Architectures for Mobile Broadband Access, in Handbook of Research on Wireless Security,, Y. Zhang, J. Zheng, and M. Miao, Editors. 2008, IGI Global.**
103. **Bayuk, J., *Systems Security Metrics*. 2012, Systems Engineering Research Center (SERC) Research Task (RT32), Proposed**
104. **Jones, R.A. and B.M. Horowitz, *A System-Aware Cyber Security Architecture.* o appear in Journal of Systems Engineering, 2012.**
105. **Fogle, C. and J. Bayuk, *Systems Security Curriculum.* TBD, 2012.**
106. **Sauser, B. and J. Bayuk, *Security ConOps.* TBD, 2012.**
107. **Bayuk, J. and A. Mostashari, Measuring Cyber Security in Intelligent Urban Infrastructure Systems, in International IEEE Conference & Expo on Emerging Technologies for a Smarter World (CEWIT 2011). 2011.**
108. **Jia, J., G.W. Fischer, and J.S. Dyer, Attribute Weighting Methods and Decision Quality in the Presence of Response Error: A Simulation Study. Journal of Behavioral Decision Making, 1997.**
109. **Merkow, M.S. and J. Breithaupt, *Computer Security Assurance, Using the Common Criteria*. 2005: Thomson Delmar Learning.**

Vita

JENNIFER L. BAYUK

EDUCATION

MS Computer Science, Stevens Institute of Technology, 1992, GPA 3.9.
MA Philosophy, The Ohio State University, 1986, GPA 3.5.
Thesis compared logic in expert systems to that of compiler design.
BA Computer Science and Philosophy
Rutgers College, Rutgers, the State University of New Jersey, 1985
GPA 3.59, Henry Rutgers Honors Scholar
Thesis in Philosophy of Expert Systems, Rutgers Academic Life Scholarship.
Certified Information Systems Auditor (CISA), 1996.
Certified Information Security Manager (CISM), 2002.
Certified in the Governance of Enterprise IT (CGEIT), 2008
Certified Information Systems Security Professional (CISSP), 2008.

EXPERIENCE

Industry Professor, Stevens Institute of Technology, 9/10 to present.

Direct cybersecurity program development for the School of Systems and Engineering. Program components include graduate curriculum in security systems engineering, course materials for security systems engineering and enterprise security architecture, and research roadmaps. Provide cybersecurity expertise for any and all Institute security-related endeavors. Perform principal investigator role in the development of a roadmap for a multi-university research program. Develop and teach courses in enterprise security management at the Howe School of Technology Management.

Independent Consultant, Jennifer L Bayuk LLC, 6/08 to present.

Engaged in a wide variety of industries with projects ranging from oversight policy and metrics for financial institutions to technical architecture and requirements for security product vendors. Lecturing at conferences. Teaching for local industry associations. Serving as the director of Cybersecurity Programs at Stevens Institute of Technology's School of Systems and Enterprises. Providing expert witness services.

Senior Managing Director, CISO, Bear Stearns & Co., Inc., 4/98 to 6/08.

Designed and implemented firmwide processes to protect, detect, and recover from harm to information. Established and maintained enterprise-wide security, change control, and business continuity metrics. Chair of the Firmwide Information Protection Committee and member of the Global Outsourcing and Firmwide Emergency Response Committees. Drafted, negotiated, and issued global security policies and processes. Devised tools, techniques, roles, responsibilities, and awareness materials for all security processes including digital identity, application inventory and information systems risk management. Provided technical requirements and test programs for new security products and security features of new applications. Directed the activities of development and infrastructure officers globally with respect to security tools and techniques. Directed information security investigations and remediation activities in coordination with human

resources, legal and compliance. Coordinated emergency response teams for information security related events. Reviewed physical security efforts in support of data center protection. Contracted and performed penetration tests. Guided management through information technology (IT) audits. Performed due diligence in support of merger, acquisition, research analyst, and investment banking activity. Testified on due diligence efforts when required by regulators. Prepared materials on security measures for prospective clients. Coordinated industry efforts in support of firm goals for information security improvements. Directly managed department budget (~3M) and security tollgates over all projects in IT budget (~600M). Chief Information Security Officer title achieved in 2002.

Manager, Information Systems Business Controls, AT&T Capital Corp., 2/97 to 4/98.
Led and executed the company's global internal audit and control assessments with respect to information systems. Conducted security investigations. Provided direction and guidance on systems control issues for the company's strategic leaders, including the Technology Leadership Team and corporate legal counsel. Developed COSO & COBIT compliant systems audit approach for AT&T Capital that includes quantitative communication of systems vulnerabilities. Evaluated and developed tools for operating system, database management system, and network security testing as well as data analysis, incident tracking, and reporting.

Information Systems Risk Manager, Price Waterhouse LLP, 1995 - 1997.
Managed a wide variety of security consulting and audit projects for the Price Waterhouse Information Systems Risk Management Practice, including penetration tests and physical infrastructure reviews. Performed systems infrastructure analysis directed at improving technical security architecture, security management processes, and information system operational risk management. Developed methodology for evaluating the effectiveness of security management processes and trained both consultants and senior managers on its use. Wrote and customized programs for security testing. Evaluated various types of commercial security software.

Information Security Technical Staff, AT&T Bell Laboratories, 1990 - 1995.
Led diverse, cross-organizational teams focused on security and data integrity, including the AT&T Network Security Requirements Team, the Security Analysis of the Network Environment Team, and the Security Assessment Team. Envisioned, designed, specified, developed, demonstrated, tested, and documented software for expert systems, graphical user interfaces, databases, and network monitors. Spent most of the last year at AT&T with the CFO Organization in Short Hills performing computer security audits and corporate security consulting for various systems comprising and supporting the AT&T Worldwide Intelligent Network.

Project Manager, UFA, Inc., Newton, MA (www.atcoach.com), 1988 - 1990.
Developed, documented, and maintained ATCoach Expert System and Networked Air Traffic Simulation program. Prioritized programming efforts. Demonstrated ATCoach to Congressional subcommittee at request of the Federal Aviation Administration (FAA) client.

Technical Support Specialist, Dynamic Applications, Inc., 1987 - 1988.
Designed, documented, and implemented employee and client training programs for Property Management Financial Accounting System. Responsibilities included custom programming and user support.

Teaching Assistant, Rutgers University (1986-88) and The Ohio State University (1985-86).

AFFILIATIONS

Stevens Institute of Technology, Professor of *Systems Security Engineering* and *Enterprise Security Architecture*

Institute for Defense Analysis, Information Technology and Systems Division, affiliated subject matter expert.

Computers and Security, an Elsevier publication, Editorial Board Member.
Information Systems Audit and Control Association (ISACA), instructor on a wide variety of topics, author, and certification exam question contributor.
Metricon Program Committee Member, and Chair for Metricon 4.0, MiniMetricon 5.5 (www.securitymetrics.org).
International Council on Systems Engineering (INCOSE), co-chair, Security Working Group, 2010+.
Computer Security Institute (CSI), member and speaker.
Association of Computing Machinery (ACM), member.
IEEE Computer Society, member.
Information Systems Security Certification Consortium (ISC^2), member.
Research and Development Committee Chair, Financial Services Sector Technology Council (FSSCC), 2006-2008
Securities Industry and Financial Markets Association(SIFMA) Information Security Committee Chair, 2003-2008.

BOOKS

Spring 2012	*Cyber Security Policy Guidebook,* lead of five authors with different areas of Cyber Security Policy Expertise, Wiley.
September 2010	*Cyber-Forensics, Understanding Information Security Investigations,* edited this collection of articles by industry experts and provided an introductory framework, Springer.
January 2010	*Enterprise Security for the Executive: Setting the Tone at the Top,* Praeger.
March 2009	*Enterprise Information Security and Privacy,* Artech House, co-edited this collection with Warren Axelrod and Dan Schutzer, and wrote chapter on "Information Classification."
November 2007	*Stepping Through the InfoSec Program,* Information Systems Audit and Control Association (ISACA), peer-reviewed book.
January 2005	*Stepping Through the IS Audit, A Guide for Information Systems Managers, 2nd Edition.* Book published by the ISACA, peer-reviewed. First Edition January 2000

SELECT OTHER PUBLICATIONS & SPEAKING ENGAGEMENTS

Fall 2011	"An Architectural Systems Engineering Methodology for Addressing Cyber Security," *Systems Engineering,* Volume 14, Issue 3.
July 2011	*Systems-of-Systems Issues in Security Engineering*, INCOSE Insight, Volume 14, No 2.
June 2011	*Cloud Security Metrics*, IEEE Systems of Systems Engineering Conference (SoSE2011).
March/April 2011	"System Security Engineering," *IEEE Security & Privacy Magazine*, Volume 9 Issue 2.

August, 2010	*Systems Security Engineering, A Research Roadmap, Final Technical Report*, primary author for DoD-sponsored publication for the Systems Engineering Research Center (www.sercuarc.org).
November 2010	"Systems Security Engineering Roadmap," *Rethinking Cyber Security: A Systems-Based Approach*, Workshop sponsored by the Center for Risk Management of Engineering Systems and the Institute for Information Infrastructure Protection (I3P), University of Virginia.
October 2010	*The Utility of Security Standards*, IEEE International Carnahan Conference on Security Technology (ICCST).
June 2010	*Pairing Organizational Strategy with Security Solutions*, CSO Executive Seminar.
June 2010	"Information Security Metrics," in *Readings and Cases in Information Security Management – Legal and Ethical Issues,* Course Technology, edited by Mattord and Whitman.
May 2010	"Systems Security Engineering," *Tenth Annual High Confidence Software and Systems Conference*, sponsored by the National Security Agency.
December 2009	"Critical Infrastructure Protection Issues in the Financial Industry," *Global Conference on Systems and Enterprises*, Stevens Institute of Technology.
September 2009	*Prevention Is Better Than Cure*, Business Trends Quarterly.
May 2009	*Third Party Data Handling*, ISACA Control Journal.
March 2009	*Data-Centric Security*, Computer Fraud and Security.
November 2008	*Security Through a Time of Crisis*, Computer Security Institute Annual Conference.
October 2008	*Key Data Points for IT Governance Metrics*, ISACA IT GRC Conference.
July 2008	*Metrics for Risk Management versus Security Attribution*, Metricon Conference.
June 2008	*Third Party Due Diligence*, Securities Industry and Financial Markets Association (SIFMA) Technology Management Conference.
October 2007	"Utilising information security to improve resiliency," *Journal of Business Continuity & Emergency Planning*.
October 2007	*Data Classification, Security and Privacy*, Securities Industry and Financial Markets Association, Internal Audit Division, Annual Conference.
Sept/Oct 2007	"IT Attestation Services: What You Need to Know," *Journal of Corporate Accounting and Finance*.
June 2007	*CISM Review Manual, Chapter 5: Information Security Program Management*, Information Systems Audit and Control Association.
October 2006	*The Homeland Security Front*, Securities Industry Association, Internal Audit Division, Annual Conference.
November 2005	*Security Review Alternatives*. The Computer Security Journal, Fall 2005, a Computer Security Institute publication.

October 2005	*Best Practices for Securing and Controlling Offshore Vendors,* Securities Industry Association, Internal Audit Division, Annual Conference.
September 2005	*Internal Security Reviews,* Fourth Annual FDIC Technology Seminar.
June 2004	*Sarbanes-Oxley for the IS Professional,* Securities Industry Association, Technology Management Conference.
October 2003	*Metrics for Due Diligence,* Best In Class Security and Operations Roundtable Conference, Carnegie Mellon Software Engineering Institute.
May 2003	*Security Forum 2003, The Secure Enterprise, Wireless LAN Panel,* Technology Managers Forum.
April 2003	*Introducing Security at the Cradle,* SANS (System Admin, Audit, Network, Security Institute) Security and Audit Controls that Work Conference.
Summer/Fall 2002	*Productive Intrusion Detection,* The Computer Security Journal Vol XVIII, No 3-4, a Computer Security Institute publication.
May 2001	*Security Forum 2001, Information Risk Management, Risk Management and Security Metrics Panel,* Technology Managers Forum.
May 2001	*Measuring Security,* Information Security System Rating and Ranking, an Applied Computer Security Associates (ACSA)Workshop.
January 2001	*Security Metrics,* The Computer Security Journal, Vol XVII, No 1, a CSI publication.
August 2000	*Assurance and Monitoring of E-business: Technical Control Points,* Seminar sponsored by Information Systems Audit and Control Association (ISACA) and the Association of Government Accountants (AGA).
June 2000	*Security Metrics: An Audit-based Approach,* Computer Systems Security and Privacy Advisory Board (CSSPAB) Security Metrics Workshop (Sponsored by NIST, the National Institute of Standards and Technology).
April 2000	*CISA Exam Certification Course,* Domain 4: Information Systems Integrity, Confidentiality, and Availability, ISACA North Jersey Chapter (Also taught in April 1998 and April 1999).
October 1999	*Infrastructure Monitoring Challenges,* 22nd Annual National Information Systems Security Conference.
May 1999	*Successful Audits in New Situations,* ISACA Control Journal, (v.III).
November 1998	*How to Survive an IS Audit,* Computer Security Institute Conference, Chicago, IL.
June 1997	*Oracle Database Control Issues,* Vanguard Information Security Expo, Orlando, FL.
January 1997	*Audit & Control of Sybase and Oracle,* ISACA NY Metropolitan Chapter.

January 1996	*Security Controls for a Client-Server Environment*, ISACA North Jersey Chapter.
July 1996	*Security Hot Topics*, Price Waterhouse Information Systems Risk Management Internal Advanced Training, Tampa FL.
October 1996	*Security Through Process Management*, 19th Annual National Information Systems Security Conference, Baltimore, MD.
June 1996	*Security Controls for a Client-Server Environment*, The EDP Audit, Control, and Security Newsletter (EDPACS).
1990-1995	Several proprietary restricted AT&T Bell Laboratories publications.
Oct-Dec 1989	*Network Simulation System for Air Traffic Control Training*, Journal of Air Traffic Control.