

Proceedings

Workshop on Information Security System Scoring and Ranking

**Information System Security Attribute Quantification or Ordering
(Commonly but improperly known as “Security Metrics”)**

May 21-23, 2001



**Sponsored by: Applied Computer Security Associates
The MITRE Corporation**

© 2002, Applied Computer Security Associates. All rights reserved.

Applied Computer Security Associates (ACSA)

ACSA had its genesis in the first Aerospace Computer Security Applications Conference in 1985. That conference was a success and evolved into the Annual Computer Security Applications Conference (ACSAC). Several years ago, the word *Aerospace* was dropped from the name to promote a wider range of government and commercial applications. ACSA was incorporated in 1987 as a non-profit association of computer security professionals who have a common goal of improving the understanding, theory, and practice of computer security. For further information, visit the World Wide Web site for ACSAC at <http://www.acsac.org>.

The MITRE Corporation

MITRE is a not-for-profit national technology resource that provides systems engineering, research and development, and information technology support to the government. Established more than 40 years ago, MITRE operates federally funded research and development centers for the Department of Defense, the Federal Aviation Administration, and the Internal Revenue Service, with principal locations in Bedford, Massachusetts, and Northern Virginia. For further information, visit the World Wide Web site for MITRE at <http://www.mitre.org>

Copyright Notice

© 2002, Applied Computer Security Associates. All rights reserved.

The public is free to download the *Proceedings* for the Workshop on Information Security System Scoring and Ranking and locally print and distribute it as desired for personal and organizational use. Specifically, the *Proceedings* may be reproduced and used, without alteration, addition, or deletion, for any nonpecuniary or nonpublishing purpose without permission. The ACSA has no intent to restrict you from doing that; rather, they encourage it. The purpose of making the *Proceedings* freely available to you is for you to be able to use it! The sole purpose of the copyright notice is to make sure that nobody else copyrights or modifies the material without ACSA permission, which might thereby restrict its use and the public's full and free use of it. However, there is no intent to restrict the public in any way from freely distributing and using the *Proceedings* material as is.

Applied Computer Security Associates, 2906 Covington Road, Silver Spring, MD 20910
acsac_president@acsac.org

The views expressed in these *Proceedings* are not necessarily those of the ACSA
or The MITRE Corporation.

Foreword

At the 2000 National Information Systems Security Conference, attendees participated in a panel discussion, “Metrics, Myths, and Magic,” where the panelists consisted of John McHugh, J. Michael Williams, Don Peebles, and myself. We had about 35 minutes of prepared remarks for a 90-minute session. As people wandered into the room, the session became standing room only, with people five deep out into the hall. When we finished our prepared remarks, the audience “took over” with questions and debate. Suffice to say, yes, we had struck a nerve and generated interest.

When Marshall Abrams came forward after the panel and approached me about the possibility of holding a workshop on measurement within the information assurance field, it never occurred to me to say, “No, I want nothing to do with it.” Fool that I was, I believed this would be a good idea, that a workshop would bring focus to a very diverse topic.

Well, that’s how this workshop came to be. The committee was formed, the budget created, web site generated, and submissions received. Yes, there was interest, there would be a workshop, and we would generate more discussion. These *Proceedings* summarize the results. I believe they have captured the essence of our three days in Williamsburg, Virginia, and hope they give the audience additional perspective and new areas for debate.

Without the gracious support of Applied Computer Security Associates (ACSA), this workshop would not have been possible. Workshop organizers appreciate the support from the ACSA board, not only for sponsorship of the workshop but for supporting a measurement discussion mailing list as well.

Thanks also go to The MITRE Corporation, for providing administrative support to the workshop as well as allowing its employees to participate on the workshop organizing committee. Diana (Dee) Akers, the ACSA conference arrangements chair, was immensely helpful in providing consultative assistance on site coordination. Deborah Bodeau provided the Executive Summary and identified related activities. Pat Hunt kept everything organized on-site and ensured a pleasant experience for all participants.

Finally, Marshall Abrams, ACSA’s resident Curmudgeon, made chairing this workshop a learning experience and walked me through the entire process. Without Marshall’s timelines and nagging, these proceedings would still be in editorial review. For his guidance and patience, as well as his expertise with workshop organizing, I am appreciative. He made my first adventure as Workshop Chair less of a job and more of an adventure.



RONDA HENNING
Workshop Chair

Workshop Participants

Marshall Abrams
The MITRE Corporation

John Alger
The MITRE Corporation

Nadya Bartol
Booz-Allen & Hamilton

Jennifer Bayuk
Security Architecture
and Engineering,
Bear Stearns &
Company, Inc.

Paul Bicknell
The MITRE Corporation

Deborah Bodeau
The MITRE Corporation

Julie Bouchard
SRI International

Julie Connolly
The MITRE Corporation

Yves Deswarte
LAAS-CNRS

Robert Dobry
A&N Associates, Inc.

Deborah Downs
The Aerospace
Corporation

Ranwa Haddad
The Aerospace
Corporation

Jonas Hallberg
Swedish Defence
Research Agency

Ronda Henning
Harris Corporation

Amund Hunstad
Swedish Defence
Research Agency

Jay Kahn
The MITRE Corporation

Stuart Katzke
National Security
Agency

Dirk Kuhlmann
Hewlett-Packard
Laboratories
Bristol – TESL

Ralph Leighton
Getronics Government
Solutions

Perry Luzwick
Logicon

Roy Maxion
Carnegie Mellon
University

Dennis McCallam
Logicon

Donald Peeples
SPARTA, Inc.

Jock Rader
Raytheon Electronic
Systems

George Rogers
Corbett Technologies,
Inc.

Paul Rubel
BBN Technologies

Edward Schneider
Institute for Defense
Analysis

Stuart Shapiro
The MITRE Corporation

Michael Skroch
ASD (C3I)

Gary Stoneburner
NIST

James Tippet
Consultant

Rayford Vaughn
Mississippi State
University

Peter Villasenor
ASD (C3I)

Bennet Yee
University of California
at San Diego

Workshop Committee

Ronda Henning
Chair

Marshall Abrams
ACSA Liaison

Jay Kahn
Treasurer

Don Peoples
Local Arrangements Chair

Rayford Vaughn
Publications Chair

Julie Connolly
Program Chair

John McHugh
Program Committee

James Tippet
Program Committee

Contents

| | |
|--------------------------------|------------|
| Executive Summary | vii |
|--------------------------------|------------|

| | |
|--|-----------|
| 1 Introduction and Conclusions..... | 1 |
| 2 Workshop Organization | 4 |
| 3 Working Group Reports..... | 5 |
| 4 Suggested Research Areas | 26 |
| 5 Future Directions..... | 30 |

Appendices

| | |
|---|-----------|
| A Agenda..... | 31 |
| B Position Paper Summaries..... | 35 |
| C Related Measurement Activities | 41 |
| D Glossary..... | 52 |

Executive Summary

Introduction

The Workshop on Information Security System Scoring and Ranking, sponsored by the Applied Computer Security Associates (ACSA) and The MITRE Corporation, was held on May 21-23, 2001, in Williamsburg, Virginia. The goals of the workshop were to characterize the information security measurement problem domain, identify “good practices,” focus needs, and determine potential research directions.

The program committee restricted attendance to those who could provide evidence of prior work, or at least thinking, about the problem. The expectation was that such people would be best equipped to make progress toward the goals of the workshop. The “intellectual price of admission” was in the form of a position paper on some aspect of the information security measurement problem domain. A total of 30 papers were received, and 34 people participated in the workshop. The Program Committee used the position papers and discussion topics as the major inputs to the structure of the workshop. Accepted position papers were shared among the authors via the ACSA Website. Position papers were considered working drafts and the basis for discussion. They were not individually presented at the workshop. Additionally, a mailing list was formed prior to the workshop to stimulate further discussion and solicit additional topics for consideration.

Workshop Scope

The workshop organizers struggled with the following questions: What are we talking about? What should we call what we’re talking about? With respect to the first question, the Call for Participation emphasized metrics for information technologies and products. However, the position papers addressed a broader spectrum of information security metrics, as reflected in the characterization described below.

With respect to the second question, the workshop organizers recognized that considerable controversy exists regarding the term *metrics*: some seek to reserve it for the results of measurements based on scientific principles, but others use it to include results of assessments based on subjective judgments. While some position papers urged reliance on a dictionary or scientific definition, others observed that broader usage has been adopted in policies and practices. As some past discussions on metrics had been totally consumed with this discussion, the expression *information security (IS)** was used in the workshop agenda to avoid long discussions on terminology. The asterisk (*) was used to mean any of the following terms: metric, measure, score, rating, rank, or assessment result (although not necessarily an exhaustive list). Therefore, IS* is defined below:

| |
|--|
| An IS* is a value, selected from a partially ordered set by some assessment process, that represents an IS-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence. |
|--|

Although participants gravitated toward use of the terms *IS metric* or *information assurance (IA) metric*, we will use *IS** in these *Proceedings*. Figure ES-1 illustrates the workshop characterization of *IS**.

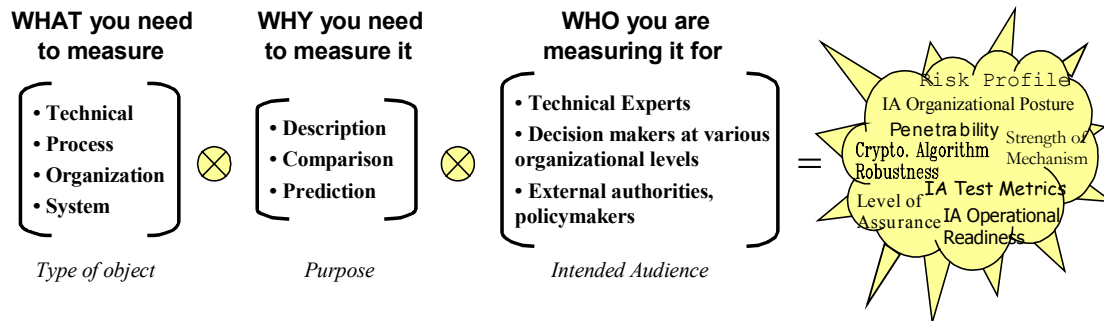


Figure ES-1. Characterization of *IS**

Ultimately, *IS*s* are intended to improve understanding or support decision making related to the *IS* posture of an entity. Several general problems were identified:

- Metrics are often ill defined; consequently, any definition of an *IS** should include a specification of the process used to construct and evaluate it.
- The definition and evaluation of *IS*s* frequently become distanced from the ultimate use, so that metrics become ends in themselves. That is, the consumer of the metric is lost in the definition of the metric.
- *IS*s* are often used or reported in contexts other than those for which they were originally intended.

As a result, many security technologists have great misgivings about the topic of *IS*s*. The workshop attempted to categorize these misgivings and tried to understand the rationale for them. In the process, the participants identified examples of good (and not-so-good) measurement practices and identified directions for further research. It became evident that *IS*s* can be characterized in terms of purpose or intended use, form, or scope. Two broad classes of uses of *IS*s* can be identified as follows:

- **Decision support.** This is the primary use of most *IS*s* and was the focus of the workshop. Assessments of security properties are used to aid different kinds of decision making, such as risk management, resource allocation, program planning, or selection of specific products or services.
- **Mandated reporting of *IS* status or posture.** Organizations also use and define *IS*s* to respond to external demands. Reporting can be mandated to determine compliance with requirements, serve as a basis for trend analysis, or justify requests for additional resources. Specific metrics can be mandated; however, usually the reporting

organization identifies the need for metrics to provide a succinct reporting mechanism.

The mandated reporting of IS status or posture is a relatively structured event, and the items reported tend to be discrete values, such as number of requirements fulfilled and number of intrusions detected. The workshop participants acknowledged the importance of mandated reporting in the determination of an organization's information security posture.

The form of an IS*, that is, how it is reported, can be numeric or non-numeric. The often-attempted distinction between quantitative and qualitative IS*s frequently breaks down in practice. Numeric metrics often represent relative rankings; the numeric difference between ranked values is significant for some metrics, but not for others. The assessment process leading to non-numeric metrics (e.g., red/yellow/green) frequently involves quantitative measurements (e.g., green means zero vulnerabilities found; yellow, one to five; red, more than five). The workshop participants avoided quantitative vs. qualitative discussions.

Workshop Tracks

The scope of an IS* is the region in the IS problem domain that it is intended to describe. Based on the interests and expertise indicated by the position papers, the workshop organizers used the following (non-disjoint) partitioning of the problem domain for workshop tracks:

- **Technical.** IS*s can be used to describe, and hence compare, technical objects, such as algorithms, specifications, architectures and alternative designs, products, and as-implemented systems, at different stages of the system life cycle.
- **Organizational.** IS*s can be used to describe, and to track the effectiveness of, organizational programs and processes.
- **Operational.** IS*s can be used to describe, and hence manage the risks to, operational environments, including as-used systems and operating practices.
- **Brainstormers.** Synthesis, cross-tracking issues, and big-picture concerns.

It was recognized that this partitioning omits significant regions, in particular:

- **Individual.** IS*s can be used to describe individual expertise.
- **Environmental.** IS*s can be used to describe security-relevant aspects of an organization's or operation's environment, in particular, threats.

Track 1: Technical

A significant observation was that very little activity has been previously reported on technical IS*s, that is, metrics used to compare or describe products or technologies. While various IS assessments of products and technologies are available, those assessments result in narrative descriptions and do not incorporate metrics. The *Trusted Computer System Evaluation Criteria* (TCSEC), Department of Defense (DoD) 5200.28-STD, provided a technical metric, but that document has been superseded by the *Common Criteria* (CC). The

CC has introduced the concept of a Protection Profile (PP). Each PP corresponds to one of the discrete levels in the TCSEC. In a sense, the CC is a standard for writing technical metrics. The Common Vulnerabilities and Exposures (CVE) list can serve as a basis for comparing vulnerability-scanning tools. The workshop position papers mention a few other proposed or in-use technical metrics, such as those used for cryptographic algorithms, but not a preponderance of metrics for describing or comparing organizational programs or processes.

The emphasis on organizational IS*s reflects a growing awareness at the highest organizational levels of the importance of IS concerns. It also reflects the difficulties decision makers face as they try to understand their organization's IS posture and manage IS risks. Thus, the concern is not that organizational IS*s are proliferating but simply that technical IS*s are not.

Based on the above discussion, two questions arise:

- Under what circumstances can technical IS*s be usefully defined and used?
- Why is the security engineering community not putting more effort into defining and using IS*s?

The following summary of observations from the technical workshop track provides a starting point for further discussion:

- Technical IS*s can be used to establish goals and measure how well the object achieves the goals, contributing to a partial ordering of the objects in a given set.
- Technical IS*s that enable comparison among like objects are useful for establishing minimum acceptable requirements or when IS becomes a discriminating factor in comparison. For example, given their other concerns, most acquisition program managers would not find IS*s for operating systems relevant. This view suggests that technical IS*s will be most useful for IS-specific products, such as intrusion detection systems.
- Technical IS*s that enable comparison among like objects are more useful when the assignment of the value is meaningful for most of the object's life span. This concept was a major problem with the use of the TCSEC process: by the time a product was sufficiently understood to complete an evaluation, the as-evaluated version was several revisions behind the as-marketed version. This outcome suggests that technical IS* efforts should (1) focus on abstract objects (e.g., cryptographic algorithms, protocol specifications), which have a long life-span; or (2) attempt to address an evolutionary life cycle.
- Technical IS*s that enable predictions will require an underlying model of IA in which the values associated with technical objects are significant factors in system security. In general, models of IA for operational systems are so rudimentary that technical metrics for components are not significant factors. For example, the TCSEC composition problem was never resolved: a system that integrated two different C2 operating systems, such as a C2 database management system and a C2 network, could not be asserted to have security functionality or assurance commensurate with

C2. In the general case, knowledge of the security properties of component systems does not necessarily lead to knowledge of the security properties of combinations of those systems. This statement suggests that before the security engineering community attempts to define predictive technical IS*s, we need to develop better models of acceptable system behavior limited to the behavior characteristics of the technical objects.

- Technical IS*s that enable prediction require an underlying model of IA in which the future resembles the past. This assumption will remain problematic; for example, the fact that no vulnerabilities have been detected in a product to date does not guarantee that multiple flaws will or will not be found and exploited next week. We need to review historical data with an eye toward trends and correlations (and, in many cases, to start recording data without clear foreknowledge of how we will use it).
- Commercial-sector users of IS*s are concerned with informing and implementing the overall risk management processes of their organizations. This affects their stance toward some technical IS*s: unlike government IS practitioners, they currently have little to no concern about product evaluations against the CC.

Track 2: Organizational

Organizational IS*s are used to describe, and to track the effectiveness of, organizational programs and processes. Examples include IA Vulnerability Assessment (IAVA) metrics, the percentage of personnel trained in security, and the percentage of systems accredited. Other examples are related to information technology (IT) modernization.

Two types of questions are asked when measuring the IS*s of organizations:

- How well is the organization doing in identifying and addressing its security concerns? How effective are organizational programs and processes? How much security does an organization need? What is the organizational “threshold of pain”? These questions are addressed by decision support metrics.
- How well is the organization meeting the requisite mandates? This question is addressed by reporting metrics.

Workshop discussions indicated that commercial organizations tend to focus on the former, while government organizations tend to focus on the latter. Commercial decision makers are motivated by the bottom line and are interested in the return on investment from programs, processes, procedures, and technical measures.

Government decision makers recognize that complying with all mandates does not guarantee adequate security. However, given the resources required to gather reporting metrics, government organizations are inclined to reuse those metrics for decision support. Mandates for reporting of security posture include:

- *Computer Security Act of 1987*
- *Paperwork Reduction Act) of 1995*¹
- *Clinger-Cohen Act of 1996*²
- Office of Management and Budget A-130, *Management of Federal Information Resources*, Appendix III, “Security of Federal Automated Information Resources.”³
- *Government Information Security Reform Act*⁴

The commercial and government sectors share a concern for conformance to standards of good practice. In the commercial sector, such conformance constitutes due diligence and provides a defense in litigation. Regulatory mandates express the government’s current definition of best practices. Organizational processes for IT modernization (i.e., acquisition, development, integration, and evolution) can benefit from IS*s. Differences between the commercial and government sectors may result in different needs for IS*s.

Among commercial users, established processes for IT modernization are driven by an enterprise-wide, bottom-line focus, which creates an environment providing end-to-end system performance with appropriate security measures. This security environment leads to well-defined IT requirements, specifications, and engineering with self-disciplined user compliance that emphasizes predictable results. The IT modernization processes for a government program and a commercial business case are similar in structure: requirements, approvals, development, and installation.

For both processes, there are established procedures with separate approval points and information security is not treated as a separate program/business case, but is a mandatory element of any program/business case. Both rely on similar internal/external auditors, penetration testing, and configuration management procedures. A key difference is that government procurements are constrained by national and organizational policies and architectures. This difference accounts for the perceived speed of the commercial IT modernization cycle. The commercial enterprise relies on the personal judgments of the security practitioner. Due diligence on the part of individuals is expected and forms the basis for management approval. This commercial process contrasts with the more structured, organizational approval processes in government.

Table ES-1 provides examples of types of IS*s relevant to IT modernization processes.

¹ Note: All Web links were verified at the time of publication, but may not work at a later time. See <http://www.rdc.noaa.gov/~pra/pralaw.htm>.

² See <http://irm.cit.nih.gov/policy/itmra.html> and.

³ See <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>.

⁴ See <http://csrc.nist.gov/policies/actmemo-guid.pdf> and <http://csrc.nist.gov/policies/M-01-241.pdf>.

Table ES-1. Example IS*s Relevant to IT Modernization Processes

| Type of Metric | Use | Issues |
|---|--|--|
| Technical IS*s (e.g., number of vulnerabilities detectable by scanners), EAL | Differentiate among technical alternatives. | Other factors (e.g., interoperability with enterprise management software) may be more relevant to product selection. |
| Product development process metrics (e.g., ISO 9000, SSE-CMM) | Differentiate among product suppliers (surrogate indicator of product quality). | Other factors (e.g., preferred supplier agreements) may be more relevant to product selection. |
| Acquisition process metrics (e.g., level of IS expertise in procurement office) | Allocate resources to provide IS expertise, determine level of effort for certification. | Process metrics may fail to indicate constraints on acquisition process or procurement office. |
| Certification level (NIACAP, DITSCAP) | Determine requirements for certification activities, documentation. | Relevant factors (e.g., system exposure) may fail to be addressed in definition of certification levels. Identification of activities does not directly indicate required level of effort. |

Thus, in answering the two questions stated above, at a minimum:

- Adequate security includes compliance with mandates. In the commercial sector, adequate security also involves conformance with common practice. Metrics can aid an organization in defining adequate security.
- For the organization to determine its specific IS needs, management must understand and be able to assess the relative value of organizational missions, business or operational functions, and the information resources that support those functions. (A particular area of difficulty is the assessment of the value of information.) A framework is useful to define adequate security and can be used to structure assessments of program effectiveness. For example, the *Federal Information Technology Security Assessment Framework* (FISAF) defines five levels of IS program effectiveness.⁵

Effective organizational metrics provide feedback into the processes they assess. Therefore, organizational metrics must be capable of evolving to accommodate the changes they have facilitated. However, because of the current focus on responding to reporting mandates, government organizations tend to use static metrics. For example, a static metric might be the

⁵ See http://www.cio.gov/documents/federal_it_security_assessment_framework.html. NIST is developing detailed guidance for performing assessments against the FISAF. See the NIST Special Publication 800-26, *Security Self-Assessment Guide for Information Technology Systems*, August 2001, available at <http://csrc.nist.gov/publications/nistpubs>. A workshop position paper described a related effort.

percentage of staff that have received an annual security-training refresher. Over time, that value should increase to 100%.

If the contents of the annual refresher course do not change over time, the meaning of the metric will degrade. Examples of more dynamic training-related metrics include the percentage of staff who have received training on secure use of the current versions of the software suite (operating system, browser, e-mail, office automation, mission applications) they use and the percentage of staff who have been made aware of policy updates.

In summary, particularly for decision support IS*s, one size does not fit all: organizational culture and values have a significant impact on decision processes and hence on organizational security practices.

Track 3: Operational

Organizations use operational IS*s to describe, and hence manage the risks to, operational environments, including as-used systems and operating practices. Risk assessment metrics (and their component metrics related to asset values, impact severity, threats, vulnerabilities, and effectiveness of security measures) comprise an important subset of operational metrics. Examples of other operational IS*s include the number of advisories responded to, the time devoted to patch installation, and the percentage of systems patched.

The definition of an operational IS* assumes a clear model of the operational environment: what is under the organization's control, what is external, and (for externals) what can be assumed or predicted. The controlled portion of the operational environment includes physical, procedural, and personnel security measures. It also includes the information systems owned or operated by the organization.⁶ External portions of the operational environment include systems with which the organization-controlled systems interface (e.g., partner organization information systems) or on which they depend (e.g., critical infrastructures such as telecommunications and power). External portions of the operational environment also include threats.

Understanding what the organization actually controls presents a significant problem: systems are increasingly distributed, layered, and administered by users. For an attribute of a system to be measurable, the system boundaries must be known. With the proliferation of portable and wireless devices, system boundaries are increasingly dynamic. Dependencies among system components, and among technology, people, and processes, must also be known.

The confidence with which assessments or characterizations of external factors is accomplished is highly variable. For such external factors as interfaced systems or power supplies, security or reliability properties can be established. In the commercial sector, properties can be established contractually, with penalties for failures. Service-level

⁶ Operational IS*s thus depend on, or incorporate, organizational and technical IS*s. Assessments of the effectiveness of procedures and personnel controls, such as background checks, can be grouped under the Organizational heading.

agreements currently focus on reliability and availability, but they could evolve to include quality of security service levels⁷ Within the government sector, properties are established by accreditation agreements and by regulatory mandates. For threats, descriptions can be assumed based on models or predicted based on past history, either of which could be wildly inaccurate. Information sharing is needed to develop better historical data but is impeded by fears of liability or loss of public trust.

Incident response highlights the cultural differences between the government and commercial sectors. The government has evolved a very structured, deliberate decision-making process that stresses inclusion of various actors at different levels of the organization's hierarchy. This includes outreach to law enforcement agencies. The commercial sector has evolved a much more rapid, matrix type of response approach at the enterprise level. Senior leadership is involved much more rapidly and involves all necessary personnel to facilitate rapid decision making. This approach stems from the financial implications, such as manufacturing lines, suppliers, contracts, customer relations, of an extended or poorly executed incident response.

The literature emphasizes a quantitative approach to operational IS*s: we count the number of vulnerabilities, intrusions, or virus outbreaks. This approach does not aid in assessing operational readiness (i.e., the ability to respond effectively and continue operations in the presence of an attack) and does not help managers understand the potential for security violations in a system or process.

The ability to contain damage, in response to detected or suspected security incidents, is part of a good operational security environment. For example, IS*s are used for damage assessment and speed of damage containment (e.g., privilege revocation). Also, processes and metrics associated with continuity of operations and disaster recovery might provide some insights.

Current hardware and software products lack an ability to monitor operational performance; few observable parameters might serve as input to operational IS*s. The kinds of operational parameters that are available are associated with audit logs, which focus on interactions between the product and the external environment while providing no information on the internal operation of the product.

The measurements delivered by security evaluation tools should represent as accurately as possible the security of the system in operation (i.e., its ability to resist possible attacks, or equivalently, the difficulty for an attacker to exploit the vulnerabilities present in the system and defeat the security objectives). Vulnerability scanners approach this problem by building a database of all known vulnerabilities and scanning the system for them.

The ESOPE approach, briefed at the workshop, looks at the operational security problem in terms of (1) the point of view of the threat (e.g., tenacious vs. lazy, focused vs. unfocused),

⁷ See, for example, "Toward Quality of Security Service in a Resource Management System Benefit Function," Irvine, C. E., and Levin, T., *Proceedings of the 2000 Heterogeneous Computing Workshop*, pp. 133-139, May 2000, and at <http://cisr.nps.navy.mil/publications/papers/htm>.

(2) the main security objectives and not every minor vulnerability, and (3) the need for security to change as the system evolves through modifications and upgrades, assuming that security is not absolute but is either improving or decaying.

IS properties of an operational environment frequently cannot be measured directly. Indirect indicators can be useful, but they must be defined and used carefully.

Track 4: Brainstormers

This track provided a forum for discussing synthesis, cross-track issues, and big-picture concerns regarding IS*s. A collective decision was made to apply a systems engineering approach to aggregate measurement, as this would accommodate the complete system life cycle. That is, technical, operational, and organizational measurement techniques and IS*s could all be integrated into this framework most effectively.

The working group decided to use the stakeholder framework as the basis for its brainstorming activity. The thought was if a list of stakeholders and their expectations from an IS* perspective could be defined, then perhaps a list of viable IS* measures could be generated.

Another activity was to map existing practices to stakeholders and their requirements, highlighting shortcomings where applicable. The conclusion was that no single item addressed all needs of a single stakeholder.

Proposed IS* Criteria

Criteria for “good” IS*s can be defined, but conflicts exist among those criteria. Examples of proposed criteria for IS*s include:

- **Scope.** The portion of the IS problem domain that the IS* describes should be clearly characterized.
- **Sound foundation.** The IS* should be based on a well-defined model of the portion of the IS problem domain it describes.⁸
- **Process.** The IS* assessment process should have the following characteristics:
 - **Well-defined.** The process definition should include qualifications of evaluators, identification of required information, instructions on how specific factors are to be measured or assessed, algorithms for combining factor values into final values, and explanations of sources of uncertainty.
 - **Repeatable.** A second assessment by the same evaluators should produce the same results.

⁸ A variety of problem domain taxonomies or descriptions may be useful. For example, the FISAF provides a definition of the IS programmatic domain. The 16 May 2001 draft NIST publication, *Underlying Technical Models for Information Technology Security* (available at <http://csrc.nist.gov/publications/drafts.html>), provides a framework for understanding the relationships among security services and objectives. The DARPA-sponsored study by Deckro, et al., proposes a variety of IA metrics based on a hierarchical model of the IA problem domain.

- **Reproducible.** A second assessment by a different set of evaluators should produce the same results.
- **Relevance.** IS*s should be useful to decision makers. Considerable discussion is related to IS* stakeholders: decision makers and the types of decisions IS*s support, and individuals and organizations supplying inputs to IS* evaluations.
- **Effectiveness.** It should be possible to evaluate the IS* quickly enough, and with low enough costs, for it to be useful to the decision makers who will use it.

Conclusions

Surprisingly common themes emerged from this workshop, summarized in the following conclusions:

- No single IS* will successfully quantify the assurance present in a system. Multiple measures will most certainly be needed and they will need to be refreshed frequently.
- Software and systems engineering are very much related to this problem. For example, the quality of software delivered, the architectures and designs chosen, the tools used to build systems, and the requirements specified are related to the assurance to be quantified.
- Penetration testing is in use today as a valid IS*. However, it is imperfect and to some extent nonrepeatable, but it is used in both government and commercial sectors.
- Government and commercial sectors have different agendas: the former is policy driven and the latter is profit driven. Thus, the two sectors may place different values on IS*s.
- Measuring defense in depth and breadth is a critical area that warrants further research.
- In the past, attempts to quantify and obtain a partial ordering of the security attributes of systems have not been successful to a large degree (e.g., the TCSEC and the CC).
- Processes, procedures, tools, and people all interact to produce assurance in systems. IS*s that incorporate these aspects will remain critical to successful IT system operation.

These conclusions indicate that the direct measurement of IS properties is desirable but not always possible. The assessment process should include activities for validating the indicator (e.g., by cross-checking it against other indicators). For example, an indicator of an organization's IS program might be the quality of its documented plans; under the assumption that an organization's commitment to information security will be reflected in its budget, an assessment of organizational plans could be correlated with financial metrics.

IS*s must evolve. A metric that is meaningful and useful today may be less relevant tomorrow, due to changes in technology, practice, or regulations. Organizational processes that use IS*s should include periodic reevaluation of those metrics and redefinition as needed. If metric evolution is not done deliberately, it will occur accidentally: the information that can be gathered will change with technology advances, and assessment that involves expert judgment will change as expertise increases. Care must therefore be exercised in comparing metrics values over time.

Organizational and operational IS*s have more in common with metrics from the social than the physical sciences. IS professionals should apply lessons learned from the social sciences, particularly from public health and safety risk management.

Better models of system behavior are needed to define predictive technical IS*s. In particular, better models are needed of the composition of (and dependencies among) subsystems that provide different security services.

Future Directions

An interesting debate influenced workshop discussions, based on each participant's objectives for attending: those who saw the workshop as a benchmarking opportunity to determine the state of measurement, rating, and ranking for the IA/security community claimed that the workshop met its goals and should stand on its own merit, while, in contrast, others believed that the workshop served a longer term purpose in the community.

As a compromise, this publication of the workshop *Proceedings* can serve as the baseline for future directions and target audiences can be reached via panel discussions at applicable technical conferences. These conferences include the Annual Computer Security Applications Conference and the Software Technology Conference. As long as diversity exists among technologies and implementation procedures, backed by the need for policy- and doctrine-mandated compliance, interested parties will want to assess the relative merits of systems and their applications.

1 Introduction and Conclusions

Introduction

In today's competitive and shifting information technology (IT) environment of networks, portals, and software component application servers, enterprises no longer question the need for IT security as a requirement for their enterprise IT architecture to provide information assurance (IA). However, the available security technologies for any one application suite are multiple and mysterious, not to mention costly and sometimes inconvenient to the point of crippling. The confluence of several such suites in an integrated environment is not only common but mandated in the enterprise, and these suites are often difficult to evaluate for information security (IS) characteristics.

The techniques of security metrics include product evaluation criteria identification, IS quantification, risk assessment/analysis methodology development, and other related activities. However, the drawbacks of these techniques have led to the widespread desire for a single number/digraph by which to rate/buy/commit to IT systems that are suitable for critical operation/improvement/retirement. Yet computer science has frustrated these activities by providing neither generally accepted nor reliable measures for rating IT security or requisite security assurance. Furthermore, inconsistent terminology usage has complicated the development of IT metrics, such as *rating*, *ranking*, *quantifying*, or *scoring* measurements.

To address these shortfalls in the IA area, a Workshop on Information Security System Scoring and Ranking was held in Williamsburg, Virginia, during May 21-23, 2001. This workshop was sponsored by the Applied Computer Security Associates (ACSA) and The MITRE Corporation. Participation in the workshop was limited to those who responded to the call for position papers. A total of 30 position papers were received and 34 participants attended the workshop. These papers were considered working drafts and were used to identify topics for discussion and to assist in developing the workshop structure. They were not presented at the workshop. Accepted papers were shared among the authors and made available at the ACSA Website. Additionally, a mailing list was formed prior to the workshop to stimulate further discussion and to solicit additional discussion topics.

Workshop Goals

The goals of the workshop were as follows:

- Clarify what researchers and practitioners are talking about when they refer to IS metrics.
- Debunk the pseudo-science associated with assurance metrics.
- Discover some indirect indicators of security.
- Precisely define the research problems in developing IS metrics methodologies.
- Recap the latest thinking on current IS metrics activities.

- Identify efforts that are successful in some sense, if they exist, and if none exist, reduce expectations on what might be achieved through IS metrics.
- Explore the unintended side effects of ratings/measures (e.g., inflating the numbers to ensure promotion, delay review by higher authority).
- Clarify what is measurable and what is not.
- Scope and characterize the measures to be addressed and explain what happens when several of these measures/applications co-exist in the same enterprise: Do they augment each other or cancel each other out?
- Describe how measures should be used in the context of IS, especially to influence purchases and for general resource allocations.
- Identify misapplications of measures, including their description as metrics.

Not all the above goals were met, as will be reported in these *Proceedings*, but the workshop, as a whole, was successful in focusing attention and discussion on this important and underserved topic. Progress in the area of information security metrics or measures for IA has been slow to non-existent over many years of effort. Follow-on effort is clearly needed and additional research warranted.

Terminology

The workshop organizers recognized that considerable controversy exists regarding the term *metrics*: some seek to reserve it for the results of measurements based on scientific principles, but others use it to include results of assessments based on subjective judgments. While some position papers urged reliance on a dictionary or scientific definition, others observed that broader usage has been adopted in policies and practices. As some past discussions on metrics had been totally consumed with this discussion, the expression *information security (IS)** was used in the workshop agenda to avoid long discussions on terminology, as defined below:

An IS* is a value, selected from a partially ordered set by some assessment process, that represents an IS-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence.

Although participants gravitated toward use of the terms *IS metric* or *IA metric*, we will use *IS** in these *Proceedings*.

Conclusions

Several surprisingly common conclusions emerged from this workshop. Regardless of whether working groups focused on technical, organizational, or operational metrics, or on the synthesis of these metrics into a meaningful aggregate, the same themes occurred with striking regularity. A summary of these conclusions follows:

- No single IS* will successfully quantify the assurance present in a system. The problem is far more complicated than that and the stakeholder community is much

- too diverse. Multiple measures will most certainly be applied and they will need to be refreshed frequently.
- Software and systems engineering are very much related to this problem. The quality of the software delivered, the architectures and designs chosen, the tools used to build systems, the specified requirements, and other topics are all related to the assurance we try to quantify.
 - Penetration testing is, today, a valid IS*. It is imperfect and to some extent non-repeatable, but nonetheless it is used in both government and commercial sectors. Several IS*s relate to such testing: level of effort, number of vulnerabilities found, number of penetrations, number of vulnerabilities not found, and more.
 - A difference exists between government and commercial sectors regarding IS*s. One is policy driven and the other is profit driven. One has the force of law, while the other has the force of its stockholders. These variables may result in different values placed on IS*s between the two sectors.
 - Defense in depth and breath is important. Knowing how to measure this defense is also important and is a related research area.
 - Attempts to quantify and obtain a partial ordering of the security attributes of systems in the past have not been successful to a large degree. Examples are the *Trusted Computer System Evaluation Criteria* (TCSEC), Department of Defense (DoD) 5200.28-STD; and the *Common Criteria* (CC). It remains to be seen if this trend will continue.
 - Processes, procedures, tools, and people all interact to produce assurance in systems. IS*s that incorporate these aspects will remain critical to successful IT system operation.

Structure of *Proceedings*

These *Proceedings* consist of the following five sections and four appendices:

- Section 1: Introduction and Conclusions
- Section 2: Workshop Organization
- Section 3: Working Group Reports
- Section 4: Suggested Research Areas
- Section 5: Future Directions
- Appendix A: Agenda
- Appendix B: Position Paper Summaries
- Appendix C: Related Measurement Activities
- Appendix D: Glossary

2 Workshop Organization

The workshop was divided into four tracks and each track into four working group sessions of approximately three hours each, for a total of sixteen separate sessions. Attendees were assigned to a specific track but not placed under any strong obligation to keep that assignment throughout the workshop. Each track was given a specific topic direction and each session within that track was provided with a refinement of its topic for each session. The detailed topics and working group session organization are provided in Appendix A. Track focus areas were provided to the working groups as follows:

- **Track 1: Technical.** IS*s of technical objects, at different stages of the system life cycle.
- **Track 2: Organizational.** IS*s of organizational programs and processes, for different organizational scopes.
- **Track 3: Operational.** IS*s of operational systems, environments, and operating practices.
- **Track 4: Brainstormers.** Synthesis, cross-track issues, and big-picture concerns.

Each of the four working group sessions had a particular overarching theme, as follows:

- **Session 1:** Answer the following questions: What are we talking about? Who needs (or wants) IS*s? Why do they need IS*s? How will IS*s be used? What constitutes an IS*? What are some examples that can be used to anchor further discussion?
- **Session 2:** Focus on needs and good practices I.
- **Session 3:** Focus on needs and good practices II.
- **Session 4:** Identify research needs or directions.

Key discussion points from each track are presented in the agenda in Appendix A. In some cases, the tracks strictly adhered to the agendas. In others, the discussion evolved beyond the track structure and digressed. Section 4 presents the compilation of research areas suggested by the working groups. The next section summarizes the working group reports.

3 Working Group Reports

Track 1: Technical

This track addressed the measurement of technical objects at various stages of their life cycle. Technical objects are components of security architectures, such as operating systems, database management systems, firewalls, and intrusion detection systems. They are the building blocks of secure systems. Discussions focused on how technical objects should be measured. An important area of consideration for technical objects is how the security properties of the objects vary over the technology life cycle. For example, a system deemed “highly secure” at its product release may become increasingly vulnerable to attack as it gains market share.

Initial discussions addressed the drive to use ratings and rankings for IA. One’s definition of a measure or metric depends on how one wants to use it. To date, there is no basic unit of measurement for security. A system is considered highly secure, moderately secure, or insecure. For example, the TCSEC characterized systems based on their ability to combine various security features into a cohesive, functional unit.

One way systems were measured in the TCSEC was based on how resistant a system was to penetration testing. For example, a system was deemed reasonably resistant to casual penetration or highly resistant to a concerted penetration attempt. There was some discussion that the best metric to date is based on penetration testing. However, previous experience in penetration testing has not been captured, and the lessons learned are not methodically recorded. Further, it would be useful if there were an ability to order the relative results so one could determine if a given technical object was “more secure” than another.

As a result, metrics tend to emerge from *Consumer Reports*-like processes, Designated Approving Authority certification, and penetration testing. These processes tend to define qualitative measures of the relative goodness of a system. We have specifications about what to measure, but no information on how to measure it. We do not have quantifiable evidence, only anecdotal evidence. We have a lot of measures and specifications of what to examine, but no assurance that what we are measuring is actually addressing assurance shortfalls.

The security marketplace was discussed. For example, there is no perceived pressure on vendors to produce better or more secure systems. For the most part, users place functional, mission-oriented requirements ahead of security functionality and assurance mechanisms. There is some inherent demand for security products, and there are vendors making a profit on security mechanisms and producing secure technical objects, such as firewalls, virus detectors, and virtual private networks.

One result seems certain: the actual costs to the business community due to poor security and assurance products are beginning to get high enough that they cannot be ignored. The amount of time spent countering worms and virus attacks, the business loss associated

with denial-of-service events, and the embarrassment of procedural security lapses all impact the bottom line of an organization. Therefore, the business community requires some way to measure the assurance associated with its systems.

From this starting point, the group moved on to devote the next discussion to addressing why we need to measure, what to measure, and who is the recipient of measurements, focusing on needs and good practices. It was also determined that we must answer the following question: Have we looked at the right things to make the security determination/decision we want to make? The determination to be made changes as one changes perspective in an organization (e.g., the system administrator's perspective is different from the business owner's perspective).

Another question that needs to be answered by the IS* follows: Is this system secure enough for my needs? The answer to this question could become the ultimate goal of the measurement process. For example, in the current environment, one can obtain a score against a checklist of processes, procedures, and parameter settings. Based on the percentage of checks generated against such a list, a system can be rated "secure enough" for a given application.

The result of such a checklist-type exercise is still the same: there is little impact on the overall security posture of an organization. Today's accepted commercial practices for development still result in relatively unreliable, insecure systems, and measuring how insecure those systems are does not improve the security posture. IS*s that can provide meaningful feedback on how well a product or process is performing to maintain the system's security posture would be useful.

To be useful from a security perspective, one must determine the object to measure and then the metric that ties the object to the security objectives. For example, it is likely that one would start with the security objective to be met, then determine what objects need to be measured to determine if the objective is met, and then determine what methods will be used and what steps will be taken to measure the ability of these objects to meet the objective.

The discussion continued with added emphasis on testing, certification, accreditation, and operations and maintenance. Although testing in general was debated as a valid path to useful metrics and measures, the discussion migrated more toward penetration testing and vulnerability analysis as potentially fruitful areas. In particular, the *Consumer Reports* kind of rating, mentioned above, was also discussed as having merit.

A pessimistic assessment was that the topic of IS*s is a red herring, designed to confuse people so they do not understand how bad the state of the practice really is with regard to IA. The thought is that by focusing on measurement of assurance characteristics, we are diverting resources from the actual problem, which is managing system development and operational procedures well. The success of this approach is not so much technology dependent as it is expertise dependent, in which case better trained security engineers and more resources are necessary than are presently expended to resolve the problem.

To follow up on the argument for the use of layered defenses, the secure state of a system is dependent on a sum-total, holistic approach that includes technical, procedural, organizational, personnel, physical, and other forms of security. This is why a single measure or metric seldom makes sense. Giving a system a single score to reflect the aggregate of all forms of security may be counterproductive and artificially inflate or deflate the actual security posture of a system.

In examination of the commercial security marketplace, there are few distinguishing characteristics among products in a single product family. For example, a firewall is considered a firewall. Vendors rarely make the claim that “brand X is more secure than brand Y.” In essence, once the basic functionality is present, products providing a given countermeasure become almost interchangeable, with little differentiation in the marketplace. This leads to a model that provides no incentive to produce “more secure” products or make the existing products trustworthy. Even the threat of a concerted information warfare attack does not motivate either the vendors to build better products or the consumers to demand them.

Vulnerability analysis, applied in conjunction with penetration testing, seems to be one of today’s more common assessment measures. Penetration testing is used during the development process, as part of certification and accreditation, and to reflect the current operational state of a system. Process-based penetration testing (methodically conducted and repeatable) versus ad hoc penetration testing is the only resource available to accurately assess the state of a given system. While there are issues of comparison or ranking associated with differences in personnel or time between penetration tests, as a whole the group agreed that it did represent the most accurate way to assess the state of a given system.

The use of IS*s can contribute some insight and standardization to the assessment activity. For example, a structured, repeatable engineering process for combining measures and developing an overall holistic conclusion would go a long way toward making IA more a process than a black art. A common language that bridges the communications gap between the security technologist and the decision maker who decides a system is “secure enough” would be another step in the right direction.

In short, security is really the combination of three basic properties:

- What I have
- What I use
- How I use it

Methods of assessing the relative security of a system involve examining its properties, studying the system characteristics about which information is being collected during the assessment, and, if possible, combining these results into a single meaningful measure obtained from the collected data. It may not be feasible to aggregate a single measure, for

the resulting measure may be extremely vague. In this case, the simplicity of a single measure greatly dilutes the impact of a security assessment process.

In reality, this is no different from traditional resource management problems regarding resource allocation. It just happens that, in this case, the resource being managed is the security of the system. Therefore, standard resource allocation management measures should apply.

The working group felt it necessary to comment on the current state of security metrics. Long-time engineering disciplines have measurement techniques that work. However, much of the commercial marketplace is building software on “Internet time” as an art form instead of as a disciplined science. So while exceptions exist, they are indeed exceptions to commercial practice.

A contributing factor to the lack of security metrics is caused by disagreement among technical people about what is needed to define a set of repeatable IS*s. For example, it is unclear whether a set of security measurements should be placed into effect during the development process or whether treating software development as a disciplined science would resolve a large proportion of perceived security problems.

For each assurance level or amount of confidence a consumer has that the security mechanisms are working effectively, there is a corresponding level of engineering discipline that is required to implement and measure that assurance level. It is not sufficient to claim implementation of a given level of assurance. A disciplined, repeatable process to validate this claim must exist. There is a struggle that exists in organizations between system functionality and system security. The general rule has been that among security, functionality, and performance features, two out of three are possible in any given system design. Most of the time, functionality that is visible to the consumer wins out over the “invisible” gains in assurance that the system performs correctly.

Of particular note, similar problems exist across multiple levels of the management/technical chain. From the hands-on system administrators to the Chief Information Officer (CIO), the lack of cost/benefit analysis data supporting capital expenditures in security countermeasures represents a major challenge. With a relative lack of data on what is considered “secure enough” for a given system, an organization has a difficult time justifying additional expenditures for enhanced security capabilities.

Based on the current state of affairs, several basic needs must be addressed to improve the posture of technical assurance measures. A series of translation mechanisms is needed to facilitate communication with management and also increase the objectivity of assurance measures. The majority of the working group suggested a primary focus of technical efforts to be the latter. For example, simply stipulating security objectives and defining a common basic set of terms used would greatly facilitate the communications process.

Measurement implies a discrete function. It may be more a case of deviation from defined best practices in security, which is a much more subjective measure. This leads to a need to differentiate between objective and subjective measurement techniques. The working group agreed that consistency is a more significant issue than the objectivity/subjectivity of a given measure. This raises the question of how a subjective measure can be considered consistent or repeatable, especially if multiple groups with differing agendas apply the measure. Gaining repeatable results in measurement techniques was deemed a much higher priority than deciding if the measurement technique should be objectively or subjectively based.

The ultimate goal of any security measurement is whether or not a Technical Object (TO) meets its security objective (SO): $O \geq SO$, where $O \geq SO$ is defined as:

$O \geq SO = F(\text{set of } f_D, \text{ set of } f_I)$, and

f = method to measure

D = direct measurement techniques

I = indirect measurement techniques

And F is the function that combines the results into a single statement of the security capability.

It should be noted that there are multiple abstraction levels for IS*s, and they should probably occur in a consistent order. For example:

Top-level combination function F

Next level – set of methods used to create function F

Third level – defining a relative measurement from a method or set of methods

Fourth level – defining a consistent measurement from a method or set of methods

Track 2: Organizational

The purpose of this track was to examine the characteristics of and the needs for IS*s of organizational programs and processes. As is normal in working group discussions, participants initially addressed the following question, What are we talking about? Some observations about measuring the IS posture of an organization evolved from considering that question. Two kinds of questions are normally asked when measuring the information security posture of an organization:

- How well are we doing (or, Are hackers successful or not?? This question has two corollary questions associated with it: How much security does a given organization require? What is the “threshold of pain” associated with that set of security countermeasures?
- How well is the organization doing at meeting the security mandates specified by management?

Commercial organizations tend to focus on the former question (How well are we doing?), while government organizations tend to focus on the latter (Am I meeting my security policy mandates?). Complying with all mandates does not necessarily mean an organization is secure, however. The point was made that in providing security to an organization, the job is never complete. It is a dynamic process, not a static one. Just because an organization's policies and procedures are all in place does not mean that the security posture is correct or complete. Continuous risk management is necessary; there are always new threats and new technologies to address.

The requirements for establishing an enclave/enterprise, and determining the boundary of an organization, need to be addressed. This is especially true in the context of trust relationships that may extend to other companies, suppliers, and customer organizations. In these cases, it may be necessary to establish service-level agreements to manage risk among various organizations, systems, and networks.

The working group also addressed the question, Who needs IS *s? All agreed that the answer is certainly government managers who are driven by relevant regulations/policies. An unanswered question remains: What are differences in the needs between government and commercial industry? It is thought that decision makers at all levels need IS*s to determine where to allocate information security resources (e.g., money, people, hardware/software).

Also, accountability is an issue. Top management sets the tone, and their involvement is a foundation for providing information security. Management must realize that security as an integral part of business, not a separate set of functionality that satisfies some legislative requirement.

The working group next addressed the question, Why do we need IS*s? Increased complexity of systems and the difficulty associated with uniform system management were two important reasons. Supporting needs follow:

- Desiring to improve information security within an organization.
- Ensuring that the United States does not lose the information war.
- Reaching the goals of staying in business, continuing to make money, and retaining current/future business.
- Ensuring that future IS requirements manage the consequences of the current IA posture (that is, if you don't do A, B may happen).
- Defining what is most important to an organization: How much is it going to cost me? When am I going to see a profit? How much am I going to make? What is the "who cares" factor (if we spend XX dollars and the script kiddies still get in, where is the value in that)?
- Knowing that sharing of information within the hacking community provides a force multiplier for script kiddies trying to compromise systems.

The facilitator discussed major components of the information environment. In a working information environment, we need to examine all of the connection points. There are

multiple areas to address in an information environment's defensive countermeasures. These areas must be organized so they can be deployed in a synchronized and coherent fashion. Defense in depth requires the integration of multiple information security disciplines. Capabilities must be analyzed from the organization's center outward to each employee or trust relationship. The full threat spectrum must be considered. Major IA shortfalls include the lack effective baseline or configuration management associated with an enterprise, no real-time automatic discovery of attacks or intrusions, no capability for modeling and simulation of an attack and the primary, secondary, and tertiary cascading effects it may cause, and no effective valuation of potential information compromise.

Information valuation is a difficult problem in that it must include all interests and must balance the valuation against the organization's priorities. Information value is located in the links and nodes that comprise the network. Information has associated with it various costs to acquire, store, and maintain it. A possible formula for valuation was proposed based upon variables such as content, context, timeliness, security aspects, and effect on operations. Accounting standards, qualitative formulas, and metrics for the value of information need to be developed. The real question is what organizations wish to accomplish in terms of information valuation capabilities. Possible answers are:

- Determine valuation of information.
- Determine an organization's relative information protection posture.
- Determine how an information protection posture needs to evolve.
- Identify what constitutes a successful information protection posture.
- Develop information protection improvement programs to achieve greater success.
- Implement these information protection programs.
- Measure the progress of improvement.
- Develop programs to maintain a successful information protection state.
- Enact and monitor continuing protection improvement programs.

There was a consensus in the working group that the emphasis should be primarily, but not solely, placed on decision support. Information is most valuable to decision makers and researchers who provide the information necessary to support those decisions and operational processes.

The working group attempted to focus on what we can learn from relevant documentation, such as the *System Security Engineering Capability Matrix Maturity Model* (SSE-CMM) and the *Federal Information Technology Security Assessment Framework* (FISAF). A question arose as to whether the focus was on information protection or protection of the information process. Attendees suggested that protection of the information process is the objective, not protection of the information. Some values of information are context sensitive or dependent on the perspectives of the various stakeholders of that information. IA should be viewed in the context of gaining competitive advantage for the stakeholders in that information.

Also examined was the programmatic and process IS*s for organizations that seek to defend themselves (i.e., users of IT). One can examine IA objectives in the following order: the objective, the supporting principle for the objective, and the mechanism to implement it. Examples follow:

- Objectives: confidentiality, integrity, availability, authentication, and non-repudiation
- Principles: continuity of operations
- Mechanisms: backup and recovery

For IA, principles are needed and perhaps could be better termed as guidance. The guidance is violated after analysis and weighting of options with the understanding that risk must be accepted. Guidance and criteria need to be self-correcting, that is, they must maintain currency with the evolving threats, vulnerabilities, and changes in technology.

A common lexicon should be established for use between management and IA technologists and practitioners. Cost, return on investment, loss avoidance, and lost productivity are examples that need to be associated with IA principles to provide the rationale of IA impact on business practices and on the corporate bottom line. Terms are frequently used erroneously. For example, high reliability in a system architecture is not equivalent to architectural robustness. Business need to determine a threshold of pain, expressed in terms of lost revenue or productivity, above which it is willing/not willing to self-insure and invest in IA?

A point of departure for linking metrics to principles/guidance may be reached by answering the following questions: Are we complying with standards for security? Are we doing well enough? What are we not doing? Should the answers be a binary “yes” or “no,” based on a scale, quantifiable metrics, or a combination of these? It may be possible to develop measures of compliance with guidance and doctrine, measures of adequacy associated with such guidance, and measures of effectiveness to support due diligence in measuring compliance. There are two types of measures in this case. Measures of collection are relatively easy to define and capture, whereas measures of effectiveness or adequacy are orders of magnitude more difficult. The following definitions for measures of effectiveness and measures of adequacy are offered for the reader’s consideration:

- Measures of Compliance—near static, but evolve:
 - Example: Organizations shall have effective audit policies.
 - Example of implementation practices: Audit policies will exist. Assets requiring audit are identified. Types of information to be collected are identified. Audit trail is protected.
- Measures of effectiveness or measures of adequacy—dynamic:
 - Example: A sufficiently broad audit archive should exist to flag intrusions and to support law enforcement forensics. The fraud control and prevention community has effective time-tested definitions and metrics that can be adopted by IA. These capabilities can provide acceptable deterrence, especially against the insider threat.

To translate between management and IA concepts, the concept of cross-walking or bridging terminology across the two communities was discussed. A representative example of cross-walking important management and IA concepts appears in Table 1.

For example, the high-level concept, “detect an attack,” is understood by management as a worthy pursuit. The purpose, defining a good security principle, is to collect data that potentially represents a malicious activity. In security policy terminology, that translates to auditing: the security auditor’s terminology would be fraud detection. The measures of evaluation would be the determination if sufficient evidence existed for prosecution and the adequacy of that evidence. The potential cost associated with such a concept would include the configuration of audit trails on enterprise devices, such as servers, firewalls, and routers, plus long-term storage of audit records.

In a similar manner, the other concepts associated with this table could be expanded to represent cross-discipline understanding of what a high-level concept or policy statement means to the various groups of stakeholders, how it should be measured to fulfill their expectations, and the associated cost of addressing a given high-level concept.

Track 3: Operational

The first discussion addressed the characteristics of, as well as the needs for, IS*s for operational systems. The commercial and government perspectives need to be examined and treated separately because different motivations and objectives affect each sector. The government is more concerned with rules, regulations, processes, and protection of assets in setting policies. Commercial businesses must relate expenditure and effort to impact on profitability and stockholders.

For example, mergers of two enterprises are relatively frequent occurrences in the commercial sector. In this case, the security organization can never make progress in merging the two enterprises unless each can explain its security posture in sufficient detail that accountability to the appropriately responsible person can be maintained (i.e., the other person’s responsibility takes over).

DoD tends more toward the use of static measures (bean counting); in fact, one of the working group members thought that there were some 15 formal measures that DoD uses (but no reference was provided). A more dynamic measure might be the result of penetration testing. Measures defined to take advantage of the results of penetration testing will involve time and a certain amount of subjectivity.

Table 1. Example Cross-Walking of Management and IA Concepts

| High-Level Concepts | Purpose: Define What Is a Good Principle | Principle | Security Mechanism | IA Measure/Metric (Measure of Effectiveness) | Potential Cost/Impact |
|----------------------------|---|--------------------------|---------------------------|---|---|
| | | Incident Response | | | |
| | | Configuration Management | | | |
| | | Continuity of Operations | | | |
| | | Access Control | | | |
| | | Training | | | |
| | | Authentication | | | |
| Detect an Attack | Collect data of potential malicious activity | Auditing | Fraud | Do we have evidence for prosecution? Determination of adequacy. | Audit configuration, short- and long-term storage, retention policies |
| | | Forensics | | | |
| | | Computer Network Attack | | | |

The problem can be thought of in terms of software engineering. The provision of security in a system is a nonfunctional requirement that must be built into it. Even so, software engineers never claim 100% reliability. The same is true with IA: we can define point measures and, with enough point measures in place, we feel more comfortable with the security of the product.

The characteristics of and needs for operational systems include supporting decisions with measurements and evidence so that an organization can determine that it is applying resources against risk correctly. A Chief Executive Officer (CEO) wants to know how much security is obtained per dollar invested. In looking at operational systems, one generally wants to know what is the level of security today versus what it was yesterday.

With respect to what we may be looking for in an IS*, the working group identified the following observations:

- Measurements should have attributes with a common set of evaluation characteristics: repeatable, reproducible, objective, timely, cost-effective, accountable, and composable.
- A multidimensional measure may be the best approach.
- An IS* could be simplified based on how well the boundary to a system is controlled.
- A measure should be a means for communicating among various system stakeholders.

The group also considered IS*s within the government sector. Specifically, what are the needs and practices for assessing informal programs and processes versus those for formal ones? How can one assess what is real and what is documented (rhetoric versus reality)?

The first line of system defense is the system administrator. A need exists to define the System Administrator (SysAdmin) functional qualifications (such as training) and the procedures for replacement, backup, and retention of SysAdmin personnel. This activity includes defining a model for adequate SysAdmin coverage. The data regarding how many SysAdmins are needed for adequately performing the tasks needs to be collected and validated. A training or certification program to ensure the capabilities of a given SysAdmin is necessary. For example, there are several SysAdmin training and certification programs but there is no apparent convergence on a particular program. No known model for ensuring a comprehensive set of technologies, policies, and procedures is in place for SysAdmin personnel.

The working group agreed that more attention needed to be devoted to the following issues:

- The linkage between organizational IS*s and organizational processes (security policies/processes, funding, resource allocation, reporting, accountability) and requisition/procurement approval authorities (upper management) needs to be better defined.
- The entire issue of how security metrics integrate with the organizational decision process needs to be explored. For example, organizations frequently race after new technology (e.g., wireless systems) for enhanced functionality without fully considering the possible security risks.
- The mechanisms and techniques to encourage information sharing among organizations need to be refined. Security information needs to be shared among industry and government representatives, but without compromising the privacy of any participating entity.

Next members addressed operational IS*s for the commercial sector. Specifically, what are the needs and practices for assessing informal programs and processes versus those for formal ones? How can we assess what's real as well as what's documented? What is rhetoric versus reality?

The discussion led to the conclusion that established processes for commercial IT modernization are much more rigorously followed. An enterprise-wide, bottom-line focus creates an environment that focuses on end-to-end system performance with appropriate security measures incorporated into the architecture. This type of environment also leads to well-defined IT requirements, specifications, and engineering, with self-disciplined user compliance that emphasizes predictable results.

Given that the working group considered the commercial development cycle as somewhat different from the government's development cycle, another discussion addressed the commercial IT modernization cycle. The IT modernization processes for a government program and a commercial business case are similar in structure: requirements identification, approvals, development, and installation. For both, processes that are established contain procedures with separate approval points. Information security is not treated as a separate program/business element but is a mandatory element of any program/business case.

Both the government and commercial development cycles rely upon the use of similar internal/external auditors, penetration testing, and configuration management procedures. One key distinction between the two sectors that would account for the perceived speed of the commercial IT modernization cycle was the reliance on the personal judgments of the security practitioner. Due diligence on the part of individuals is expected and forms the basis for management approval. This practice contrasts with the more structured, organizational approval processes in government.

The emphasis on standardized processes, whether for macro enterprise decision making or micro user rules for system operation, is based on the belief that all processes should be documented and everyone should know where to go for answers and assistance. Enterprise-wide standard processes imply an emphasis on configuration management of and strict adherence with the processes.

In summarizing the differences between the government and private sectors, it was pointed out that commercial enterprises could shield the proprietary parts of their business using off-line or protected systems. The government might have better security models than commercial enterprises that have extensive interfaces with the general public (e.g., Amazon, eBay, VISA, American Express).

The discussion concluded with a look at what might be needed for operational security IS*s in the commercial sector. A quantitative approach to current operational security IS*s would have a tendency to count negative things that have happened. A qualitative approach might look at the potential for security violations in a system or process and act accordingly. This approach would encourage performance IS*s and not the more traditional compliance IS*s.

A different approach was the suggestion that operational security IS*s might be more process oriented. Assuming that security policies and procedures have been well thought out, what is required is the assurance that the processes are being followed and, therefore,

that the operational security need is being met. This would require a process-oriented approach and not a more traditional compliance-oriented approach.

A key IS* associated with a good operational security environment is the ability to revoke privileges rapidly. Such an environment would allow the security team to anticipate a security situation, be able to rapidly assess the implications, and quickly adapt. Therefore, processes and IS*s associated with continuity of operations and disaster recovery might provide some insights.

The discussion pointed out that one shortfall with current hardware and software products is the lack of an ability to monitor operational performance (i.e., that there are no observable operational IS* parameters. The few types of operational IS* parameters that are available are associated with audit logs. These logs tend to discuss the external environment but provide no information on the internal operation of the product. Operational IS* considerations could logically lead to a need for the following capabilities:

- Ideally, full transparency with the operational processes, preferably based on open standards and open software, that would allow for the full auditing and reconstruction of all events associated with a given process.
- Some way to translate operational security policy to configuring the network security devices, such as the audit log. An alternative would be to record everything and configure a filter through which to view the information. This policy translation would not be limited to audit logs; it should be extended to setting policy on distributed firewall devices, the main firewalls, and guards, for example.

If these capabilities are possible, then this type of approach could change the paradigm for operational security IS*s. For example, with greater transparency in the operational process, we could look at access to a database without authentication and improve the quality of the authentication operational process to six-sigmas, or essentially zero. Thus, the government could associate digital signatures with need-to-know authorizations and drive anomalies to zero.

This discussion concluded that operational security IS*s were viewed more as a qualitative, process-oriented issue. There was a sense of the need for a checklist of separate procedures (for contingencies, normal operations, initialization, reconstruction, and incident handling) that are validated as achievable, with optional weightings of importance (i.e., processes of established security rules). Each process would have its own built-in IS*s or allow feedback indicating how well the process is working in terms of security.

The next discussion focused on answering the following question: If IS*s cannot be measured directly, could any measures serve as proxies or surrogates that can be collected? The argument ultimately depends on having a good model for how all of the different factors interrelate. There is the consideration that one of the key IS* attributes is

the value we put on the reputation of the evaluator. At least in some environments, there is a tendency to trust the answer more based upon the reputation of the evaluator.

The existence of surrogate IS*s implies the presence of both direct and indirect indicators of operational security. The overall security process of the commercial sector follows:

- Strategy
- Policy
- Awareness
- Implementation
- Monitoring
- Compliance
- Periodic assessment

For example, the process implies that there are direct indicators of an effective information security policy (e.g., the policy covers all systems) and indirect indicators (e.g., the policy is/is not being followed). Examining IS*s in terms of direct and indirect indicators moves the evaluator/evaluation to within three steps of the target objective. Building on this approach, Table 2 identifies typical direct and indirect indicators of IS*s.

Table 2. Typical Direct/Indirect IS* Indicators

| Activity | Direct Indicator | Indirect Indicator |
|-----------------|---|--|
| Strategy | Mission, vision, architecture | Resources |
| Policy | Covers all systems | Followed |
| Awareness | Certifications | Formal awareness programs. Good collaboration schemes across economic sectors or like entities. |
| Implementation | SysAdmin body counts | Tools/references available |
| Monitoring | Real-time alerting/reporting, log availability, tool-based automated reports | Tested procedures, audit logs, self-assessment tools, and checklists. Self-assessment to cover all direct and indirect indicators (suggests the desire to tailor the Monitoring activity). |
| Compliance* | *External checks on processes (external to operational process), including third-party independent checks. Internal checks come from the Monitoring activity. | |

The working group received a briefing on the ESOPE security tool with respect to research efforts. ESOPE is a prototype operational security tool that has been in development for some time by a team led by Yves Deswarte.⁹ Points made during the briefing are outlined below:

- The measurements delivered by security evaluation tools should represent as accurately as possible the security of the system in operation (i.e. its ability to resist possible attacks or, equivalently, the difficulty for an attacker to exploit the vulnerabilities present in the system and defeat the security objectives).
- Current vulnerability scanners approach this problem by building a database of all known vulnerabilities and scanning the system for them.
- The ESOPE approach looks at the operational security problem in terms of (1) the point of view of the threat (e.g., tenacious-lazy, focused, unfocused), (2) the main security objectives and not every minor vulnerability, and (3) the need for security to evolve as the system evolves, through modifications and upgrades, understanding security is not absolute but is either improving or decaying.
- ESOPE has a theoretical framework to identify and compute such operational security measures based on the following items:
 - A theoretical model exhibiting the system vulnerabilities
 - A definition of the security objectives
 - A mathematical model based on Markov chains to compute the security measures

Track 4: Brainstormers

Brainstormers were expected to deviate from suggested themes. The overall theme assigned to this track was “synthesis, cross-track issues, and big-picture concerns.”

A collective decision was made to apply a systems engineering approach to aggregate measurement, as this would accommodate the complete system life cycle. That is, technical, operational, and organizational measurement techniques and IS*s could all be integrated into this framework most effectively. If this exercise was successful, it should be possible to generate the characteristics of the various IS*s.

The working group decided that the best approach to take was to characterize the various stakeholders in IS*s. Realizing that different groups of consumers have different requirements, the group considered the various types of consumers to determine possible requirements. For example, consumers want security delivered as promised. In both the government and commercial sectors, these consumers included management, technical, and administrative personnel, which each have a different interpretation of how security is defined and how it is delivered.

⁹ R. Ortalo, Y. Deswarte, M. Kaâniche, *Experimenting with Quantitative Evaluation Tools for Monitoring Operational Security*, Rapport LAAS N°96369, 6th IFIP International Conference on Dependable Computing for Critical Applications (DCCA-6), Garmisch, Germany, 5-7 March 1997, pp. 289-310.

The group adopted the term *information value* to identify the person who may “get hurt” or be damaged in some way if something undesirable (e.g., loss of confidentiality, availability, integrity, or non-repudiation) happened to his/her information. This terminology designation led to a debate that the working group might be missing the entire lifecycle/systems personnel orientation. This debate resulted in a discussion of a three-dimensional model of the various aspects of a system. In this model, the information, information system, and the information *evaluator* are placed on the three axes. Figure 1 illustrates this representation. In this case, the problem becomes simpler if the information is not dynamic in nature, which would result in an N-dimensional context. The ideal situation would be to enter the information once and then apply it to several different scenarios.

The group decided to use the stakeholder framework as the basis for its brainstorming activity. The thought was if a list of stakeholders and their expectations from an IS* perspective could be defined, then perhaps a list of viable IS* measures could be generated.

Discussion then focused on the topic of defining stakeholder requirements for IS*s in the information delivery pipeline. The working group felt that establishing IS* requirements for a given stakeholder essentially amounted to identifying risks, where *risk* is defined as a function of the harm caused by a security breach and its likelihood. Different stakeholders require different types of IS*s at different levels of abstraction and in different formats depending on the stakeholder’s domain of responsibility.

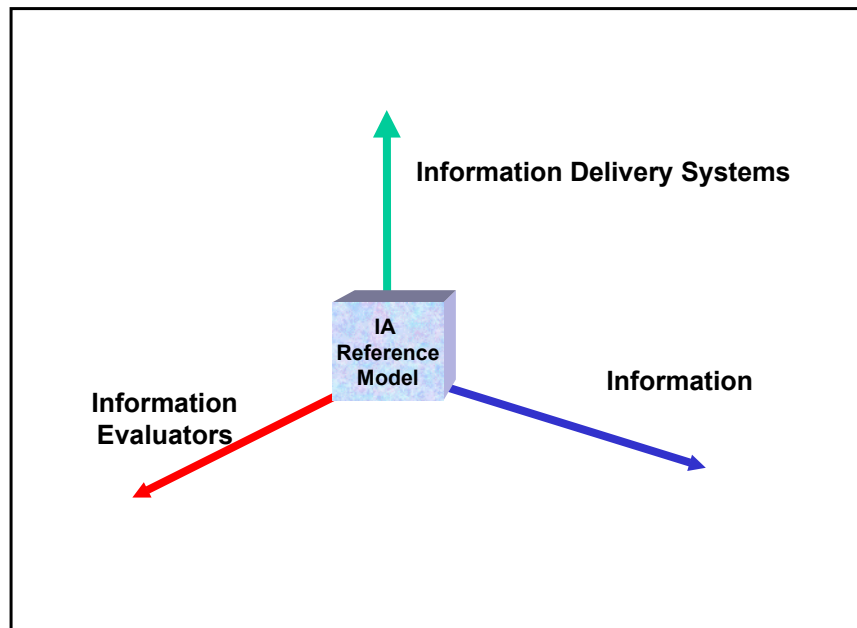


Figure 1. Three-Dimensional Information Access Model

IS* requirements for the information valuee, as well as other stakeholders, would be defined at a higher level of abstraction. The information valuee would require (a) a list of ways of being hurt (relative to the information valuee's mission requirements) and for each way of being hurt, the aggregation of {(b) likelihood, (c) impact} at any particular time. This same identification of requirements could probably be extended to all stakeholders in some form.

The group moved on to consider system administrators and their management chain, including what became known as the *C-people*: CIO, CFO, CTO, CSO, and CKO. The system administrator's responsibility was conceptualized as translating security policies into discrete machine languages and procedures and in this way ensuring enforcement of the policies. To properly carry out his/her responsibilities, the system administrator needs information from the information valuee as well as policies from others. Thus, in addition to requiring IS*s to measure the security state of the system, they also inherit requirements—the (a)s and (c)s—from others. At this point it became clear that any systematic high-level description of stakeholder requirements would involve chains of inheritance from other stakeholders and that the complete IS* requirements in any given context could be “rolled up” the chain of stakeholders.

The group briefly looked at the stakeholder issue from a different perspective, that of an information life cycle which characterizes information from production or collection through processing and storage to destruction. This discussion prompted an attempt to place or define the information valuee in the context of an information life cycle. Is the data producer equivalent to the information valuee? Does information producer imply a different granularity or format with respect to IS* requirements?

Working group members also spent time on refining earlier ideas with respect to mapping IS*s to stakeholders. The term *valuee* was not understood in the plenary session in the opinion of the group. The term was introduced in an attempt to make sure that all stakeholders of an IS* system are considered. However, after considerable debate, the group could not agree on a single definition. The term *intermediate users* (e.g., Internet Service Providers, database companies, servers) was introduced to describe those who provide services to store, move, and manipulate data as a commodity (i.e., data handlers). They have a different set of requirements for IS*s.

The group agreed on the need for an integrated security approach (and integrated IS*s) for an organization or a system. Some common needs exist for standards in general, which also apply to IS*s, specifically, usefulness, usability, acceptance, and credibility.

Public relations advantages could be realized in publicizing an organization's security policy/posture. However, revealing too much information can be harmful to competitive advantage or can lower IS*s by revealing special security features.

Mapping of Metrics to Stakeholders

This discussion addressed the mapping of existing practices to the previously created stakeholder lists and stakeholder needs. The chosen approach was to go through the list of current practices, evaluate them from the point of view of usefulness, and map the practices to stakeholders. An attempt was made to determine the extent to which these practices provide value and capabilities for the stakeholders and to identify the gaps between existing practices and what is needed. Where applicable, shortcomings would be cited. It was agreed that *no single item in the list below address all needs of a single stakeholder.*

Trusted Computer Security Evaluation Criteria/Trusted Product Evaluation Process (TCSEC/TPEP):

- Are useful for testers and product assessors, as they are supposed to meet the needs of product developers.
- Do not meet the needs of valuees, C-people, and system administrators in terms of being practical and easy to execute.
- Address a cross-section of stakeholders and respond to some needs very nicely but placed undue burden on other stakeholders.
- Can be considered a subset of the *Common Criteria* (see below). The TCSEC can fit the notion of protection profiles (for example, for B1, B2, and C2 systems) and may be useful for engineers.
- Meet some needs of the engineering community and some needs of government C-people.
- Attempt to provide absolute ranking of products against objective criteria.
- Provide ranking within a particular application domain.

Shortcomings:

- Address products, not systems.
- Are time and resource intensive.
- Minimum requirements are more than the industry is willing to pay for.

Common Criteria/National Information Assurance Partnership (CC/NIAP):

- Meet some needs of engineering community and some needs of government C-people.
- Provide systems with relative ranking within particular application domains.

Shortcomings:

- Address products, not systems.
- Are time and resource intensive.
- Minimum requirements are more than the industry is willing to pay for.

[Note: The TCSEC and CC do not address good system engineering. Some people argue that if good system engineering is done, then there is no need for product assessment.]

System Security Engineering Capability Maturity Model (SSE-CMM):

- Provides indirect measure of system security.
- Is a good tie-breaker.
- Provides a long-range look at systems that will be produced in the future. Predicts better security capability of an organization.
- Reflects a process-oriented, reductionistic measure in terms of assigning a maturity level to a particular organization.
- Could be useful for planners and C- people, and for defining security benefits. Could be useful to both developers and consumers of systems (valuees).

Shortcomings:

- Acceptance and usability are still questionable.
- Is labor intensive.

Certification and Accreditation/Defense Information Technology Security Certification and Accreditation Process/National Information Assurance Certification and Accreditation Process (C&A/DITSCAP/NIACAP):

- Useful to government C-people, designers/developers, SysAdmins/Information System Security Managers/Information System Security Officers (ISSOs) for comparing required state with the current state.

Shortcomings:

- Used to evaluate an existing system that is either about to go operational or is already operational.
- Are labor and resource intensive, and are slow.
- Levy requirements on the engineering process but do not provide IS*s for the engineering process.

[Note: These processes are currently being harmonized with the CC, to define a smooth transition and common terms of reference between the technical object and the systems-oriented operational communities.]

Federal CIO Council Metrics, Draft

Summary:

This document was published on May 29, 2001. To establish a set of commonly accepted metrics, the Federal CIO Council's Security, Privacy, and Critical Infrastructure

Committee established a small working group composed of people who are engaged in managing and measuring security. The Metrics Working Group relied primarily on the *Federal Information Technology Security Assessment Framework* as the central organizing structure for its work. To develop the specific metrics, it supplemented the Framework with information from these sources:

- Recent General Accounting Office audit reports that identified specific weaknesses in federal information security programs.
- Pioneering information security metrics programs at several federal agencies, including the National Aeronautics and Space Administration and the Department of Energy.

[Note: Some organizations have distilled information security metrics to ten representative elements. It may be possible to consult other organizations and define a generally accepted baseline collection of measurements.]

Intrusion Statistics – Computer Emergency Response Team (CERT); other intrusion-type research (papers from academia: the Massachusetts Institute of Technology and Lawrence Livermore Laboratory):

- Help quantify and describe amounts and types of intrusions by using different levels of categorization and organization.
- Will help vulnerability analysts, threat-source analysts, SysAdmins, C-people people, and values.

Shortcomings:

- Lack common language and sharing format for vulnerability analysts. Common data structures are required for data sharing and creating meaningful metrics. DoD and federal government CERTs are just starting to share information in a more formalized way. The concept is that the larger the data pool for intrusion information, the easier it is to generalize.
- Cost and impact information for intrusions is limited.
- Useful way of recording vulnerability, threat, and impact information is needed.

Other assessments of organizations – Defense Information Systems Agency Security Readiness Reviews (DISA-SRRs):

- Directed at operational organizations and operational systems.
- Scope is limited to military, but the results are used extensively by commanders.
- Could be translated into commercial context.
- Could be useful to C-people, SysAdmins, and their management.

Pedigree activities – Certified Information System Security Professional (CISSP), INFOSEC Assessment Methodology (IAM), Information System Security Engineer (ISSE), Global Incident Analysis Center (GIAC):

- Same value as SSE-CMM only applied to training issues (i.e., smaller scope).

Cost/Benefit Metrics:

- Specific metrics (*s) already exist. A language is needed to translate from “security engineering” into “finance.”
- Some of this may be starting, for example, the Incident Sharing and Analysis Center (ISAC) was established to share information. However, no information leaves room due to proprietary and public relations concerns, so it is unknown whether they discuss costs and impacts of security events.
- Information on costs and impacts that may apply to more than one organization should be shared within and across organizations.
- Useful to C-people, CEOs, and valuees.

Insurance Policy Valuations:

- Current cyber insurance providers must have some cost and impact information. They must also limit their exposure to liability. It would be interesting to know how they agree on the amount of liability.
- Some current providers are Counterpane (Schneier) with Lloyds of London, ISS with J. D. Marsh, and ICSA/Truesecure with Can E&S. Organizations cannot get insured unless the insurance trusted partner assesses the network. Furthermore, in the case of Counterpane, an organization must also purchase services to continue protecting the network.
- A database of past incidents must exist to predict future impacts. Actuarial risk assessments must be performed. It would be interesting to examine offered policies. It may be valuable to pull the data, because the total amount of available data is small; however, we are sure that the companies do not share their data, since sharing would provide competitive advantage.
- An insurance premium is an IS* for high risk vs. low risk.
- Useful to C-people and valuees.

4 Suggested Research Areas

One of the objectives of this workshop was to try to determine the research agenda for information security rating, ranking, measurement, or scoring. As the four working groups completed their final collective reporting, one point was most striking: the major issues across the groups did not appear to be scientific in nature. Rather, the topics were more oriented toward social science types of measurement. This section consolidates the research suggestions from the four working groups.

The working groups agreed that today the calibrations focus is on the relative capabilities of organizations, objects, or operational procedures. The groups advocated *Consumer Reports* types of ranking (ranking similar products against performance characteristics that are common within a product group) or school grading systems that assess the relative merits of capabilities when compared to similar products or their peers. In either case, however, the products are judged against their peers, not a set of fixed criteria.

Beyond these types of rankings, the working groups agreed that meaningful abstractions of information security characteristics are difficult to define. Individual measures or attributes make it difficult for decision makers to understand the specific security attributes of a device. However, the aggregation of multiple individual measures into a single representative score seems to be an artificial abstraction that causes volumes of data to be lost in the translation. For example, claiming that the residual risk of a system is low, without having the list of remaining risks provided, makes the abstraction highly subjective and potentially prone to additional scrutiny.

Further, the working groups expressed a universal need for repeatability and consistency in rating and ranking. If the same system is analyzed in the same context, then the same results should be generated. Unfortunately, with so much assurance information based on anecdotal case law that is passed from evaluator to evaluator, it is difficult to gain agreement on the characteristics of a given solution. Therefore, more formalism in lessons learned is required. It is necessary to capture the history of rating and ranking, including the experience base that is currently working in the field, to calibrate the case law into concise heuristics that can be applied in a standardized fashion.

Before identifying specific research areas, the working groups attempted to answer the following question: If IS*s cannot be measured directly, could any measures serve as proxies or surrogates that can be collected? The argument ultimately depends on having a good model showing the interrelationship of all factors. A critical consideration is that a key IS* attribute is the value we place on the reputation of the evaluator.

The following paragraphs summarize the research areas identified by the working groups.

Need for a Common Vocabulary

Just as there are various audiences for information security rating and ranking data, different vocabularies are used by these audiences. This variation leads to a failure to

translate/communicate the state of the relative security associated with a system among the audiences. End users sacrifice security functionality to obtain mission-oriented functionality. If they could understand the contribution of security functionality to their mission objectives, they might not be so willing to sacrifice it.

Similarly, management must have a working knowledge of the consequences associated with allocating or de-allocating security resources and the resulting impact of their actions on the security posture of the enterprise. To make informed decisions, management must be able to assimilate a protection posture or picture of the enterprise's security status. If it is possible to abstract from the technical details a management-friendly level of detail, then security rating and ranking will be useful as decision support environment criteria.

Audience Requirements

Diverse constituencies will benefit from effective assurance rating and ranking information, and attempts to address all of the audiences simultaneously have not worked. At least the following five audiences would be affected:

1. Product vendors – who need to assess the relative capabilities of their technical objects.
2. System integrators/developers – who need to be able to reason about the security of technical objects as they are integrated to form a functional system.
3. System consumers – who need to address the operational capabilities of a given system and determine if the security functionality meets their operational mission.
4. System security personnel – who need to take the results of audiences 1-3 above and put them in a big-picture context.
5. Management personnel – who need to allocate resources based on the requirements of the organization and ultimately determine what comprises a sufficient system.

Each audience will have a different and potentially divergent set of requirements. For example, speaking to management about firewall configuration, test case coverage, or potential covert channels will not fulfill management's requirement to know if an organization's security posture is improving.

To date, standards have been written to address all audiences. Such is the case for the *Common Criteria*. A vendor is supposed to be able to use the functional and assurance requirements to build a technical object. An integrator is supposed to be able to use a protection profile to specify requirements for a system and generate a target of evaluation to describe how a system meets the protection profile. The system user is supposed to use the target of evaluation and the protection profile to determine if a given technical object or system meets his/her requirements. However, the result would be a very large, ambiguous document.

Like product positioning and marketing organizations, the information security community needs to take a good look at the various stakeholder organizations and determine how best to serve their rating and ranking requirements.

Feasible Rating and Ranking Scales

Precise assessment of the security functionality in a given system or technical object is not possible with current technology. New vulnerabilities occur almost daily. To believe a definitive statement can be made about a given entity's security posture over time is naïve at best. Therefore, it would seem prudent to try to determine common component functionality and focus on how a component might distinguish itself from others through improvement of particular aspects of security or assurance functionality.

A Calculus of Composability

One can argue that from experience with the *Trusted Computer System Evaluation Criteria* and the *Common Criteria*, the security practitioner community has developed a reasonable competency in determining what a reasonable collection of assurance evidence needs to contain for a single technical object. To date, aggregates of component objects have not been examined in depth. The assumption has been that if the security mechanisms of one object are at least preserved, if not enhanced by, the object integrated with it, then the security policy has been successfully preserved. However, this is not usually the case. As applications, network protocols, and infrastructures become more protocol rich and complex, it will become increasingly difficult to determine if the security properties of a technical object have been preserved during integration.

Since technical objects rarely function alone but rather as an integral component of a system, it makes reasonable sense to investigate the security properties associated with composability of systems. Very little empirical work has been accomplished in this field. The work that has been accomplished has been under the purview of certification and accreditation activities. Investigators need to understand the interactions between objects and how they impact each other. Protocol verification provides a starting point for these activities.

Objectivity

Objectivity research, in this context, focuses on defining assurance measures that are more objective in nature than subjective. For example, the *Common Criteria* project has recognized a need for more objective assurance measures and is now organizing a working group to define these measures. Workshop attendees stated a desire to assist in making this a reality by joining the *Common Criteria* working group or commenting on its products.

Tools

Current hardware and software products lack an ability to monitor operational performance; there are few observable parameters that might serve as input to operational IS*s. The kinds of operational parameters that are available are associated with audit logs, which focus on interactions between the product and the external environment while providing no information on the internal operation of the product.

The measurements delivered by security evaluation tools should represent as accurately as possible the security of the system in operation (i.e., its ability to resist possible attacks, or equivalently, the difficulty for an attacker to exploit the vulnerabilities present in the system and defeat the security objectives). Current vulnerability scanners approach this problem by building a database of all known vulnerabilities and scanning the system for them.

The ESOPE security tool approach, which is to assist network penetrability analyses, was briefed at the workshop. This approach looks at the operational security problem in terms of (1) the point of view of the threat (e.g., tenacious vs. lazy, focused vs. unfocused); (2) the main security objectives and not every minor vulnerability; and (3) the need for security to evolve as the system evolves through modifications and upgrades, assuming that security is not absolute but is either improving or decaying. Researchers should monitor all such security evaluation tool development activities.

Best Practices

Finally, research is needed to establish and define best IA practices. The government has done this fairly well with establishment of the CIO Council's Best Security Practices Initiative. Consideration should be given to exercising these best security practices in the commercial sector. Sharing methodologies horizontally and communicating results vertically is desperately needed.

Another example for study is the insurance industry, using it as a basis for writing computer security policies and thus insuring against cyber security losses. A relevant briefing was presented on this topic by Mary Guzman at the January 2001 Information Assurance Technical Framework (IATF) meeting. Slides are available at the IATF Web site for registered members.

6 Future Directions

An interesting debate influenced workshop discussions, based on each participant's objectives for attending. Those who saw the workshop as a benchmarking opportunity to determine the state of measurement, rating, and ranking for the IA/security community claimed that the workshop met its goals and should stand on its own merit. In contrast, others believed that the workshop served a longer term purpose in the community.

An examination of the working group reports finds a strong need for improved communication between management and technical security personnel. Part of the drive toward security rating and ranking is the management sector's requirement to demonstrate continuous improvement as a prerequisite for resource allocation. However, the abstraction of the collection of individual measurements into a single value loses a considerable amount of context in the translation.

Some workshop participants expressed the belief that a simple benchmarking of the current state of measurement, rating, and ranking progress in IA is insufficient. Yes, it serves a checkpoint that reflects the current state of the practice and even generates ideas for near-term research in the community. However, the process has another dimension: communicating what measurement means in the current context of IA. This dimension changes the purpose of the workshop from strictly an information exchange to communication improvement and cross-fertilization among interested groups of domain experts.

A compromise position was put forward: develop and publish the workshop proceedings and hold panel discussions at conferences where the target audience should be interested in the topic. These conferences include the Annual Computer Security Applications Conference and the Software Technology Conference. Once the responses to these panel discussions have been calibrated, another workshop or a different type of workshop could take place. A suggested alternate workshop could focus on sharing information with other audiences, such as those that evaluate technical objects or security processes. Other topics for tracks could be considered, such as one with a more systems-oriented focus.

Is this the last the community will hear of information assurance rating and ranking techniques and technologies? That is doubtful. As long as diversity exists among technologies and implementation procedures, backed by the need for policy and doctrine mandate compliance, interested parties will want to assess the relative merits of systems and their applications.

This workshop indeed served as a benchmark for determining the capabilities of rating and ranking. It also fostered additional understanding on the parts of its participants. And, perhaps most significantly, it continues to generate discussion, research, and debate on a subject that can only further the state of the practice.

Appendix A Agenda

Table A-1. Workshop Agenda

| Session\Track | Track 1: Technical (IS*s of technical objects, at different stages of the system life cycle) | Track 2: Organizational (IS*s of organizational programs and processes, for different organizational scopes) | Track 3: Operational (IS*s of operational systems, environments, and operating practices) | Track 4: Brainstormers (synthesis, cross-track issues, and big picture concerns) |
|---|---|--|--|---|
| Monday 1:00-1:15 p.m. | Plenary Session | | | |
| 1:15-4:15 p.m. What are we talking about? Who needs (or wants) IS*s? Why do they need/want IS*s? How will IS*s be used? What constitutes an IS* (what characteristics)? ? What are some examples we can use to anchor our discussion? ¹⁰ | What are the characteristics of IS*s of technical objects? Who needs or wants them? What can we learn from experience with the TCSEC and the CC? | What are the characteristics of, needs for IS*s of organizational programs and processes? | What are the characteristics of, needs for IS*s of operational systems, environments, and operating practices? | What are the big picture characteristics of, needs for IS*s, across all domains? What are the characteristics of and needs for IS*s that do not currently exist? |
| 4:15-5:00 p.m. | Session Readout | | | |

¹⁰ The discussion will use a systems engineering, top-down examination of the problem domain. Other follow-up questions may include: Is the format of the IS* important? If so, what and why? Is the precision of the IS * important? If so, why and what?

| Session\Track | Track 1: Technical | Track 2: Organizational | Track 3: Operational | Track 4: Brainstormers |
|--|--|---|---|--|
| Tuesday 8:00-8:15 a.m. | Plenary Session | | | |
| 8:15-11:15 a.m. Focused needs and good practices I | What IS*s are needed to aid at different phases in the product or system life cycle? (1) when defining requirements for products or systems? Are there measurable aspects of the environment? (2) during development, integration, or acquisition? | Programmatic and process IS*s for organizations that produce, acquire, integrate, information technology. What can we learn from SSE- CMM? FISAF? SP 800? What can we learn from other disciplines that have instituted organizational IS*s? For instance, EEO. How is IS and IS* different? | Operational IS*s for the government sector What are the needs and practices for assessing informal programs and processes, vs. those for formal ones? How can we assess what's real as well as what's documented? Rhetoric vs. reality? | Drawing upon the output of all tracks' sessions, what sort of aggregate IS* is possible? What is unique and what is redundant? Are there benefits from drawing from one domain vs. another? What does an aggregate IS* buy you? Who would use it? |
| 11:15 a.m.- 12:00 p.m. | Session Readout | | | |
| 12:00- 1:00 p.m. | Lunch | | | |
| 1:00-1:15 p.m. | Plenary Session | | | |

| Session\Track | Track 1: Technical | Track 2: Organizational | Track 3: Operational | Track 4: Brainstormers |
|--|---|---|---|---|
| Tuesday 1:15-4:15 p.m. Focused needs and good practices II | (3) for Testing, Certification and Accreditation (4) for Operations and Maintenance | Programmatic and process IS*s for organizations that seek to defend themselves (users of information technology) | Operational IS*s for the commercial sector What are the needs and practices for assessing informal programs and processes, vs. those for formal ones? How can we assess what's real as well as what's documented? Rhetoric vs. reality? | What are the characteristics of an assessment process that have some hope of working to provide IS* input data? What strategies for data normalization are effective and defensible? |
| 4:15-5:00 p.m. | Session Readout | | | |

| Session\Track | Track 1: Technical | Track 2: Organizational | Track 3: Operational | Track 4: Brainstormers |
|--|--|--|--|--|
| Wednesday 8:00-8:15 a.m. | Plenary Session | | | |
| 8:15-10:30 a.m. Identify research needs or directions. | Identify research needs or directions, as related to IS*s of technical objects. Answer the question: Can we solve this problem? Does some type of useful IS*s exist for technical objects or is this a lost cause? | Identify research needs or directions, as related to IS*s of organizational objects. | Identify research needs or directions, as related to IS*s of operational objects | Discuss other needs: aggregation, modeling |
| 10:30-11:15 p.m. | Session Readout | | | |
| 11:15-12:00 p.m. | Wrap Up and Next Steps | | | |

Appendix B Position Paper Summaries

This appendix presents summaries of points made in position papers. “Type” indicates the types of objects for which measurement is discussed.

- Title: Coming to Acceptance of Ways for Measuring and Ranking Security Properties
Type: Technical Objects (e.g., products, algorithms, protocols), Systems
Author: Marshall D. Abrams
Summary: Coming to agreement on what constitutes meaningful measures is a social process; no consensus regarding IS currently exists. The security engineering community has much to learn from the social sciences.
- Title: On Assurance, Measures, and Metrics: Definitions and Approaches
Type: Organizational Programs
Author: John Alger
Summary: Crucial to clarify relationship among concepts of assurance, measurement, and metrics. Measurement does not guarantee assurance. Metrics (objectively and subjectively arrived at, depending on analysis and used as a decision tool) are useful in gaining assurance.
- Title: IA Metrics Development
Type: Organizational Programs, Systems
Author: Nadya Bartol
Summary: Need well-defined process for metrics development. Can measure three types of IA outcomes: level of policy implementation, changes in IA posture, and business value gained or lost from IA-related activities.
- Title: Measuring Security
Type: Organizational Programs, Organizational Processes, Systems, Technical Objects
Author: Jennifer Bayuk
Summary: Five categories of security assessment models: external audit, internal audit, capability maturity, risk analysis, and defect elimination. Only defect elimination allows an automated assessment approach. If the goal is security product evaluation, no qualitative criterion (even yes/no) will stand without comment.
- Title: Security Assertions, Criteria, and Metrics Developed for the IRS
Type: Organizational Programs
Author: Paul Bicknell
Summary: To apply a high-level assessment framework (the FISAF), it has proven useful to construct assertions of desired properties, and assessable performance criteria.

Title: Information Assurance Assessment: Lessons-Learned and Challenges
Type: Organizational programs, Organizational processes, Systems, Technical objects
Author: Deborah Bodeau
Summary: Without a process description, an assessment function is at best of limited usefulness. To be successful, an IA assessment should be appropriate to its intended use, have a clear definition of its domain, and result in values that are easily communicated to their ultimate users.

Title: Red Team Work Factor as a Security Measurement
Type: Systems
Author: Julie Bouchard, Bradley Wood
Summary: RTWF is a function of preparation time, attack time, equipment cost, and access to information, equipment, and/or assistance. This can be converted to dollar values.

Title: IA Operational Readiness Metrics
Type: Organizational Programs
Author: Julie Connolly
Summary: The existing OR infrastructure provides a good starting point for IA OR self-assessment. External IA OR assessments are more problematic.

Title: Experimental Validation of a Security Metric
Type: Systems
Author: Yves Deswarte, Mohamed Kaâniche, Rodolphe Ortalo
Summary: An approach for quantitative evaluation of the security of operational systems can and should be based on a theoretical model, and validated by experimentation.

Title: Which Way Is Up? Input on Improving the Technical Basis within the Security Risk Management Process
Type: Systems, Technical Objects
Author: Jim Freeman
Summary: Subjectivity is a given. Good models are needed. Use an architecture-based rationale as much as possible. Bring security engineering more into systems engineering.

Title: How I Lost and Then Regained My Faith in Metrics Type:
Type: Technical Objects
Author: Steven Greenwald
Summary: Most things termed *metrics* are snake oil, but true measurement is possible in very specific cases (e.g., to compare crypto algorithms).

Title: Penetration Testing – The Gold Standard for Security Rating and Ranking
Type: Systems, Technical Objects
Author: Ranwa N. Haddad, Deborah Downs
Summary: If the goal is to differentiate between products that are meant to have the same security functionality, penetration testing is a promising assessment method.

Title: Towards Quantifying Computer Security: System Structure and System Security Models
Type: Systems
Author: Jonas Hallberg, Amund Hunstad
Summary: A system can be viewed at abstract, intermediate, and concrete levels. Quantitative measurement is most likely to succeed at the concrete level, but measurement at the abstract level (and good systems engineering) are made possible by a good intermediate-level model.

Title: Certification of Intelligence Community Systems and Measurement of Residual Risks
Type: Systems
Author: Jay Kahn
Summary: The IC Risk Management Methodology provides a consistent, repeatable approach to IA risk assessment.

Title: Security Metrics
Type: Organizational Programs, Organizational Processes, Systems, Technical Objects
Author: Stu Katzke
Summary: A security metrics model consists of (1) the object being measured, (2) the security objectives against which it is measured, and (3) the method of measurement.

Title: Decision Support Metrics Framework
Type: Organizational Programs, Systems
Author: Ralph Leighton
Summary: Metrics must be defined appropriately to the circumstances of their use. A five-phase approach to program assessment and evolution is proposed: quick-fix, architectural, compliance, adjustment, and testing.

Title: Measuring Information Security
Type: Organizational Programs
Authors: Adèle Martins, JHP Eloff
Summary: International standards can serve as a basis for measurement on the management and business process level (BS 7799), and the level of security management of implemented controls (ISO 17799). A questionnaire is a useful measurement tool.

- Title: Dependable Measurement
Type: Technical Object
Author: Roy Maxion
Summary: Factors in effective, dependable measurement include benchmarks, reliability, validity, reproducibility, control, experimental methodology, sampling bias, ground truth, error, and terminology.
- Title: The Case Against Numerical Measures for Inform
Type: Systems
Author: Dennis McCallam
Summary: “80% of what?” Logicon’s Resiliency Assurance Index defines ten levels that aid in what can (and should) be expected of a system as used.
- Title: The Perception of Assurance
Type: Organizational Programs, Organizational Processes, Systems, Technical Objects
Authors: Molly McDermott, Rob Dobry
Summary: IA includes five aspects: personnel, sound design principles and processes, appropriate technology, T&E, and sound operating procedures. Existing security metrics address these aspects separately; a unified metric is needed.
- Title: Quantitative Measures of Assurance: Prophecy, Process, or Pipedream?
Type: Systems, Technical Objects
Author: John McHugh
Summary: Little evidence exists that IS measures are possible. The underlying science is lacking, and Murphy rules.
- Title: Information Assurance Risk Metric Tree
Type: Systems
Author: Don Peeples
Summary: Risk metrics depend on having a good integrated model of IA and of an information system in its operational/support context. A hierarchy of eight risk metrics is defined.
- Title: A Look at Measures of Computer Security from an Insurance Premium Perspective
Type: Organizational Programs, Systems, Technical Objects
Author: Jock Rader
Summary: Insurance companies rely on large databases to estimate probabilities and magnitudes of loss. Expected loss could be an important IS metric.

Title: An Approach to INFOSEC Program Metrics
Type: Organizational Programs
Author: George Rogers, Barry Stauffer
Summary: To apply the FISAF, a questionnaire should be developed with responses on a scale of 1-4; metrics related to scanning and incident reports could also be developed.

Title: Measurements of System Security
Type: Systems
Author: Edward A. Schneider
Summary: System security measures are inherently multidimensional. We are currently unable to measure the strength of security effectively, leaving process quality as the measure of choice.

Title: The Bull in the China Shop: The “Merrill Lynch” IA Assessment Manifesto
Type: Systems
Author: Stuart Shapiro
Summary: Multi-modal assessment, drawing on techniques from social as well as hard sciences, could be useful. What’s needed: taxonomy and supporting tools/methods, fundamental IA assessment, and technical IA assessment. External as well as internal state must be addressed.

Title: Assessments for Rating and Ranking Information Assurance
Type: Systems, Technical Objects
Author: Michael Skroch
Summary: A number of well-defined approaches exist to identify metrics and should be used. The stage in the system life cycle at which assurance is measured affects choice of metrics. Qualitative metrics should not be rejected en masse. However, we should move toward quantitative, objective measures.

Title: High Assurance ≠ More Secure
Type: Technical Objects
Author: Gary Stoneburner
Summary: Unless the author of requirements drawn from the *Common Criteria* understands the measurement needs, it’s possible that the PP or ST will call out assurances that provide overkill in one area and shortfalls in another.

Title: Are Measures and Metrics for Trusted Information Systems Possible?
Type: Organizational Processes, Systems, Technical Objects
Author: Rayford B. Vaughn
Summary: While a 100% predictive metric for information systems is unachievable, useful metrics can be defined and validated empirically. The goal should be improved quality.

Title: Security Metrology and the Monty Hall Problem
Type: Systems, Technical Objects
Author: Bennet Yee
Summary: Security is truly binary only in an information theoretic setting. One possible measure is resources-needed-to-penetrate. A multi-dimensional security measure is more useful than a single score.

Appendix C Related Measurement Activities

This appendix lists related measurement activities. This information was derived from the workshop position papers and other publicly available information, notably the National Institute of Standards and Technology (NIST) Computer System Security and Privacy Advisory Board (CSSPAB) metrics workshop and the Defense Advanced Research Projects Agency (DARPA) Information Assurance Science and Engineering Tools (IASET) program. The set of activities is heavily oriented toward U.S. government organizations, in particular the Department of Defense, for two reasons. First, government organizations have mandated reporting requirements and must be prepared to justify decisions. Government investment in the development and use of IS metrics is therefore significant. Second, IS metrics defined and used in the commercial sector (e.g., by auditors, insurers, or security consultants) are frequently proprietary.

On June 13-14, 2000, the NIST CSSPAB conducted a workshop on security metrics. The goal of the workshop was to survey current information infrastructure protection metrics and their uses and to determine any voids. The focus emphasized non-classified systems. A report on the workshop and many of the presentations are available at <http://csrc.nist.gov/csspab/june13-15/sec-metrics.html>. The discussion centered on non-technical metrics.

The DARPA IASET Program sponsored investigations and held workshops and program reviews. Papers and briefings can be found at <http://schafercorp-ballston.com/may99wkshp/iaset2/iaset2.html>. At the July 1999 IASET workshop, the following “success criteria” for IA metrics were proposed: evident utility, widespread adoption, and (for a set of IA metrics) coverage of the problem space. Properties of “good” IA metrics were also proposed: metric values should be computable within a time frame useful to decision makers, assessment should be repeatable and consistent, a metric should measure what it claims to measure, and it should make intuitive sense.

Table C-1 identifies activities related to the development and use of IS or IA metrics. The table identifies the organization responsible for defining the metric, the name or title of the metric, a brief description, a characterization of its goal or intended use, its type and scope, its target audience or user community, and reference(s). *Type* means the way the assessment results are presented: quantitative or qualitative. *Scope* means the domain of objects for which measurement is discussed: T for technical objects (e.g., products, algorithms, protocols), S for systems, O for organizational programs, P for organizational processes, E for environmental factors (e.g., threat environment, mission importance, information value), and I for individual expertise. An asterisk next to the name of an IS metric indicates that it was described in a position paper for the workshop and abstracted from the position paper to the metric

summary. Position papers were used to form working groups and generate working group topics. The authors did not necessarily have them approved for public release; therefore, they are not included in these proceedings.

Table C-1. Related Measurement Activities

| Developing Organization | IS or IA Metric | Description of Metric | Goal(s) | Type and Scope | Target Audience | Reference |
|--------------------------------------|--|--|---|------------------------------------|--|--|
| OSD(C3I)/I&IA USSPACECOM/ J39D | Computer Network Defense (CND) operational readiness metrics for Joint Monthly Readiness Review (JMRR) | CND inputs to the JMRR | Assess CND readiness | Qualitative (ranked values); O | DoD Decision makers | FY2000 DIAP Annual Report http://c3i.osd.mil/org/sio/ia/diap/documents/DIAP2000.pdf |
| OSD(C3I)/I&IA USSPACECOM/ J39D | INFOCON | Level of threat to DoD CND | Enable commander to determine level of protection and control appropriate to current conditions | Qualitative (ranked values); E | DoD Decision makers | FY2000 DIAP Annual Report |
| OSD(C3I)/I&IA | Defense-Information Assurance Red Team (D-IART) metrics | Metrics collected on attack/response pairings during red team exercises. | Provide an assessment of blue team and a means for blue team improvement | Quantitative and qualitative; P | Personnel subject to and participants of an IA Red Team; DoD decision makers | |
| DISA | Information | % systems | Identify systems | Quantitative; | DoD decision | http://www.ce |

| Developing Organization | IS or IA Metric | Description of Metric | Goal(s) | Type and Scope | Target Audience | Reference |
|---|--|---|--|---|--|--|
| | Assurance Vulnerability Alerts (IAVA) metrics | remediated, % vulnerability alerts addressed | and vulnerabilities that are remediated or require remediation | O | makers | rt.mil/iava/iava_index.htm , FY2000 DIAP Annual Report |
| Defense-Wide Information Assurance Program (DIAP - part of OSD(C3I)/I&IA) | IA Readiness Assessment | Develop an approach, to include IA metrics, for assessing IA readiness of DoD units. May tie into SORTS and JMRR readiness reporting. | Establish a DoD-wide IA readiness assessment process | Quantitative and qualitative; O | DoD decision makers | FY2000 DIAP Annual Report Terry Bartlett, SAIC, DIAP lead, 703-602-9991, terry.bartlett@osd.pentagon.mil |
| DoD | DITSCAP Certification Levels | Level of effort and rigor in system certification process | Provide consistency in C&A activities | Qualitative (4 levels); S | System certifiers, Designated Accrediting Authorities (DAAs) | http://Mattche.iie.disa.mil/ditscap/ditsdoc.html |
| Intelligence Community | INFOSEC Risk Management metrics (originally defined for TSABI Initiative)* | Level of residual risk, as a function of threat, vulnerability, and significance of results | Provide consistent way to assess and present residual risk | Qualitative (VL-VH), based on numeric inputs; S | DAAs | |
| Intelligence | Protection levels & | Protection levels for | Provide | Qualitative | System | http://www.fa |

| Developing Organization | IS or IA Metric | Description of Metric | Goal(s) | Type and Scope | Target Audience | Reference |
|--------------------------------|---|--|---|--|--|---|
| Community | levels of concern in DCID 6/3 Manual | confidentiality, levels of concern w.r.t. integrity, availability | consistent way to identify system requirements | (five levels for confidentiality and three for integrity and availability); S | certifiers, Acquisition Program Managers, DAAs | s.org/irp/offdocs/DCID_6-3_20Manual.htm |
| Joint Chiefs of Staff | CJCSI 6510.04, IA Readiness Metrics | Self assessment checklist of IA-related capabilities (e.g., “Adequate detect tools policy in place and configurations properly managed”) | Capture a snapshot of an organization’s IA operational readiness | Qualitative; O | DoD organizations | FY2000 DIAP Annual Report |
| Joint Staff | Assessment of CINC IA Capabilities for Defense-in-Depth, 1 September 2000 | Assessment of CINC IA Capabilities for Defense-in-Depth | Provide first look at Defense-in-Depth capabilities, as a basis for a roadmap to identifying deficiency areas within capabilities that will require resources | Qualitative (4 levels, based on numbers of responses to specific questions); O | CINCs | |

| Developing Organization | IS or IA Metric | Description of Metric | Goal(s) | Type and Scope | Target Audience | Reference |
|--|---|---|--|------------------------------------|---|---|
| AF Electronic Systems Center (ESC)/DIW | IA SPO Profiles | Assess IA capabilities and needs of Air Force program offices | Ensure IA needs are met throughout the AF acquisition process | Quantitative and qualitative; O | Air Force decision makers, ESC/DIW, Air Force SPOs | |
| ESC/DIW and DIAP | IA Metrics for Assessing and Improving IA Operational Readiness (OR) (planned)* | Combined live operational testing and implementation plans/policy review to provide third-party validation of an organization's IA OR | Provide a process, to include IA metrics, for third-party validation of IA OR and improvement of IA OR | Quantitative and qualitative; O | DoD decision makers involved in deployment, resources, policy | |
| ESC/DIW | IA Vulnerability Assessment/ Risk Management (VA/RM) metrics | Assess level of IA risk to an information system | Provide an assessment process, supported by a tool, for IA risk management to systems, individually and composed | Quantitative and qualitative; S | DAAs, Program Managers, operational commanders | |
| Air Force Software Systems Group (SSG) | Air Force Network Operations Center metrics | Network performance metrics such as # intrusions, # virus incidents, # DDOS | Provide high-level view of network situational | Quantitative; S | Air Force network operators, Air Force decision | http://www.afnoc.af.mil |

| Developing Organization | IS or IA Metric | Description of Metric | Goal(s) | Type and Scope | Target Audience | Reference |
|---|---|--|--|---------------------------------|--|---|
| | | attacks | awareness, to include IA incidents and attacks | | makers | |
| Air Force Communications Agency (AFCA) | Information Protection Metrics and Measurement Program | Collects data on training, system accreditation, security incidents | Measure compliance with, and effectiveness of, Information Protection policy | Quantitative; O | Air Force organizations, Air Force decision makers, AF policy makers | AFI 33-205, 1 August 1997, Information Protection Metrics and Measurement Program |
| Air Force Information Warfare Center (AFIWC) | Statistics from vulnerability assessments conducted against Air Force bases (primarily) | # systems obtained root password on, # systems with NFS mount vulnerabilities, etc. | Provides a comparative sense of an Air Force Base's network security | Quantitative; S | MAJCOMs, SPOs, Base Comm. Squadrons, System Developers and Users | Carol Hiltbold, AFIWC/EAS E, DSN 969-3113 |
| Air Force Institute of Technology (AFIT) Center for Modeling, Simulation, and | Value model for Information Operations (IO) | Value-focused thinking approach to identifying and assessing IO courses of action. Ascribes weights to different | Provide the IO decision makers with a weighted and well-reasoned set of options. | Quantitative and qualitative; P | IO decision makers | http://www.ia.set.org Dr. Richard Deckro, rdeckro@afit.af.mil |

¹¹ See *A Strategy for Information Assurance*, R. F. Deckro, J. T. Hamill, and J. M. Kloeber, Jr., CMSA-TR2000-02, September 2000, Air Force Institute of Technology Center for Modeling, Simulation, and Analysis, Wright-Patterson AFB, OH.

¹² Ibid.

| Developing Organization | IS or IA Metric | Description of Metric | Goal(s) | Type and Scope | Target Audience | Reference |
|--|--|--|---|---|---|---|
| Analysis (in support of DARPA) | | attributes in the process. | | | | |
| Marine Corps Operational Test and Evaluation Activity (MCOTEA) | Operational Effectiveness and Suitability Determinations | Determine Operational Effectiveness and Suitability as part of Operational Test and Evaluation | Establish and implement OSD- mandated IA OT Requirements | Quantitative and qualitative; S | Operational testers | |
| Department of Energy (DOE) | Cyber Security Program Plan (CSPP) metrics | Quality of an organization's CSPP (and, by inference, its program) | Assess quality of an organization's CSPP; identify areas in which improvement is needed department-wide | Qualitative; O | DOE CIO's office, heads of DOE organizations, managers of DOE cyber security programs | John Przysucha, Deputy Director DOE Cyber Security Office |
| Department of Energy | Protection levels & levels of concern in DOE M 471.2-2 | Levels of concern w.r.t. confidentiality, integrity, availability, disclosure risk | Provide consistent way to identify system requirements | Qualitative (3 levels of concern for C, I, A; 6 protection levels); S | System certifiers, Acquisition Program Managers, DAAs | |
| Common Vulnerabilities | Vulnerability scanner coverage, expressed | Assess breadth of coverage of | Compare vulnerability | Quantitative; T | System developers and | http://www.cve.mitre.org |

| Developing Organization | IS or IA Metric | Description of Metric | Goal(s) | Type and Scope | Target Audience | Reference |
|--|---|--|---|---------------------------|--|--|
| and Exposures (CVE) Editorial Board and Advisory Council | as number of CVE entries ¹³ | vulnerability scanning tools | scanning tools | | administrators | |
| NIAP, NSA, NIST, International Community | <i>Common Criteria</i> (CC) | Specification and evaluation of levels of functionality and of assurance | Assess compliance of IT components or systems with pre-specified set of CC requirements | Qualitative; T | System developers, System integrators, DoD decision makers | http://www.niap.nist.gov http://www.commoncriteria.org |
| Federal CIO Council, NIST | Federal IT Security Assessment Framework (FISAF) | Assess the maturity of an organization's IT security program, using NIST-developed questionnaire | Assess the maturity of an organization's IT security program | Qualitative (5 levels); O | CIOs, enterprise decision makers | |
| Lincoln Labs (in support of DARPA) | Intrusion Detection algorithm performance metrics | Measure performance (speed, accuracy) of intrusion detection algorithms, systems | Strengthen intrusion detection algorithms and systems | Quantitative; T | Intrusion detection algorithm/system developers, users | Dr. Rob Cunningham, Lincoln Labs rkc@ll.mit.edu |
| Sandia National Laboratories | Information Design and Assurance Red Team (IDART) metrics | Red team attack metrics (e.g., time to implement, probability of attack) | Tool for selecting and implementing red team attacks | Quantitative; P | Red team members | http://www.sandia.gov/idart Mike Eckley, 505-844- |

¹³ This metric is enabled by CVE, but is not espoused by MITRE or the CVE Editorial Board or Advisory Council.

| Developing Organization | IS or IA Metric | Description of Metric | Goal(s) | Type and Scope | Target Audience | Reference |
|---|---|---|--|---------------------------------------|--|---|
| | | success) | | | | 4767, mreckle@sandia.gov |
| SRI (in support of DARPA) | Red Team Work Factor* | RTWF is a function of preparation time, attack time, equipment cost, and access to information, equipment, and/or assistance. This can be converted to dollar values. | Assess system resistance to attack. | Quantitative and qualitative; S | | Bradley Wood, Julie Bouchard |
| Decision Science Associates (DSA) (in support of DARPA) | IA Metrics Decision Support Tool | Develop IA metrics and related decision making support that use multi-attribute utility (MAU) analysis | Assist system designers in making IA decisions, tradeoffs | Quantitative and qualitative; T, S | System developers, DoD decision makers | http://www.rl.af.mil/tech/programs/ia/ia12.html |
| Software Engineering Institute (SEI) | Survivable Network Analysis methodology | Applying fault tolerance approach to build contingency capabilities into systems and networks to sustain IA incidents and attacks. | Maintaining capabilities of mission critical systems and networks amidst IA incidents and attacks. | Quantitative and qualitative; S | System developers, Real-time mission planners, decision makers | http://www.sei.cmu.edu/programs/nss/surv-net-tech.html |
| Information | System Security | Process-focused | System security | Qualitative (5 | System | |

| Developing Organization | IS or IA Metric | Description of Metric | Goal(s) | Type and Scope | Target Audience | Reference |
|--|---|---|--|-------------------------------|--|---|
| Systems Security Engineering Association (ISSEA) | Engineering Capability Maturity Model (SSE CMM) | approach to developing secure IT systems; metrics are used to measure and improve processes | engineering process improvement | levels); P | developers, system integrators | |
| GartnerGroup | Gartner Security Process Maturity Model | Assess an organization's security maturity | Assist in strategic planning, process re-engineering | Qualitative (4 levels); O | Decision makers | |
| Logicon | Resiliency Assurance Index* | Assess a system's resilience to attack | Improve security design and administration | Qualitative (10 levels); S | Decision makers, system administrators | Dennis McCallam, Logicon |
| Sparta | IA Risk Metric Tree* | Assess a system's level of IA risk | Improve IA risk management | Quantitative; S | DAAs, Certifiers | Don Peeples, Sparta |
| LAAS-CNRS | Attacker success measures* | Use privilege graph to assess four measures for an insider seeking root (or administrator) privilege: SP (shortest path), NP (# of paths), Mean Effort assuming attacker has total memory, and Mean | Improve security monitoring and administration | Quantitative; S | System administrators | Yves Deswarte, Mohamed Kaaniche, Rodolphe Ortalo, LAAS-CNRS |

| Developing Organization | IS or IA Metric | Description of Metric | Goal(s) | Type and Scope | Target Audience | Reference |
|--|--|--|--|--|--------------------------------------|---|
| | | Effort assuming memoryless attacker. | | | | |
| Dartmouth Institute for Security Technology Studies (ISTS) | Vulnerability scanner testing against SANS Top Ten | Assess the breadth of coverage of vulnerability scanners | Compare vulnerability scanning tools | Qualitative; T | System developers and administrators | http://www.ists.dartmouth.edu/IRIA/top_ten/results_summary.htm |
| Counterpane/Lloyd's of London | Cyber insurance tiers | Level of insurance against cyber attack | Risk transfer | Qualitative (four tiers) and quantitative (insurance premiums); S, O | Risk managers | http://www.counterpane.com/pr-lloydswp.html |
| SANS | SANS Institute Certification Levels | Level of individual expertise | Compare individual's IA expertise | Qualitative (four values, beginner to advanced); I | Decision makers | http://www.sans.org/giactc.htm |
| ISSA | Information value metrics | Alternative approaches to assessing the value of information | Assess information value as input to risk management | Quantitative and qualitative; S, P, E | Policymakers, risk managers | http://www.issa.org/publications.html |

Appendix D Glossary

| | |
|---------|--|
| ACSA | Applied Computer Security Associates |
| ACSAC | Annual Computer Security Applications Conference |
| C&A | certification and accreditation |
| CC | <i>Common Criteria</i> |
| CEO | Chief Executive Officer |
| CERT | Computer Emergency Response Team |
| CFO | Chief Financial Officer |
| CIO | Chief Information Officer |
| CKO | Chief Knowledge Officer |
| CSO | Chief Security Officer |
| CTO | Chief Technical Officer |
| CVE | Common Vulnerabilities and Exposures |
| DARPA | Defense Advanced Research Projects Agency |
| DITSCAP | Defense Information Technology Security Certification and Accreditation Process |
| DoD | Department of Defense |
| EAL | Evaluated Assurance Level |
| ESOPE | An operational security tool by Yves Deswarte & Company |
| FISAF | <i>Federal Information Technology Security Assessment Framework</i> |
| IA | information assurance |
| IATF | Information Assurance Technical Framework |
| IAVA | IA Vulnerability Assessment |
| ICSA | International Computer Security Association |
| IS | information security |
| IS* | information security metric, as defined for this workshop: An IS* is a value, selected from a partially ordered set by some assessment process, that represents an IS-related quality of some object of concern. It provides, or is used to create, a description, prediction, or comparison, with some degree of confidence. |
| ISO | International Organization for Standardization |
| IT | information technology |
| NIACAP | National Information Assurance Certification and Accreditation Process |
| NIAP | National Information Assurance Partnership |
| PP | Protection Profile |
| SSE-CMM | System Security Engineering Capability Matrix Maturity Model |
| TCSEC | <i>Trusted Computer System Evaluation Criteria</i> |
| TPEP | Trusted Product Evaluation Process |