SOAR

State-of-the-Art Report (SOAR)
May 8, 2009

Information Assurance
Technology Analysis Center (IATAC)

Measuring
Cyber Security and Information Assurance

IATAC

Distribution Statement A

Approved for public release;
distribution is unlimited.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)* D
05/18/2009

2. REPORT TYPE
Report

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Measuring Cyber Security and Information Assurance: A State-of-the-Art Report

5a. CONTRACT NUMBER
SPO700-98-D-4002

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Bartol, Nadya; Bates, Brian; Goertzel, Karen M.; Winograd, Theodore

5d. PROJECT NUMBER

5e. TASK NUMBER
N/A

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
IATAC
13200 Woodland Park Road
Herndon, VA 20171

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Technical Information Center
8725 John J. Kingman Road, Suite 0944
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

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

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Code A / Approved for public release; distribution is unlimited.

13. SUPPLEMENTARY NOTES
IATAC is operated by Booz Allen Hamilton, 8283 Greensboro Drive, McLean, VA 22102

14. ABSTRACT
This Information Assurance Technology Analysis Center (IATAC) State of the Art report (SOAR) provides a representative overview of the current state of the art of the measurement of cyber security and information assurance (CS/IA). It summarizes the progress made in the CS/IA measurement discipline and advances in CS/IA measurement research since 2000. Topics addressed include: terms and definitions used to describe CS/IA measurement; standards, guidelines, and best practices for development and implementation of quantitative and qualitative measures and measurement; activities that provide measurable data and statistics; current efforts to make security more measurable through a variety of protocols and enumerations; research within and outside of the Department of Defense (DoD) and the federal government on the subject of CS/IA measurement; approaches to quantifying economic value of security; existing gaps between expectations and the state of the art, with recommendations for filling these gaps.

15. SUBJECT TERMS
IATAC Collection, SOAR, security, information assurance, cyber security, IA, CS/IA: measurement, metrics, measures, quantification, statistics, ratings, rankings, scoring systems

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
					Tyler, Gene
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**	None	244	**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED			703-984-0775

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

Information Assurance Technology Analysis Center (IATAC)

Measuring Cyber Security and Information Assurance

State-of-the-Art Report (SOAR)
May 8, 2009

Acknowledgements

This SOAR was planned and executed under the guidance of:

Steven King, Ph.D., Associate Director for Information Assurance, Office of the Deputy Under Secretary of Defense (Science and Technology) [DUSD(S&T)], representing the Steering Committee of the Information Assurance Technology Analysis Center (IATAC)

John Frink, Office of the Deputy Under Secretary of Defense (Science and Technology)

Paul Repak, Air Force Research Laboratory/RIGA, the IATAC Contracting Office Representative (COR)

This SOAR was provided for review to a number of organizations across DoD and the civil agencies, industry, and academia. We would also like to thank the following individuals for their incisive and extremely helpful comments on the drafts of this document:

Lee Badger, Ph.D., Computer Scientist, Computer Security Division (CSD), National Institute of Standards and Technology (NIST)

Wayne F. Boyer, Ph.D., Advisory Engineer/Scientist, Idaho National Laboratory

Shari Lawrence Pfleeger, Ph.D., Senior Information Scientist, RAND Corporation

Ronald Ritchey, Ph.D., Booz Allen Hamilton

Angela Orebaugh, Booz Allen Hamilton

Authors
Nadya Bartol
Brian Bates
Karen Mercedes Goertzel
Theodore Winograd

Coordinating Editor
Cynthia Karon

Copy Editor
Lindsay Marti
Jennifer Swartz

Creative Director
Christina P. McNemar

Art Direction and Book Design
Don Rowe

Cover Design
Holly Walton

Illustrations
Tammy Black
Don Rowe

Production
Tammy Black
Kathryn Cummings
Michelle DePrenger
Azadeh Pajouhesh
Ricardo Real
Don Rowe

About the Authors

Nadya Bartol, CISSP, CGEIT, ISSPCS

Nadya Bartol has worked with multiple government and industry organizations to develop and implement information security measurement programs. She co-authored National Institute of Standards and Technology (NIST) guidelines on security measurement, and is one of the primary experts working on ISO/IEC 27004, *Information Security Management Measurement*. Ms. Bartol is serving as Co-Chair of the Department of Homeland Security (DHS) Software Assurance Measurement Working Group (SwA WG), and was the primary author of the group's *Practical Measurement Framework for Software Assurance and Information Security*. She is an active member of the ISO standards community developing information security and privacy standards.

Brian J. Bates, PMP

Brian J. Bates possesses more than 13 years of progressive leadership and experience in the fields of performance measurement and dashboards, project and program management, data center management, and information assurance/security. Mr. Bates possesses a MBA focused on IT Program Management, Human Resources, and Marketing Research, and a BA in Economics and Employment Relations. He received his PMP certification in 2006. Mr. Bates serves the leaders of higher education, commercial, and

government by providing guidance and support to their respective projects and programs. Since 2002, he has been a key lead in efforts to build and support security program offices for federal agencies focusing heavily on security performance measurement and monitoring.

Karen Mercedes Goertzel, CISSP

Karen Mercedes Goertzel leads Booz Allen Hamilton's Security Research Service. She is a subject matter expert in software assurance, cyber security, and information assurance. She was lead author of *Software Security Assurance: A State-of-the-Art Report* (July 2007) and *The Insider Threat to Information Systems* (October 2008), published by the Defense Technical Information Cener (DTIC). Ms. Goertzel has advised the Naval Sea Systems Command (NAVSEA) and the DHS Software Assurance Program; for the latter, she was lead author of *Enhancing the Development Life Cycle to Produce Secure Software* (October 2008). Ms. Goertzel was also a contributing author of the National Security Agency's (NSA) *Guidance for Addressing Malicious Code Risk,* and chief technologist of the Defense Information Systems Agency (DISA) Application Security Program, for which she co-authored a number of secure application developer guides. She contributed to several NIST Special Publications including SP 800-95, *Guide to Secure Web Services.* She also tracks emerging technologies, trends, and research in information assurance, cyber security, software assurance, information quality, and privacy. Before joining Booz Allen (as an employee of what is now BAE Systems), Ms. Goertzel was a requirements analyst and architect of high-assurance trusted systems and cross-domain solutions for defense and civilian establishments in the United States, NATO, Canada, and Australia.

Theodore Winograd, CISSP

Theodore Winograd has been involved in software security assurance and information assurance for over five years, particularly service-oriented architecture security and application security. He has supported the DHS Software Assurance Program, the DISA Application Security Program, and the DISA Net-Centric Enterprise Services project. Mr. Winograd has also supported security engineering efforts for multiple government organizations. Mr. Winograd has served as lead author for multiple NIST Special Publications (SP), including SP 800-95, *Guide to Secure Web Services,* and has served as a contributing author for SOARs for the DoD IATAC.

About IATAC

The Information Assurance Technology Analysis Center (IATAC) provides the Department of Defense (DoD) with emerging scientific and technical information to support information assurance (IA) and defensive information operations. IATAC's mission is to provide DoD with a central point of access for information on emerging technologies in IA and cyber security. These include technologies, tools, and associated techniques for detection of, protection against, reaction to, and recovery from information warfare and cyber attacks that target information, information-based processes, information systems (IS), and information technology (IT). Specific areas of study include IA and cyber security threats and vulnerabilities, scientific and technological research and development, and technologies, standards, methods, and tools through which IA and cyber security objectives are being or may be accomplished.

As one of 10 Information Analysis Centers (IAC) sponsored by DoD and managed by the Defense Technical Information Center (DTIC), IATAC's basic services include collecting, analyzing, and disseminating IA scientific and technical information; responding to user inquiries; database operations; current awareness activities (*e.g.,* the *IAnewsletter, IA Digest,* IA/IO Events Scheduler, Tools Reports, and *IA Research Update*); and publishing critical review and technology assessments (CR/TA) reports and state-of-the-art reports (SOAR).

SOARs provide in-depth analyses of current and emerging technologies and technological trends; based on analyses and syntheses of the latest information produced by research and development activities, SOARs provide comprehensive assessments of those technologies and trends. Topic areas for SOARs are solicited from the DoD IA community to ensure applicability to warfighter needs.

Inquiries about IATAC capabilities, products, and services may be addressed to:

Gene Tyler, Director
13200 Woodland Park Road, Suite 6031
Herndon, VA 20171
Phone: 703/984-0775
Fax: 703/984-0773
Email: iatac@dtic.mil
URL: http://iac.dtic.mil/iatac
SIPRNET: https://iatac.dtic.mil

Table of Contents

About the Authors i
About IATAC iii
Executive Summary xi

Section 1 Introduction 1
1.1 Scope 2
1.2 Audience 3
1.3 Assumptions and Constraints 3
1.4 Terms and Definitions 4
1.5 Document Structure 6

Section 2 Background 10
2.1 Progress Made Since 2000 12
2.2 Perceptions of IA Measurement: Skeptics and Detractors 15
2.3 Research and Emerging Methods 16

Section 3 Laws, Regulations, Standards, and Guidelines 20
3.1 Legal, Regulatory, and Policy-Driven Requirements for Measurement 22
3.1.1 FISMA 22
3.1.2 FEA 23
3.1.3 GPRA and Security Reporting 24
3.1.4 CJCSI 6510.04 and 3401.03 24
3.1.5 Other Security and Privacy-Relevant Legislation Requiring Compliance Verification 25
3.2 NIST SP 800-55 Rev 1: Performance Measurement Guide for Information Security 25
3.3 ISO/IEC 27004 – Information Security Management – Measurement 30
3.4 ISO/IEC 21827, SSE-CMM 31
3.5 ISO/IEC 15408, Evaluation Criteria for Information Technology Security 33
3.6 FIPS 140 Evaluation 34
3.7 NSA INFOSEC Assurance – IA-CMM 35
3.8 ISA ISA99 – Manufacturing and Control Systems Security 36

Section 4 Best Practices 40
4.1 Practical Measurement Framework for Software Assurance and Information Security 41
4.2 Assurance for CMMI 43

Section 5 Government Initiatives and Programs 46
5.1 DoD IA Metrics Program 47
5.1.1 OASD(NII) Efforts 48
5.1.2 DON CIO Efforts 49
5.1.3 Mission Oriented Risk and Design Analysis (MORDA) 49
5.2 DHS 51
5.2.1 DHS NIPP and Cyber Security Metrics 51
5.2.2 DHS/DoD/NIST Software Assurance Measurement Working Group 52
5.2.3 US-CERT Cyber Security Metrics for Control Systems 54
5.3 NIST 54
5.3.1 SAMATE 54
5.3.2 Attack-Based Measures 55
5.3.3 SCAP 56
5.4 OMB FISMA Measures 57
5.5 NASA Metrics Programs 60
5.5.1 NASA JPL Information Security Metrics Program 60
5.5.2 Comparison of NASA and DoD IA Metrics Programs 60
5.5.3 NASA Deputy CIO Information Security Performance Measures 61
5.6 BJS NCSS 62

Section 6 Industry Initiatives 66
6.1 CISWG Metrics 67
6.2 OWASP Efforts 68
6.2.1 OWASP Top Ten 68
6.2.2 Application Security Metrics Project 69
6.2.3 ASVS 69
6.3 CIS Security Metrics Initiative 71
6.4 ISACA 72
6.5 Securitymetrics.org 75
6.6 Security Knowledge and Awareness Measures 76
6.7 PSM Security Measurement 80
6.8 Microsoft Security Measures 81
6.8.1 DREAD 81
6.8.2 RASQ 82
6.9 ISECOM RAVs 83
6.10 @Stake BAR 84
6.11 EDUCAUSE/Internet 2 Security Task Force Sub-Working Group on Security Metrics 84
6.12 JCIAC: Statistics for Computer-Related Crime 85
6.13 DRM Effectiveness and Impact Measures 86
6.14 Web Application Security Metrics Framework 86
6.15 SecMet 87
6.16 Surveys of "Real World" CS/IA Measurement Usage 88

6.16.1 Frost & Sullivan 2005 Survey of Private Sector IT Security Metrics Usage 88
6.16.2 Forrester Research 2007 and 2008 CISO Surveys 89
6.17 Commercial Providers of CS/IA Measurement Services 90

Section 7 Measurable Data 94
7.1 Red/Blue Team Evaluations 95
7.2 Network Management and Security Measures 98
7.3 Software Testing Output 99
7.4 Scoring Schemes 101
7.4.1 CVSS 101
7.4.2 Chris Wysopal's CWE System Scoring 105
7.4.3 CCSS 105
7.4.4 CMSS 106
7.4.5 CWSS 106
7.4.6 Software Vendor Vulnerability Severity Ratings 107
7.4.7 Vulnerability Reporting/Advisory Service Ratings 107
7.4.8 Attack and Threat Scoring Systems 108
7.5 Vulnerability Assessment and Management 109
7.5.1 IAVA Statistics 109
7.5.2 US-CERT Vulnerability Note 110
7.6 Risk Management and Compliance Outputs 110
7.6.1 CNDSP C&A 111
7.6.2 NIST FDCC Compliance Metrics Initiative 113
7.6.3 C&A Risk Measures 114
7.6.4 Risk Measures from Event-Driven Security Products 115
7.7 Measures Categorization and Taxonomy Efforts 115
7.7.1 WISSSR Structure 116
7.7.2 NIST Types of Measures 117
7.7.3 I3P Taxonomy of Security Metrics for Process Control Systems [154] 118
7.7.4 Department of Public Safety and Emergency Preparedness Canada Taxonomy [155] 120
7.7.5 VTT Technical Research Centre of Finland Security Metrics Taxonomy for R&D Organizations [156] 121
7.7.6 Daniel Geer's Balanced Scorecard-based Taxonomy 122
7.8 Quantifying the Economic Value of Security and Assurance 123

Section 8 Tools and Technologies 130
8.1 Integration 132
8.2 Collection/Storage 133
8.3 Analysis/Assessment 134
8.4 Reporting 137

Section 9 Recommendations 142
9.1 Stakeholder Expectations 143
9.2 Success Factors 144
9.3 Methodology Gaps 146
9.4 Technology Gaps 147
9.5 Knowledge Base Gaps 148

Appendix A Abbreviations, Acronyms, and Definitions 150

Appendix B Resources 158
B.1 Materials Used in Developing this SOAR 158
B.2 Additional Print Sources of Information for Suggested Reading 170
B.3 Additional Online Sources of Information for Further Reading 170
B.4 Publicly Available CS/IA Measures Lists 172

Appendix C CS/IA Measurement Before 2000 174
C.1 Background 174
C.2 Annualized Loss Expectancy as a CS/IA Measure 175
C.3 DARPA IASET Measures of Assurance Research: Value-Focused Thinking 177
C.4 RAI 178
C.5 D-IART 178
C.6 SM Framework [180] 179

Appendix D Conferences and Workshops 180
D.1 Workshop on Information Security System Scoring and Ranking (WISSSR) 180
D.2 Fourth Workshop on Assurance Cases for Security "The Metrics Challenge" 181
D.3 Workshop on "Measuring Assurance in Cyberspace" 181
D.4 MetriCon and Mini-MetriCon 182
D.5 International Workshop on Quality of Protection "Security Measurements and Metrics" 182

Appendix E Research and Emerging Methods Summary 184

Appendix F Why is CS/IA Measurement Challenging 212
F.1 IRC Hard Problem No. 8 Enterprise-Level Security Metrics Definition: 212
F.2 NSTC IWG on Cyber Security and Information Assurance Federal Plan for Cyber Security and Information Assurance Research and Development 216

List of Figures

Figure 3-1 Information Security Measurement Program Implementation Process [26] 27
Figure 3-2 Information Security Measures Development Process [27] 27
Figure 3-3 ISO/IEC 21827 Architecture [33] 32
Figure 4-1 Practical Measurement Framework for Software Assurance and InformationSecurity [44] 43
Figure 5-1 Software Assurance Measure Example [55] 53
Figure 6-1 Most Prevalent Measures Reported to Non-IT Managers [120] 89
Figure 7-1 CVSS Framework [136] 102
Figure 8-1 Security Dashboard Example [169] 140
Figure 9-1 Information Security Measurement Program Maturity Path [171] 145

List of Tables

Table 1-1 Audience and Uses of the *Measuring Cyber Security and Information Assurance* SOAR 3
Table 1-2 CS/IA Measurement Terminology Summary 4
Table 1-3 Definitions of "Metrics," "Measures," and "Measurement" 5
Table 2-1 Surveys of CS/IA Measurement "State-of-the-Art" 12
Table 2-2 CS/IA Measurement Discipline Progress Summary 13
Table 3-1 NIST SP 800-55 Rev. 1 Document Structure 26
Table 3-2 Measures Template and Instructions [28] 28
Table 5-1 Selected DoD IA Metrics Working Group Metrics [50] 49
Table 5-2 Set of 10 Core Technical Security Metrics with Corresponding Ideals [57] 54
Table 5-3 SCAP Components [65] 56
Table 5-4 Government-wide Security Status and Progress from Fiscal Years 2002 to 2007 [74] 58
Table 5-5 FISMA IG Assessments Government-Wide in Fiscal Year 2007 Results Excerpt [76] 59
Table 5-6 Comparison of DoD, USAF, and NASA JPL IA Metrics Programs [80] 61
Table 6-1 CIS Consensus Security Metrics 71
Table 6-2 IsecT Information Security Awareness Metric 78
Table 6-3 Gartner Group Metrics for Information Security Awarenes 79
Table 6-4 Example of DREAD Rating of Two Attacks 82
Table 6-5 EDUCASE/Internet 2 Security Metrics 85
Table 6-6 IA Measurement Service Providers 90
Table 7-1 Metrics Data Captured by IDART Red Team Activities 96
Table 7-2 Categories of IDART Red Team Metrics 97

Table 7-3 Software Testing Measures 100
Table 7-4 CVSS Metrics by Metric Group 103
Table 7-5 DISA Vulnerability Compliance Tracking System Measures 109
Table 7-6 WISSSR Measures 116
Table 7-7 NIST Types of Measures 117
Table 7-8 Mapping of Measurable Security Elements to Metrics Categories 119
Table 7-9 I3P Taxonomy of Security Metrics for Process Control Systems 120
Table 7-10 Department of Public Safety and Emergency Preparedness Taxonomy 121
Table 7-11 VTT Technical Research Centre of Finland Security Metrics Taxonomy for R&D 121
Table 7-12 Daniel Geer's Balanced Scorecard Taxonomy with Sample Metrics 123
Table 8-1 CS/IA Measurement Integration (Frameworks/Platforms) Tools 132
Table 8-2 CS/IA Measurement Collection/Storage Tools 133
Table 8-3 CS/IA Measurement Analysis and Assessment Tools 134
Table 8-4 CS/IA Measures Reporting Tools 138
Table 9-1 Common CS/IA Measurement Stakeholder Expectations 143
Table C-1 Renowned Existing CS/IA Measures 175
Table E-1 CS/IA Measurement Research 185

Executive Summary

The rapid growth of connections, processing, bandwidth, users, and global dependence on the Internet has greatly increased vulnerabilities of information technology (IT) infrastructure to increasingly sophisticated and motivated attacks. Despite significantly increased funding for research, development, and deployment of information assurance (IA) defenses, reports of attacks on, and damage to the IT infrastructure are growing at an accelerated rate.

While a number of cyber security/IA (CS/IA) strategies, methods, and tools exist for protecting IT assets, there are no universally recognized, reliable, and scalable methods to measure the "security" of those assets. CS/IA practitioners' success in protecting and defending an uninterrupted flow of information on IT systems and networks is critically dependent upon their ability to accurately measure in real time the security status of the local system as well as on their understanding of the security status of regional, national, and international networks.

This report assesses the current "state of the art" in CS/IA measurement to facilitate further research into this subject. Progress has been made, but much remains to be done to achieve the goal of real-time, accurate CS/IA measurement. Enabling such measurement would make it is possible to understand, improve, and predict the state of CS/IA.

While the CS/IA measurement discipline—which encompasses a number of associated areas of interest, including system security, software assurance, and privacy—is still evolving, progress has been made since the Defense Technical Information Center's (DTIC) Information Assurance Technical Analysis Center (IATAC) published its *IA Metrics* Critical Review/Technology Assessment (CR/TA) Report nearly 10 years ago. Clear themes and success factors have emerged as a result of research, publication of standards and guidelines, and a number of government and industry initiatives. However, further efforts are needed to advance the CS/IA measurement discipline, including new policy, processes, and research.

Increasing awareness is needed within the stakeholder community about what is required to make measures useful for quantifying and improving CS/IA. This shared understanding is critical to defining and mounting successful research and implementation efforts in this field.

The following are critical success factors for organizations that embark on implementing CS/IA measures—

- Management commitment to provide appropriate resources for CS/IA measurement programs, to use CS/IA measures produced by these programs for decision making, and to mature those programs over time;
- Investment in obtaining solid data that can support increased fidelity of and confidence in produced results;
- Continuous use of CS/IA measures to proactively determine and implement CS/IA improvements;
- Establishment of meaningful and easy to use measures to ensure maximum usability and cost-effectiveness of CS/IA measurement.

Background

The CS/IA measurement discipline has experienced significant positive change since 2000, when debates raged about whether measuring CS/IA was even possible, how measurement could be performed (*i.e.*, what processes should be used, what should be measured), and whether measuring "it" would even be useful. Today, many building blocks are in place to enable further progress and research, and IA practitioners mostly agree that CS/IA measurement is valuable and desirable.

In July 2003, the National Institute of Standards and Technology (NIST) published its Special Publication (SP) 800-55, *Security Metrics Guide for Information Technology Systems*, which represented one of the first major efforts to define CS/IA measurement, and to provide a methodology for implementing CS/IA measurement across the federal government. The SP was revised in July 2008 to bring it into closer alignment with legislative and regulatory requirements and with emerging best practices in the CS/IA measurement field.

State of the Art

The current state of the art for CS/IA measurement is characterized briefly below.

Standards, Guidelines, and Best Practices Documents

Standards, guidelines, and best practices documents have emerged to define and describe processes, frameworks, and metamodels for CS/IA measurement. Those interested in embarking upon CS/IA measurement can use and tailor these standards and guidelines to structure their programs and processes in a robust and repeatable way to facilitate long-term viability and success. Generally, these standards and guidelines fall into the following categories—

- Processes for developing information security measures to assess effectiveness of enterprise or system-level security controls and implementing the measures (These types of documents often include example measures, such as "percentage of high impact vulnerabilities mitigated within organizationally defined time periods after discovery," "percentage of users with access to shared accounts," and "number of relevant attack patterns covered by executed test cases");
- Maturity model frameworks that provide a method for evaluating IA processes and assigning a maturity level to a grouping of security processes, based on specific criteria (These frameworks provide a means for benchmarking of IA aspects of projects and organizations against these criteria.);
- Product evaluation frameworks that assess the level of assurance CS/IA products provide against specific criteria, and assigning a product evaluation level based on these criteria.

"Measurable" Data

An abundance of CS/IA data can now be collected, analyzed, and presented *via* a variety of manual, and semi- and fully automated techniques and tools. The resulting measurable data can be used to combine, correlate CS/IA data and report status to decision makers, and to create and employ increasingly sophisticated, complex CS/IA measures to advance overall understanding of CS/IA status and health. Emerging enumeration and scoring systems, such as Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), and Common Vulnerabilities Common Scoring System (CVSS), provide uniform means for quantification, ranking, and evaluation of CS/IA, and enable identification, prioritization, and targeted remediation of specific weaknesses or vulnerabilities, based on severity and impact.

Regulatory Drivers and Federal Government Activity

Numerous laws, rules, and regulations include or imply requirements for CS/IA performance measurement; for example, most IA compliance verification requirements are best satisfied using measurement techniques. Many CS/IA measurement tools and measures are being generated as a means of demonstrating compliance with legislation, regulation, and policy, such as the Federal Information Security Management Act (FISMA) and the President's Management Agenda (PMA).

The federal government has become increasingly active in pursuit of CS/IA measurement, and has established a number of programs to—

- Provide guidance for implementing measurement programs within the government,
- Research additional measures for future programs,
- Provide oversight by measuring the security posture of different government systems and agencies.

Industry Initiatives

A multiplicity of industry consortia are working to create, implement, and deploy CS/IA measures of various sorts, including the Center for Internet Security (CIS), Open Web Application Security Project (OWASP), securitymetrics.org, and others. The goal of these industry initiatives is to improve CS/IA measurement programs throughout both industry and government; much of their work is publicly accessible.

Research Landscape

Research abounds within academic, industrial, and government research organizations to define meaningful measures and measurement methodologies of the security and assurance of technologies and processes, criticality of vulnerabilities, and severity of threats and attacks. Government research efforts have most notably focused on context-specific approaches to measurement of software assurance, control system security, and attack-based measurement.

Industry research has also focused on specific CS/IA measurement approaches and lists of measures, and on providing community forums for practitioners and others interested in the CS/IA measurement discipline.

Automation through Tools

Automated tools are available that provide a means to non-intrusively collect quantifiable data that can facilitate better quality of measurement. However, aside from some compliance and analytical tools, few commercial software products are being actively marketed as CS/IA measurement tools. Most tools that serve this purpose are purpose-built custom applications, which may or may not incorporate commercial technologies. While there is much

information posted on the Web about CS/IA measurement methodologies, lessons learned, sound practices, and examples, there is little available public information regarding CS/IA measurement tools.

Recommendations for Further Research

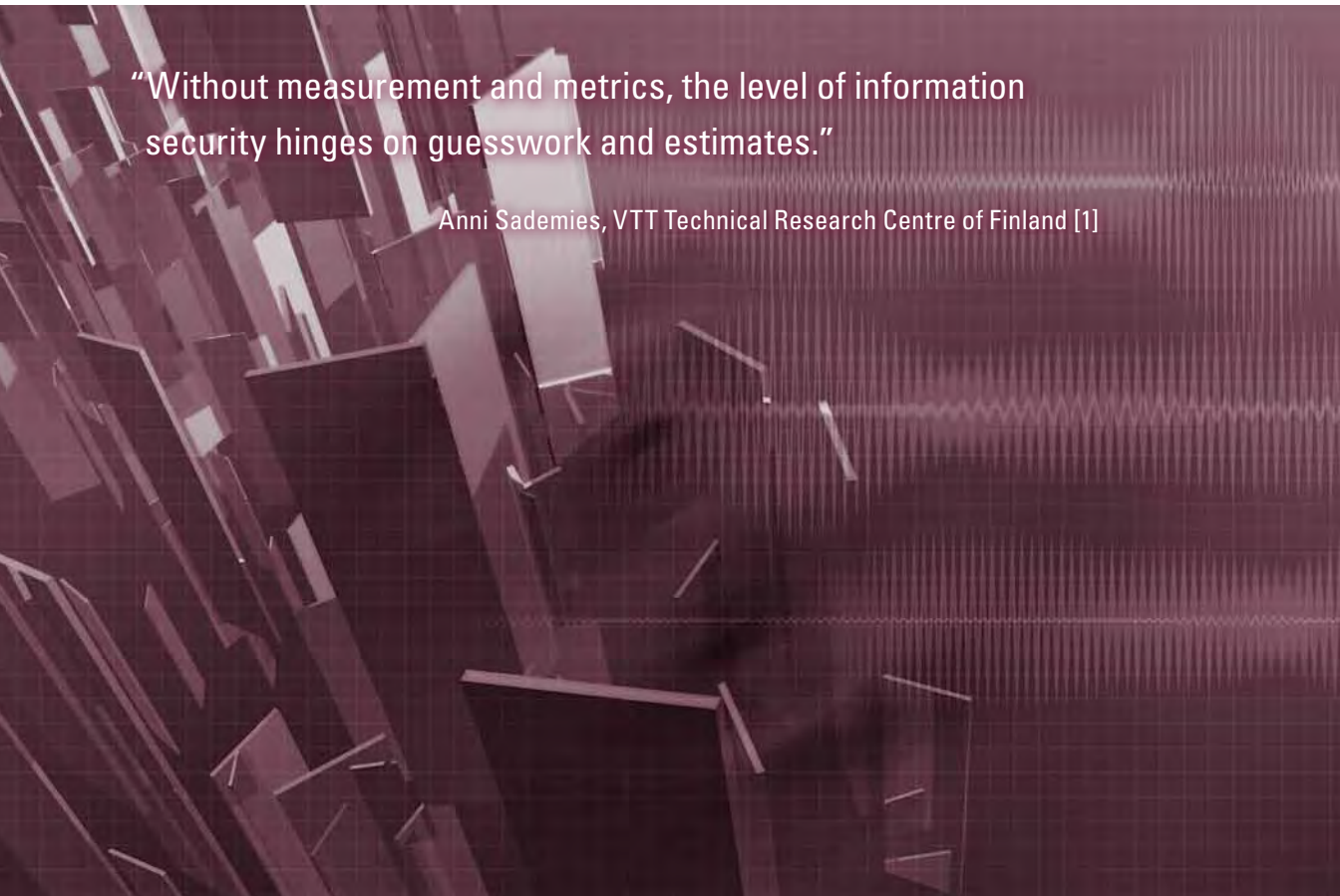
Work continues in the CS/IA community to define what exactly is measurable, which measures are most useful and meaningful, and how to maximize the value of measurement. However, those in the CS/IA stakeholder community still vary in their expectations and opinions regarding the feasibility of CS/IA measurement, and the value that CS/IA measurement can provide.

Further progress is required to reach the desired end state that has been defined by many stakeholders, including researchers and users of CS/IA measures and measurement methodologies. The following are areas in which further effort is needed to advance the state of the art—

- A standard set of converged definitions and vocabulary needs to be adopted for discussions of CS/IA measurement and measures.
- Common data formats for expressing CS/IA measures information need to be developed and adopted across commercial CS/IA measurement tools and methodologies.
- Existing CS/IA measurement efforts need to be actively sustained and advanced.
- Organizations need to define and adopt standardized sets of minimum measures and standardized techniques for measurement.
- Methodologies for creating real-time measures need to be researched and implemented to provide immediate feedback and diagnosis of security events (*e.g.*, intrusions).
- Methodologies for creating "self-healing" measures need to be developed, whereby a measurement threshold would trigger the autonomic response, correction, *etc.*, of the condition that tripped the threshold.
- There needs to be investment into data modeling of CS/IA measures and measurable outcomes associated with CS/IA activities.
- Measurement expertise and lessons learned from other disciplines, such as quality and safety, should be leveraged to refine and improve CS/IA measurement.
- Training/education and, ultimately, professional certification need to be made available to create a skilled/trained labor force that is expert in and dedicated to CS/IA measurement.

1

Introduction



"Without measurement and metrics, the level of information security hinges on guesswork and estimates."

Anni Sademies, VTT Technical Research Centre of Finland [1]

Measuring information assurance (IA) and cyber security has occupied the minds of information security practitioners for a long time. Enabling such measurement would mean that it is possible to understand, improve, and predict the state of IA and cyber security, which is still an elusive objective.

While cyber security and information assurance (CS/IA) measurement is an evolving discipline, much progress has been made in the last 10 years. Clear themes and success factors have emerged as a result of research, publication of standards and guidelines, and a number of United States (US) government and industry initiatives.

This State of the Art Report (SOAR) presents the current state of the CS/IA measurement discipline and associated areas of interest, such as system security, software assurance, and privacy. It summarizes the progress made in the CS/IA measurement discipline since the publication by the Defense Technical Information Center's (DTIC) Information Assurance Technical Analysis Center (IATAC) of its Critical Review/Technology Assessment (CR/TA) Report, titled *IA Metrics* (available for download from .gov and .mil at: http://iac.dtic.mil/iatac/pdf/ia_metrics.pdf).

This SOAR also identifies gaps in the current efforts and proposes areas of focus for the future to enable further progress in the CS/IA measurement discipline.

1.1 Scope

This *Measuring Cyber Security and Information Assurance* SOAR includes a broad set of subjects, from current CS/IA measures development methodologies and the multitude of definitions of CS/IA measures, to research on attack-based measures and software assurance measurement. The report lists currently used terms and definitions that describe CS/IA measurement activities found in national and international standards and best practices documents, including those addressing IA, cyber security, and information security.

The SOAR summarizes existing standards, guidelines, and best practices for development and implementation of CS/IA measurement, including those defined by the National Institute of Standards and Technology (NIST), International Organization for Standardization (ISO), Department of Homeland Security (DHS) Software Assurance (SwA) Measurement Working Group (WG), Open Web Application Security Project (OWASP), securitymetrics.org, and others. The SOAR addresses both quantitative and qualitative measures, such as maturity model rankings and other ratings methods.

This report describes a variety of CS/IA activities that provide measurable data and statistics on IA, which are sometimes referred to as "measures" or "metrics," such as blue team/red team evaluations, Computer Network Defense (CND) assessments, static and dynamic code reviews, vulnerability and network management, Federal Information Security Management Act (FISMA) evaluations, Certification and Accreditation (C&A), and other activities.

The SOAR also describes current efforts to make security more measurable through a variety of protocols and enumerations as well as through activities that leverage these protocols and enumerations. These activities include the National Vulnerabilities Database (NVD), Common Vulnerabilities and Exposures (CVE), Common Weakness Enumeration (CWE), Common Configurations Enumeration (CCE), Common Vulnerabilities Common Scoring System (CVSS), Common Configurations Scoring System (CCSS), and Secure Content Automation Protocol (SCAP) Program. This SOAR provides pointers and links to publicly available CS/IA measures lists, including those available from NIST Special Publication (SP) 800-55 Revision (Rev.) 1, *Performance Measurement Guide for Information Security,* July 2008, DHS SwA Measurement WG, and others.

The SOAR summarizes existing research within and outside of the Department of Defense (DoD) and the federal government on the subject of CS/IA measurement, and identifies gaps in the research. The report also summarizes current views and existing approaches to quantifying economic value of security, such as return on investment (ROI) and other economic indicators, and identifies linkages with CS/IA measurement activities required to support creation of these economic indicators.

Finally, the SOAR also addresses the reasons why so many CS/IA measurement efforts fall short of the expectations that stakeholders place on these efforts, and describes characteristics of successful efforts. The SOAR identifies existing gaps between expectations and the state of the art, and provides recommendations for filling the identified gaps, where appropriate.

This SOAR is not intended to provide a comprehensive or exhaustive depiction of the entire CS/IA measurement discipline. Rather, it seeks to provide enough information to accurately represent the current state of the art in CS/IA measurement and associated research, without covering every single set of CS/IA measures, CS/IA measurement model or methodology, or CS/IA measurement activity or research project undertaken in the past decade.

1.2 Audience

This *Measuring Cyber Security and Information Assurance* SOAR is intended to speak to a broad audience of CS/IA practitioners, researchers, and government officials. The authors of the report hope that its readers will use the SOAR for a number of purposes, as depicted in Table 1-1.

Table 1-1 Audience and Uses of the *Measuring Cyber Security and Information Assurance* SOAR

	Education and Awareness	Future Research	Lessons Learned	Value and Appropriate Expectations
Government and industry CS/IA practitioners	✔	✔	✔	✔
Science and technology/research and development community, including DoD and civil agency Science and Technology (S&T) organizations and Research and Development (R&D) labs, and academic and industry research organizations that support the government	✔	✔	✔	✔
Senior DoD and civil agency officials responsible for governance, compliance, certification, accreditation, risk management, and/or any aspect of CS/IA or Information Technology (IT)-related metrics/ measurement	✔	✔	✔	✔

1.3 Assumptions and Constraints

In this document, "CS/IA" is used in the broadest possible sense to include the following disciplines: IA, computer security, cyber security, network security, information technology security, system security, system assurance, software security, software assurance, application security, privacy, and quality of protection. CS/IA is also used to address security, privacy, and related assurance concerns, activities, and practices within business and technical processes.

The authors of this SOAR assume that the reader is well-versed in CS/IA concepts and terminology. The authors also assume that the reader has a basic understanding of measurement concepts before undertaking to read this SOAR.

The source material used by the authors in preparing this SOAR was limited to publicly accessible and open source information that is unclassified and without distribution restriction.

The time frame covered by this SOAR, and considered to represent the current "state of the art," is 2000 to the present.

1.4 Terms and Definitions

> ***"There is often confusion with the words we use when discussing measurement—metrics, measures, indicators, and predictors are frequently used interchangeably." [2]***

The terms "metric," "measure," and "measurement" tend to be considered interchangeable across the CS/IA community. Based on the research performed for this SOAR, there is a distinction between how these terms are viewed, as illustrated in Table 1-2.

Table 1-2 CS/IA Measurement Terminology Summary

Term	Definition
A measurement	Raw data that quantifies a single dimension of the thing to be measured, *e.g.,* the number of vulnerabilities in a software module
Metric	Data processed from two or more measurements to demonstrate a significant correlation between them; for example the correlation between "number of vulnerabilities" (measurement #1) and "number of lines of code" (measurement #2)—a metric that demonstrates a direct relationship between the size of a software module and the number of vulnerabilities it contains. Metrics can, in this way, be used to quantify the degree to which a system, component, or process possesses a given security attribute.
Measure	Same as metric. Adopted by national and international standards and guidelines in lieu of "metric."
Measurement	The act (or process) of measuring

Many IA-focused standards and documents define "metrics," "measures," and/or "measurement" generically, without qualifying that their definitions apply to *IA* metrics/measures/measurement. It is expected that because these standards/documents are IA-focused, readers understand that IA is the intended context for these definitions.

Various measurement scales should be considered for CS/IA measurement: nominal, ordinal, interval, and ratio. It is important to note that CS/IA measures tend to be ordinal.

The word "metric," used by many in the industry, has been slowly disappearing from national and international standards and guidelines, which increasingly favor the term "measure" (in lieu of "metric") to indicate a quantifiable statement, with "measurement" being the process of obtaining a

measure. For example, while the original NIST SP 800-55, *Performance Measurement Guide for Information Security,* published in July 2003, used the word "metric," Rev. 1 of this Special Publication, published in July 2008, uses the word "measure." International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 27004, *Information technology – Security techniques – information security management – Measurement,* [3] and ISO/IEC 15939, *Systems and software engineering – Measurement process,* [4] use the word "measures" as well.

Regardless of specific terminology, there appears to be near-universal agreement that the ability to quantify the effectiveness of security protections/ countermeasures and the security of processes are highly desirable.

Table 1-3 lists leading definitions of "metric(s)," "measure(s)," and "measurement," specifically those presented in documents about IA (in the broad sense in which it is used in this document), and those that directly pertain to quantification or measurement in the context of IA.

Table 1-3 Definitions of "Metrics," "Measures," and "Measurement"

Definition	Source
Metrics—Data used to facilitate decision-making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data	Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson. NIST SP 800-55 Rev. 1, *Performance Measurement Guide for Information Security.* Accessed 19 December 2009 at: *http://csrc.nist.gov/publications/nistpubs/800-55-Rev.* 1/ SP800-55-rev1.pdf.
Measure—[5] A variable to which a value is assigned as the result of measurement	ISO/IEC 27004, *Information Technology – IT Security Techniques – Information Security Management – Measurement* and ISO/IEC 15939, *Systems and software engineering – Measurement process. [6]*
Measurement—The process of obtaining information about the effectiveness of Information Security Management Systems (ISMS) and controls using a measurement method, a measurement function, an analytical model, and decision criteria	ISO/IEC 27004, *Information technology – Security techniques – Information security management – Measurement*
Security Metrics—A set of key indicators that tell [organizations] how healthy their security operations are, on a stand-alone basis and with respect to peers	Andrew Jaquith. *Security Metrics: Replacing Fear, Uncertainty, and Doubt.* (Upper Saddle River, NJ: Addison-Wesley, 2007)
Security Metric—A measurement that is coupled with a scale or benchmarks to evaluate security performance	Institute for Information Infrastructure Protection
Security Metric—The standard measurement of computer security	Rosenblatt, Joel. "Security Metrics: A Solution in Search of a Problem," in *EDUCAUSE Quarterly,* Vol. 31 No. 3, July-September 2008. Accessed 22 December 2008 at: *http://connect.educause.edu/Library/ EDUCAUSE+Quarterly/SecurityMetricsASolutioni/47083*

Definition	Source
Metric—A system of related measures enabling quantification of some characteristic. A measure is a dimension compared against a standard. Security metric—A system of related dimensions (compared against a standard) enabling quantification of the degree of freedom from possibility of suffering damage or loss from malicious attack	Abbadi, Zed, The Public Company Accounting Oversight Board. "Security Metrics: What Can We Measure?" Presented at OWASP Northern Virginia Chapter Meeting, Herndon, Virginia, 19 April 2007. Accessed 2 January 2009 at: *http://www.owasp.org/images/b/b2/Security_Metics-_What_can_we_measure-_Zed_Abbadi.pdf*
Metrics—Quantifiable measurements of some aspect of a system or enterprise. For an entity (system, product, or other) for which security is a meaningful concept, there are some identifiable attributes that collectively characterize the security of that entity. Security metric (or combination of security metrics)—A quantitative measure of how much of that attribute the entity possesses. A security metric can be built from lower-level physical measures. Security metrics focus on the actions (and results of those actions) that organizations take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defenses are breached.	SSE-CMM Security Metrics. Accessed 6 January 2009 at: *http://www.sse-cmm.org/metric/metric.asp*
IA Metrics—(1) Standards of measurements used in IA; (2) evaluation of overall security "goodness" or quality, or the quality of some specific attribute; (3) measures that gauge an organization's ability to protect against, detect and respond to IA attacks; and/or (4) IA performance trends over time based on repeatable measurements at regular intervals	Participants in the 2001 Workshop on Information Security System Scoring and Ranking (WISSSR) [7]

The remainder of the SOAR uses the terms used in the original materials summarized in this SOAR. When no term is used, the SOAR uses the term "measure" to the maximum possible extent.

1.5 Document Structure

In addition to the executive summary, this SOAR is composed of nine sections and six appendices, described below—

- **Section 1. Introduction**—Provides the rationale for publishing this SOAR and describes the intended audience and content. In addition, the Introduction describes several definitions of the terms "metric," "measure," and "measurement" that are in use.
- **Section 2. Background**—Provides an overview of the progress of CS/IA measurement research and practice since 2000, cross-referencing the rest of the document where applicable. It summarizes background information on previous surveys of the CS/IA measurement state of the art, in particular, the IATAC *IA Metrics* CR/TA released in 2000. This section also provides insight into criticism of CS/IA measurement as well as a brief discussion of ongoing CS/IA measurement research.

- **Section 3. Laws, Regulations, Standards, and Guidelines**—Provides an overview of relevant laws and regulations as well as major standards and guidelines published at the time of this writing.
- **Section 4. Best Practices**—Provides a general overview of published best practices that describe the development and implementation of CS/IA measurement programs and activities.
- **Section 5. Government Initiatives and Programs**—Provides an overview of CS/IA measurement initiatives and programs run by the federal government. Specifically, this section focuses on activities underway at DoD, DHS, NIST, Office of Management and Budget (OMB) and National Aeronautics and Space Administration (NASA).
- **Section 6. Industry Initiatives**—Provides an overview of CS/IA measurement initiatives and programs within industry, illustrating the large number of efforts underway for creating, implementing, and deploying measures. There is a wide range of interest in CS/IA measurement throughout industry, including security consulting firms, commercial off-the-shelf (COTS) product vendors, and security consortia as well as organizations dedicated solely to the advancement and development of CS/IA measures and measurement techniques.
- **Section 7. Measurable Data**—Provides an overview of various activities that collect and capture IA-related data that can be used to produce CS/IA measures.
- **Section 8. Tools and Technologies**—Provides an overview of the tools and technologies available for gathering, processing, and reporting CS/IA measures within an organization. Specifically, this section provides lists of tools needed to support CS/IA measurement: integration, collection/storage, analysis, and reporting.
- **Section 9. Recommendations**—Provides observations and recommendations that resulted from the analysis of the data gathered for this report, specifically regarding common CS/IA stakeholder expectations, success factors, gaps in current approaches, and areas for additional investment and research.
- **Appendix A. Abbreviations, Acronyms, Definitions**—Lists and amplifies all abbreviations, acronyms, and definitions used in this SOAR.
- **Appendix B. Resources**—Lists online and print works and other resources cited and suggested for further investigation by interested readers.
- **Appendix C. CS/IA Measurement Before 2000**—Summarizes CS/IA measurement efforts performed prior to the period addressed in this SOAR. Specifically, this appendix describes the use of Annualized Loss Expectancy, Value-focused Thinking, Resilience Assurance Index, Defense Information Assurance Red Team Methodology, and the Security Measurement Framework.

- **Appendix D. Conferences and Workshops**—Lists conferences and workshops for further investigation by interested readers.
- **Appendix E. Research and Emerging Methods Summary**—Lists current CS/IA measurement research activities with short summaries of these efforts.
- **Appendix F. Why Is CS/IA Measurement Challenging**—Discusses the Information Security (INFOSEC) Research Council's *Hard Problems List* and National Science and Technology Council Interagency Working Group on Cyber Security and Information Assurance's *Federal Plan for Cyber Security and Information Assurance Research and Development*, which describe the difficulties associated with CS/IA measurement research.

References

1 Anni Sademies, VTT Technical Research Centre of Finland. *Process Approach to Information Security Metrics in Finnish Industry and State Institutions*. Thesis for University of Oulu, Finland; published as VTT Publication 544, 2004. Accessed 6 January 2009 at: *http://www.vtt.fi/inf/pdf/publications/2004/P544.pdf*

2 Rayford B. Vaughn and Ambareen Siraj, Mississippi State University, and Ronda Henning, Harris Corporation, Government Communications Systems Division. "Information Assurance Measures and Metrics—State of Practice and Proposed Taxonomy," in *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS-36),* 6-9 January 2003. Accessed 19 January 2008 at: *http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.71.184*

-and-

Rayford B. Vaughn, Ambareen Siraj, and David A. Dampier, Mississippi State University. "Information Security System Rating and Ranking." *CrossTalk: The Journal of Defense Software Engineering,* May 2002. Accessed 19 January 2009 at: *http://www.stsc.hill.af.mil/crosstalk/2002/05/vaughn.html*

3 IsecT Ltd. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27004, *Information Technology – IT Security Techniques – Information Security Management – Measurement (Draft).* Accessed 20 April 2009 at: *http://www.iso27001security.com/html/27004.html*

4 International Organization for Standardization. Abstract available at: *http://www.iso.org/iso/catalogue_detail.htm?csnumber=44344 (accessed 20 April 2009).*

5 This definition applies to what some sources refer to as "a measurement," not to be confused with "measurement," which is the act of measuring. Note that the term "measures" is used to refer collectively to base measures, derived measures, and indicators. For example, the comparison of a measured defect rate to a planned defect rather, along with the assessment of whether or not the discrepancy between them indicates a problem.

6 The source documents avoid the term "metrics" altogether. However, the document's definition of the term "measurement results," *i.e.,* "one or more indicators and their associated interpretations that address an information need," makes it clear that "measurement results" is a new term intended to replace to what many sources refer to as "metrics."

7 Applied Computer Security Associates and The MITRE Corporation (co-sponsors) *Proceedings: Workshop on Information Security System Scoring and Ranking Information System Security Attribute Quantification or Ordering (Commonly but improperly known as security metrics),* Williamsburg, Virginia, May 21-23, 2001, (commonly referred to as the Workshop on Information Security System Scoring and Ranking [WISSRR]). Accessed 8 April 2009 at: *http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf*

2

Background

"The dearth of quantitative methods for measuring, forecasting, and improving computer security has left those of us who depend on information systems in a precarious state.... Because quantitative metrics have not been available, our security decisions have instead relied upon the opinions of those believed to be experts, anecdotal evidence, and other heuristics."

Stuart Edward Schechter, Harvard University [8]

In 2000, IATAC released its CR/TA entitled *IA Metrics,* [9] which intended to engender and facilitate the discussion of measurement within the IA community, and to provide guidance to organizations in the development of IA metrics and the establishment of organizational IA metrics programs. Specifically, the CR/TA described a metrics development methodology (with specific examples of metrics that could be derived when the methodology was used) that later formed the basis for NIST SP 800-55, *Security Metrics Guide for Information Technology Systems,* [10] published in July 2003.

To some extent, the CR/TA also provided a "snapshot" of the state of the art of the CS/IA measurement discipline in the late 1990s, including descriptions of ongoing initiatives at that time to develop, collect, and use CS/IA measures.

In terms of depicting the state of the art, this SOAR picks up where that CR/TA left off, providing a more extensive and detailed depiction of the state of the art of CS/IA measurement since the CR/TA's publication in 2000.

In addition to the *IA Metrics* CR/TA, a number of research reports, papers, and books predating this SOAR have attempted to characterize the state of the art of CS/IA measurement. Appendix C provides a more detailed description of some of the concepts and research produced before 2000 when the CR/TA was published.

Since 2000, further reports, papers, and books have been published that are dedicated to the study of CS/IA measurement and proposing ways and means for implementing it. The most noteworthy among these surveys are listed in Table 2-1.

Table 2-1 Surveys of CS/IA Measurement "State-of-the-Art"

Reference	CS/IA Measurement Content
Martin Stoddard, Deborah Bodeau, Rolf Carlson, Cliff Glantz, Yacov Haimes, Chenyang Lian, Joost Santos, James Shaw. "Process Control System Security Metrics—State of Practice," I3P Research Report No. 1, August 2005. Accessed 1 April 2009 at: *http://www.thei3p.org/docs/publications/ResearchReport1.pdf*	Appendix A provides an extensive survey of security measurement activities and resources, with matrices describing the scope of each activity/resource and commenting on its relevance to process control system security.
Adam R. Bryant, Capt. USAF. *Developing a Framework for Evaluating Organizational Information Assurance Metrics Programs.* Master of Science Thesis for Air Force Institute of Technology, Dept. of the Air Force Air University. AFIT/GIR/ENV/07-M5, March 2007. Accessed 1 April 2009 at: *https://www.afresearch.org/skins/rims/q_mod_be0e99f3-fc56-4ccb-8dfe-670c0822a153/q_act_downloadpaper/q_obj_217f0dc1-baf2-47c8-a458-60956d23bc05/display.aspx?rs=enginespage*	Includes an extensive review of existing CS/IA measurement literature
Anni Sademies, VTT Electronics. *Process Approach to Information Security Metrics in Finnish Industry and State Institutions.* Thesis for University of Oulu, Finland; published as VTT Publication 544, 2004. Accessed 6 January 2009 at: *http://www.vtt.fi/inf/pdf/publications/2004/P544.pdf*	Includes a survey of literature on CS/IA measurement as well as a survey of information security metrics used in Finnish industrial companies and state institutions, with the rationales behind their use
Nabil Seddigh, Peter Pieda, Ashraf Matrawy, Biswajit Nandy, John Lambadaris, and Adam Hatfield (for Dept. of Public Safety and Emergency Preparedness Canada). "Current Trends and Advances in Information Assurance Metrics." Accessed 1 April 1, 2009 at: *http://dev.hil.unb.ca/Texts/PST/pdf/seddigh.pdf* -and- Solana Networks. "Evaluating the Information Assurance of IT Networks Using Quantitative Metrics," in *Proceedings of the 2nd Annual Conference on Privacy, Security, and Trust,* New Brunswick, Canada, 13-15 October 2004 (paper dated 22 September 2004).	Includes an overview of existing CS/IA measurement studies, trends, tools, and taxonomies
Andrew Jaquith. *Security Metrics: Replacing Fear, Uncertainty, and Doubt* (Upper Saddle River, New Jersey: Addison-Wesley/Pearson Education, 2007).	Integrated throughout are informative discussions of many existing metrics, measurement methodologies, and related standards
Debra S. Hermann. *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI* (Boca Raton, Florida: Auerbach Publications, 2007).	A comprehensive study of security and privacy metrics with proposed lists of metrics for a number of areas
Victor-Valeriu Patriciu and Iustin Priescu, Military Technical Academy, Bucharest, Romania, and Sebastian Nicolaescu, Verizon. "Security Metrics for Enterprise Information Systems," in *Journal of Applied Quantitative Methods,* Volume 1, Issue 2, 30 December 2006. Accessed 23 March 2009 at: *http://jaqm.ro/issues/volume-1,issue-2/4-SecurityMetricsForEIS.php; also http://jaqm.ro/issues/volume-1,issue-2/pdfs/patriciu_priescu_nicolaescu.pdf*	A presentation of existing standards and measures from across numerous sources, including Jaquith and NIST SP 800-55

2.1 Progress Made Since 2000

The CS/IA measurement discipline has experienced significant positive change since 2000. Then, the debate was about whether measuring CS/IA was possible, how measurement was to be performed, what processes should be used, what should be measured, and whether measuring "it" would ever be useful.

Today, there is no doubt—CS/IA measurement is possible, there are plenty of processes and methodologies to do it, and it is definitely valuable. While work continues in defining what exactly is measurable, which measures are most useful, and how to maximize the value of measurement, there has been significant forward movement.

The current "state of the art" period for CS/IA measurement (*i.e.*, the period covered by this SOAR) could be said to have begun with the 2001 WISSSR, [11] which was the first such gathering devoted solely to the discussion, by IA and measurement practitioners, of the state of the CS/IA measurement discipline. Participants in the workshop submitted position papers regarding the state of the discipline and, in many cases, describing the work they had done to define CS/IA measures, measurement techniques, and measures definition methods. Participants discussed (and often debated) the relative merits of different approaches and emphases in the subject matter addressed by the workshop.

Since then, through research, standardization, and technological advancements, a number of building blocks have been put in place that can be used today to begin measuring CS/IA. While these building blocks are not perfect, they are sufficient to start the process, provide useful information about the status of CS/IA to their users, and evolve CS/IA measurement toward measuring outcomes and the value of CS/IA. Table 2-2 lists the most noteworthy efforts and activities that facilitate advancement of CS/IA measurement discipline. The table also provides references to sections in this SOAR where particular CS/IA measurement efforts are addressed. Sections 3 through 8 provide further information on these and other relevant efforts.

Table 2-2 CS/IA Measurement Discipline Progress Summary

Description	Reference	SOAR Section
Standards, guidelines, and best practices documents that provide processes, frameworks, and metamodels for CS/IA measurement. Those interested in embarking upon CS/IA measurement can use these standards and guidelines to structure their programs and processes in a robust and repeatable way to facilitate long term viability and success.	NIST SP 800-55 Rev. 1, *Performance Measurement Guide for Information Security,* July 2008	Section 3.2
	ISO/IEC 27004, *Information technology – Security techniques – Information security management – Measurement* (draft)	Section 3.3
	SwA Measurement Working Group. *Practical Measurement Framework for Software Assurance and Information Security, Version 1.0,* October 2008	Section 4.1
Automated tools focused on specific challenges that gather quantifiable data. These tools provide ways of gathering data that can be quantified in a more exact and less intrusive way than widely spread manual data collection to facilitate better quality of data and less disruption to operations for the sake of measurement.	Static and dynamic code analyzers	Section 8.3
	FISMA tools	Section 8.2
	Reporting and dashboard tools	Section 8.4

Description	Reference	SOAR Section
US Government research efforts focusing on specific aspects of CS/IA measurement. These efforts explore context-specific approaches for CS/IA measurement that address software assurance, control systems, attack-based measures, and other applications of the broader CS/IA measurement question.	DHS/DoD/NIST SwA Measurement WG	Section 5.2.2
	United Statement Computer Emergency Response Team (US-CERT) Cyber Security Metrics for Control Systems	Section 5.2.3
	NIST Software Assurance Metrics And Tool Evaluation (SAMATE) Program	Section 5.3.1
	Attack-Based Measures	Section 5.3.2
	NIST SCAP Program	Section 5.3.3
Industry efforts focusing on specific aspects of CS/IA measurement. These efforts provide specific approaches for measuring, lists of measures as well as community forums for those interested in this subject to learn about and contribute to progression of the discipline.	Corporate Information Security Working Group (CISWG)	Section 6.1
	OWASP	Section 6.2
	Center for Internet Security (CIS)	Section 6.3
	Securitymetrics.org	Section 6.5
	Security knowledge and awareness measures	Section 6.6
CS/IA data collected by a variety of manual, automated, and semi-automated efforts that can be leveraged to collect, analyze, and report complex Certified Information Systems Auditor (CISA) measures. These efforts provide valuable data that can be used to— ► Combine, correlate, and report CS/IA status to decision makers; ► Create and use sophisticated CS/IA measures to advance overall understanding of CS/IA heath and status.	IA Assessments	Section 7.1
	Network management and security measures	Section 7.2
	Software testing output	Section 7.3
	Vulnerability assessment and management	Section 7.5
Emergence of enumerations and scoring systems. Enumerations and scoring systems provide means of uniform counting, ranking, and evaluating CS/IA that were not possible in 2000.	CVSS	Section 7.4.1
	CCSS	Section 7.3.3
	Common Misuse Scoring System (CMSS)	Section 7.4.4
	Common Weakness Scoring System (CWSS)	Section 7.4.5
Several categorizations or taxonomies of CS/IA measures have emerged to focus analysis and interpretation of data.		Section 7.7
The legislative and regulatory environment is now requiring measures or proof of accomplishment, providing motivation for organizations to establish CS/IA measurement activities.		Section 3.1

2.2 Perceptions of IA Measurement: Skeptics and Detractors

> ***"I would like to believe that metrics relating to security are possible, but there is little evidence to support this view at present." [12]***

As with many technologies that are still in the conceptual phase or the early adoption phase, CS/IA measurement is considered with skepticism by some. Most of the skeptics do not doubt the value of CS/IA measurement in theory; they simply question whether anything approaching a set of useful CS/IA measures has–or can–be defined; or, if defined, whether such measures have any real utilitarian value, given what they see as the current "unmeasurable" state of security technology and process.

These detractors share several assumptions in common that motivate their skepticism—

- They all assume that what is to be measured is security or assurance of technical security (*e.g.,* defense in depth protections, computer security controls) rather than process effectiveness.
- They all agree that measurement of security assurance is a laudable goal in theory.
- They all consider the current state of the art of security technology so poor and/or unpredictable that any attempt to measure its assurance would be a waste of time.

Security "guru" Steven Bellovin of Columbia University is one such detractor. In his presentation, "On the Brittleness of Software and the Infeasibility of Security Metrics," [13] Bellovin argues that security metrics for security mechanisms implemented by software are simply not possible for the following reasons—

- All software is inherently vulnerable, due to the unavoidable presence of numerous design weaknesses and implementation flaws. These weaknesses and flaws are not recognized or detected by the software's developer. They are, however, fairly easily discovered by software-knowledgeable adversaries.
- An adversary needs only exploit a single significant undetected weakness or flaw to render a software-based security mechanism ineffective.
- The assumption that a "defense-in-depth" security architecture composed of aggregate layers of software-based protections will be stronger than any individual layer's protections is false. Individual software-based protections are so "brittle" that it is impossible for them to be adequately robust or resilient, even in aggregate.

- Until the engineering of software is radically improved to the extent that software is no longer inherently riddled with weaknesses and flaws, attempting to measure the strength of fatally "brittle" software-based protections will remain a waste of time.

Other factors Bellovin cites as militating against meaningful, useful security strength metrics are—

- The fact that there has not yet been devised a metric for accurately measuring the amount of effort a skilled adversary requires to locate and exploit a software bug;
- The lack of a science of security mechanism composition that can avoid the problem of an incommensurately weak protective layer interfering with the strength of the other layers and the aggregate strength of all layers in a defense-in-depth layered architecture.

Bellovin concludes that current defense-in-depth-based security architectures are not amenable to metrics, and "very reluctantly conclude[s] that security metrics are chimeras for the foreseeable future. We can develop probabilities of vulnerability, based on things like Microsoft's Relative Attack Surface Quotient, the effort expended in code audits, and the like, but we cannot measure strength until we overcome brittleness." [14]

Nguyen Pham *et al.* [15] question the practical usefulness of security evaluations based on tree-based metrics taxonomies. After providing a brief survey of efforts to do so, they conclude that—

- Many such metrics are meant to be applied over long periods of time, making their utility for real-time evaluations infeasible.
- The limitation of some measurement systems to predefine a single weighted value to each metric, to reflect the metric's relative importance, is too inflexible in real-world systems for which the importance of metrics changes over time.
- There are no modeling techniques or tools to support the evaluation of system assurance based on the 75 strategic metrics that Andrew Jaquith [16] reports organizations use to assess their security postures, diagnose security issues, and measure infrastructure security activities.

2.3 Research and Emerging Methods

Active research into CS/IA measurement methods and techniques really began with the measurement of the robustness of cryptographic systems. However, R&D of measurement methods for security, privacy, and associated assurance across the broader domain of technical and non-technical measures, processes, knowledge/awareness, *etc.*, really emerged in the

mid-to-late 1990s. The results of that earlier research have, in many cases, made the transition into practical use, and have formed the basis for much of what is discussed in Sections 2 to 8 of this SOAR.

There are a number of efforts within academic, industrial, and government research organizations to define meaningful CS/IA measurement methodologies as well as the specific measures to quantify, for instance, criticality of vulnerabilities, severity of threats and attacks, and other aspects of CS/IA.

Increasingly, over the past few years, members of the CS/IA measurement community are discussing existing and emerging approaches and, in some cases, collaborating to come up with common approaches. The cooperation between Microsoft and Carnegie Mellon University (CMU), for example, in refining the Relative Attack Surface Quotient (RASQ) (discussed in Section 6.8.2) is one example of such collaboration. In Europe, the collaboration of research institutions, not just within academia, but across academia, industry, and government, has led to a breaking down of competitive barriers that, in the past, may have explained some of the lack of success of measurement and, indeed, many other technology initiatives.

Current and emerging CS/IA measurement research tends to focus in one of the following areas—

- Quantification of the economic value of security and assurance;
- Quantification of robustness of technical security measures;
- Measurement for non-technical security (*e.g.*, process security);
- Measurement in support of risk assessment;
- Measurement focusing on attacks;
- Measurement focusing on vulnerabilities and weaknesses;
- Measurement of the security properties, attack exposure/resistance, *etc.*, of software;
- Control system security measurement;
- Privacy measurement.

References

8 Stuart Edward Schechter. "Toward Econometric Models of the Security Risk from Remote Attack," in *IEEE Security & Privacy,* Vol. 3, No. 1, January/February 2005, pp. 40-44. Digital Object Identifier: 10.1109/MSP.2005.30; Earlier version published in *Proceedings of the Third Workshop on Economics and Information Security,* Minneapolis, MN, May 2004, Accessed 25 March 2009 at: *http://www.eecs.harvard.edu/~stuart/papers/eis04.pdf*

9 IATAC. *IA Metrics* CR/TA. 2000. Available to .mil and .gov at: *http://iac.dtic.mil/iatac/reports.jsp#CR/TA*

10 Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash and Laurie Graffo. NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems,* July 2003. Accessed 26 March 2009 at: *http://webharvest.gov/peth04/20041027033844/csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf*

11 Vaughn, Siraj, and Henning, "Information Assurance Measures and Metrics—State of Practice and Proposed Taxonomy," *op cit.*

12 John McHugh, Carnegie Mellon University Center for Survivable Systems. "Information Assurance Metrics: Prophecy, Process, or Pipedream?," in *Proceedings of the 23rd National Information Systems Security Conference,* Baltimore, Maryland, 16-19 October 2000. Accessed 20 January 2009 at: *http://csrc.nist.gov/nissc/2000/proceedings/papers/201.pdf*

13 Steven M. Bellovin, Columbia University. "On the Brittleness of Software and the Infeasibility of Security Metrics." Keynote presentation at Metricon 1.0, Vancouver, BC, Canada, 1 August 2006 (slides revised 21 November 2006). Accessed 10 December 2008 at: *http://www.cs.columbia.edu/~smb/talks/brittle-metricon.pdf;* original version accessed 7 January 2009 at: *http://www.securitymetrics.org/content/Wiki.jsp?page=Metricon1.0Keynote#section-Metricon1.0Keynote-OnTheBrittlenessOfSoftwareAndTheInfeasibilityOfSecurityMetricsStevenBellovinColumbiaUniversity*

14 *Ibid.*

15 Nguyen Pham, Loic Baud, Patrick Bellot, and Michel Riguidel, Telecom ParisTech. "A Near Real-time System for Security Assurance Assessment," in *Proceedings of the Third International Conference on Internet Monitoring and Protection (ICIMP 2008).* Bucharest, Romania, 29 June-5 July 2008. Accessed 1 April 2009 at: *http://www.infres.enst.fr/~bellot/publis/ICIMP2008.pdf*

16 Andrew Jaquith. *Security Metrics: Replacing Fear, Uncertainty, and Doubt.* (Indianapolis, IN: Addison-Wesley Professional, 2007).

3

Laws, Regulations, Standards, and Guidelines

"Security metrics programs are still driven largely by compliance concerns."

Khalid Kark and Paul Stamp, Forrester Research [17]

There are numerous laws, rules, and regulations that include or imply requirements for information security performance measurement, including IA compliance verification requirements that are best met through measurement techniques. While some organizations may choose to design, implement, and deploy their own security measures, the adoption of standards and guidelines for security measurement greatly improves the quality of an organization's measurement program, and allows organizations to better share and improve their security postures.

Several standards and guidelines documents have emerged over the last eight years to address the challenge that many organizations face in developing CS/IA measurement programs. Generally, these standards and guidelines fall into the following categories—

- Processes for developing information security measures to assess effectiveness of enterprise or system-level security controls and implementing the measures (These types of documents often include example measures.);
- Maturity model frameworks that provide a framework for assigning a maturity level to a grouping of security processes, based on specific criteria;
- Product evaluation frameworks that assess the level of assurance the products provide against specific criteria, and assigning a product evaluation level based on this criteria.

This section provides an overview of relevant laws and regulations as well as the major standards and guidelines that are currently available to organizations seeking to deploy or improve CS/IA measurement programs. It is important to note that a majority of these

documents were developed by the federal government (*i.e.,* NIST and National Security Agency [NSA]) and by ISO.

3.1 Legal, Regulatory, and Policy-Driven Requirements for Measurement

A number of laws, regulations, and policies include compliance verification requirements that mandate the use of measurement for verifying compliance or, at a minimum, suggest the use of or imply a preference for measurement as the best approach to verification of compliance.

A wide variety of tools and methodologies are available for verifying the compliance of information systems and applications of various sorts with the relevant legislative and regulatory mandates. Most of these tools and methodologies generate measures for compliance verification. Indeed, there appears to be an entire set of tools devoted to verifying compliance with Sarbanes-Oxley, FISMA, the Health Insurance Portability and Accountability Act (HIPAA), and other legislative and regulatory mandates with CS/IA elements. [18]

With compliance verification comes the need to generate data for measuring compliance; in the case of compliance with CS/IA-relevant mandates, this combination results in CS/IA measures. The following sections describe a cross-section of such mandates, and some associated measurement-based compliance verification efforts of note. These examples are meant to be representative only, and are not intended to be exhaustive.

3.1.1 FISMA

FISMA provides a comprehensive framework for securing federal government IT resources by defining key federal government and agency roles and responsibilities, and by requiring agencies to integrate information security into their capital planning and enterprise architecture processes. FISMA requires that agencies conduct annual information security reviews of all programs and systems, and report the results of those reviews to OMB. [19]

FISMA has a number of key provisions, including—

- Delegating to NIST the responsibility to develop detailed information security standards and guidance for federal information systems, with the exception of national security systems;
- Designating OMB to oversee federal agencies' information security implementation.

OMB publishes annual FISMA guidance that includes specific performance measures to be reported as a part of annual and quarterly reporting. In Fiscal Year (FY) 2007, OMB added a requirement that agencies describe three performance metrics that agencies use to measure the effectiveness or efficiency of security policies and procedures. OMB guidance required that these metrics are different from the ones agencies already report for FISMA, and suggested using NIST SP 800-80, *Guide for Developing*

Performance Metrics for Information Security, as a source of metrics to tailor. In FY 2008, OMB modified its guidance to point to NIST SP 800-55, *Performance Measurement Guide for Information Security,* as NIST SP 800-80 did not progress from its draft stage. Instead, the content from NIST SP 800-80 was folded into the revision of NIST SP 800-55 Rev. 1, July 2008. OMB also specified that the three metrics to be reported must be outcome/ output-based.

3.1.2 FEA

The Federal Enterprise Architecture (FEA) is a business-based framework for government-wide improvement. The purpose of the FEA is to facilitate cross-agency analyses, and to identify duplicative investments, gaps, and opportunities for collaboration within and across federal agencies. [20]

The FEA defines five reference models—

- Performance Reference Model (PRM),
- Business Reference Model (BRM),
- Service-Component Reference Model (SRM),
- Technology Reference Model (TRM),
- Data Reference Model (DRM). [21]

Collectively, these reference models identify the set of performance, business, capability, technical, and data handling requirements as well as standardized measures for measuring the organization's success in achieving these objectives.

According to the FEA Security and Privacy Profile (SPP) [22]—

> ***"The Security and Privacy category falls under PRM Measurement Area 'Process and Activities.' Measurement Indicators show the extent to which security is improved and privacy addressed."***

The FEA SPP identifies the federal legislative and policy source documents from which a minimum set of security and privacy objectives should be derived. These objectives include—

- **Security**—FISMA, as implemented in accordance with OMB Circular A-130, Management of Federal Information Resources (OMB A-130) and relevant NIST guidance;
- **Privacy**—The Privacy Act of 1974 (Privacy Act) and the E-Government Act of 2002, as implemented in accordance with OMB Memorandum 03-22 [23] as well as OMB's specific guidance on the implementation of the Privacy Act and agency responsibilities for protecting privacy.

The FEA SPP also provides the following examples of quantifiable security and privacy indicators for PRM measurement, which appeared in the FY 2005 FISMA report—

- Percentage of employees who received annual security awareness training,
- Percentage of agency Web sites with a machine-readable privacy policy,
- Percentage of systems that have obtained C&A,
- Percentage of applicable systems that have received a privacy impact assessment.

The FEA SPP also explains which measures in the other reference models are directly relevant to the Security and Privacy category, and describes the activities that the organization should undertake to identify its business-related performance, business, and data security and privacy requirements. These activities include—

- Assessment of the FEA descriptions of performance objectives to ensure that they can support the measurement of compliance;
- Assessment of performance adequacy;
- Establishment of Service Level Agreements (SLA).

Specifically, the organization is instructed to document its performance objectives and the metrics associated with each of its requirements. These performance metrics must then be evaluated to ensure that they are consistent with NIST SP 800-55 Rev. 1 or "a comparable agency methodology."

3.1.3 GPRA and Security Reporting

The Government Performance Results Act (GPRA) does not explicitly mandate security planning, measurement, or reporting. However, it is desired that federal government agencies tie all their activities to their strategic and performance planning processes. NIST SP 800-55 Rev. 1 suggests that agencies tie their information security goals and objectives to the overall agency goals and objectives, and that agencies use information security measures to track accomplishment of their information security goals and objectives.

3.1.4 CJCSI 6510.04 and 3401.03

Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6510.04, "Information Assurance Readiness Metrics," published on 15 May 2000, provided a set of metrics for use by DoD organizations in preparing their Joint Monthly Readiness Reports (JMRR). This instruction was cancelled on 15 October 2002 with the publication of the first version of CJCSI 3401.03, "Information Assurance (IA) and Computer Network Defense (CND) Joint Quarterly Readiness Review (JQRR) Metrics," which defined a comparable set of IA and CND metrics for use by DoD organizations in preparing Joint

Quarterly Readiness Reports (JQRR). The most recent version of this instruction, CJCSI 3401.03A, published on 15 July 2003, was cancelled on 6 August 2008. No subsequent CJCSIs devoted to metrics have been published.

3.1.5 Other Security and Privacy-Relevant Legislation Requiring Compliance Verification

Because there are some commonalities between security and privacy, responsibility for assuring both—and measuring compliance with and effectiveness of both—often falls to the same individuals. Indeed, this single focal point for responsibility is strongly implied by HIPAA, which includes both security and privacy rules; by the federal government's capital planning process, which requires an accounting of both security and privacy controls and costs; and by the requirement that FISMA reports to OMB include both security and privacy performance data.

As noted earlier, the FEA SPP identifies the Privacy Act and the E-Government Act of 2002 as the key privacy legislation from which a minimum set of measurable privacy objectives should be derived. The FEA SPP also suggests that "privacy is more complex than just an application of security." For this reason, privacy includes controls that may not be familiar to security practitioners, such as requirements for public disclosure, notice, and consent.

Debra S. Herrmann [24] identifies the key security and privacy legislation for which compliance metrics have been defined—

- Privacy Act of 1974;
- E-Government Act of 2002;
- HIPAA;
- Electronic Communications Privacy Act (ECPA);
- Computer Fraud and Abuse Act;
- Organization for Economic Cooperation and Development in Europe (OECD) Security and Privacy Guidelines;
- Financial Modernization Act of 1999 (also known as the Gramm-Leach-Bliley Act; Pub.L. 106-102, 113 Stat. 1338): specifically, the act's Financial Privacy Rule, Safeguards Rule, and Pretext Protection;
- USA Patriot Act.

3.2 NIST SP 800-55 Rev 1: Performance Measurement Guide for Information Security

NIST published NIST SP 800-55 Rev. 1, *Performance Measurement Guide for Information Security,* [25] in July 2008 to update NIST SP 800-55, *Security Metrics Guides for Information Technology Systems,* July 2003, by aligning the content of the guidance with information security controls in NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* and to expand the document contents from addressing systems to covering

information security programs. NIST SP 800-55 Rev. 1 merged the content of the original NIST SP 800-55 and Draft NIST SP 800-80, *Guide to Performance Measures for Information Security,* May 2006.

The processes and methodologies described in NIST SP 800-55 Rev. 1 link information system security performance to agency performance by leveraging agency-level strategic planning processes. By doing so, these processes and methodologies help demonstrate how information security contributes to accomplishing agency strategic goals and objectives. Performance measures developed according to NIST SP 800-55 Rev. 1 will enhance the ability of agencies to respond to a variety of federal government mandates and initiatives, including FISMA, FEA's PRM requirements, and any other enterprise-specific requirements for reporting quantifiable information about information security performance.

NIST SP 800-55 Rev. 1 focuses on three key measurement categories: (1) implementation measures, (2) effectiveness/efficiency measures, and (3) impact measures, described in greater detail in Section 7.7.2. NIST SP 800-55 Rev. 1 is structured to provide a comprehensive view of information security measurement, as illustrated in Table 3-1.

Table 3-1 NIST SP 800-55 Rev. 1 Document Structure

Section	Description
1.0 Introduction	Introduces the document and discusses the purpose, scope, audience, history, and critical success factors of information security performance measurement
2.0 Roles and Responsibilities	Describes the roles and responsibilities of agency staff that have a direct interest in the success of the information security program, and in the establishment of an information security measurement program
3.0 Information Security Measures Background	Provides background and context for information security measures, the benefits of implementation, various types of information security measures, and the factors that directly affect information security measurement program success
4.0 Legislative and Strategic Drivers	Links information security measurement to strategic planning through relevant legislation and guidelines
5.0 Measures Development Process	Presents the approach and processes used for development of information security measures
6.0 Information Security Measurement Implementation	Discusses those factors that can affect the implementation of an information security measurement program
Appendix A: Candidate Measures	Provides practical examples of information security measures that can be used or modified to meet specific agency requirements

NIST SP 800-55 Rev. 1 describes two primary processes: (1) the measures implementation process (depicted in Figure 3-1), discussed in Section 6 of the Special Publication, and (2) the measures development process (depicted in Figure 3-2), discussed in Section 5 of the Special Publication, which serves as the first phase of measures implementation process.

Figure 3-1 Information Security Measurement Program Implementation Process [26]

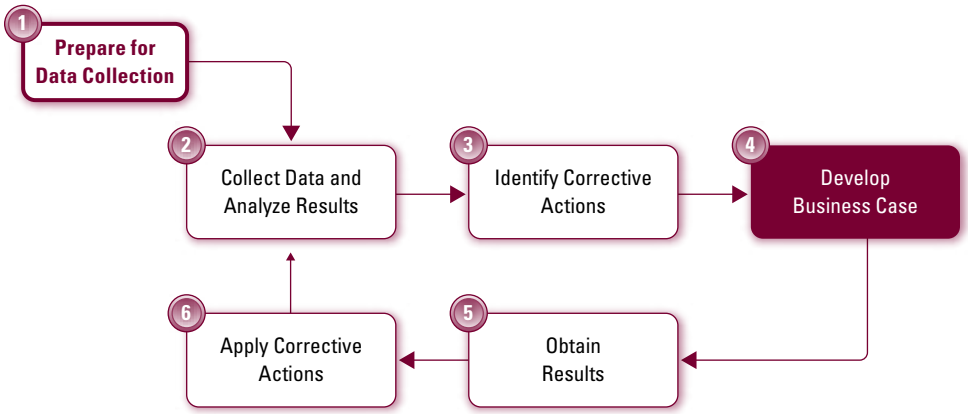
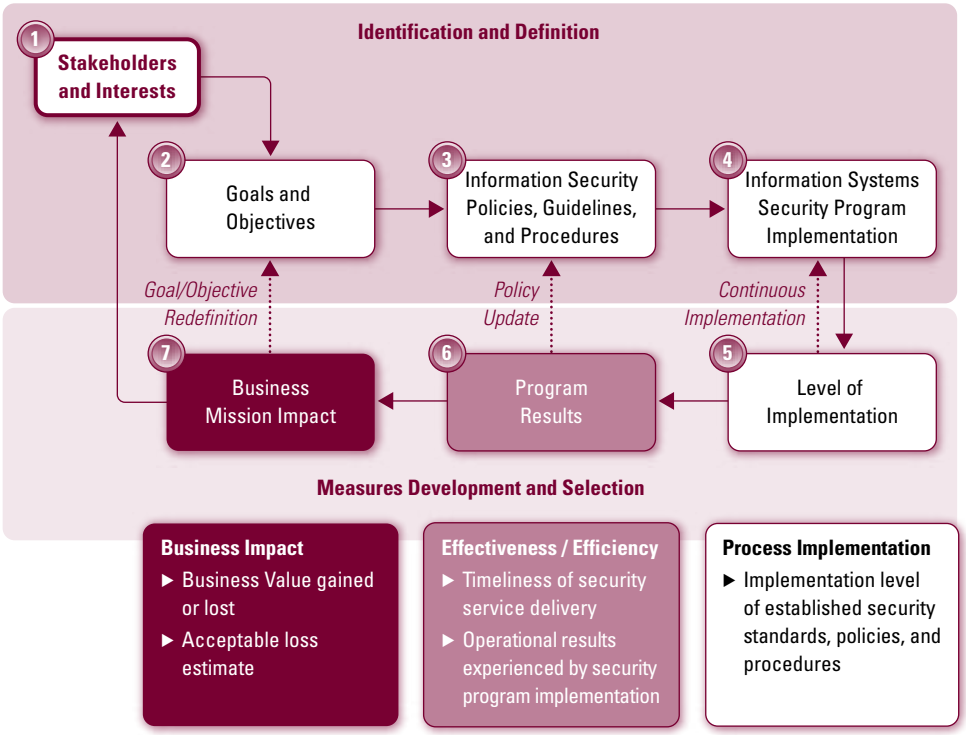


Figure 3-2 Information Security Measures Development Process [27]



Section 3 of NIST SP 800-55 Rev. 1 contains an extensive discussion about the benefits of using measures, types of measures, and the relationship of the types of measures to the maturity of security program being measured. The authors state that the difficulty of implementing information security measures and the level of sophistication that can be expected from the measures is directly proportional to the maturity of information security program.

Security programs that do not have established processes and procedures, and where data needs to be collected manually, are likely to have greater difficulty collecting effectiveness/ efficiency and impact measures. These programs are advised to focus on implementation measures. NIST SP 800-55 Rev. 1 also advises its audience to limit a number of measures to two to three per individual stakeholder to ensure that the stakeholders are able to focus on improving the status of CS/IA in a meaningful way. As CS/IA measurement programs mature, old measures that are no longer useful can be phased out and new measures can be introduced to continue monitoring and improving the status of CS/IA.

Programs with a greater number of institutionalized processes and some level of automated data collection tools are likely to be more successful in leveraging effectiveness/efficiency measures. These programs are also better equipped to move toward the business impact measures, which are more sophisticated then the other types of measures.

NIST SP 800-55 Rev. 1 proposes a measures development template, depicted in Table 3-2, to specify individual measures and provide the corresponding detail that will be required to implement such a measure program.

Table 3-2 Measures Template and Instructions [28]

Field	Data
Measure ID	Statement of the unique identifier used for measure tracking and sorting. The unique identifier can be from an organization-specific naming convention or can directly reference another source.
Goal	Statement of strategic goal and/or information security goal. For system-level security control measures, the goal would guide security control implementation for that information system. For program-level measures, both strategic goals and information security goals can be included. For example, information security goals can be derived from enterprise-level goals in support of the organization's mission. These goals are usually articulated in strategic and performance plans. When possible, include both the enterprise-level goal and the specific information security goal extracted from agency documentation, or identify an information security program goal that would contribute to the accomplishment of the selected strategic goal.
Measure	Statement of measurement. Use a numeric statement that begins with the word "percentage," "number," "frequency," "average," or a similar term. If applicable, list the NIST SP 800-53 security control(s) being measured. Security controls that provide supporting data should be stated in Implementation Evidence. If the measure is applicable to a specific FIPS 199 impact level (high, moderate, or low), state this level within the measure.
Type	Statement of whether the measure is implementation, effectiveness/efficiency, or impact
Formula	Calculation to be performed that result in a numeric expression of a measure. The information gathered through listing implementation evidence serves as an input into the formula for calculating the measure.
Target	Threshold for a satisfactory rating for the measure, such as milestone completion or a statistical measure. Target can be expressed in percentages, time, dollars, or other appropriate units of measure. Target may be tied to a required completion time frame. Select final and interim target to enable tracking of progress toward stated goal.

Field	Data
Implementation Evidence	Implementation evidence is used to compute the measure, validate that the activity is performed, and identify probable causes of unsatisfactory results for a specific measure. ▶ For manual data collection, identify questions and data elements that would provide the data inputs necessary to calculate the measure's formula, qualify the measure for acceptance, and validate provided information. ▶ For each question or query, state the security control number from NIST SP 800-53 that provides information, if applicable. ▶ If the measure is applicable to a specific FIPS 199 impact level, questions should state the impact level. ▶ For automated data collection, identify data elements that would be required for the formula, qualify the measure for acceptance, and validate the information provided.
Frequency	Indication of how often the data is collected and analyzed, and how often the data is reported. Select the frequency of data collection based on a rate of change in a particular security control that is being evaluated. Select the frequency of data reporting based on external reporting requirements and internal customer preferences.
Responsible Parties	Indicate the following key stakeholders: ▶ Information Owner: Identify organizational component and individual who owns required pieces of information; ▶ Information Collector: Identify the organizational component and individual responsible for collecting the data. (Note: If possible, Information Collector should be a different individual or even a representative of a different organizational unit than the Information Owner, to avoid the possibility of conflict of interest and ensure separation of duties. Smaller organizations will need to determine whether it is feasible to separate these two responsibilities.); ▶ Information Customer: Identify the organizational component and individual who will receive the data.
Data Source	Location of the data to be used in calculating the measure. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information.
Reporting Format	Indication of how the measure will be reported, such as a pie chart, line chart, bar graph, or other format. State the type of format or provide a sample.

Guidance contained in NIST SP 800-55 Rev. 1 suggests the following actions for implementing measures within organizations—

- Map measures addressing overall information security program performance to information security goals and objectives that may encompass performance of information security across the spectrum of security controls.
- Map measures corresponding to security control families or individual security controls directly to the individual security control(s).
- Use the data describing the security control's implementation and security program performance, such as that found in Plans of Action & Milestones (POA&M), testing, and project tracking to generate required measures.

Appendix A of Draft NIST SP 800-55 Rev. 1 provides sample programmatic and system level measures with explicit links to NIST SP 800-53 security controls.

3.3 ISO/IEC 27004 – Information Security Management – Measurement

ISO/International Electrotechnical Commission (IEC) 27004, *Information technology – Security techniques – Information security management – Measurement,* is an emerging ISO standard that addresses information security measurement. ISO/IEC 27004 is currently a Final Committee Draft (FCD), and is projected to be published by the end of 2009.

ISO/IEC 27004 is being developed in response to a requirement in ISO/IEC 27001, *Information technology – Security techniques – Information security management systems – Requirements requirement,* to measure effectiveness of Information Security Management System (ISMS) controls.

ISO/IEC 27004 does not contain requirements; rather, it contains recommendations. That means it is a guidance document and is not intended to serve as a set of requirements for conducting conformance assessments. ISO/IEC 27004 contains several annexes that provide a sample template for constructing measures and example measures that are using the template.

As an international standard, ISO/IEC 27004 is being developed by a group of experts from across the globe. Many national standards bodies have provided contributions and inputs to amalgamate into a comprehensive solution for measuring the effectiveness of ISMS controls and of ISMSs. Among these inputs, ISO/IEC 27004 incorporates materials from NIST SP 800-55 Rev. 1 and other nations' standards and guidelines on information security measurement. The measures development and implementation processes used by ISO/IEC 27004 are very similar to processes detailed in NIST SP 800-55 Rev. 1, but the document uses ISMS terminology, rather then NIST terminology.

ISO/IEC 27004 is also harmonized with ISO/IEC 15939, *System and software engineering – Measurement process,* and uses the overall measurement process and the measurement model originally published in ISO/IEC 15939. The measurement process used in ISO/IEC 27004 consists of the steps of—

- Developing measures,
- Operating measurement program,
- Analyzing and reporting results,
- Evaluating and improving the measurement program itself.

The evaluation and improvement of the measurement program ensures that the program continues to be effective, and is refreshed regularly or when the needs or operating environment change.

The measurement model in ISO/IEC 27004 provides a detailed top-down and bottom-up structure for identifying the information that is being sought from the measures, the individual attributes required to construct individual measures, and a hierarchical structure for rolling up and consolidating the data with increasing complexity.

Several layers of measures are described, including—

- Base measures that are quantifying individual attributes,
- Derived measures that are based on one or more base measures,
- Indicators to consolidate derived measures into a result that is presented to management.

The hierarchical method of a vertical structure that provides for top-down and bottom-up definition of measures allows for consolidation of information about different aspects of information security into a coherent picture that helps assess effectiveness of individual ISMS controls and processes as well as the overall ISMS effectiveness. The ISO/IEC 27004 template contains fields that are similar to those in the NIST SP 800-55 Rev. 1 template and the ISO/IEC 15939 template.

Once published, ISO/IEC 27004 can be used as a part of ISO/IEC 27001 implementation as well as a standalone guidance that assists organizations in measuring the effectiveness of their information security processes and controls. Within US government context, it could be useful for measuring effectiveness of information security programs, processes, and controls in conjunction with NIST SP 800-55 Rev. 1.

3.4 ISO/IEC 21827, SSE-CMM

> ***"Security metrics focus on the actions (and results of those actions) that organizations take to reduce and manage the risks of loss of reputation, theft of information or money, and business discontinuities that arise when security defenses are breached." [29]***

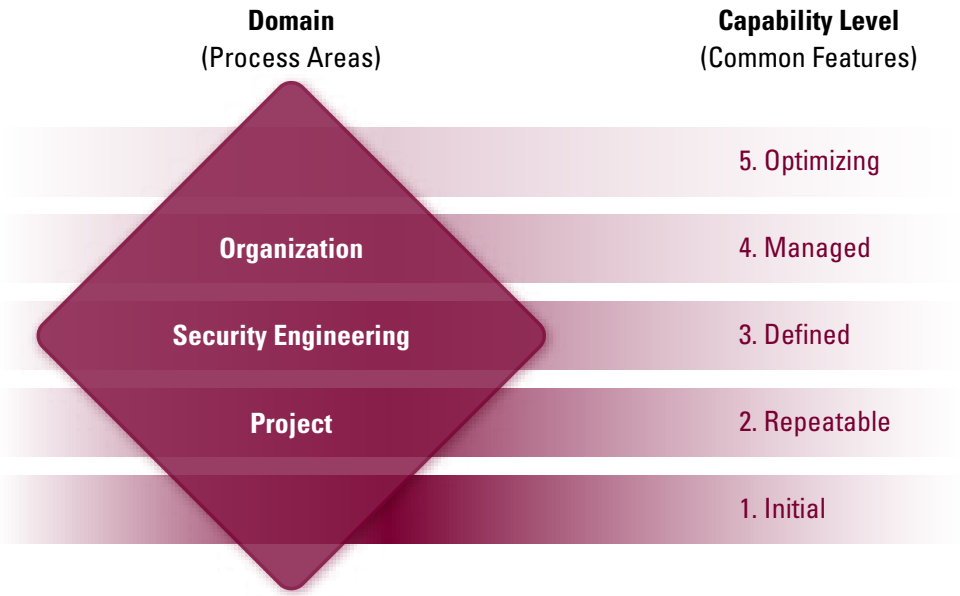
ISO/IEC 21827, *Information technology – Systems security engineering – Capability Maturity Model Capability Maturity Model* (SSE-CMM) [30], provides a structured approach for the implementation and assessment of the institutionalization of systems security engineering practices. This standard provides a framework for security engineering practices that covers the system life cycle, including identification of security risks, development, operation, and maintenance activities. [31] It includes project, organizational, and security engineering activities.

ISO/IEC 21827 can be used in conjunction with Capability Maturity Model Integration (CMMI). [32] Similar to CMMI, ISO/IEC 21827 has two dimensions—

- Generic Practices (GP) that define the characteristics of the different capability levels,
- Process Areas (PA) that describe security engineering goals and base practices.

ISO published a revised version of ISO/IEC 21827 in 2008 that includes greater detail for incorporating measurement activities into the SSE-CMM. The SSE-CMM model architecture consists of five capability levels, similarly to CMMI, and is depicted in Figure 3-3.

Figure 3-3 ISO/IEC 21827 Architecture [33]



Multiple aspects of SSE-CMM can be useful for measurement—

- The goals and practices can be used for developing, implementing, and using measures for security engineering efforts. These measures can be repeated over time. They provide relevant performance trends over time, and support security improvement and budget recommendations.
- The Build Assurance Argument PA identifies the base practices associated with collecting measurement and other data to support system security engineering claims made about the system. The PA defines the base practices to produce evidence that substantiates assurance cases, and can be used as guidance for implementing measures.
- SSE-CMM ratings can be used to provide understanding of the expected consistency in the products of security engineering efforts by providing distinct criteria for evaluating the institutionalization of security engineering efforts, and by categorizing them into five capability levels.

The International System Security Engineering Association (ISSEA), which sponsored ISO/IEC 21827, has developed a list of measures intended to use in conjunction with the SSE-CMM to assess whether PAs have been implemented and are effective. These metrics can also be useful for quantifying security

engineering activities, even when not included in SSE-CMM implementation. These metrics were finalized in 2004 and 2005 by the ISSEA Metrics Working Group that used the NIST SP 800-55 Rev. 1 process and template.

It should be noted that, while multiple attempts to implement SSE-CMM have been made and it is regularly mentioned in papers and presentations, SSE-CMM has not been widely implemented due to its complexity and the level of effort required to achieve, evaluate, and maintain Level 2 and above. However, the existence of SSE-CMM has generated several follow-on efforts, one of which, the development of the Assurance Focus Area for CMMI, is getting traction with the software assurance and IA communities. This effort is described in Section 4.2.

For Further Reading

Bartol, Nadya. "IA Metrics—Why and How to Measure Goodness of Information Assurance." Presented to ISSEA PSM User's Group Conference, July 2005. Accessed 29 December 2008 at: *http://www.psmsc.com/UG2005/Presentations/15_Bartol_IA_Metrics.pdf*

US-CERT. "Briefings from Workshop on Assurance with CMMI," August 2007. BuildSecurityIn. Accessed 10 February 2009 at: *https://buildsecurityin.us-cert.gov/swa/procresrc.html*

David A. Chapin and Steven Akridge. "How Can Security be Measured?," in *Information Systems Control Journal*, Volume 2, 2005. *http://www.isaca.org/Template.cfm?Section=* Home&Template=/ ContentManagement/ContentDisplay.cfm&ContentID=24173. Also: *http://www.isaca.org/Content/ ContentGroups/Journal1/20058/How_Can_Security_Be_Measured_.htm*

Lora Shinn. "Instituting Security Metrics," in Inc. Technology, June 2008. Accessed 13 April 2009 at: *http://technology.inc.com/security/articles/200806/metrics.html*

3.5 ISO/IEC 15408, Evaluation Criteria for Information Technology Security

ISO/IEC 15408, *Information technology – Security techniques – Evaluation criteria for IT security* [34] (commonly referred to as the Common Criteria), is a multi-part standard that provides a framework for defining and evaluating the level of assurance for individual hardware and software IT products. It allows for comparisons between different products by providing a common set of requirements for security functions and assurance techniques applied to these products during security evaluation.

There are seven Evaluation Assurance Levels (EAL) defined in the Common Criteria. These EALs are intended to indicate the level of assurance that the Target of Evaluation (TOE) (*i.e.,* the product to be evaluated) has satisfied the requirements in its Security Target (ST). Acquirers of products may describe sets of security requirements for specific types of solutions in a Protection Profile (PP), which provides a consolidated point of reference for product vendors.

Product vendors submitting their products to be evaluated describe the security functionality provided by the product in an ST. The ST describes the security functionality provided by the product, either by referencing a PP;

pointing to Common Criteria components; or stating the functionality explicitly. As such, the ST sets expectations for the acquirer on what those claims are and in what environment the product can operate as tested.

Under the US Common Criteria Evaluation and Validation Scheme, companies submit their product to Common Criteria Testing Laboratories (CCTL), where the products are evaluated.

The Common Criteria Recognition Arrangement is a multi-lateral agreement accepted by a number of countries to recognize evaluations conducted in the member countries up to the EAL4 level. A subgroup of European countries recognizes higher level evaluations as well, while in the United States, NSA will participate in evaluations above EAL4.

In terms of measurement, the Common Criteria assesses a measurable level of assurance for individual security products that enables consumers of these products to make educated decisions about suitability of these products to the consumers' security requirements and their operating environment. The Common Criteria provides the basis for benchmarking products in terms of assurance that they provide. Application of this standard allows for comparison of products providing similar functionality as well as for making decisions about integrating different products into the system based on the level of assurance that each individual product provides.

3.6 FIPS 140 Evaluation

NIST operates the Cryptographic Algorithm Validation Program (CAVP) and the Cryptographic Module Validation Program (CMVP). Together, these programs serve to provide organizations with a framework for validating cryptographic devices against the Federal Information Processing Standard (FIPS) 140 standard, *Security Requirements for Cryptographic Modules,* as well as against other NIST cryptography standards, including FIPS 180-3, the *Secure Hash Standard;* FIPS 186-2, the *Digital Signature Standard;* and FIPS 197, the *Advanced Encryption Standard*.

The CAVP is a prerequisite to the CVMP, ensuring cryptographic modules are implemented correctly prior to validating their security properties. The CAVP provides guidelines for each algorithm validation suite. [35] For example, the Advanced Encryption Standard (AES) validation suite guidelines describe the procedures used to verify that a particular AES implementation complies with FIPS 197.

FIPS 140-2 [36] defines four security levels against which a cryptographic module can be validated. Similarly, the draft of FIPS 140-3 [37] defines five security levels. Each level has specific security requirements that a cryptographic module must meet in order to receive certification, including—

- **Identification, authentication and authorization**—Each level specifies how access control and authentication should be performed within the module.

- **Physical security**—Each level specifies how much physical security must be in place to protect the integrity of the cryptographic module.
- **Operational environment**—Each level specifies what Common Criteria evaluation the overall environment should have.
- **Design assurance**—Each level specifies an increasingly strict review of the cryptographic module's design and implementation.

FIPS 140-3 will define additional security requirements, including resistance to non-invasive attacks, and more in-depth analysis of the module's design and implementation.

Because cryptographic modules must adhere to very specific requirements (*e.g.*, implementing one or more of the FIPS-approved algorithms) with well-defined input and output, they are better suited to rigorous analysis than are general purpose computing systems. As such, a cryptographic module's FIPS 140 rating provides a distinct measurement of the security controls in place for a given cryptographic module. The CAVP certificates associated with a cryptographic module will also provide full evidence of which specific algorithms have been FIPS-validated within the cryptographic module. Nevertheless, one of the primary drawbacks of the measurement provided by FIPS 140 validation is that it only applies to a specific component within an organization's enterprise.

3.7 NSA INFOSEC Assurance – IA-CMM

> ***"The first step of any successful INFOSEC Program is the understanding of the missions, critical information supporting the missions, and the information flow throughout the IT infrastructure. Too many organizations spend tremendous amounts of resources implementing 'secure' hardware, only to have their information exploited by a lack of proper security procedure." [38]***

The NSA INFOSEC Assurance Training and Rating Program (IATRP) establishes standards for INFOSEC assurance services through the INFOSEC Assurance Methodologies, the INFOSEC Assessment Methodology (IAM), and the INFOSEC Evaluation Methodology (IEM). The organization also trains and certifies individuals in these methodologies, and rates the "IA maturity" of INFOSEC assurance organizations through the use of a standard IA Capability Maturity Model (IA-CMM). This information is provided to consumers so they are better informed when working with INFOSEC assurance providers.

IATRP heavily leverages CS/IA measures in its IAM, IEM, and IA-CMM programs. Data generated from these programs can also be used for additional CS/IA measures. Due to IATRP having a specific purpose with a structured methodology, its programs can serve as a standard or guideline for other operational CS/IA measurement programs.

An IAM or IEM assessment or an IA-CMM Appraisal can be requested by contacting any one of the companies listed on the IATRP Web site, which can be accessed at: http://www.iatrp.com/companies.php

3.8 ISA ISA99 – Manufacturing and Control Systems Security

Founded in 1945, the International Society for Automation (ISA) is a professional association that publishes standards pertaining to safety and productivity of industrial automation and control systems. ISA also issues professional certifications and licenses to industrial control and automation system designers, managers, technicians, and mechanics; and performs education, training, awareness, and outreach.

In its capacity as a standards body, ISA has drafted two standards, ISA99.03.01 and ISA99.03.02 (titles not yet finalized), [39] that are intended to provide a basis for specifying the allocation of system-level security requirements to subsystems and components of Manufacturing Process Control System data repositories and data storage devices. Both standards define metrics to support the verification of such a system's compliance with its specified security requirements.

Specifically, ISA99.03.01 defines a set of subjective security assurance levels, while ISA99.03.02 uses the methodology described by Andrew Jaquith [40] to translate the subjective security assurance levels in ISA99.03.01 into a set of quantitative system security metrics for measuring system compliance with a set of derived requirements that ISA intends to publish in future specifications in its "99.03 series" of standards (*i.e.*, ISA99.03.03, ISA-DS99.03.04, and others).

References

17 Khalid Kark and Paul Stamp, Forrester Research. "Defining an Effective Security Metrics Program," 16 May 2007. Accessed 29 December 2008 at: *http://www.scribd.com/doc/2935458/best-practices-defining-an-effective-security-metrics-program*

18 The firm Unified Compliance has published online an extensive matrix of requirements for various security monitoring, or measurement controls (including individual metrics), cross-referenced against the numerous laws, regulations, standards, and configuration guides that mandate those requirements. The matrix can be used to identify which laws/regulations/standards (identified down to the section or paragraph level) call out requirements for various security-relevant compliance metrics. Among the laws and regulations in the matrix are: Sarbanes Oxley, HIPAA, NERC, PCI, FIPS 140-2, Clinger-Cohen, FISMA, NIST 800-53A and NIST 800-55, the Privacy Act, and DISA STIGs as well as dozens of other Federal, state, and private sector mandates. Of all of those references, only three include significant mandates for metrics: CISWIG2, NIST SP 800-55, and NIST SP 800-55. The Unified Compliance matrix can be accessed at: *http://www.unifiedcompliance.com/matrices/MonitoringandMeasurement_United_States.html*

19 US Congress. H.R. 2458–48, "Federal Information Security Management Act," 2002. Accessed 8 April 2009 at: *http://csrc.nist.gov/groups/SMA/fisma/index.html*

20 Pauline Bowen, Joan Hash, and Mark Wilson. NIST SP 800-100, *Information Security Handbook: A Guide for Managers,* October 2006.

21 These various reference models, including their constituent categories, domains, *etc.*, are identified and defined in OMB *FY07 Budget Formulation: FEA Consolidated Reference Model Document,* Version 2.3, October 2007. Accessed 8 April 2009 at: *http://www.whitehouse.gov/omb/assets/fea_docs/FEA_CRM_v23_Final_Oct_2007_Revised.pdf*

22 CIO Council, Federal Information Architecture Program Management Office. *FEA Security and Privacy Profile, Version,* Version 2.0, 1 June 2006. Accessed 9 April 2009 at: *http://www.cio.gov/documents/Security_and_Privacy_Profile_v2.pdf*

23 OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," 26 September 2003. Accessed on 15 April 2009 at: *http://www.whitehouse.gov/omb/memoranda/m03-22.html*

24 Debra S. Hermann, US Nuclear Regulatory Commission. *Complete Guide to Security and Privacy Metrics* (Boca Raton, Florida: Auerbach Publications, 2007). A number of information privacy and security experts suggest a far more extensive list of security- and privacy-relevant laws and regulations for which compliance must be verified. These experts include the following: Daniel J. Solove, Marc Rotenberg, and Paul M. Schwartz. *Privacy, Information, and Technology* (New York, New York: Aspen Publishers, 2006). Joel Rosenblatt. "Security Metrics: A Solution in Search of a Problem," in *EDUCAUSE Quarterly,* Vol. 31, No. 3, July-September 2008. Accessed 22 December 2008 at: *http://connect.educause.edu/Library/EDUCAUSE+Quarterly/SecurityMetricsASolutioni/47083.* A subset of their list is directly relevant for defining security and privacy requirements for information systems and networks as they address how information must be handled by such systems/networks. Examples include: the Controlling the Assault of Non-Solicited Pornography And Marketing (CAN-SPAM) Act of 2003; the Children's Online Privacy Act; the Identity Theft Assumption and Deterrence Act; US Securities and Exchange Commission (SEC) Regulation S-P (22 June 2000); the Digital Millennium Copyright Act (DCMA); and others. However beneficial these laws and regulations may be in expanding the criminal and civil recourses available to victims of privacy and security violations, identity theft, *etc.*, the rules and protections these laws mandate for confidentiality and privacy of information do not explicitly include requirements for the automated systems and networks that process, transmit, and/or store the affected information. Therefore, use of metrics in verifying compliance to these laws is not discussed here. Nor is use of metrics in verifying compliance to the non-US privacy and security laws, regulations, directives, *etc.*, identified by Herrmann, *i.e.,* the European Union Data Protection Directive 95/46/EC (1998; also known as the Safe Harbour Act), the United Kingdom's Data Protection Act, and the Canadian Personal Information and Electronic Documents Act (PIPEDA), or the Personal Health Information Act.

25 Chew, *et al.*, *Performance Measurement Guide for Information Security, op cit.*

26 *Ibid,* Figure 6-1.

27 *Ibid,* Figure 5-1.

28 *Ibid,* Table 2.

29 Systems Security Engineering Capability Maturity Model (SSE-CMM), Version 3. Accessed 1 April 2009 at: *http://www.sse-cmm.org/model/model.asp*

30 ISO/IEC 21827:2008, *Information technology – Systems security engineering – Capability Maturity Model Capability Maturity Model*® (SSE-CMM®). Accessed 1 April 2009 at: *http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44716*

31 Nadya Bartol and Joyce Richardson. "Measuring Capability-Based Assurance," in *Proceedings of the Fifth Annual Information System Security Engineering Association (ISSEA) Conference,* Arlington, Virginia, 13-15 Oct. 2004

32 Capability Maturity Model, Capability Maturity Modeling, Capability Maturity Model Integration, CMM and CMMI are registered in the US Patent & Trademark Office.

33 *Ibid.*

34 Paraphrased from ISO/IEC 15408-1:2005(E), *Information technology – Security techniques – Evaluation criteria for IT Security,* which can be downloaded at no cost from the Common Criteria Portal. Accessed 10 February 2009 at: *http://www.commoncriteriaportal.org/thecc.html*

35 Lawrence E. Bassham III., NIST Information Technology Laboratory Computer Security Division. "Advanced Encryption Standard Algorithm Evaluation Suite (AESAVS)." 15 November 2002. Accessed 4 February 2009 at: *http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf*

36 NIST. *Security Requirements for Cryptographic Modules* (Federal Information Processing Standards Publication [FIPS PUB] 140-2). 25 May 2001. Accessed 4 February 2009 at: *http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf*

37 NIST. *Security Requirements for Cryptographic Modules* (FIPS PUB 140-3 (DRAFT); will supersede FIPS PUB 140-2, 2001 May 25). Accessed 9 February 2009 at: *http://csrc.nist.gov/publications/fips/fips140-3/fips1403Draft.pdf*

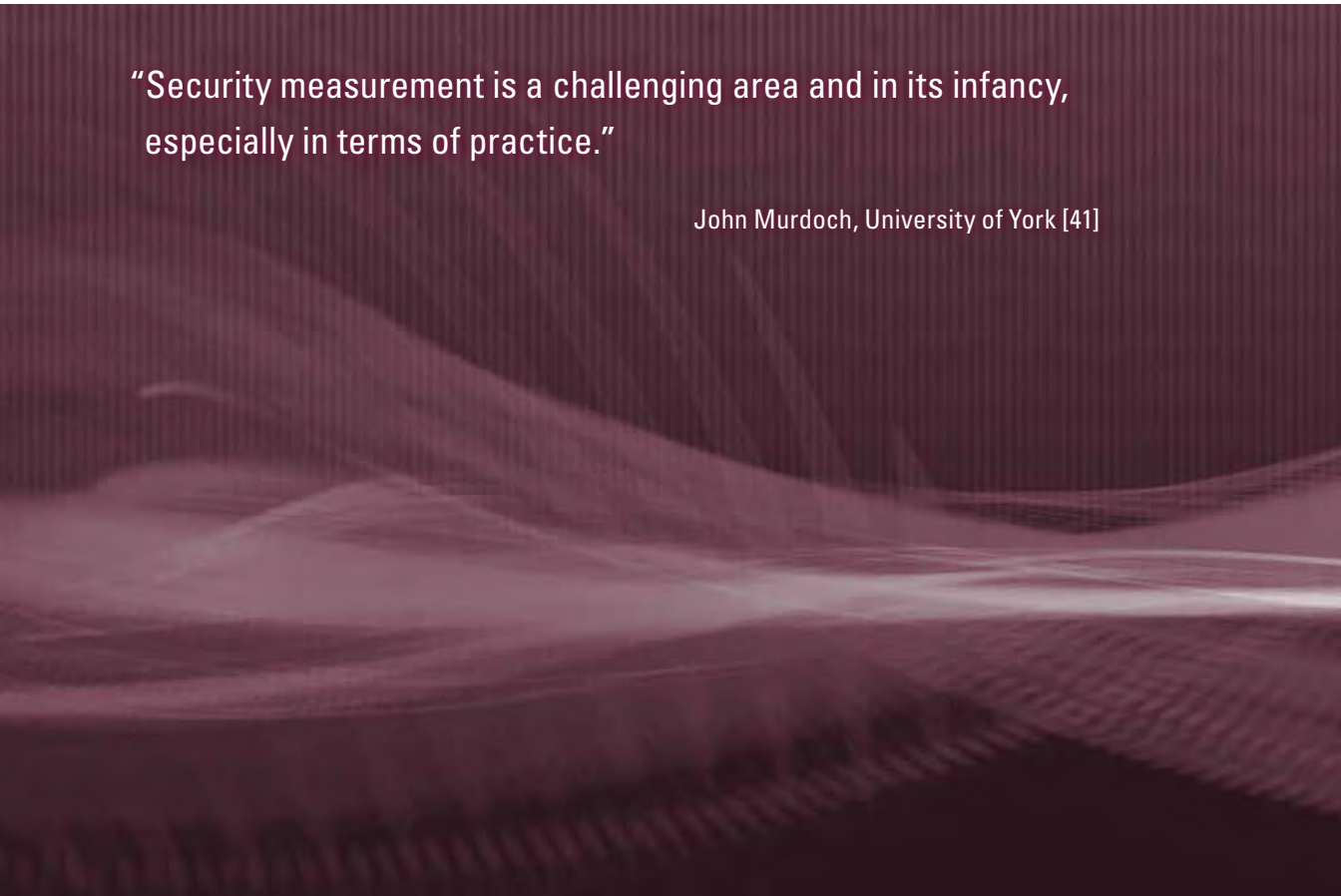
38 INFOSEC Assurance Training and Rating Program. "INFOSEC Vulnerabilities Technical and Non-Technical Solutions." Accessed 8 February 2009 at: *http://www.iatrp.com/infosec.php*

39 Nicholas Sheble, ISA. "Control system security occupies time, cyberspace," in *InTech,* 15 October 2008. Accessed 11 December 2008 at: *http://www.isa.org/InTechTemplate.cfm?Section=Industry_News&template=/ContentManagement/ContentDisplay.cfm&ContentID=72373*

40 Jaquith, *Security Metrics, op cit.*

4

Best Practices



"Security measurement is a challenging area and in its infancy, especially in terms of practice."

John Murdoch, University of York [41]

This section presents a general overview of best practices that are being adopted in government and industry for the development and operation of CS/IA measurement efforts within organizations. These measurement practices leverage the concepts introduced by the guidelines and standards discussed in Section 3, and provide a more hands-on approach for developing and running a CS/IA measurement program within an organization.

It is important to note that these practices are procedural in nature, and do not rely on specific tools or technologies—nor do they require the use of specific CS/IA measures. The goal of these best practices is to define a repeatable process that organizations may use to measure and assess the performance of their security processes and controls.

This section discusses the most widely distributed best practices. The *Practical Measurement Framework for Software Assurance and Information Security,* [42] sponsored by the SwA Measurement WG, provides a comprehensive discussion of the processes and practices required to develop an effective security measurement program. This section also discusses ongoing work to integrate security into the CMMI framework to provide benchmarking of assurance throughout system and software development efforts.

4.1 Practical Measurement Framework for Software Assurance and Information Security

The *Practical Measurement Framework for Software Assurance and Information Security* (the Framework) was developed by the SwA Measurement Working Group under the auspices of SwA Forum. The SwA Forum and its SwA Measurement WG, which are co-sponsored by DHS, DoD, and NIST, provide a forum for joint government, industry, and academia experts to work together on solving a challenging problem of software

assurance. The Framework was recently published by the Practical Software and the Systems Measurement (PSM) Support Center. According to the SwA Measurement WG Web site, it—

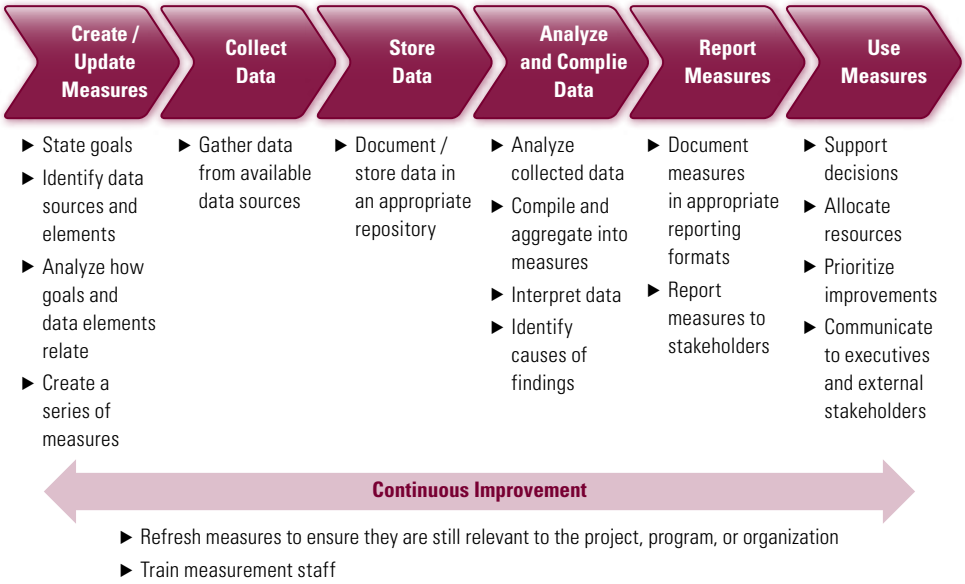
> ***"…provides an approach for measuring the effectiveness of achieving Software Assurance (SwA) goals and objectives at an organizational, program or project level. It addresses how to assess the degree of assurance provided by software, using quantitative and qualitative methodologies and techniques. This framework incorporates existing measurement methodologies and is intended to help organizations and projects integrate SwA measurement into their existing programs." [43]***

The Framework does not create a new process for developing and implementing SwA measures; rather, it leverages existing measurement approaches in information security and in system and software measurement to propose a harmonized approach that can be used by practitioners in both the information security industry and the system and software development and integration industry. The following approaches were used as the basis for developing the Framework—

- NIST SP 800-55 Rev. 1,
- ISO/IEC 27004,
- ISO/IEC 15939,
- CMMI Measurement and Analysis PA,
- CMMI Goal, Question, Indicator, Measure (GQIM) methodology.

In the process of developing the Framework, the SwA Measurement WG identified similarities and differences among these five methodologies, and created a harmonized measurement process and template. As shown in Figure 4-1, the process and the template summarize and generalize the base methodologies, and proposes a high-level process applicable to many contexts in the information security industry and in the system and software development and integration industry. The Framework also advises the audience on how to begin integrating software assurance and security measures into the organization's or project's existing measurement programs, which may not be covering these subjects.

Figure 4-1 Practical Measurement Framework for Software Assurance and Information Security [44]



The Framework identifies common stakeholders for software assurance and information security, and acknowledges a variety of roles within acquirer and supplier organizations that, at a minimum, include executive decision makers and practitioners. The Framework lists examples of information needs (*i.e.*, a high-level goal statement of what measurement aims to accomplish). It also provides examples of measures for different types of common stakeholders. Examples include—

- **Executive**—Cost to correct vulnerabilities in operational applications;
- **Supplier**—Number and percent of tests that evaluate application response to misuse, abuse, or threats;
- **Practitioner**—Number and percent of relevant high impact vulnerabilities (*i.e.*, CVEs) present in the system.

These measures can be tailored to the specific needs of the individual organizations that intend to use them.

4.2 Assurance for CMMI

Many organizations have worked on the problem of integrating assurance into CMMI. The purpose of this integration is twofold—

- To use process improvement techniques available from CMMI to address security challenges that fall outside technical mechanisms or controls frameworks;
- To gauge the level of assurance provided by the projects and organizations that are implementing CMMI.

In terms of measurement, integration of assurance into CMMI provides a benchmarking capability for assessing how well and how extensively assurance activities are integrated into system and software development and integration activities of individual projects or larger organizational units.

Currently, the CMMI approach does not specifically address security. The security track at the Software Engineering Process Group (SEPG) 2007 conference was developed to provide a forum for identifying the appropriate ties between process improvement and security.

As a result of a Security Birds of a Feather (BOF) Session at SEPG 2007, coordinated by a speaker from Motorola, an industry group was stood up with participants from Lockheed Martin, Motorola, DHS, and Booz Allen Hamilton to develop a set of consolidated assurance practices compatible with CMMI, and to provide a basis for projects and organizations to evaluate their assurance efforts as a part of their CMMI efforts. The goal of this working group is a harmonization of existing security standards with CMMI, so that an increased focus on security and assurance will be easy for CMMI users to implement. [45]

Since May 2007, the industry group has briefed its progress at a number of industry conferences, including SEPG, the National Defense Industrial Association (NDIA), and the SwA Forum. The group developed two sets of products to help address the challenges of developing more secure software and systems—

- A draft set of assurance goals and practices that harmonize and enhance existing Security CMMs (*i.e.,* MSSDM, SSE-CMM);
- A mapping of the draft set of assurance goals and practices to the CMMI-DEV v1.2.

The group is currently using the mapping of the practices to CMMI-DEV v1.2 to create an Assurance Focus Topic as a third work product. This work product will document the assurance thread within the CMMI. The Assurance Focus Area can be used by organizations to benchmark the existence and institutionalization of their integrated assurance practices. While the original purpose of the Assurance Focus Area is to integrate assurance into CMMI, the materials are being created in such way that they will be useful with or without CMMI for those organizations that are integrating assurance into their business goals and would like a way to guide and benchmark their efforts.

References

41 John Murdoch, University of York. "Security Measurement White Paper," 13 January 2006. Accessed 3 April 2009 at: *http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper_v3.0.pdf*

42 SwA Measurement Working Group. *Practical Measurement Framework for Software Assurance and Information Security,* Version 1.0, October 2008. Accessed 7 April 2009 at: *https://buildsecurityin.us-cert.gov/swa/downloads/SwA_Measurement.pdf*

43 Software Assurance Community Resource and Information Clearinghouse Measurement Working Group. Accessed 1 April 2009 at: *https://buildsecurityin.us-cert.gov/swa/measwg.html*

44 SwA Measurement Working Group. *Practical Measurement Framework for Software Assurance and Information Security,* Version 1.0, October 2008, *op cit.*

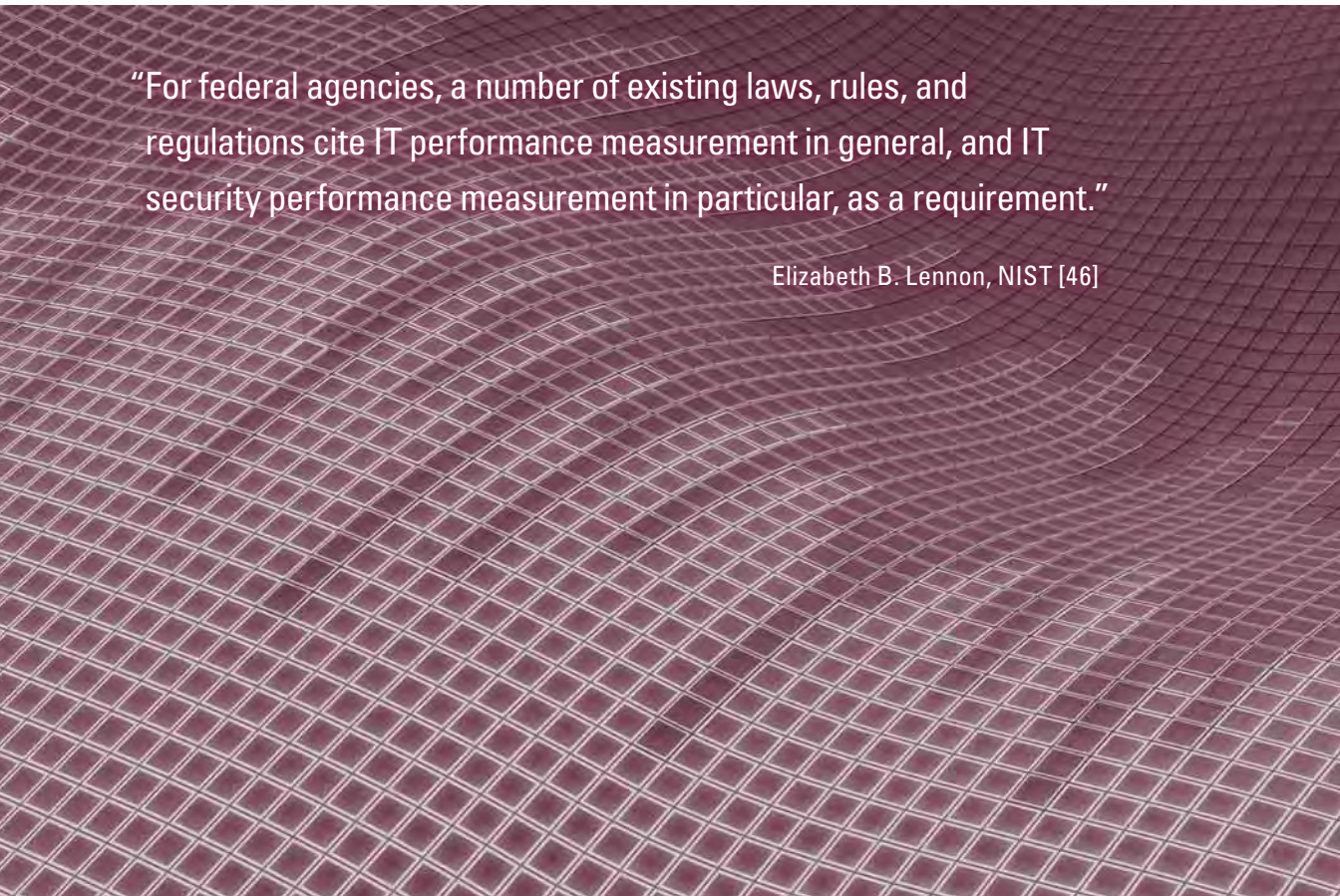
45 Carol Woody, CMU SEI CERT/CC. "Strengthening Ties between Process and Security," on DHS National Cyber Security Division's BuildSecurityIn Web portal, 1 Aug 2008. Accessed 2 April 2009 at: *https://buildsecurityin.US-CERT.gov/daisy/bsi/articles/knowledge/sdlc/1049-bsi.html#dsy1049-bsi_harm*

-and-

Carol Woody. "Process Improvement Should Link to Security: SEPG 2007 Security Track Recap." Technical Note CMU/SEI-2007-TN-025, September 2007. Accessed 6 April 2009 at: *http://www.sei.cmu.edu/publications/documents/07.reports/07tn025.html*

5

Government Initiatives and Programs



"For federal agencies, a number of existing laws, rules, and regulations cite IT performance measurement in general, and IT security performance measurement in particular, as a requirement."

Elizabeth B. Lennon, NIST [46]

Over the past eight years, the federal government has become increasingly active in pursuit of CS/IA measurement. To this end, it has established a number of programs to provide guidance for implementing CS/IA measurement programs within the government, researching additional measures for future programs as well as providing oversight by measuring the security posture of different government agencies.

This section outlines the major CS/IA measurement initiatives in place throughout the federal government, including DoD, DHS, NIST, OMB, NASA, and the Department of Justice. The scope of DHS and NIST measurement efforts addressed in this section extend beyond their respective agencies, with the goal of improving CS/IA measurement programs throughout government, academia, and industry. OMB's measurement efforts are unique in that they encompass CS/IA measurement programs for the federal government as a whole—providing insight into the effectiveness of security controls within various government agencies and departments.

5.1 DoD IA Metrics Program

IA metrics and associated programs exist at all levels within DoD—from the executive and policy-making organizations to the various branches of service and their commands—in various shapes and forms. Each organizational unit may have different metrics, tools, and processes for IA metrics. All have focused on the identification and development of IA metrics to be used to assess performance of selected missions within DoD. Common key goals and challenges have included—

- Difficulty assessing IA performance and effectiveness;
- Need to qualify IA costs for budget development;

- Determination of budget area focus and investment, high cost of compliance, and the need to develop an efficient strategy to achieve and maintain compliance;
- POA&M identification and mitigation.

DoD components report compliance statistics and other measures up the chain on a regular basis in common reporting formats, but the processes and tools used within each individual component are left to their discretion.

5.1.1 OASD(NII) Efforts

IA metrics efforts in the Office of the Assistant Secretary of Defense (Network and Information Integration) (OASD(NII)) are based on specific goals and objectives derived from the organization's mission. IA metrics are a means to uniformly monitor and objectively document the organization's security posture, and to determine appropriate corrective actions for specific "needs improvement" areas, including justifying investments in those areas.

OASD(NII) is focusing on providing a means to track IA investments and effectiveness; metrics provide an objective way of comparing strategies for deploying security solutions, and of instituting and implementing security processes, policies, and procedures. The interpretation of metrics results leads to the determination of appropriate remedial actions and, ultimately, to improvements in organizational goals. [47]

In 2005, OASD(NII) articulated the following goals for DoD's IA metrics initiative—

- Determine what measurements were being collected at present.
- Evaluate the quality of metrics in terms of their ability to measure alignment to objectives.
- Generate increased awareness of the use of/need for metrics. [48]

Over 700 metrics from existing DoD metrics efforts (*e.g.*, Joint Task Force-Global Network Operations [JTF-GNO], Defense Information Systems Agency [DISA], NSA, JQRR, Director, Operational Test & Evaluation [DOTE] metrics, FISMA, and CND assessments) were collected, documented, and categorized by the DoD IA Metrics Working Group (DIAP WG). These metrics were analyzed to determine how effective they are in providing knowledge needed for assessing each goal area of the *IA Strategic Plan*. Existing metrics were analyses from two perspectives—

- Which ones supported knowledge needed in assessing progress toward IA goals?
- What was the quality of each metric in terms of objectivity *vs.* subjectivity? (The more reliable the data on which the metric was based, the more objective it was considered.)

Ultimately, "quality" metrics were those considered adequate for use in assessing strategic plan goals.

DIAP WG findings indicated that over 200 existing metrics were inadequate for these purposes (as they were implementation metrics, rather than effectiveness metrics), and that more metrics were needed to fill in gaps in knowledge base. ASD(NII) suggested some metrics that may fill in these gaps: JTF-GNO incident metrics, red team result metrics, and vulnerability assessment results. [49] Selected metrics generated by the DIAP WG are described in Table 5-1.

Table 5-1 Selected DoD IA Metrics Working Group Metrics [50]

Metrics Data Generated by DIAP included the following:
▶ Critical Issue to be measured: Are We (Getting) Ready? ▶ Approach: Link program outputs to mission outcomes
Metrics data generated by Joint Staff:
▶ Critical Issue to be measured: Network impacts to mission accomplishment ▶ Approach: Link systems to specific missions to determine risk
Metrics data generated by GIG IA Portfolio (GIAP) program:
▶ Critical Issue to be measured: What mix of investments get the most results? ▶ Approach: Link programs/investments to capability threads
Metrics data generated by USSTRATCOM/JTF-GNO:
▶ Critical Issue to be measured: What issues need immediate solutions? ▶ Approach: Broad survey of available parameters

5.1.2 DON CIO Efforts

Since earlier in the decade, the Department of the Navy Chief Information Officer (DON CIO) has been maintaining and implementing IA performance management efforts to comply with the DON IA Strategy and FISMA. DON CIO has performed gap analyses of the DON CIO IA Strategy and DON IA Strategy against NIST SP 800-55 Rev. 1. The resulting gap analysis findings allowed DON CIO to augment and improve its FISMA Action Plan.

Once the analysis was complete, DON CIO compiled IA performance measures needed to comply with governance, and to satisfy stakeholders additional information requests; established a process for retrieving data from various data sources, including mapping measures to those data sources; and created detailed reports of measurement results in dashboard views. [51]

5.1.3 Mission Oriented Risk and Design Analysis (MORDA)

The MORDA methodology was developed for DoD's Cyber Defense Agency by NSA-sponsored researchers at Johns Hopkins University's Applied Physics Laboratory (JHU APL) to provide a quantitative risk assessment and management methodology that leverages state-of-the-art security modeling, analysis, and measurement techniques. To this end, MORDA employs a variety of tools, including attack trees and other IA models and multiple-

objective decision analysis. Each model yields mathematical outputs that express measures, such as estimated losses from attacks, predicted attack frequency, and effectiveness of countermeasures. Collectively, these quantitative outputs are intended to drive investment decisions associated with enhancement of security controls and reengineering, upgrading, or downgrading of existing system features.

The MORDA process is implemented according to the Security Optimization Countermeasure Risk and Threat Evaluation System (SOCRATES) model, also developed by JHU APL. The model, which is supported by the SOCRATES tool, enables teams of subject matter experts and analysts to define the assumptions under which three MORDA models—(1) an adversary model; (2) a user model; (3) a service provider model—will be developed, and then to identify and characterize the data needed to generate those models.

For the adversary model, such data includes identified adversaries, their preferred attack functions, and their specific attack patterns. For the service provider model, data includes characterizations of the countermeasures and design alternatives needed to resist the identified attack patterns, and an explicit description of the security requirements for each design alternative.

Also to be considered are user and service provider concerns (*e.g.,* functionality, interoperability, usability) that could be affected by the attacks or the countermeasures/design alternatives, a characterization of decision-maker functionality preferences, and the complex interdependencies among countermeasures, among attacks, and between countermeasures and attacks.

Based on the three MORDA models, the SOCRATES tool enables the analyst to—

- Qualitatively label attacks and use a quantitative scale to evaluate their potential impact, in terms of loss of value (SOCRATES differs from many quantitative risk assessment methodologies in that it does not rely on adversary probability of attack to quantify attack impact.);
- Capture and quantify each countermeasure's ability to enhance the security of the network/system under consideration;
- Quantify the loss of value to the network/system operator that would result from a degradation of the network's/system's user functions as a result of failed security.

As a result of the quantitative evaluation of countermeasure effectiveness (using aggregated value, optimization, and cost-benefit analysis), decision-makers can more effectively allocate risk-reducing resources.

According to MORDA's developers, [52] its main shortcomings are its reliance on significant access to subject matter experts and large data sets for providing the input needed to generate the MORDA models. These onerous data gathering requirements really make MORDA practical only for critical information systems that require thorough, accurate risk analyses.

For Further Reading

DON CIO, Department of the *Navy Federal Information Security Management Act (FISMA)* Guidance, March 2006. Accessed 1 April 2009 at: *http://www.doncio.navy.mil/Download.aspx?AttachID=294*

DON CIO Blog. Accessed 1 April 2009 at: *http://www.doncio.navy.mil/tagresults.aspx?ID=28*

Government Accountability Office (GAO) Report to Congressional Addressees. *Information Technology: DOD Needs To Ensure That Navy Marine Corps Intranet Program Is Meeting Goals And Satisfying Customers,* December 2006. Accessed 1 April 2009 at: *http://www.gao.gov/new.items/d0751.pdf*

United States Marine Corps. *Initial Capabilities Document (ICD) for Marine Corps Enterprise Information Technology Services (MCEITS),* Version 3.4, 20 May 2005. Accessed 1 April 2009 at: *http://www.mceits.usmc.mil/docs/05-05-20_MCEITS_ICD_(v3.4).pdf*

Secretary of the Navy. *Federal Managers' Financial Integrity Act.* FY 2008 Statement of Assurance, 28 August 2008. Accessed 1 April 1, 2009 at: *www.fmo.navy.mil/mic/docs/SOA_Final_WEB.pdf*

5.2 DHS

DHS is a unique government entity in this document as it was created after the publication of the IA Metrics CR/TA.

5.2.1 DHS NIPP and Cyber Security Metrics

The DHS National Infrastructure Protection Program (NIPP) addresses cyber security metrics to the extent that it addresses performance, process, and outcome metrics for all Critical Infrastructure Protection (CIP) programs and activities. Within its definition of Critical Infrastructure and Key Resources (CI/KR), the NIPP includes the national cyber infrastructure, which encompasses the networks, computer systems, and other elements that critical infrastructure activities rely upon to perform their missions. Therefore, the metrics prescribed by the NIPP apply to the performance, processes, and outcomes related to the national cyber infrastructure.

The National CIP Program defined in the NIPP is based on a risk-management approach that includes the use of metrics to "measure and communicate program effectiveness," including the effectiveness of the National CIP Program itself as well as the degree to which goals of CIP Plans undertaken by the individual CI/KR sectors are satisfied. In addition to these performance metrics, individual activities within CIP programs and plans (*e.g.,* vulnerability assessments) are to be measured by a combination of process metrics (*e.g.,* the number of assessments performed by a certain date) and outcome metrics (*e.g.,* the number of facilities assessed as high risk before *vs.* after instituting protective controls.)

While it is understood by DHS that selecting meaningful outcome metrics for protection programs is challenging because risk reduction is not directly observable (*i.e.,* it is difficult to determine whether a terrorist attack has been prevented), DHS also recognizes that process metrics alone are not sufficient to measure the value of CIP activities.

The NIPP's *Guidance for Developing Sector-Specific Plans as input to the National Infrastructure Protection Plan* [53] includes extensive guidance for completing Section V of the sector-specific plans, which describes the methodology—consistent with the Government Performance and Results Act (GPRA)—that will be used to measure CIP program progress. The guidance also cites NIST SP 800-55 Rev. 1 as the recommended source for cyber security performance measurement.

5.2.2 DHS/DoD/NIST Software Assurance Measurement Working Group

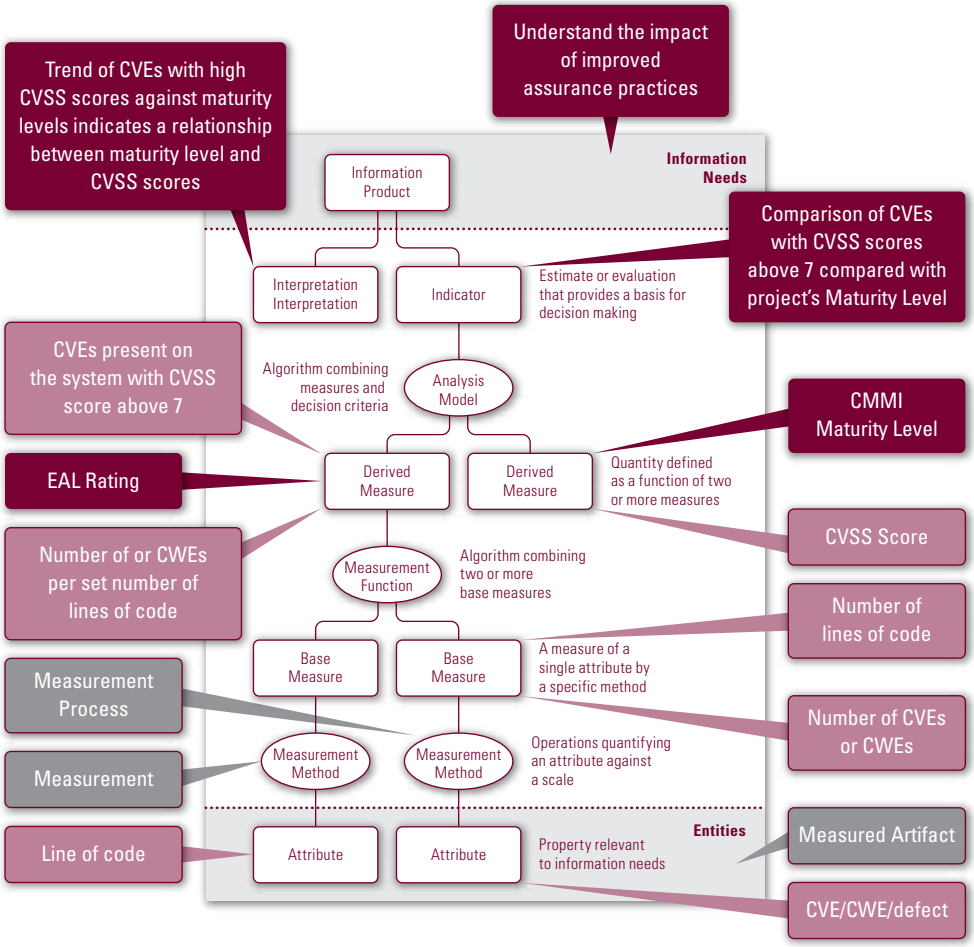
The DHS/DoD/NIST SwA Measurement WG, introduced in Section 4.1, has been in existence since 2005. The WG meets several times a year to work on common deliverables and provide an opportunity to SwA and information security practitioners to share lessons learned implementing or developing measures. Specifically, its goals [54] are to—

- Provide practical SwA measurement framework and resources to the community;
- Encourage integration of SwA practices into software and system development through integrated measurement approach;
- Make SwA measurement resources, including case studies, articles, methods, measures examples, *etc.*, available to the community;
- Create SwA measurement community of practice that shares its experiences and lessons learned;
- Collaborate with other SwA WGs to integrate measurement into their activities.

Up until recently, the SwA Measurement WG has been focusing on developing and publishing *Practical Measurement Framework for Software Assurance and Information Security*. (See Section 4.1 for more details.)

One of the recent efforts of the SwA Measurement WG is to create a series of case studies of measurement constructs that projects and organizations can use to create useful measures and use them to improve software assurance, security, and quality. An example of such a mini-case study is illustrated in Figure 5-1.

Figure 5-1 Software Assurance Measure Example [55]



The example presented in Figure 5-1 leverages one of the measurement models (adopted from ISO/IEC 15939) used by the Practical Measurement Framework for Software Assurance and Information Security, and assigns a specific software assurance-related item to each item within the model. The purpose of this mini-case study is to satisfy stakeholders' need to "understand the impact of improved assurance practices" by leveraging a number of measures, such as numbers of defects and lines of code, numbers of weaknesses, EAL ratings, CMMI maturity levels, and comparison and correlation of these measures combined into a trend. While this mini-case study has not yet been tested, it has been well received by the WG and published among the proceedings of the DHS SwA Forum.

The SwA Measurement WG is also in the process of creating a Web-based community of interest that includes a repository of SwA and security measurement resources. This community of interest is envisioned as a place where SwA and information security measurement practitioners can exchange ideas, post generic measures that they find useful, and find

measurement resources. SwA Measurement WG resources available on the site include pointers to standards, guidelines, books, articles, and community-posted examples. These resources can be found at https://buildsecurityin.us-cert.gov/swa/measresrc.html

5.2.3 US-CERT Cyber Security Metrics for Control Systems

Idaho National Laboratory, under contract to DHS's US-CERT Control Systems Security Center, developed a security framework with associated metrics for Supervisory Control and Data Acquisition (SCADA) system security, based on a set of seven security "ideals." [56] The implementation of this framework and the use of the ideal-based metrics were then published by US-CERT and briefed at S4: SCADA Security Scientific Symposium 23 January 2008.

The metrics themselves and the security ideals to which they are mapped are depicted in Table 5-2.

Table 5-2 Set of 10 Core Technical Security Metrics with Corresponding Ideals [57]

Security Ideal	Metric
1. Security Group (SG) knows current control system perfectly.	Rogue Change Days
	Security Evaluation Deficiency Count
2. Attack Group (AG) knows nothing about the control system.	Data Transmission Exposure
3. The control system is inaccessible to AGs.	Reachability Count
	Attack Path Depth
4. The control system has no vulnerabilities.	Known Vulnerability Days
	Password Crack Time
5. The control system cannot cause damage.	Worst Case Loss
6. SG detects any attack instantly.	Detection Mechanism Deficiency Count
7. SG can restore control system integrity instantly.	Restoration Time

5.3 NIST

The mission of NIST is to "promote US innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life." [58] Researching ways to measure is a core part of NIST's mission. Several NIST projects that are dedicated to advancing the state of practice and state of the art for measuring software security, information security, and other relate disciplines are discussed in the following subsections.

5.3.1 SAMATE

Launched in summer 2005, NIST's SAMATE project aims to improve the state of the art of existing software assurance methodologies and tools. The project's primary objectives include—

- Developing metrics to gauge the effectiveness of existing software assurance tools,
- Assessing current software assurance methodologies and tools to identify deficiencies that may introduce software vulnerabilities or contribute to software failures.

SAMATE's activities in the software assurance realm are outlined in the 2007 IATAC *Software Security Assurance: A State-of-the-Art Report (SOAR)*. [59]

One of SAMATE's primary goals is to provide a metric against which individual software assurance tools can be measured. Initially, this is a measurement of how well a specific tool performs against the SAMATE Reference Dataset (SRD), a collection of source code with known security flaws. In the long run, SAMATE plans to support laboratories that can be used to assess software assurance tools.

A future SAMATE goal is to identify effective metrics against which the security of software can be measured. [60] Most software assurance tools provide their own proprietary measurement that represents the security of assessed software against "other" software. Eventually, these metrics could be incorporated into software assurance tools—and verified by SAMATE laboratories. With these metrics in place, organizations could deploy such tools (*e.g.,* source code scanners, binary scanners, Web application scanners) and produce robust, well-understood measures of the software's security posture.

5.3.2 Attack-Based Measures

NIST is currently funding a research effort on attack-based measures, led by researchers at NIST, members of the George Mason University (GMU) Center for Secure Information Systems (CSIS), and the Concordia Institute for Information Systems Engineering. Researchers from these organizations have been developing a security metric based on attack graphs, which are sets of "actions that increase adversaries' capabilities." [61]

By analyzing attack graphs, researchers explore different techniques that can be used to quantify the potential success of an attack on the system—providing a metric that can gauge the relative attack resistance among multiple networks.

One of the primary features of the attack resistance metric under development is that it provides a general framework under which other, similar metrics still apply (*e.g.,* the weakest-adversary metric). [62] In 2008, research on the attack-resistance metric was extended to generate a probabilistic metric that can be used to identify the potential damage of a successful attack as well as the effects of possible mitigation strategies. [63]

5.3.3 SCAP

The Security Content Automation Protocol (SCAP) [64] is "a suite of vulnerability management standards that together enable standardization and automation of vulnerability management, measurement, and technical policy compliance checking (soon remediation) along with enhanced product and database integration capabilities with machine readable reporting."

While the SCAP is not directly associated with generating security measures, many of the standards within the SCAP suite provide well-documented measures than can be accessed through SCAP-enabled products. SCAP components are as described in Table 5-3.

Table 5-3 SCAP Components [65]

SCAP Components	Description
Common Vulnerabilities and Exposures (CVE) [66]	Provides a standard name and identifier for individual vulnerabilities and exposures that have been publicly identified
Common Configuration Enumeration (CCE) [67]	Provides a standard name and identifier for individual configuration issues associated with software components
Common Platform Enumeration (CPE) [68]	Provides a standard name and identifier for specific systems, platforms and packages
Common Vulnerability Scoring System (CVSS) [69]	Provides a metric for quantitatively communicating the impact of a specific vulnerability. CVSS is discussed in-depth in Section 7.4.1
Extensible Configuration Checklist Description Format (XCCDF) [70]	Provides a language for writing security checklists, benchmarks, and related documents
Open Vulnerability and Assessment Language (OVAL) [71]	Provides a language for describing system information, including its current state as well as the results of a vulnerability assessment

The CVE, CCE, and CPE are essential in producing machine-readable information that can, in turn, produce security metrics. The CVSS, XCCDF, and OVAL can be used to produce useful security metrics within an organization. The CVSS provides explicit metrics as defined in Section 7.4. While the XCCDF and OVAL do not provide such metrics, they provide a framework against which organizations can measure their systems' compliance to organizationally defined configurations or information, based on systems' assessment results.

The OSD Computer Network Defense (CND) pilot [72] aims to leverage the SCAP standards to produce a better understanding of DoD's networks. The expected benefit is to provide—

- An architecture that leverages the SCAP standards to correlate asset data, event data, policy, and vulnerability data;
- The ability to generate metrics based on these values.

Within the scope of the pilot, the SCAP serves as an important building block for generating DoD-wide security metrics. Using the OVAL and CVE, DoD can identify how well assets have performed during vulnerability assessments and Information Assurance Vulnerability Alert (IAVA) patch

compliance. Using the XCCDF, OVAL, CCE, and CPE, DoD can identify whether systems have followed appropriate configuration checklists, and whether users and roles have the correct, assigned permissions. Additionally, DoD can leverage the XCCDF and OVAL to identify whether certain systems manifest artifacts indicating malicious activity. As of September 2008, the CND Pilot interface can answer the following metrics questions—

- What vulnerabilities affect my assets?
- How many assets are affected by each vulnerability?
- What patches are available?
- What patches have been applied?

It is expected that the SCAP will provide a robust framework for automating these metrics for organizations of a variety of sizes; by doing so, it will help greatly improve the security posture of organizations as large as DoD.

5.4 OMB FISMA Measures

The interest of OMB in CS/IA measures is a direct result of its role in verifying government agencies' compliance with FISMA. The following is an excerpt from an article focused on the plain truth for finding success with FISMA.

> ***"The key element in demonstrating FISMA compliance is the comprehensive annual report that the CIO and the head of each agency provide to Congress and to the Office of Management and Budget (OMB). This report includes evaluations of the effectiveness of the information security programs, including providing evidence that the agency has developed a coordinated strategy of analyzing security threats and responding accordingly. If an agency implements a technology solution to boost their score in one year, they may score lower following year if they fail to demonstrate how the solution fits into the agency's overall information security strategy." [73]***

Ongoing changes in federal laws, standards, and requirements continue to focus federal agencies on measurement and monitoring. Public security events/incidents also drive the need for security to improve through measurement and monitoring efforts. As described in Section 3.1.1, OMB releases new reporting requirements for agencies to follow and delivers an annual report to the US Congress on government-wide status and progress. Current OMB FISMA guidance requires agencies to report security performance measures provided by OMB as well as three outcome/output security performance measures developed by agencies, based on NIST SP 800-55 Rev. 1. Proposed new FISMA legislation requires Chief Information Security Officers (CISO) to "create, maintain, and manage an information security performance measurement system that aligns with agency goals and budget process."

Currently, FISMA evaluation information security performance measures focus on—

- Tracking system boundaries and configuration of the FISMA systems inventory,
- C&A of systems,
- Testing of security controls and contingency plans,
- Mitigating weaknesses using a POA&M,
- Training employees and security specialists,
- Privacy and protection of personally identifiable information.

Part of the annual process is the OMB annual Computer Security Report Card for federal departments and agencies. The most recent annual report shows strong progress toward implementation. Table 5-4 summarizes overall progress in meeting selected government-wide IT security goals from fiscal years 2002 to 2007, based on input for each agency's CIO.

Table 5-4 Government-wide Security Status and Progress from Fiscal Years 2002 to 2007 [74]

Percentage of Systems with a:	FY 2002	FY 2003	FY 2004	FY 2005	FY 2006	FY 2007
Certification and Accreditation	47%	62%	77%	85%	88%	92%
Tested Contingency Plan	35%	48%	57%	61%	77%	86%
Tested Security Controls	60%	64%	76%	72%	88%	95%
Total Systems Reported	7,957	7,998	8,623	10,289	10,595	10,304

Since FY 2002, security measures have been a key function of the OMB annual Computer Security Report Card. Through security measures, federal departments and agencies have been able to show improvement in their compliance programs.

> ***"The 25 major agencies of the Federal government continue to improve information security performance relative to C&A rates and testing of contingency plans and security controls. Several larger agencies reported especially notable progress regarding these measures, including the National Aeronautics and Space Administration (NASA), the Departments of State, Treasury, and the Department of Defense (DOD). Agencies have also maintained or improved performance relative to IG qualitative assessments of IT security processes. Federal agencies also showed improvement in IG assessments of the quality of their C&A processes." [75]***

Each agency report consists of the—

- CIO part, which is compiled and submitted by the CIO;
- Inspector General (IG) part, which is independently compiled and submitted by the agency IG.

Each agency's IG also contributes an equal part to the FISMA report. Table 5-5 shows an excerpt from government-wide findings for FY 2007.

Table 5-5 FISMA IG Assessments Government-Wide in Fiscal Year 2007 Results Excerpt [76]

Agency	Effective POA&M	Certification and Accreditation Process Quality	System Inventory Completeness	Privacy Impact Assessment Process Quality
Agency for International Development	Yes	Excellent	96–100%	Good
Department of Agriculture	No	Poor	71–80%	Poor
Department of Commerce	Yes	Poor	96–100%	Unaudited
Department of Defense	Unaudited	Unaudited	Unable to Determine	Failing
Department of Education	Yes	Satisfactory	96–100%	Satisfactory
Department of Energy	Yes	Satisfactory	96–100%	Satisfactory
Environmental Protection Agency	Yes	Satisfactory	96–100%	Satisfactory
General Services Administration	Yes	Satisfactory	96–100%	Satisfactory
Department of Health and Human Services	Yes	Good	96–100%	Excellent
Department of Homeland Security	Yes	Satisfactory	96–100%	Good
Department of Housing and Urban Development	Yes	Satisfactory	96–100%	Good
Department of the Interior	No	Poor	96–100%	Poor

Based on the suggested changes associated with the newly proposed FISMA legislation, these performance measures are expected to evolve. The following article excerpt highlights a common status of how FISMA is working, and what elements of the act may need improvements.

> *"Even without something like FISMA, improvements will continuously be added as new uses for technology open new attack surfaces, say experts. But FISMA brings structure to what would otherwise be a chaotic, voluntary process. What many would like to lose is the FISMA scorecard, which experts say is not an accurate representation of the true security posture of an organization. Many have seen organizations get an A when they believe they should have received an F, and vice versa. Weaknesses identified in certification and accreditation activities remain to be mitigated and corrected," says Howard. "Additionally, FISMA reporting emphasizes the existence of processes and does not focus on the quality of those processes." [77]*

5.5 NASA Metrics Programs

As an organization devoted to ensuring the safety of its personnel and the success of its missions, NASA has a long-standing tradition of using metrics to illustrate its internal status. Traditionally, these metrics have been focused specifically on safety (*i.e.,* metrics developed by the NASA Software Assurance Program), but the administration has increasingly been developing security-oriented measures. This section describes metrics programs underway at NASA's Jet Propulsion Laboratory (JPL) and by the NASA CIO. Section 5.5.2 also discusses an analysis performed by Captain Adam Bryant (US Air Force), comparing NASA's metrics programs to DoD's.

5.5.1 NASA JPL Information Security Metrics Program

The Security Metrics Program [78] at NASA JPL has defined three categories of security metrics for reporting to JPL management—

- Compliance,
- Incident response,
- Risk assessment.

Within each category, the JPL Security Metrics Program has defined only nine metrics to be collected because, while more data is available, the program has chosen to focus on those elements that have a significant impact on organizational security, and which thus need to be considered by managers.

Whenever possible, JPL Security Metrics Program managers automate the collection of metrics data; this is particularly true for data in the incident response and risk assessment categories. However, compliance metrics data is virtually always collected manually through database queries and/or by data calls to the information owner or the responsible individual or department.

5.5.2 Comparison of NASA and DoD IA Metrics Programs

In his Masters thesis, *Developing a Framework for Evaluating Organizational Information Assurance Metrics Programs,* [79] Captain Adam Bryant (US Air Force) did an extensive comparison of three IA metrics programs: those of DoD, the US Air Force (USAF), and NASA JPL. Table 5-6 provides Capt. Bryant's summary of the key similarities and differences between these three IA metrics programs.

Table 5-6 Comparison of DoD, USAF, and NASA JPL IA Metrics Programs [80]

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

5.5.3 NASA Deputy CIO Information Security Performance Measures

In 2002, NASA Deputy CIO presented a case study on how information security performance measures were being leveraged for NASA headquarters. [81] NASA CIO viewed IT security and measurement as part of mission accomplishment. A focal point of the philosophy was to identify good metrics that do not impede progress toward the goals. Key process steps included—

- Stakeholder group reviews success of previous-year measures;

- Review, debate, and approval of proposed modifications by IT Security Managers;
- Approval of metrics by department CIOs, and brief presentation of the measures to the NASA Security Council;
- Quarterly measures data collection and analysis, identification of trends, and identification and communication of corrective actions, as required.

The NASA CIO program discovered a way, not only to meet compliance goals, but to reuse information for more advanced measures, including—

- Ratio of observed vulnerabilities to systems to the total number of systems,
- Ratio of penetration rate to attack rate.

Once the baseline implementation of the security program was completed and stable, the organization moved to act smarter without spending more money; increase intelligence through better data, analysis, and increased automated processes; and more tightly integrate security measures into program and capital planning.

5.6 BJS NCSS

In 2001, the Bureau of Justice Statistics (BJS) in the US Department of Justice's Office of Justice Programs (OJP) conducted a pilot Computer Security Survey (CSS) to gather information from 500 US businesses on their computer infrastructure and security measures. Based on the pilot-survey results, BJS, in collaboration with the DHS National Cyber Security Division (NCSD), decided to field a far more extensive National Computer Security Survey (NCSS) of "a nationally representative sample" that constituted 36,000 US businesses across 36 different industry sectors.

In 2004, the RAND Corporation was contracted to develop the survey methodology for the NCSS, which it then applied when the survey was fielded in 2006. The purpose of the survey was to collect statistics intended to be comparable to traditional FBI crime statistics that would enable BJS and NCSD "to produce reliable national- and industry-level estimates of the prevalence of computer security incidents (such as denial of service attacks, fraud, or theft of information) against businesses and the resulting losses incurred by businesses." [82] The statistical data captured by the NCSS could also form the basis for defining key cyber security and computer crime measures; indeed, RAND performed a number of analyses to generate such measures, which are included in the survey report.

In the end, the more than 7,000 businesses that participated in the survey were offered feedback intended to "allow them to benchmark themselves against the rest of their industry sectors." [83]

The report is available online at: http://www.ojp.usdoj.gov/bjs/pub/pdf/cb05.pdf (accessed 10 March 2009).

RAND also published a report detailing the methodology it used to develop and field the NCSS as well as its sampling design and weighting methodology; this RAND report is available for purchase online at: http://www.rand.org/pubs/technical_reports/TR544/ (accessed 10 March 2009).

References

46 Elizabeth B. Lennon. "IT Security Metrics," in *NIST Information Technology Laboratory (ITL) Bulletin,* August 2003. Accessed 8 May 2009 at: *http://www.itl.nist.gov/lab/bulletns/bltnaug03.htm*

47 *IAnewsletter,* Volume 7, Number 3, Winter 2004. Accessed 2 February 2006 at: iac.dtic.mil/iatac/IA_newsletter.html

48 Vivian A. Cocca, OSD(NII). "DoD's Approach to IA Metrics." Presentation at PSM Technical Working Group meeting, 23 March 2005. Accessed 28 December 2008 at: *http://www.psmsc.com/Downloads/TWGMarch05/05_Cocca_DoD_Metrics_Initiative.pdf*

49 *Ibid.*

50 Dave Aland, Johns Hopkins APL, supporting the OSD DOT&E Deputy Director of Naval and C4ISR Systems. "Metrics Lessons Learned from Conducting Operational Assessments of Networks." Briefing at the MORS Workshop on Transforming IA for Netcentric Operations, March 2007. Accessed 10 December 2008 at: *http://www.mors.org/meetings/2007_tia/pres/aland.pdf*

51 DON CIO Blog. Accessed 1 April 2009 at: *http://www.doncio.navy.mil/tagresults.aspx?ID=28*

-and-

US Congress. FISMA, *op cit.*

-and-

Department of the Navy. *CHIPS - The Department of the Navy Information Technology Magazine.* Accessed 2 April 2009 at: *http://www.chips.navy.mil/archives/06_Jul/web_pages/FISMA.htm*

52 Donald L. Buckshaw, Gregory S. Parnell, Willard L. Unkenholz, Donald L. Parks, James M. Wallner, and O. Sami Saydjari, "Mission Oriented Risk and Design Analysis of Critical Information Systems," in *Military Operations Research,* Volume 10 Number 2, November 2005. Accessed 14 April 2009 at: *http://www.mors.org/awards/mor/2006.pdf*

53 DHS. "Guidance for Developing Sector-Specific Plans as input to the National Infrastructure Protection Plan," 2 April 2004. Accessed 4 February 2009 at: *http://cees.tamiu.edu/covertheborder/TOOLS/SSAGuidance.pdf*

54 DHS-DoD-DoC. "Software Assurance Forum Measurement Working Group Status Briefing," May 2008

55 ISO/IEC 15939, *Systems and software engineering—Measurement process.* Accessed on 15 April 2009 at: *http://www.psmsc.com/ISO.asp*

56 Miles McQueen, Wayne Boyer, Sean McBride, Marie Farrar, Zachary Tudor. *Measurable Control System Security through Ideal Driven Technical Metrics,* January 2008. Presented at SCADA Security Scientific Symposium, January 23, 2008. Accessed 6 April 2009 at: *http://www.inl.gov/technicalpublications/Documents/3881671.pdf*

57 *Ibid.*

58 NIST. "NIST Mission, Vision, Core Competencies, and Core Values." Accessed 2 April 2009 at: *http://www.nist.gov/public_affairs/nist_mission.htm*

59 IATAC. *Software Security Assurance: A State of the Art Report (SOAR),* 31 July 2007. Accessed 1 April 2009 at: *http://iac.dtic.mil/iatac/download/security.pdf*

60 NIST SAMATE. "Metrics and Measures." Accessed 6 January 2009 at: *http://samate.nist.gov/index.php/Metrics_and_Measures*

61 Todd Heberlein, Senthil Ebina, Melissa Danforth, and Tye Stallard, University of California at Davis. "Attack Graphs: Identifying Critical Vulnerabilities within An Organization." Seminar presented by University of California-Davis Computer Security Lab, 10 March 2004. Accessed 6 February 2009 at: *http://seclab.cs.ucdavis.edu/seminars/AttackGraphs.pdf*

62 Joseph Pamula, Sushil Jajodia, Paul Ammann, and Vipin Swarup. "A weakest-adversary security metric for network configuration security analysis," in *Proceedings of the 2nd ACM workshop on Quality of Protection (QoP '06),* New York, NY, USA, 2006, pp. 31–38.

63 Lingyu Wang, Tania Islam, Tao Long, Anoop Singhal, and Sushil Jajodia. "An attack graph-based probabilistic security metric," in *22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security,* London, UK, 13-16 July 2008

-and-

Lingyu Wang, Anoop Singhal, and Sushil Jajodia. "Measuring the overall security of network configurations using attack graphs," in *Data and Applications Security XXI* (Berlin/Heidelberg, Germany: Springer Verlag, 2007), pp. 98–11.

64 NIST. "The Information Security Automation Program and The Security Content Automation Protocol." Accessed 26 March 2009 at: *http://nvd.nist.gov/scap.cfm*

65 *Ibid.*

66 The MITRE Corporation. "Common Vulnerabilities and Exposures (CVE)." Accessed 26 March 2009 at: *http://cve.mitre.org*

67 The MITRE Corporation. "Common Configuration Enumeration (CCE)." Accessed 26 March 2009 at: *http://cce.mitre.org*

68 The MITRE Corporation. "Common Platform Enumeration (CPE)." Accessed 26 March 2009 at: *http://cpe.mitre.org*

69 NIST. "NVD Common Vulnerability Scoring System Support v2." Accessed 26 March 2009 at: *http://nvd.nist.gov/cvss.cfm*

70 NIST. "XCCDF - The Extensible Configuration Checklist Description Format." Accessed 26 March 2009 at: *http://nvd.nist.gov/xccdf.cfm*

71 The MITRE Corporation. "OVAL Open Vulnerability and Assessment Language." Accessed 26 March 2009 at: *http://oval.mitre.org*

72 NIST. "CND Data Strategy and Security Configuration Management." September 2008. Accessed 26 March 2009 at: *http://nvd.nist.gov/scap/docs/2008-conf-presentations/day1/CM-and-Data-Strategy-Brief-NIST-2008-SCAP-Conf-Final-Slides.pdf*

73 Cyber Security Industry Alliance. "FISMA: Get the Facts." Accessed 3 February 2009 at: *http://www.csialliance.org/issues/fisma/index.html*

74 OMB. "Fiscal Year 2007 Report to Congress on Implementation of the Federal Information Security Management Act of 2002." Accessed 3 February 2009 at: *http://www.whitehouse.gov/omb/inforeg/reports/2007_fisma_report.pdf*

75 *Ibid.*

76 *Ibid.*

77 Deb Radcliff. "Government Vertical: Is FISMA Working?," in *SC Magazine,* 1 November 2007. Accessed 3 February 2009 at: *http://www.scmagazineus.com/Government-vertical-Is-FISMA-working/article/58396*

78 Described in: Adam R. Bryant, Capt. USAF. *Developing a Framework for Evaluating Organizational Information Assurance Metrics Programs.* Master of Science Thesis for Air Force Institute of Technology. AFIT/GIR/ENV/07-M5, March 2007. Accessed 11 December 2008 at: *https://www.afresearch.org/skins/rims/q_mod_be0e99f3-fc56-4ccb-8dfe-670c0822a153/q_act_downloadpaper/q_obj_217f0dc1-baf2-47c8-a458-60956d23bc05/display.aspx?rs=enginespage*

-and-

Corporate Information Security Working Group. "Report of the Best Practices and Metrics Team," 17 November 2004 (Revised 10 January 2005). Accessed 3 February 2009 at: *http://infotech.aicpa.org/NR/rdonlyres/9C87179C-7F68-4EA0-8FA6-1B8A2EF2768A/0/CISWG_Report_of_best_practices_and_metrics_teams.pdf* (also at: *http://educause.edu/ir/library/pdf/CSD3661.pdf)*

79 Bryant, *Developing a Framework for Evaluating Organizational Information Assurance Metrics Programs, op cit.*

80 *Ibid.*

81 Dr. David B. Nelson, CISSP Deputy CIO, NASA. "Performance Measures for Information Security: NASA Case Study," April 22, 2002, in SecurIT, Spring 2002.

82 US Department of Justice, Bureau of Justice Statistics. "National Computer Security Survey." Accessed 10 March 2009 at: *http://www.ojp.usdoj.gov/bjs/survey/ncss/ncss.htm*

83 RAND Corporation. "DOJ/DHS National Computer Security Survey." Accessed 10 March 2009 at: *http://www.ncss.rand.org/index.html*

6

Industry Initiatives

"As they become aware of the increasing security threats and the implications of these threats to their organizations, executives are asking for security metrics that talk about business impact….CISOs today have no choice but to arm themselves with the right security metrics to address the concerns of their executive management."

Khalid Kark and Paul Stamp, Forrester Research [84]

This section provides an overview of CS/IA measurement initiatives and programs within industry. This section covers efforts underway for creating, implementing, and deploying CS/IA measures from a range of entities within industry. Efforts are underway from security industry consortia, including the CISWG, OWASP, and CIS as well as ISACA, which is not a security-focused organization. Other initiatives are described from Microsoft, @stake, and EDUCAUSE/Internet2. This section also describes the activities put forth by CS/IA measurement-focused organizations: securitymetrics.org and the Security Metrics Consortium.

Like many of the initiatives discussed in Section 5, the goal of these industry initiatives is to improve security measurement programs throughout industry and government. To this end, much of the work described in this section is publicly accessible. (See Appendix B for more information.)

6.1 CISWG Metrics

CISWG was established in 2004 by Representative Adam Putnam (R-FL), under the auspices of the Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census. CISWG included four subgroups, one of which was devoted to promoting Best Practices and Guiding Principles. Within this subgroup, a Metrics Team was established.

On 17 November 2004, the CISWG Metrics Team, along with the Best Practices Team, issued a report [85] for use by executives, managers, and technical staff in large and small organizations, as the basis for defining their own comprehensive sets of performance metrics for measuring the people, process, and technology aspects of information security.

The CISWG Metrics Team's report specifically described a set of Information Security Program Elements and Supporting Metrics. The Security Program elements include—

- **Governance (Board of Directors/Trustees)**—With seven activities that those responsible for this element should perform;
- **Management**—With 10 activities that those responsible for this element should perform;
- **Technical**—With 13 sub-elements that those responsible for this element need to address.

For each activity associated with the Governance and Management elements, and each sub-element of the Technical element, the report defines a set of metrics to be used in determining how well those responsible have performed with regard to those activities/sub-elements.

For example, within the Governance element, one activity is "Oversee Risk Management and Compliance Programs Pertaining to Information Security (*e.g.*, Sarbanes-Oxley, HIPAA, Gramm-Leach-Bliley, *etc.*)." Three metrics are defined for this activity, one of which is "Percentage of key external requirements for which the organization has been deemed by objective audit or other means to be in compliance."

In the Management element, the activity "Identify and Classify Information Assets" has three metrics, one of which is "Percentage of information assets with defined access privileges that have been assigned based on role and in accordance with policy."

In the Technical element, the sub-element "Malicious Code Protection" has three metrics, including "Percentage of mobile devices with automatic protection in accordance with policy."

6.2 OWASP Efforts

OWASP [86] defines itself as "an open source community" of software and application security practitioners dedicated to helping organizations in the private and public sectors develop, purchase, and maintain trustworthy application software. OWASP produces tools and documents, and sponsors forums, chapters, and development projects. Its products are available under open source licenses to any interested party.

OWASP projects are organized as collections of related tasks with a single defined roadmap and team leader. The team leader is responsible for defining the vision, roadmap, and tasking for the project. OWASP projects have produced artifacts ranging from guidance documents, to tools, teaching environments, checklists, and other materials. [87]

6.2.1 OWASP Top Ten

One of the most well-known OWASP projects is the OWASP Top Ten. Released in 2004 and updated in 2007, the OWASP Top Ten project identifies the most critical application security flaws at the time of release. Since its original release in 2004, the OWASP Top Ten has become a security "floor" against which many organizations are assessing their applications.

Many application security analysis tools (*e.g.,* Web application vulnerability scanners or source code analysis scanners) provide OWASP Top Ten compliance reports out-of-the-box. To this end, Gunnar Peterson and other security researchers have identified security metrics for each of the OWASP Top Ten vulnerabilities so that organizations can better gauge their security postures. A paper edited by John Steven and Peterson [88] defines a design-time, deployment-time and run-time metric that organizations may use to rate their systems against the OWASP Top Ten over a period of time. (See Section 6.14 of this report for a discussion of these metrics.)

6.2.2 Application Security Metrics Project

In August 2006, OWASP launched the Application Security Metrics project. [89] This project was intended to shed light on the state of the art in application security metrics. During the first phase, project participants developed an application security metrics survey to be distributed to various organizations. The survey solicited information about the organization's existing Web application security metrics programs. Specifically, project members were interested in the following information—

- Security standards or regulations used to shape the metrics program;
- The use of trending metrics, ROI, and process metrics within each organization;
- Information on discarded metrics;
- Tools used to generate the data for the metrics;
- Tools used to store and track metrics;
- Detailed information about each metric, including how it is created and disseminated.

The Application Security Metrics Project has been on hiatus since April 2007, due primarily to a lack of survey participants. In the second phase of the project, members intended to take the information from the surveys to identify gaps in current metric reporting and begin research into new metrics that would be beneficial to participating organizations.

For Further Reading

Blake Causey. "Why Application Security Metrics are broken." 22 December 2008 on the "Hancock"/Attack Vectors blog. Accessed 2 February 2009 at:
http://attackvectors.com/~/blog/index.php?m=12&y=08&entry=entry081222-141210

6.2.3 ASVS

Started in April 2008 as an OWASP *Summer of Code* project, the Application Security Verification Standard (ASVS) aims to provide a comprehensive assessment framework for Web applications. The ASVS was developed by

OWASP as an evaluation framework that incorporates lessons learned from performing product evaluations using the Trusted Computer System Evaluation Criteria (TCSEC), Common Criteria framework, and FIPS 140 framework.

The need for the ASVS arose from the fact that the Common Criteria and FIPS 140 evaluation methodologies are targeted for Web applications. FIPS 140 evaluation can only be performed on the cryptographic modules used by a Web application. In contrast, the Common Criteria provides a very generic framework, through which Web applications can be evaluated, but the level of rigor and *coverage,* the portions of the application that are physically verified, will very for each Web application, as the Common Criteria STs and PPs may vary with each evaluation.

The ASVS identifies four "levels" against which a Web application can be evaluated. Each level signifies the amount of coverage and rigor that goes into the evaluation, based on documentation and verification procedures outlined in the standard. ASVS defines sets of documentation and verification requirements of three different types—

- **Level requirements**—Define the high-level Web application implementation and verification requirements;
- **Derived verification requirements**—Identify specific items within the Web application implementation to verify;
- **Derived reporting requirements**—Describe how the verification should be documented.

The ASVS levels are themselves composed of multiple component levels. Web applications can be evaluated against a specific component level, but cannot receive the level rating until all component levels have been evaluated (similar to FIPS 140 and Common Criteria evaluation levels).

Each ASVS component level describes a single verification procedure that must be performed. For example, Level 2B requires a manual code review while Level 1A requires a Web application vulnerability scan. As the level increases, the effort associated with the review also increases. For example, Level 4 requires verification that the internal security controls behave correctly. The specific verification requirements for an application are defined and broken down by level. This ensures a minimum set of tests have been performed for each level.

As with FIPS 140 verification, the thoroughness of the ASVS ensures that Web applications evaluated at a specific ASVS level provide an objective measurement of the specific verifications requirements and testing techniques that have been performed on a specific Web application. Measures based on ASVS can illustrate what specific testing techniques have been applied to an ASVS-evaluated Web application as well as what specific verification requirements have been met by the application.

6.3 CIS Security Metrics Initiative

Sponsored by CIS, the Security Metrics Initiative [90] was undertaken by a "consensus team" of CIS members, including representatives from Fortune 50 and smaller commercial and non-profit organizations (with special focus on the banking and finance sector); federal, state, and local governments; security and other vendors; industry experts; universities; independent researchers, mathematicians, statisticians, actuaries, CISOs, and security managers; and other institutions and individuals that specialize in information security.

The goals of the Security Metrics Initiative are to reach consensus on an initial small set of (10 or fewer) unambiguous security metrics, and to facilitate their widespread adoption among CIS members. In addition, the initiative seeks to establish an operational benchmarking service to facilitate—

- Communication of internal security status over time,
- Inter-enterprise benchmarking of security status,
- Development of a database from which security practice/outcome correlations can be derived.

The initiative intended, by the end of 2008, to reach consensus on final definitions of those metrics (to populate the security metrics schema also developed by the initiative), and to develop the benchmarking technology platform that would enable CIS to launch its Security Metrics and Benchmarking Service, with CIS members contributing data and producing benchmark reports. [91]

In Spring 2009, CIS published *The CIS Security Metrics* [92] that provided 21 definitions of security control metrics for six business functions. The metrics presented in this document were developed through a consensus-building process working with industry stakeholders. The business functions and the associated metrics are listed in Table 6-1.

Table 6-1 CIS Consensus Security Metrics

Business Function	Consensus Metrics
Incident management	▶ Meantime to incident discovery ▶ Number of incidents ▶ Percentage of incidents detected by internal controls ▶ Meantime between security incidents ▶ Meantime from discovery to containment ▶ Meantime to recover
Vulnerability management	▶ Vulnerability scanning coverage ▶ Percentage of systems with no known severe vulnerabilities ▶ Number of known vulnerabilities
Patch management	▶ Patch policy compliance ▶ Patch management coverage ▶ Meantime to patch ▶ Meantime to deploy critical patches

Business Function	Consensus Metrics
Application security	▶ Number of applications ▶ Percentage of applications that are critical ▶ Risk assessment coverage ▶ Security testing coverage
Configuration management	▶ Meantime to complete changes ▶ Percentage of changes with security reviews ▶ Percentage of changes with security exceptions
Finance	▶ IT security spending as percentage of IT budget ▶ IT security budget allocation

The metrics and their definitions were arrived at by the consensus of a group of subject matter experts in the business function areas, a group that included consultants, software developers, audit and compliance professionals, security researchers, operational security experts, and government and legal sector representatives. This consensus group's objective was to identify a set of standard metrics that could be used in a wide range of organizations for measurement of effectiveness and value of common security functions and concepts, such as data availability, security management, and security performance.

In addition to the metrics themselves, the consensus group identified a full set of data attributes about security incidents that need to be collected to provide the raw data for determining the values for many of the consensus metrics.

According to CIS, additional consensus metrics are still being defined for these and other business functions. These functions include—

- Anti-malware controls,
- Authentication and authorization,
- Data and network security,
- Software development life cycle,
- Remediation efforts,
- Third-party risk management.

6.4 ISACA

ISACA [93] is an international industry association that counts more then 85,000 members worldwide. Its members work in many IT positions, including consultants, educators, security professionals, regulators, CIOs, and internal auditors. [94]

Over the last several years, ISACA has published several articles dedicated to the subject of security metrics and return on security investment (ROSI) as well as broader documents, substantial portions of which are dedicated to security measurement. One such document is *Information Security Governance: Guidance for Boards and Executive Management.* [95] ISACA has an ongoing Information Security Program Metrics project that intends to expand on the information in this document, and to provide a

guide for information security managers on how to develop business- and performance-focused security program measures and reports. The results of these projects will be available in the second quarter of 2009.

Section 6 of ISACA's *Information Security Governance* document provides a useful overview of issues and challenges associated with establishing an information security metrics and monitoring capability to support information security governance. The section indicates that measurement is essential for effective governance, and addresses a number of challenges associated with measuring information security, including the fact that traditional measures, such as annualized loss expectancy (ALE), downtime due to security incidents, and numbers of patched servers, have limited utility in providing an overall indicator of how secure the enterprise is.

It goes further to state that an absence of an adverse event is not a useful indicator of whether an organization is secure, and that using "simulated" exercises, such as penetration testing, also has limited use. The section concludes that—

- Some organizations are attacked more frequently and/or suffer greater losses than others.
- There is a strong correlation between good information security management and practices, and relatively fewer incidents and losses.

The rest of the section of ISACA's *Information Security Governance* document discusses the fact that, while measuring governance is equally challenging to measuring security, it is nevertheless essential for organizations to attempt to measure security governance to gauge their progress in governing the security program with the ultimate purpose of reducing the security risk to the enterprise. The document states that, while there is no universal method for measuring information security governance, each organization needs to establish its own method and scale based on its business objectives. It proposes several ways to look at measuring information security governance, including some indicators in the following areas1 [96]—

- Governance implementation to gauge implementation of governance framework (The report suggests that while information security is too far removed from governance, Key Goal Indicators [KGIs] and Key Performance Indicators [KPIs] can be used to provide information about the achievement of processes and goals.);
- Strategic alignment of information security activities with business or organizational goals and objectives;
- Risk management and its success at performing against defined objectives;
- Value delivery to evaluate whether acceptable risk posture is achieved at a the lowest possible cost;
- Resource management that assesses whether the organization has effectively allocated its information security resources;

- Performance management that monitors whether the organizational objectives are achieved;
- Assurance process integration that gauges the level of integration of a variety of assurance processes that have traditionally been operating in silos.

These themes are further developed in another article posted by ISACA, "Developing Metrics for Effective Information Security Governance," by John P. Pironti. [97] Several key principles are articulated in this article, including—

- Use of KPIs,
- Clearly defining individual measures,
- Tailoring measures to the audience,
- Keeping the measures simple and consistent,
- Aligning the measures with the business goals.

Pironti states that creating a baseline framework for information security measurement is key to success, and proposes use of a business value-based metric that measure security governance in people, process, procedures, technology, and compliance areas.

He further proposes to break down the information security measurement framework by organizational and performance metrics, operational metrics, technological metrics, business process metrics, business value metrics, and compliance metrics, with examples within each vertical. The examples occasionally overlap, demonstrating that a single measure may be useful across multiple dimensions.

Pironti also mentions that meaningful reporting, tailored to different audiences, is key to making the measures useful. He recommends a tiered reporting model, where the top tier would be of more interest to the executives, the middle tier to business process owners and managers, and the lowest tier to the operational stakeholders, such as system administrators.

Pironti also indicates that benchmark reporting in a variety of graphs and charts might be useful for those occasions when stakeholders want to see their organization's performance against available industry information. The author concludes with a call for flexible and adaptable information security governance measures that will be an asset to an organization by providing meaningful reporting for management.

Another article on security measurement available from the ISACA Web site is "How Can Security Be Measured?" [98] by David A. Chapin and Steven Akridge. This article's authors propose a security program maturity model to provide a venue for measuring progress in achieving security program maturity. Chapin and Akridge point out the fact that traditional security metrics have limited utility, as they do not address the overall improvement

in security, but rather focus on individual aspects of security, such as number and cost of incidents, time, and materials assigned to security, and compliance with policy.

Chapin and Akridge's proposed maturity model is based on ISO/IEC 17799, *Information technology – Code of practice for information security* (which has been renumbered to ISO/IEC 27002, *Information technology – Security techniques – Code of practice for information security management*). Chapin and Akridge's security program maturity model has two dimensions—

- The first one, which lays out the activities that the security program would undertake in a natural progression;
- The second one, which assesses the maturity of each activity.

The structure of this model is similar to that of traditional CMMs, but the content focuses on specific steps that are required to establish an information security program, based on ISO/IEC 17799 information security controls. The authors demonstrate examples of a variety of visual representations of the measurement, including bar charts, pie charts, and a score card that combines the graphics with verbal representation and interpretation of the results.

6.5 Securitymetrics.org

Securitymetrics.org [99] is a community Web site set up by Andrew Jaquith in 2004. The goal of securitymetrics.org is to foster a community of security metrics professionals. In the words of its founder—

> ***"This Web site offers a rational, empirical alternative for decision-makers and security practitioners. Through the efforts of its members, securitymetrics.org intends to put the sword to the failed legacy of squeamish, squishy, non-metrics-based security decision-making. With luck and a bit of hard work, fear will yield to facts, and statistics will supplant scare tactics." [100]***

Securitymetrics.org offers a number of services to its members, including—

- An exclusive mailing list, through which security metrics practitioners can share knowledge and collaborate;
- MetriCon and Mini-MetriCon, conventions co-located at the USENIX and RSA conferences;
- Posts pointing users to articles and other information published by members;
- An additional source for members to publish original research.

Several projects fostered by securitymetrics.org have grown to be important aspects of the security metrics community. The most notable example is the MetriCon conference, launched in 2006, which has provided a

venue for security metrics practitioners to gather, share knowledge, and collaborate. (It is important to note that MetriCon is not the only security metrics convention available to practitioners.)

Another project currently under development at securitymetrics.org is the Metrics Catalog Project, [101] a repository for organizing and sharing metrics definitions. These resources include a database of information to completely define specific metrics, editors for submitting metrics, metric versioning, metric ratings, metric rankings, and metric licensing. The goal of the Metrics Catalog Project is to provide a central location where organizations and researchers can locate, define, and choose metrics for use within their own organizations. In its current form, the Metrics Catalog provides information about the following metrics—

- PCI Data Security Standard (DSS)-1.1,
- NIST metrics,
- NIST 800-53 security controls,
- ISO/IEC 27002,
- CISWG.

While the current list is limited, the Metrics Catalog has the potential to be an important resource for information about various metrics available to organizations.

6.6 Security Knowledge and Awareness Measures

> ***"While measuring the impact of information security education and training, one is actually trying to measure the resulting change in human behaviour and its impact on the organisation's ability to reach its goal. One problem with such measurements is the discrepancy between what people say and what they do. There is a possibility that some employees won't state the truth about their own attitudes or level of awareness. Therefore, the focus should not be on what an employee knows but on what he or she does with this knowledge." [102]***

Several efforts have been made to measure the level of security-awareness within organizations (or by the individuals that constitute them), and to determine whether such awareness results in improved security (expressed in terms of improvements in user behavior, resulting in fewer user-instigated security breaches). Appendix B of NIST SP 800-50 [103] includes a sample awareness and training metric that focuses specifically on measuring direct aspects of security training/awareness programs, such as number of employees trained, and percentage of those trained who have security-related responsibilities or roles.

Other efforts to define security awareness measures focus on measuring actual awareness and knowledge *vs.* effectiveness of awareness/training programs, usually by measuring the direct or indirect evidence of changed user behavior, such as fewer user-originated security policy violations, or fewer malicious code incidents (implying a decrease in risky user behaviors that lead to malicious code entering the IT infrastructure). For example, the United Kingdom (UK) Chapter of the Information Systems Security Association (ISSA) has published a short list of metrics [104] indicating increased employee security knowledge as well as changed employee behaviors as a result of security awareness. These metrics are—

- Percentage of employees that passes information security tests, certification exams, *etc.*;
- Percentage of employees that signs security awareness statements, memoranda of understanding, *etc.*;
- Number of disciplinary actions for security violations;
- Number of employee-originated security incidents;
- Number of serious employee-originated security incidents.

In his Master of Science thesis, *Measuring Information Security Awareness,* [105] Johnny Mathisen suggests a set of nine metrics that are intended to provide inspiration for others to define similar metrics for assessing security awareness. (The thesis also describes the methodology used to come up with these metrics.) These metrics also focus on measuring direct and indirect evidence of changes in the behavior of those who receive security awareness training—

- Percentage of employees that have finished the necessary security training;
- Number of reported security incidents;
- Percentage of employees leaving their desks clean at the end of the day;
- Percentage of waste paper that is shredded;
- Percentage of illicit traffic on the internal computer network;
- Percentage of weak user passwords;
- Number of hits on Web pages about security;
- Number of requests for information or assistance received by the security department;
- Customer satisfaction.

In Appendix I of his thesis, Mathisen provides complete explanatory details on each of these metrics, including how the metric demonstrates employee security awareness.

According to Mathisen, the Internet Security Forum (ISF) also defined metrics for awareness based on suggestions from its members. These metrics were described in the ISF "Effective Security Awareness: Workshop Report," published in April 2002. The report is, however, only available to ISF members.

Most commercial firms in the business of security awareness program consulting and/or awareness training have developed their own sets of awareness metrics. (These examples represent only a sampling of such metrics, and are no way intended to provide an exhaustive listing.)

Gary Hinson of IsecT, Ltd. has identified 10 potential information security awareness metrics, [106] which are described in Table 6-2.

Table 6-2 IsecT Information Security Awareness Metric

Metrics	Examples of Statistics to be Collected	What Metric Indicates
IT change	▶ Relative proportions of emergency-high-medium-low risk changes ▶ Numbers/trends of rolled-back/reversed/rejected changes *vs.* successful changes	Increased awareness results in fewer overall changes, fewer emergency and high risk changes, and fewer changes that need to be undone or rejected.
Security-related IT process maturity	▶ "Half life" for applying patches	Increased awareness leads to more timely patching.
Malware	▶ Number of viruses, worms, Trojans, spams, *etc.*, detected and stopped ▶ Number of malware incidents overall	Increased awareness leads to greater vigilance and faster, more effective response to malware incidents, and reduction of risky behaviors that introduce malware into the environment.
Computer audit	▶ Closed-open-new-overdue ▶ High-medium-low risk	Increased awareness reduces the number of pending audit issues, and the number of high-risk issues.
Control self-assessment and other risk management	▶ [Not provided by source]	Increased awareness will lead to better assessment results and lower quantified risk.
IT Help Desk	▶ Calls relating to information security (*e.g.,* password retrieval/change requests, queries about risks and controls) as a proportion of all calls	Increased awareness will reduce the proportion of Help Desk calls on security topics/issues.
IT incident	▶ Number and seriousness of breaches ▶ Costs to analyze, contain, and recover from breaches ▶ Tangible losses incurred	Increased awareness will help reduce number and seriousness of breaches, and associated costs impacts.
Firewall	▶ Proportion of outbound packets/sessions blocked (*e.g.,* attempts to access blacklisted Web sites) ▶ Number of potential trivial/moderate/critical hacking attacks repelled	Increased awareness will reduce the number of internally originated firewall policy breaches, and enable the tuning of firewall policy to increase the number of externally-originated breaches.

Metrics	Examples of Statistics to be Collected	What Metric Indicates
System/network vulnerability	▶ Number of known open, closed, or novel vulnerabilities ▶ Average time to patch	Increased awareness will enable more secure configuration and more timely patching of systems/networks.
Response to security awareness activities	▶ Number of emails/calls pertaining to individual awareness initiatives	This metric provides a direct measure of the interest generated by awareness initiatives. It may also indicate effectiveness of outcomes.

Additional security awareness metrics are reported by K. Rudolph of Native Intelligence, Inc., a security awareness and training firm, [107] including metrics suggested by Chad Robinson of the Robert Frances Group—

- Number of attempts to access unauthorized Web site content,
- Number of invalid login attempts,
- Number of incidents of storage of unauthorized file content (*e.g.*, audio, video),
- Number of unauthorized attempts to access controlled resources (*e.g.*, VPN),
- Number of incidents of disclosure of sensitive information,
- Number of incidents of data or intellectual property theft,
- Number of incidents of unauthorized use of administrator privileges.

The implication for all of these metrics is that increased security awareness will lead to a decrease in the number of such incidents/breaches.

Rudolph also cites awareness metrics from the Gartner Group's "Metrics for Information Security Awareness," which fall into the categories of Process Improvement, Attack Resistance, Efficiency/Effectiveness, and Internal "Crunchiness" (*i.e.*, hardness). These metrics are summarized in Table 6-3.

Table 6-3 Gartner Group Metrics for Information Security Awarenes

Category of Metrics	Examples of Metrics in Category
Process Improvement Metrics	▶ Percentage of staff that knows that the security policy exists ▶ Percentage of staff that has seen or read the security policy ▶ Percentage of individuals tested on the policy (passing and failing) ▶ Are internal and external security audits showing improvement?
Attack Resistance Metrics	▶ Percentage of surveyed individuals recognizing a security event scenario ▶ Percentage of surveyed or tested individuals susceptible to social engineering ▶ Percentage of users tested that revealed their passwords ▶ Percentage of administrators tested that failed an improper password change attempt ▶ Percentage of users activating a test virus
Efficiency/Effectiveness Metrics	▶ Percentage of security incidents having human behavior as a major factor

Category of Metrics	Examples of Metrics in Category
Internal "Crunchiness" Metrics	▶ Percentage of corporate software, partners, and suppliers reviewed for security ▶ Percentage of critical data that is strongly protected ▶ Percentage of critical data not protected according to security standards ▶ Percentage of systems having malware and/or unapproved software installed

Native Intelligence also offers its own four-page listing of potential security awareness program metrics [108] in two categories—

- Internal User Behaviors: Ranked as "Good," "Bad," and/or "Ugly;"
- End User Knowledge and Perceptions of IT Security.

Native Intelligence also provides suggestions on how and from what source(s) to collect data for each metric.

6.7 PSM Security Measurement

The PSM is a US Army-sponsored measurement process for use in software and system acquisition and development projects. The PSM defines a process that includes four activities—

- Measurement planning;
- Measurement performance;
- Ongoing evaluation and enhancement of measures and measurement process;
- Establishment and sustainment of management commitment.

The PSM measurement approach was adopted by the CMMI community, and formed the basis for the ISO/IEC15939 Software Engineering Software Measurement Process.

In 2006, the PSM Safety and Security Technical Working Group published a Security Measurement Whitepaper [109] that described research on existing security measurement methodologies and the attempt to measure security properties of software-intensive systems. The objective of the white paper, which proposes a PSM-based "system-theoretic" model for security measurement, is to integrate security measurement principles into the general measurement principles of PSM, consistent with its related standard: ISO/IEC 15939:2002.

For Further Reading

Fred Hall. "Measurement of Security Processes." Presentations from workshop presented at PSM Technical Working Group Meeting, Herndon, Virginia, March 2006. Accessed 2 February 2009 at: *http://www.psmsc.com/Downloads/TWGMarch06/3%20-%20Measurement%20of%20Security%20Processes.Hall.zip*

Cheryl Jones, USA. "Making Measurement Work," in *CrossTalk: The Journal of Defense Software Engineering,* January 2003. Accessed 2 February 2009 at: *http://www.stsc.hill.af.mil/Crosstalk/2003/01/jones.html*

Cheryl Jones, CIV USA AMC, and John Murdoch, University of York. "Security Measurement: Applying PSM Principles." Presented at Practical Software and Systems Measurement Users' Group Conference, 14-18 July 2008, Mystic, CT. Accessed 3 February 2009 at: *http://www.psmsc.com/UG2008/Presentations/14%20-%20Murdoch-Security%20Measurement-17Jul08.pdf*

6.8 Microsoft Security Measures

As part of its Trustworthy Computing initiative, Microsoft published its Security Development Lifecycle Threat Modeling methodology, in the context of which were defined two levels of security measures: the DREAD vulnerability rating system, and the RASQ. (Note that the Microsoft Security Bulletin Severity Rating System is not discussed here because it is covered in Section 7.4.6.)

6.8.1 DREAD

The DREAD model is used, and promoted, by Microsoft as a means to prioritize risks associated with exploitable vulnerabilities, and to do so with a greater granularity than is possible with a simple numerical or red-yellow-green type rating system. "DREAD" is an acronym made up of the first letters of five attributes that threat modeling uses to "measure" each vulnerability in the system being assessed—

- ***Damage potential***—How much damage will result if the vulnerability is exploited?
- ***Reproducibility***—How easy would it be reproduce the exploit?
- ***Exploitability***—How easy is it to exploit the vulnerability?
- ***Affected users***—How many users (rough percentage) would be affected by the exploit if it were successful?
- ***Discoverability***—How easy is it to find the vulnerability?

Microsoft suggests using a simple priority rating scale to enable a consistent "sense" of priorities across all the exploits ("threats") to be assessed. For example, it uses a rating scale as simple as "High = 3, Medium = 2, Low = 1" for individual DREAD attributes, plus the assignment of "High," "Medium," and "Low" to the aggregation of the DREAD ratings for each exploit, as illustrated in the example in Table 6-4.

Table 6-4 Example of DREAD Rating of Two Attacks

Threat	D	R	E	A	D	Total	Rating
Man-in-the-middle capture of authentication credentials sent in an unencrypted HTTP session	3	2	3	2	2	12	High
SQL injection attack against Web portal front-end to legacy database	2	3	3	3	1	12	High

To be meaningful as a measure, the DREAD rating for a given exploit should be calculated for both the unmitigated and mitigated vulnerability. For example, the rating for the first exploit in Table 6-4 would be repeated with the variation that secure socket layer was used to encrypt the HTTP session over which the credentials were transmitted, thus eliminating the vulnerability.

In this way, DREAD ratings can be used not just to prioritize vulnerabilities but to help assess the anticipated effectiveness of countermeasures to those vulnerabilities.

6.8.2 RASQ

The RASQ is a measure for determining whether one version of a system is more secure than another with respect to a fixed set of dimensions. Rather than count flaws at the code level or vulnerability reports at the system level, Microsoft has defined a measure for quantifying the "attack opportunities" presented by a system. The RASQ model computes the attack opportunities of a system by identifying and describing all of its potential exploit points, then assigning each of them a relative vulnerability level, based on exploits that have been observed in the real world.

RASQ provides a means to demonstrate what seems to be logically intuitive, *i.e.,* that the number of attack opportunities will increase with the increased exposure of the system's "attack surface," [110] with increased exposure increasing the likelihood that the system will become a target of attack. The RASQ thus provides a mechanism for measuring attack surface (and its exposure), and also for gauging whether and by how much attack surface/exposure is reduced by applied countermeasures.

In March 2003, Microsoft hired Ernst & Young to validate its RASQ model for each of the company's Window server platforms. Ernst & Young's assessment included a review of the RASQ model, plus tests of the model against specific configurations of the different Windows server operating systems, to obtain their RASQ rankings.

Microsoft has also collaborated with researchers at CMU to improve the RASQ model. The progress of this collaboration inspired CMU to go even further in efforts to extend and refine attack surface measurement, using the RASQ as a starting point, in hopes of defining a methodology and measures superior to the RASQ. This research is summarized in Table E-1 of this SOAR.

For Further Reading

Michael Howard, Microsoft Corporation, and Jon Pincus and Jeannette M. Wing, Carnegie Mellon University. "Measuring Relative Attack Surfaces," in *Proceedings of Workshop on Advanced Developments in Software and Systems Security,* Taipei, December 2003. Accessed 29 January 2009 at: *http://www.cs.cmu.edu/~wing/publications/Howard-Wing03.pdf*

6.9 ISECOM RAVs

The Institute for Security and Open Methodologies (ISECOM) is best known for publishing the Open Source Security Testing Methodology Manual (OSSTMM). [111] The OSSTMM refers to security measures as Risk Assessment Values (RAVs). A RAV calculates "base numbers" (which are percentages of risk) to influencing factors in three categories—

1. **Operational Security (OpSec)**—In essence, security design, including such factors as system visibility, access, and trust relationships;
2. **Actual Security (ActSec)**—Characterizes the current security situation, comprising vulnerabilities, weaknesses, exposures, anomalies, and other security concerns;
3. **Loss Controls (LCs)**—Security measures derived from best practices, such as authentication, non-repudiation, confidentiality, privacy, indemnification, integrity, safety, usability, continuity of operation, and alarms.

The OpSec base number represents the percentage of risk mitigation the OpSec requires. The ActSec base number represents the level of risk caused by the unmitigated ActSec. The LC base number represents the amount of risk mitigation provided by the LC.

The RAV represents a calculation of the system's security level in relation to a level of "perfect security" (defined based on best practices), and also a "degradation curve," depicting the system's ability to continue reacting securely and appropriately to unexpected events (anomalies and security incidents) over time (expressed as a percentage of full control [100%], with a sliding scale beneath, ranging from weak control down to deficient control and ultimately to non-existent control). [112]

The OSSTMM provides the set of equations necessary for performing these calculations, from calculating these base numbers from relevant data obtained from interviews, security tests, and vulnerability scans (specified in the OSSTMM); to assumptions based on system configurations; and security problems identified (and manually verified) by auditors.

According to the BNET Business Wire, "RAV is increasingly the most common security measure demanded by regulatory bodies." [113]

6.10 @Stake BAR

Business Adjusted Risk (BAR) [114] is an intentionally simple technique for classifying security defects (or vulnerabilities) by their associated risk of exploitation (rated from 1-5, depending on the business context in which the system exists) and potential business impact (also rated from 1-5), then assigning an overall score to each defect that represents the combination of these two factors.

A "risk of exploitation" score of 5 denotes a high-risk, well-known defect that an attacker can exploit through use of off-the-shelf tools or canned attack scripts. A score of 3 indicates a defect that can only be exploited by an attacker with intermediate-level skills and knowledge, such as the ability to write simple scripts. Finally, a score of 1 indicates a defect that only a professional-caliber expert malicious attacker can exploit.

A "business impact" score of 5 would be assigned to a defect which, if exploited, could result in significant financial damage, negative media exposure, and damage to the organization's reputation. A business impact score of 3 would be assigned to a defect wherein a successful exploit could cause limited or quantifiable financial damage, and possible negative media exposure. Defects that would have no significant impact, financial or otherwise, would be assigned a score of 1.

The BAR is then calculated simply by multiplying the risk score together with the business impact score. The resulting BAR score is intended to be interpreted similarly to an ALE calculation, *e.g.*, a BAR rating of 20 would be understood to denote an order of magnitude more risk than a rating of 2.

6.11 EDUCAUSE/Internet 2 Security Task Force Sub-Working Group on Security Metrics

In July 2000, EDUCAUSE and Internet2 formed the EDUCAUSE/Internet2 Computer and Network Security Task Force to improve information security and privacy across the higher education sector. Within the Security Task Force, a number of working groups and committees pursue projects and initiatives to develop and promote best practices and solutions for achieving security and privacy of IT assets and infrastructures in the higher education sector.

In mid-2007, the EDUCAUSE/Internet 2 Security Task Force established a Security Metrics Sub-Working Group within its Effective Practices and Solutions Working Group. The Security Metrics Sub-Working Group's stated goal is to identify and promote practices, tools, and procedures that will lead to the development of metrics that can provide a comprehensive picture of a security environment. The resulting best practices will be compiled and shared with institutions of higher education, to help them develop their own security metrics and measurement practices.

The subgroup evaluated and ranked the importance of a number of metrics in the four categories indicated in Table 6-5.

Table 6-5 EDUCASE/Internet 2 Security Metrics

Metrics Category	Number of Metrics in Category	Intended Use of Metrics in Category
Operational Metrics	3+	Intended to be useful to technologists
Incident Metrics	3+	Enable academic institutions to communicate to each other data about incident detection and response, such as number of new incidents discovered or number of incidents responded to in a given timeframe
Compliance Metrics	3+	Demonstrate IT organizations' compliance with security policy
Executive Metrics	TBD	Communicate security information to administrative leaders of educational institutions

The sub-working group also began work on a "cookbook" to specify what an academic institution needs to do to build and implement each metric as well as methods for diagnosing problems. The Security Metrics Sub-Working Group also plans to develop a benchmark process, in which institutions begin running metrics and share the results in a way that is independent of their specific systems and environments.

These resources will be made available to EDUCAUSE and Internet 2 members *via* a Web site that contains all of the tools for building and implementing the metric tools. The metrics themselves are being tested by a committee composed of EDUCAUSE member institutions.

6.12 JCIAC: Statistics for Computer-Related Crime

In 2003 and 2004, the Joint Council on Information Age Crime (JCIAC) [115] undertook a study in which it used statistics collected from multiple computer crime surveys to depict the current state of computer-related crime, and to identify a set of desirable standard measures that could be used to "ascertain the incidence and impact of computer-related crime in the United States." These measures were intended to be applied to specific types of information systems and network security incidents and specific types of industries and organizations. The proposed measures included—

- Gross annual losses and average annual number of incidents;
- Losses and number of incidents by category;
- Losses and number of incidents by industry and size of organization;
- Gross and categorical annual expenditures on computer systems security;
- Expenditures on computer systems security by category, industry, and size of organization;
- Increases or reductions in losses and incident counts over previous year by category, industry, and size of organization;
- Disposition of incidents (investigation, administrative action, civil or criminal prosecution, recoveries, if any).

The study report [116] also called for the development of a measurement process for collecting computer-related security incident and crime data that could be used to measure this type of crime.

6.13 DRM Effectiveness and Impact Measures

In 2006, the Center for Democracy and Technology (CDT) published a white paper [117] proposing four categories of measures that it encourages evaluators of Digital Rights Management (DRM) services and device capabilities to consider. These categories include—

- **Transparency**—Presence of a clear disclosure to users of the impact DRM may have on their uses of a work, and the functioning/interoperability of their digital devices;
- **Effect on use**—Clear statement of the specific parameters and limitations DRM enforces on the possible use of a work;
- **Collateral impact**—Any other potential impact DRM technology may have on the user;
- **Purpose and consumer benefit**—Evidence that DRM is being used innovatively, to facilitate new business models and satisfy previously unaddressed demands, provide new consumer choices, *etc.*, rather than locking consumers into old business models, limiting their choices, *etc.*

The CDT white paper further described a robust set of specific measures within each category, and proposed a methodology for DRM evaluators to implement these metrics.

6.14 Web Application Security Metrics Framework

In 2007, Elizabeth Nichols and Gunnar Peterson described the Web Application Security Metrics Framework. [118] In their initial discussion of the framework, Nichols and Peterson define a set of metrics based on the OWASP Top Ten and the three phases of the software development life cycle: design, development, and runtime. The metrics at each phase of the life cycle will provide the following benefits—

- **Design-time metrics**—Can aid in identifying weaknesses early in the application life cycle, decreasing the cost to mitigate them.
- **Deployment-time metrics**—Quantify the change that occurs to the system over time to establish baselines for anomaly detection.
- **Runtime metrics**—Quantify the application's behavior and identified vulnerabilities.

With this baseline, Nichols and Peterson identify design-time, deployment-time, and run-time metrics that can be associated with each of the OWASP Top Ten. Example metrics include—

- **Unvalidated input**—The authors identify the design-time metric *V/T,* where *T* equals the number of POSTs and GETs in the application, and *V* equals the number of those fields with input validation enabled.
- **Cross-site scripting**—The authors identify the run-time metric *XsiteVulnCount,* which is the number of cross-site scripting vulnerabilities found during penetration testing.
- **Buffer overflow**—The authors identify the deployment-time metric *OverflowVulnCount,* which is based on the patching latency of buffer overflows vulnerabilities for the components of the system.

Using these relatively simple metrics, organizations can easily calculate scorecards against which their Web applications can be measured. In addition, organizations can use these metrics to gauge the performance of their organization over time.

Nichols and Peterson acknowledge that the OWASP Top Ten—or the metrics identified in the examples—may not meet the needs of a particular organization. As such, they include a series of steps inspired by Six Sigma that organizations can use to generate their own metrics and scorecards—

1. Express each metric in terms of defects divided by opportunities.
2. Map values to colors by comparing each value to thresholds.
3. Aggregate all individual Web application scores into a single summary score.

Using these steps as a starting point, organizations can develop their own scorecards using relatively easy to calculate metrics early on, with the goal of including more robust and well-understood metrics. According to the authors, a simple automated scorecard can be developed with two weeks.

6.15 SecMet

The establishment of the Security Metrics Consortium (SecMet) was announced at the RSA Conference in February 2004. Founded by a group of Chief Security Officers (CSO) and CISOs from major corporations, including Motorola, Macromedia, and McKesson Corporation, SecMet hoped to transform the "black-magic art" of security measurement "into more of a science" by analyzing existing risk models developed by NIST, CMU, and others to derive a set of quantifiable security measurements, to include security policy compliance measurements. SecMet's hope was that the identified measurements could then be used to create a security "dashboard."

SecMet began its work with the assistance of technology vendors, though the consortium leadership was clear that vendors were welcome only as advisers to the consortium, and not as active members (although Scott McClure of McAfee appears to have been a founding member, contrary to this policy).

SecMet was a short-lived effort, however. As there has been no news of SecMet since the end of 2005, it is impossible to know why the consortium failed, and why the group never published or released any products.

6.16 Surveys of "Real World" CS/IA Measurement Usage

This section highlights two surveys taken of IT managers and executives, to determine to what extent and how CS/IA measures of various types are actually being used to drive decision-making about security in "the real world."

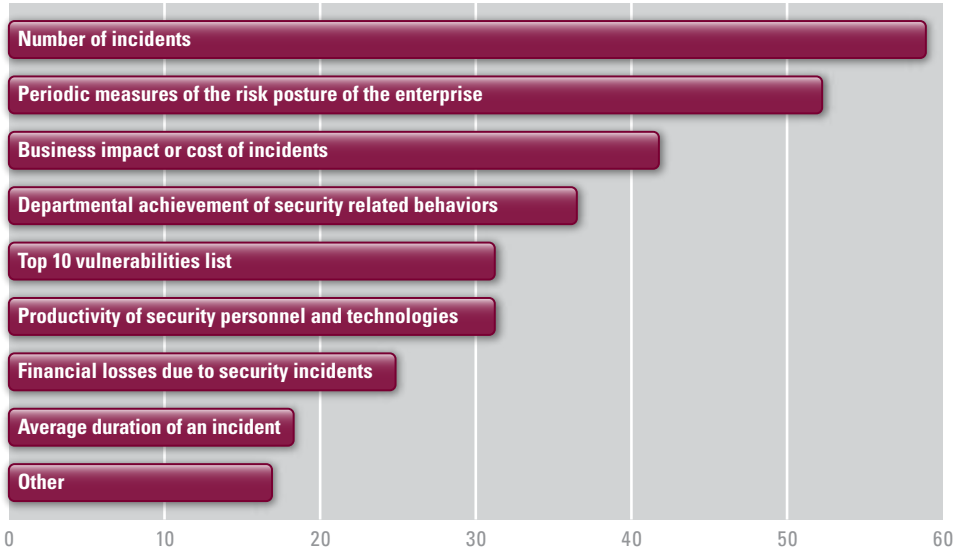
6.16.1 Frost & Sullivan 2005 Survey of Private Sector IT Security Metrics Usage

In a recent survey conducted by Frost & Sullivan, [119] top IT decision makers at over 80 companies were polled for input on their interest in measuring security value, and their current practices for generating and communicating such measures. Several findings of the report were of particular interest—

- 75% of respondents indicated that IT security teams provide reports to business partners and other functional managers outside of IT.
- Of those respondents who replied that IT security reports are provided to partners and other functional business managers, nearly 90% indicated that those reports are provided at least monthly and, in some cases, weekly and even daily.
- Almost 90% of organizations that produce periodic reports use those reports to describe their current security posture. 46% have already begun using measures to articulate security value. Approximately 43% plan to do so in 2006.
- Nearly 60% of respondents answered that they use reports or measures to justify security spending—almost 80% believed demonstrating IT security effectiveness to non-IT functional managers helps IT to justify its actions and budgets.
- 50% of companies surveyed had begun to realize the importance of trending as a tool for measuring security. Over 66% of respondents had already implemented or were planning to implement (within the coming year) different forms of trending data.

Figure 6-1 quantifies the types of measures most often reported to non-IT managers, as indicated by the Frost & Sullivan survey findings.

Figure 6-1 Most Prevalent Measures Reported to Non-IT Managers [120]



6.16.2 Forrester Research 2007 and 2008 CISO Surveys

Since 2006, Forrester Research has done significant research on security performance measures, with particular focus on best practices for security performance measurement, and case studies of CS/IA measures usage. Some examples of the firm's research reports in this area include: "Case Study: Verizon Business Builds an Asset-Based Security Metrics Program," "Best Practices: Security Metrics," "How to Measure what Matters in Security," "Are We Secure Yet? Defining Business-Centric Metrics for Information Security," and "Trends 2006: Information Security Reporting." [121]

In 2007, Forrester Research interviewed 19 CISOs about their current IT security practices. The survey [122] revealed that, in the area of security measurement, only five of the 19 respondents had a formal security measurement program in place, while 10 more respondents reported plans to develop such a program within six to 12 months.

The top challenges to establishing a good measurement program were perceived to be: (1) finding the right metrics (13 respondents) and (2) translating security metrics into "business language" (10 respondents). Forrester's analysts made the following observations—

- The security metrics in use focused on operational and project status, and were still largely driven by compliance concerns.
- Many people still confuse security measurements with security metrics.
- Many security metrics collected are not useful for their intended purpose or audience.

Forrester followed up this survey on 22 July 2008 with its report entitled "Best Practices: Security Metrics," [123] in which 20 CISOs were interviewed more extensively about their firms' security metrics programs, and the best

measurement practices and lessons learned that emerged from them. According to the report, "The three main themes that came out of this research are: Be very selective in picking your security metrics, think beyond the security organization, and focus on reporting and presentation."

6.17 Commercial Providers of CS/IA Measurement Services

The need for CS/IA measurement has engendered an industry in services to assist IT organizations in establishing their own measurement programs, or in providing such programs to organizations under a "fee for service" type arrangement. In September 2007, Forrester Research identified "developing dashboards to streamline security measurement and reporting" as one of four security consulting service areas in the third quarter of 2007 that yielded the highest revenues from among all security consulting services. [124]

The majority of companies providing CS/IA measurement services fall into one of two categories—

- Companies that provide regulatory compliance consulting/services, and that have extended their capabilities to include measures in support of compliance assessment for security and/or privacy mandates, such as FISMA, HIPAA, and ISO/IEC 27001;
- Companies that provide other IA-related services, and that have extended their capabilities to include measurement.

In a few cases, these companies provide other types of services, such as business intelligence reporting based on CS/IA measures (*e.g.*, Trust Informatics). Table 6-6 provides a representative listing of commercial CS/IA measurement service providers. Excluded are service providers that simply use others' measures to perform security audit, compliance assessments, and other such services; and consulting services specific to a single product or product set. Again, this listing is intended to be representative/illustrative only, and not exhaustive.

Table 6-6 IA Measurement Service Providers

Company	Context	URL	Specific Offering/Focus
Certified Security Solutions	Security performance management	*http://www.css-security.com/securitymetricdvlpmt.html*	"Security Metric Development" (offered as a component of "Security Performance Management" service)
Fred Cohen & Associates	CS/IA measurement research	*http://all.net/resume/papers.html*	Security measurement guidance development and training
Metrus Group	Measurement consulting	*http://www.metrus.com/products/security-strategy.html*	"Strategic Measurement Services for Security Professionals"
Orange Parachute	ISO 27001/27002 compliance	*http://www.orangeparachute.com/infosec_security_metrics.aspx*	Information security measures definition and measurement

Company	Context	URL	Specific Offering/Focus
Security Leadership Solutions Executive Council	Business intelligence for security/risk executives	*https://www.securityexecutivecouncil.com/research*	Customer-targeted research reports and benchmarks with strong security measurement focus/content
Sify ASSURE	Security and risk management consulting	*http://www.sifyassure.com/scripts/iaconsult_iss_enterpriseINFO.asp*	Information security measures development
Treadstone 71	IA and risk management consulting	*http://www.treadstone71.com/corpinfo/T71_Security_Metrics.html*	"Security Metrics Service"
Trust Informatics	Business intelligence	*http://www.trustinform.com*	"Managed Security Metrics Program"

References

84 *Op cit.* Kark and Stamp.

85 CISWG. "Report of the Best Practices and Metrics Team," *op cit.*

86 OWASP. Accessed 25 March 2009 at *http://www.owasp.org/index.php/Main_Page*

87 IATAC. *SOAR: Software Security Assurance, op cit.*

88 John Steven and Gunnar Peterson, Editors. "A Metrics Framework to Drive Application Security Improvement," in *Building Security In,* IEEE Security and Privacy, 2007. Accessed 25 March 2007 at *http://www.arctecgroup.net/pdf/0703-OWASPMetrics.pdf*

89 OWASP Web page. "OWASP Application Security Metrics Project." Accessed 13 January 2008 at: *http://www.owasp.org/index.php/Category:OWASP_Application_Security_Metrics_Project*

90 Clint Kreitner, CIS. "The CIS Security Metrics and Benchmarking Service." Presented at Metricon 3.0, San Jose, California, 29 July 2008. Accessed 30 January 2009 at: *http://www.securitymetrics.org/content/attach/Metricon3.0/metricon3-kreitner.pdf*

91 *Ibid.*

92 CIS. *The CIS Security Metrics,* May 2009.

93 ISACA was known previously as the Information Systems Audit and Control Association; the organization now goes by its acronym only.

94 ISACA. Accessed 10 February 2009 at: *www.isaca.org*

95 W. Krag Brotby, IT Governance Institute. *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition.* (Rolling Meadows, IL: ISACA, 2006.) Complimentary PowerPoint presentation and book order information available at: *http://www.isaca.org/Template.cfm?Section=Research2&CONTENTID=21462&TEMPLATE=/ContentManagement/ContentDisplay.cfm* (accessed 8 April 2009).

96 *Ibid.*

97 John P. Pironti. "Developing Metrics for Effective Information Security Governance," in *Information Systems Control Journal,* Volume 2, 2007. Accessed 2 April 2009 at: *http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=35913&TEMPLATE=/ContentManagement/ContentDisplay.cfm*

98 David A. Chapin, CISA, CISM, CISSP, IAM, and Akridge, Steven, JD, CISM, CM, CISSP, IAM. "How Can Security Be Measured," in *Information Systems Control Journal,* Volume 2, 2005. Accessed 8 February 2009 at *http://www.isaca.org/Content/ContentGroups/Journal1/20058/How_Can_Security_Be_Measured_.htm*

99 Andrew Jaquith. "Securitymetrics.org: Who We Are Wiki." Accessed 5 February 2009 at: *http://www.securitymetrics.org/content/Wiki.jsp?page=WhoWeAre*

100 *Ibid.*

101 Metrics Center. *Metrics Catalog Project.* Accessed 5 February 2009 at: *http://www.metricscenter.org* (Log-in required)

102 Johnny Mathisen. *Measuring Information Security Awareness.* Gjøvik University College Master of Science Thesis, 17 June 2004. Accessed 30 January 2009 at: *http://www.dsv.su.se/en/seclab/pages/pdf-files/2005-x-213.pdf*

103 Mark Wilson and Joan Hash. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program,* October 2003. Accessed 30 January 2009 at: *http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf*

104 ISSA, UK Chapter. "Is Security Awareness wasted on End Users?," 13 March 2008, pg. 12. Accessed 29 January 2009 at: *http://www.issa-uk.org/downloads/Security%2520awareness%2520presentation.pdf*

105 J. Mathisen, *Measuring Information Security Awareness, op cit.*

106 Gary Hinson, IsecT Ltd. "Seven myths about information security metrics," in *ISSA Journal,* July 2006. Accessed at: *http://www.noticebored.com/IsecT_paper_on_7_myths_of_infosec_metrics.pdf*

107 K. Rudolf, Native Intelligence, Inc. "Security Awareness Metrics: Measure What Matters." Accessed 29 January 2009 at: *http://www.nativeintelligence.com/ni-programs/metrics-01.asp*

108 Native Intelligence, Inc. "Security Awareness Program Metrics." Accessed 30 January 2009 at: *http://www.nativeintelligence.com/ni-programs/ni-program-metrics-4pg.pdf*

109 PSM Safety and Security Technical Working Group. "Security Measurement Whitepaper, " Version 3.0, 13 January 2006. Accessed 2 February 2008 at: *http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper_v3.0.pdf*

110 For an explanation of the concept of "attack surface," see Michael Howard. "Attack Surface: Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users," in *MSDN Magazine,* November 2004. Accessed 30 January 2009 at: *http://msdn.microsoft.com/en-us/magazine/cc163882.aspx*

111 ISECOM. *Open Source Security Testing Methodology Manual (OSSTMM).* Accessed 2 April 2009 at: *http://www.isecom.org/osstmm*

112 Pete Herzog, ISECOM. "Calculating Risk Assessment Values." ISECOM Whitepaper. Accessed 29 January 2009 at: *http://isecom.securenetltd.com/RAVs.pdf -and-* Dreamland Technologies. "OSSTMM: measurable security." Corporate brochure. Accessed 30 January 2009 at: *http://www.dreamlab.net/download/documents/dlt_OSSTMM_engl.pdf*

113 BNET Business Wire. "CIOview Delivers SecurityNOW!: Provides Financial Transparency for IT Security; Increases Security Auditor Productivity 90%," 14 September 2004. Accessed 30 January 2009 at: *http://findarticles.com/p/articles/mi_m0EIN/is_/ai_n6193303*

114 Introduced in: Daniel Geer, Kevin Soo Hoo, and Andrew Jaquith. "Information security: Why the future belongs to the quants," in *IEEE Security and Privacy,* Volume 1 Issue 4, July/August 2003, pp. 24-32. Digital Object Identifier: 10.1109/MSECP.2003.1219053

115 JCIAC was established in January 2001 to coordinate public-private sector prevention of high-tech crime, including computer-related crime. Its activities ended in 2006. The council included: The International Association of Chiefs of Police, High Tech Crime Investigation Association, Transported Asset Protection Association, International Electronic Security Group, National White Collar Crime Center and ASIS International. JCIAC research was funded, for the most part, by the US Department of Justice's National Institute of Justice.

116 JCIAC. "Computer-Related Crime Impact: Measuring the Incidence and Cost." White Paper, January 2004. Accessed 25 March 2009 at: *http://www.jciac.org/JCIAC%20docs/Computer-Related%20Crime%20Impact%20010904.pdf*

117 CDT. "Evaluating DRM: Building a Marketplace for the Convergent World," Version 1.0, September 2006. Accessed 19 January 2009 at: *http://www.cdt.org/copyright/20060907drm.pdf*

118 Gunnar Peterson and Elizabeth Nichols. "Web Application Security Metrics Framework," in *IEEE Security & Privacy,* March/April 2007.

119 Described in: Robert Ayoub, Frost & Sullivan. "Analysis of Business Driven Metrics: Measuring for Security Value," in *DM Review,* March 2006. Accessed 10 December 2008 at: *http://www.dmreview.com/white_papers/2290613-1.html* (requires online registration to download)

120 *Ibid.*

121 Executive summaries for these articles are available at *http://www.forrester.com* (accessed 13 April 2009). Full access to articles available only to Forrester Research clients.

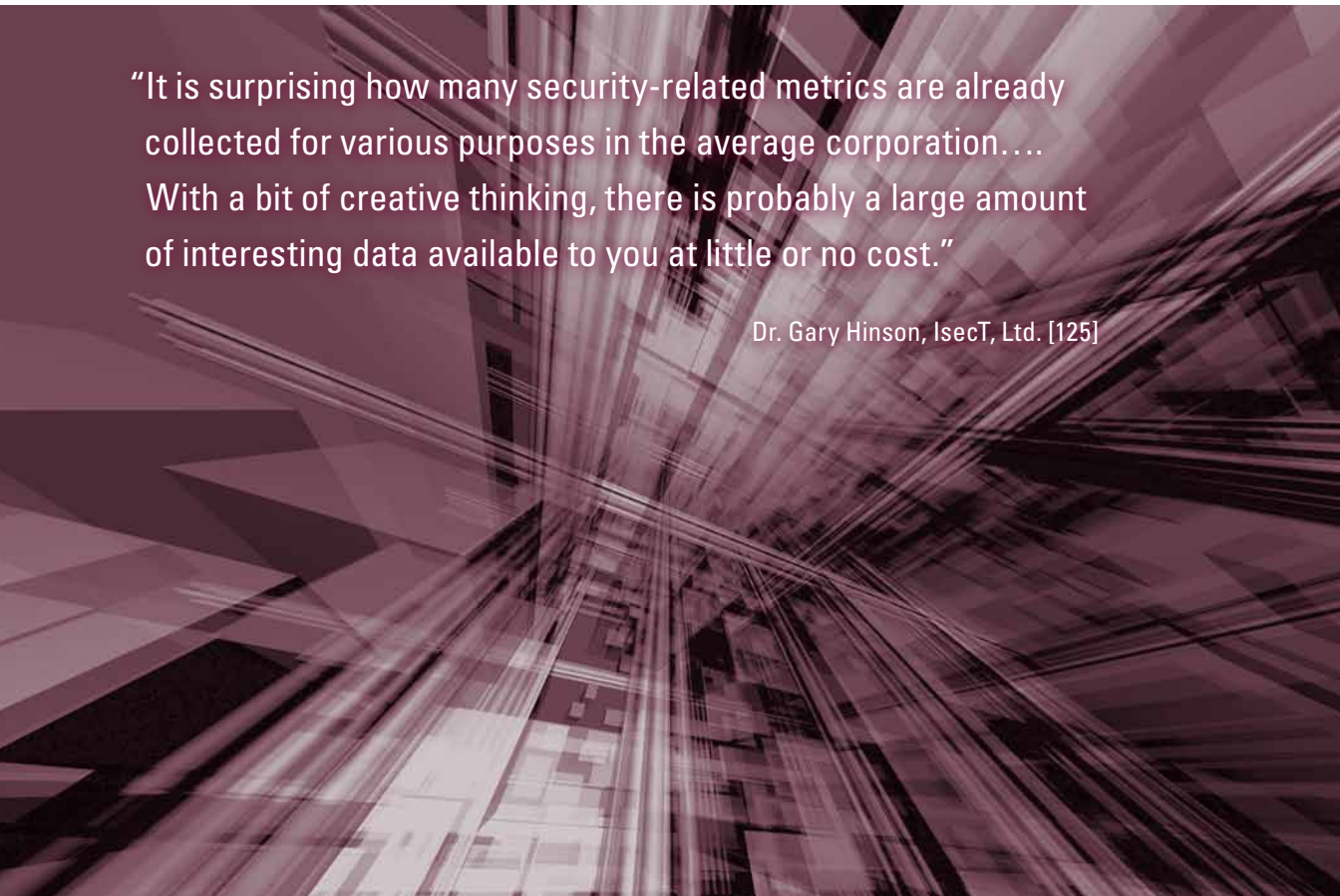
122 Described in: Khalid Kark and Paul Stamp. "Defining an Effective Security Metrics Program," 16 May 2007. Accessed 29 December 2008 at: *http://www.scribd.com/doc/2935458/best-practices-defining-an-effective-security-metrics-program*

123 Khalid Kark, Forrester Research. "Best Practices: Security Metrics," July 22, 2008. Accessed 8 February 2009 at: *http://www.forrester.com/Research/Document/Excerpt/0,7211,45787,00.html* (Executive summary; full access to articles available only to Forrester Research clients.)

124 Khalid Kark and Chris McClean, Forrester Research. "The Forrester Wave: Security Consulting, Q3 2007," 25 September 2007. Accessed 2 February 2009 at: *http://www.wipro.com/analyst_reports/pdf/Forrester_Security_Consulting_Wave_07.pdf* (Executive summary; full access to articles available only to Forrester Research clients.)

7

Measurable Data



"It is surprising how many security-related metrics are already collected for various purposes in the average corporation…. With a bit of creative thinking, there is probably a large amount of interesting data available to you at little or no cost."

Dr. Gary Hinson, IsecT, Ltd. [125]

Measurable data come in a variety of forms. In fact, CS/IA measures can be generated from any IA activity within an organization. When selecting data to support CS/IA measurement, organizations must ensure that the selected measures are meaningful and repeatable, and can be generated with reasonable effort. (For example, the amount of time it takes a penetration tester to break into a network may be a meaningful measure, but it may not be repeatable with different testers and the costs associated with it may be prohibitive.)

This section summarizes activities that collect and capture CS/IA measurement data that can be rolled up into measures as well as those activities that define data attributes that can be measured. [126] It also summarizes taxonomies of CS/IA measures that have emerged since 2000, and presents some representative research on quantifying the value of CS/IA.

7.1 Red/Blue Team Evaluations

Red and blue team evaluations simulate potential real-world scenarios. Skilled attackers (the red team) attempt to subvert a target system or network, while systems administrators and incident response specialists (the blue team) attempt to minimize the red team's effects on the system or network. These simulations can provide organizations with valuable information about their procedures and methodologies, in addition to identifying potential vulnerabilities within their systems and networks. In a well-prepared organization, effective IA procedures, methodologies, and personnel may be able to successfully mitigate the risks introduced by identified vulnerabilities with the organization's systems or networks.

However, because red and blue team evaluations are far more complex and interactive than traditional IA assessments, organizations may have difficulty defining and collecting meaningful measures based on these simulations. By developing, testing, and modifying methodologies

specifically for red and blue team evaluations, researchers aim to improve both the repeatability of these exercises as well as provide a better understanding of the types of measures that can be collected and used to gain insight into the status of CS/IA in organizations undergoing red/blue team evaluations.

The Information Design Assurance Red Team (IDART) at Sandia National Laboratories has developed a methodology for Information Operations Red Team and Assessments (IORTA) that includes a methodology for capturing data that can be quantified as a product of red team assessments. IDART's IORTA methodology captures the following data, listed in Table 7-1.

Table 7-1 Metrics Data Captured by IDART Red Team Activities

Source of Metric Data	Types of Metric Data Captured
Design Assurance Red Teaming	▶ Attack ▶ Adversary ▶ Protection ▶ Threat
Hypothesis Testing	▶ Attack ▶ Adversary
Red Team Benchmarking	▶ Vulnerability ▶ Consequence ▶ Adversary ▶ Protection ▶ Threat
Behavioral Red Teaming	▶ Consequence ▶ Adversary ▶ Threat
Red Team Gaming	▶ Attack ▶ Consequence ▶ Adversary ▶ Threat
Operational Red Teaming	▶ Attack ▶ Vulnerability ▶ Adversary ▶ Protection ▶ Threat
Penetration Testing	▶ Attack ▶ Vulnerability ▶ Protection
Analytical Red Teaming	▶ Consequence ▶ Adversary ▶ Protection ▶ Threat

The actual data/values captured during attack simulations, exercises, or actual incidents fall into the categories described in Table 7-2. [127]

Table 7-2 Categories of IDART Red Team Metrics

Types of Metrics	Purpose	Examples
Attack-based metrics	Describe capabilities and commitment required to undertake a successful attack	▶ Knowledge/skill required ▶ Time required ▶ Probability of detection (*i.e.,* Likelihood that defender will detect the attack)
Vulnerability-based metrics	Count or measure vulnerabilities or weaknesses discovered	▶ Boolean existence (*i.e.,* Is there a vulnerability?) ▶ Percentage of platforms with the vulnerability ▶ Reachability (*i.e.,* Can the attacker access the vulnerability?)
Consequence-based metrics	Describe or measure consequences of a successful attack	▶ Number of deaths ▶ Downtime ▶ Nightmare consequences
Adversary-based metrics	Describe the adversary model(s) used by the red team; the model may pertain to external ("outsider") or insider adversaries	▶ Knowledge or skill level ▶ Number of team members ▶ Tools or techniques
Protection-based metrics	Count or measure protection systems (existing or planned countermeasures)	▶ Percentage of systems protected ▶ Number of protections/layers of protections ▶ Number of incidents/compromises
Threat-based metrics	Describe the degree of threat as calculated from combinations of the other metrics	▶ Expected cost to repair damage ▶ Expected number of systems affected ▶ Mean time to restore services

As it specified the IORTA metrics, the IDART team considered other possible metrics, but rejected them as problematic for various reasons.

Among these other possible metrics was Red Team Work Factor, a metric researched at DARPA from 1999 to 2003, and rejected by IDART as being too unstable, difficult to reproduce, and inaccurate in capturing true adversary costs. Instead, the IDART team chose to use adversary-based metrics.

Other metrics considered and rejected by the IDART team included Information Warfare Intensity (another DARPA-researched metric, considered conceptually useful, but incomplete), and Value-Driven Measures (developed by the Air Force Institute of Technology).

The IDART team also developed an IORTA tool for producing attack graphs and capturing metrics, and a training course, "Red Team Metrics," that complements the IDART course "Red Teaming for Program Managers." [128]

7.2 Network Management and Security Measures

> ***"Evaluation of network security is an essential step in securing any network. This evaluation can help security professionals in making optimal decisions about how to design security countermeasures, to choose between alternative security architectures, and to systematically modify security configurations in order to improve security. However, the security of a network depends on a number of dynamically changing factors such as emergence of new vulnerabilities and threats, policy structure and network traffic. Identifying, quantifying and validating these factors using security metrics is a major challenge in this area. In this paper, we propose a novel security metric framework that identifies and quantifies objectively the most significant security risk factors, which include existing vulnerabilities, historical trend of vulnerability of the remotely accessible services, prediction of potential vulnerabilities for any general network service and their estimated severity and finally policy resistance to attack propagation within the network. We then describe our rigorous validation experiments using real-life vulnerability data of the past 6 years from National Vulnerability Database (NVD) to show the high accuracy and confidence of the proposed metrics. Some previous works have considered vulnerabilities using code analysis. However, as far as we know, this is the first work to study and analyze these metrics for network security evaluation using publicly available vulnerability information and security policy configuration." [129]***

Data from network security devices, like Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS), can be used as primary sources for CS/IA measures. For example, IDS data can be used to populate measures on incoming and outgoing network traffic. As IPSs are designed to block or prevent malicious or unwanted behavior in real-time, their use can facilitate the ability for real-time measures calculation. Criteria for selection of IDSs can be found in "A Metrics-Based Approach to Intrusion Detection System Evaluation for Distributed Real-Time Systems." [130]

SecurityMetrics, Inc. [131] has IDSs, IPSs, and Vulnerability Assessment appliances that quantify the following—

- Attack recognition,
- Attack prevention,
- Real-time attack notification,
- Recent attacks,
- Recent attackers,
- Recent attacked IPs,
- Rank of attack types,
- Information leakage,
- Open shares,
- Password problems.

Users of these appliances can have their own secure results Web pages to review their network checks.

Aladdin's Attack Intelligence Research Center [132] contains over 20 additional network security statistics, including those that can be used to design, monitor, and quantify network security. Through Aladdin's Research Center, several key findings based on the have been calculated as follows—

- 55% of online users have been infected with spyware.
- For 52% of networks, the perimeter is the only defense.
- There are 651 million email users globally.

7.3 Software Testing Output

Many COTS tools provide users with a *score,* indicating the security of the underlying system. In most cases, these scores are loosely generated by aggregating the weighted severity of the vulnerabilities discovered by the tool.

While these scores are not necessarily generated against a published methodology—nor can they truly be compared across multiple COTS tools—these scores can be used as an initial step or, more likely, an input into an organization's overall CS/IA measurement methodology.

In addition, organizations can develop CS/IA measures based on the results of their own software testing and analysis. These techniques can provide reproducible and comparable measures that can be used to quantify and monitor the organization's security posture over time.

The types of software testing measures available are listed and described in Table 7-3.

Table 7-3 Software Testing Measures

Category	Focus/Key Data Source	Examples
Severity-based	Vulnerability severity or quantity	▶ NIST risk matrix: Finding of high-severity vulnerability produces high vulnerability rating ▶ Number of high-severity vulnerabilities: Commonly used in certification and accreditation programs wherein presence of one or more high severity vulnerabilities prevents the system from being certified
Mitigation-based	Amount of time or effort involved in mitigating the vulnerability	▶ Amount of time it takes for defects within an organization to be mitigated after the vulnerability is identified ▶ Comparison of "time to patch" averages for proprietary commercial software *vs.* open source software
Category-based	Trending of vulnerability types identified in an organization's systems: useful for identifying aspects of an organization or system that may be the primary cause of many of the vulnerabilities of a given type. Resources deployed to mitigate the systemic risk indicated by the measure would likely greatly improve the organization's security posture.	▶ Number of cross-site scripting vulnerabilities within an organization's Web applications—a high number indicating the systemic inadequacy or lack of input and/or output validation by the applications

Organizations have been using these types of measures for assessing the *quality* of software for a number of years. In fact, modern development methodologies (*e.g.,* agile methods and extreme programming) focus exclusively on testing results to determine the progress and quality of software being developed. The majority of testing involved in these development processes is unit testing, which focuses exclusively on ensuring that the functionality of a specific component meets the defined requirements. However, organizations taking advantage of these development methodologies can easily include software security-related testing, resulting in security measures that can be based on and calculated using the same methodologies used to determine the quality and completeness of the software.

For Further Reading

Satish Chandra and R.A. Khan. "Software security metric identification framework (SSM)," in *Proceedings of the ACM International Conference on Advances in Computing, Communication and Control (ICAC3 '09),* Mumbai, India, 23–24 January 2009, pp. 725–731. Digital Object Identifier: *http://doi.acm.org/10.1145/1523103.1523250*

7.4 Scoring Schemes

Significant advances have been made in creating units for counting CS/IA-related items to begin developing means for uniform measurement and comparison of CS/IA across applications, platforms, and organizations. This section describes the development of scoring systems that have allowed for these advances. The scoring and ranking systems described in this section are all intended to apply quantitative or qualitative rankings of priority, severity, or impact to reported vulnerabilities. The sources of the vulnerability data are also indicated in the descriptions of these different scoring systems.

7.4.1 CVSS

The CVSS is a free, open standard maintained by the Forum of Incident Response and Security Teams (FIRST), and defined by the CVSS Special Interest Group (SIG). The latest version, CVSS Version 2, was published jointly by FIRST and the CVSS SIG in Summer 2007.

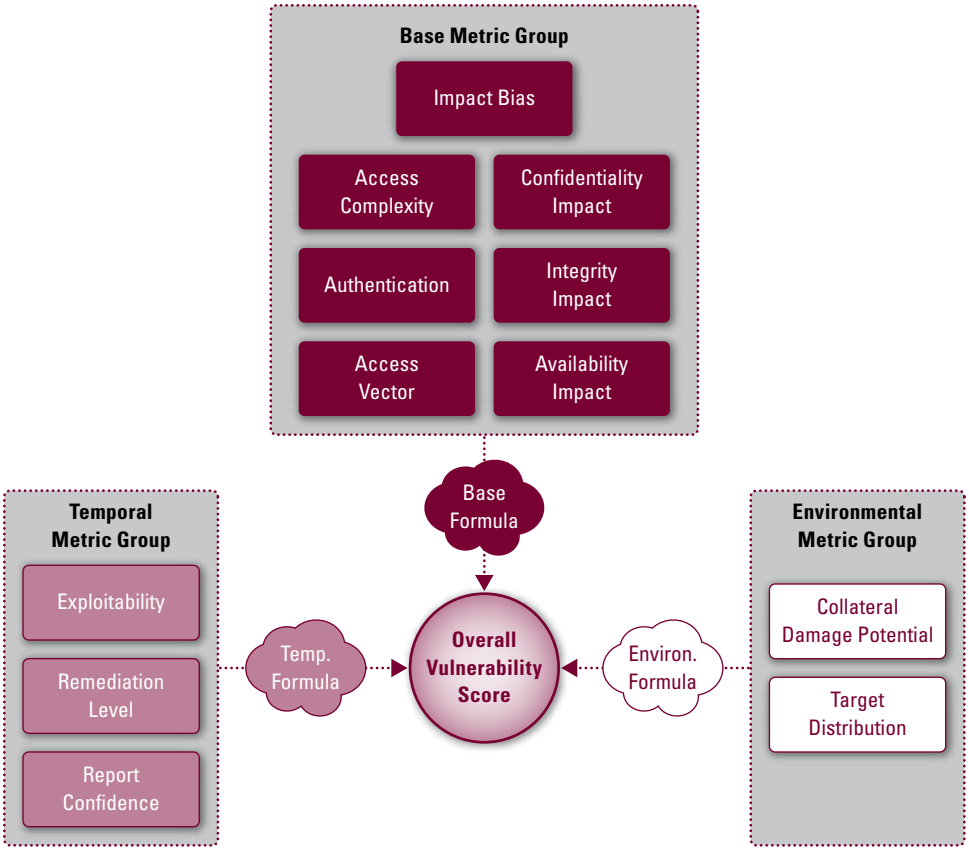
In essence, the CVSS is a scoring system for vulnerabilities, specifically those vulnerabilities described by the CVE, [133] a dictionary of publicly known information security vulnerabilities and exposures. In this system, each vulnerability is assigned a CVE Identifier comprising—

- A unique CVE number (*e.g.*, "CVE-1999-0067");
- An indication of the status of the CVE entry ("entry," meaning it has been approved for inclusion in the dictionary, or "candidate," meaning its inclusion is still under consideration pending technical analysis);
- A brief description of the security vulnerability or exposure;
- Any pertinent references (*i.e.*, vulnerability reports and advisories or Open Vulnerability and Assessment Language Identifier [OVAL-ID]). [134]

A CVSS score represents an overall composite of the severity and risk associated with a given vulnerability. The score is derived by performing certain calculations (based on defined equations) of values in three different categories or groups.

The CVSS "framework" consists of the three metric groups of which the CVSS is composed, and their component metrics. [135] This framework is depicted in Figure 7-1.

Figure 7-1 CVSS Framework [136]



The three CVSS metric groups are—

1. *Base metrics:* Express those innate fundamental characteristics of a vulnerability that remain constant over time and across user environments. Base metrics are the most widely used of the three CVSS metrics groups. Those who use only base metrics to the exclusion of temporal and environmental metrics generally do so because they wish to avoid the additional effort and uncertainty involved in defining metrics specific to their own systems; they feel that base metrics, by contrast, are unchanging and thus easier to use and/or more reliable. Within the base metrics group, seven metrics (described in Table 7-4) represent the most fundamental characteristics of a vulnerability.
2. *Temporal metrics:* Express those characteristics of a vulnerability that change over time, but which remain constant across user environments. Within the temporal metrics group, three metrics (described in Table 7-4) represent the time-dependent characteristics of the vulnerability.

3. *Environmental metrics:* Express the characteristics of a vulnerability that are specifically relevant and unique to how that vulnerability manifests in a particular environment. Within the environmental metrics group, two metrics (described in Table 7-4) represent implementation- and environment-specific characteristics of the vulnerability.

The metrics within each of the three metric groups and their possible values are described in Table 7-4.

Table 7-4 CVSS Metrics by Metric Group

Metric Group	Metrics	Description	Possible Values
Base Metrics	Access vector	Indicates how the vulnerability can be reached by an attacker, *i.e.,* through remote (distant or nearby) or local access	▶ Local ▶ Adjacent ▶ Network
	Access complexity	Measures how complex an attack would have to be to exploit the vulnerability once that attacker gained access to the target	▶ High ▶ Low
	Authentication	Indicates whether or not authentication of the attacker by the target is required before he/she can access the vulnerability	▶ Required ▶ Not required
	Confidentiality impact	Indicates whether a successful exploit of the vulnerability will have any impact on the confidentiality property of the target, and if so how much impact	▶ None ▶ Partial ▶ Complete
	Integrity impact	Indicates whether a successful exploit of the vulnerability will have any impact on the integrity property of the target, and if so how much impact	▶ None ▶ Partial ▶ Complete
	Availability impact	Indicates whether a successful exploit of the vulnerability will have any impact on the availability property of the target, and if so how much impact	▶ None ▶ Partial ▶ Complete
	Impact bias	Indicates whether any of the three impact metrics is of greater importance (*i.e.,* needs to be assigned a greater weight) than the other two	▶ Normal (all three impacts are of equal importance) ▶ Confidentiality ▶ Integrity ▶ Availability

Metric Group	Metrics	Description	Possible Values
Temporal Metrics	Exploitability	Indicates the complexity of the process required to exploit the vulnerability in the target	▶ Unproven ▶ Proof of concept ▶ Functional ▶ High
	Remediation level	Indicates the level of an available countermeasure to the vulnerability	▶ Official fix ▶ Temporary fix ▶ Workaround ▶ Unavailable
	Report confidence	Indicates the degree of confidence that the vulnerability exists/the credibility in the report of that vulnerability	▶ Unconfirmed ▶ Uncorroborated ▶ Confirmed
Environmental Metrics	Collateral damage potential	Indicates the potential/likelihood that an exploitation of the vulnerability could result in loss of physical equipment, damage to property, loss of human life, or major physical injury to human	▶ None ▶ Low ▶ Medium ▶ High
	Target distribution	Indicates the relative size (quantity, dispersion) of the field of targets susceptible to the vulnerability	▶ None ▶ Low ▶ Medium ▶ High

Each of the non-numeric values is assigned a numeric value, which is then used in the calculation of the score for the vulnerability. The base metric values are combined to calculate the *base score* of 0 to 10. Once calculated, the base score for a given vulnerability is not expected to change. The base score is further refined by combining that score with the values assigned the vulnerability's temporal and environmental metrics, and calculating the *temporal score* and *environmental score* respectively (each also a number from 0 to 10).

In addition to the base score, CVSS includes temporal and environmental scoring vectors. A scoring vector is a text string that contains the values assigned to the base metrics that are calculated to produce the base score. In this way, the scoring vector clarifies the meaning of the base metrics by making it clear how those metrics were ranked before being combined to produce that score. Designers of the CVSS intend for the scoring vector to always be displayed with the base score.

According to its developers, the CVSS has advantages over other scoring systems in that it is an open standard, and it ranks vulnerabilities in a consistent fashion, while also allowing for customization to express metrics for specific user environments.

Several organizations have made online and offline calculators available to assist in the calculation of CVSS scores. Examples of such calculators are available at the following Web sites—

- NIST CVSS Version 2 Calculator. Accessed 27 March 2009 at: http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2

- Information-Technology Promotion Agency of Japan, CVSS 2.0 Calculator. Accessed 27 March 2009 at: http://jvnrss.ise.chuo-u.ac.jp/jtg/cvss/en/index.02.html
- ERNW CVSS Calculator. Accessed 27 March 2009 at: http://www.ernw.de/content/e6/e180/e1043/ernw-cvsscalc_ger.zip

7.4.2 Chris Wysopal's CWE System Scoring

Recognizing that the CVSS was not directly applicable to software applications and systems, Chris Wysopal, Chief Technology Officer of source code analysis tool company Veracode, devised a CWE scoring system, [137] whereby he assigned CVSS-type equations to scoring of metrics for the weaknesses enumerated in the CWE. The intent of his scoring system was to provide a means of scoring weaknesses discovered by software security analysis techniques (automated static, automated dynamic, manual code review).

Wysopal felt that the CVSS environmental score could be used unchanged, but that the process for generating the base score and temporal score were too complex. He specifically proposed the following simplified, four-step calculation process to produce Weakness Base Scores and Weakness Likelihood Scores for CWE entries—

1. At the class level, assign the CVSS values for impact metrics to the CWE entry's "Common Consequences." These values are: Confidentiality, Integrity, and Availability. The resulting computation will be a numerical impact metric for the entry.
2. At the code context level, use the CVSS values for Access Vector, Access Complexity, and Authentication to calculate the CWE entry's exploitability metric.
3. Combine the new Impact and Exploitability metrics to calculate the CWE entry's Weakness Base Score.
4. Calculate a Weakness Likelihood Score for the CWE entry by applying the CVSS temporal score equation to the CWE entry. The resulting Weakness Likelihood Score will express the perceived potential that "bad things will come" from a given weakness.

A critic of Wysopal's CWE Scoring System observes that the "CVSS was created to score vulnerabilities, not weaknesses. In the end, these two things exist at differing levels of abstraction and require scoring systems of differing complexity and levels of abstraction." This critic goes on to state that "there is still a need for a true Common Weakness Scoring System."

7.4.3 CCSS

Under development by NIST, the CCSS [138] defines a set of measures for security configuration issues, and a formula to combine those measures into scores for each issue. The CCSS is derived from the CVSS, but adjusts the basic components of the CVSS to focus on security configuration issues, rather than

software flaws. The CCSS uses six of the seven base metrics from the CVSS—Access Vector, Access Complexity, Authentication, Confidentiality Impact, Integrity Impact, and Availability Impact (Impact Bias is not used)—to compute the CCSS base score. Like the CVSS scores of CVE vulnerabilities, CCSS scores are intended to indicate how readily CCE weaknesses and vulnerabilities can be exploited, and how such exploitations may affect the targets.

At present, the CCSS addresses only base metrics; NIST plans to expand the scoring system to include support for environmental metrics as well. Nothing has been said by NIST of plans to add support for temporal metrics.

7.4.4 CMSS

Under development by NIST, the CMSS [139] defines a set of measures for software feature *misuse* vulnerabilities (in contrast to software implementation vulnerabilities), along with a formula to combine those measures into scores for each issue.

Like CCSS, the CMSS is derived from the CVSS to complement its sister scoring systems. The CMSS adjusts the components of the CVSS to focus on software misuse vulnerabilities, rather than on software flaws or configuration issues.

The CMSS uses the same six core measures as both the CVSS and CCSS (*i.e.,* Access Vector, Access Complexity, Authentication, Confidentiality Impact, Integrity Impact, Availability Impact) to compute the base score.

As noted in the draft specification, the CMSS does not have a misuse dictionary available to it, whereas the CVSS and CCSS rely on the CVE and CCE, respectively. However, developing a CMSS score does not require a misuse dictionary. An organization can successfully deploy the CMSS against its own internal misuse dictionary.

CMSS scores are intended to indicate how readily software misuse weaknesses and vulnerabilities can be exploited, and how such exploitations may affect the target system. The CMSS does not yet address temporal or environmental metrics in its current draft, but these will be developed in the future.

7.4.5 CWSS

CWE users quickly determined that the CVSS does not work well for scoring weaknesses enumerated in the CWE, and initiated development of the CWSS [140] to address this deficiency. This deficiency is mainly because the amount and depth of information available is different for weaknesses in the CWE than it is for vulnerabilities in the CVE.

The CVSS is linked to known vulnerabilities, *i.e.,* those reported and captured in the CVE. By contrast, the CWE includes both general (potential) and specific (discovered) weaknesses—

- General weaknesses are weaknesses, such as those enumerated in the CWE/ SysAdmin, Audit, Network, Security (SANS) Top 25 Most Dangerous Programming Errors, to which most or all software is prone.
- Specific weaknesses are those discovered in specific software products but which have yet to be exploited as vulnerabilities (and thus they remain weaknesses in CWE rather than being added to CVE as reported vulnerabilities).

In many cases, there is little or no knowledge of how specific weaknesses were discovered (*e.g.,* by automated scanning or manual code review, or in what environment/under what conditions).

Recognizing this disconnect between the CVSS and CWE, an effort has been undertaken to define a CWSS comparable to, but distinct from, the CVSS. The effort began with the development of a mapping of the CWE to the SANS Top 25, in hopes that this mapping would clarify the best approach for developing a CWSS. The SANS Top 25 was used as the basis for determining weakness prevalence and severity.

The developers of the CWSS are also considering ways in which to link the weakness scores more closely to business/mission context; they feel this context is only partly addressed by the CVSS environment score (which is not widely used).

Development of the CWSS is in early days yet, and there is little information available as to what it will involve. This said, there is a Web page devoted to the CWSS in the CWE section of The MITRE Corporation's "Making Security Measurable" Web portal. [141] Progress on CWSS definition is expected to be reported there. The Web page can be found at: http://cwe.mitre.org/cwss/index.html (accessed 13 March 2009).

7.4.6 Software Vendor Vulnerability Severity Ratings

Many software vendors have instituted their own rating systems for the vulnerabilities they discover and report—

- Microsoft uses a Security Bulletin Severity Rating System of four ratings ("Critical," "Important," "Moderate," "Low").
- Oracle uses CVEs to characterize all vulnerabilities in its Security Alerts, and provides the CVSS base score for each vulnerability (thereby, leveraging the CVE and CVSS as their designers intended).
- McAfee reports the Microsoft Security Bulletin number and severity rating, although the CVE (if there is one) is also identified.

7.4.7 Vulnerability Reporting/Advisory Service Ratings

There are a number of commercial organizations, including security services/consulting firms, vulnerability scanner vendors, and penetration test service providers, that issue reports or advisories about vulnerabilities discovered by their own analysts and/or reported to them by their customers.

These organizations all apply some methodology for rating the vulnerabilities they report by severity, with severity in some cases indicating likelihood or ease of exploitation and, in other cases, importance of applying a patch.

Some of these rating systems are numeric; more often, they are qualitative (*e.g.*, "high risk," "low risk"). Some organizations use a color-coded graphical scale instead of, or in addition to, a numeric or qualitative rating; the colors are most often based on red-yellow-green traffic signals (red = major, yellow = moderate, green = minor). Secunia, for example, assigns both qualitative ("critical," "moderately critical," *etc.*) and color-scale indicators to its vulnerability severity ratings.

While many of these organizations also identify the CVEs for the vulnerabilities they report, few, if any, appear to use the CVSS as the basis for their various rating systems.

7.4.8 Attack and Threat Scoring Systems

As with vulnerability scoring systems, these scoring systems attempt to apply quantitative or qualitative rankings of likelihood, severity, impact, or priority to various threats or attack types. The sources of the threats/attack types thus scored are indicated in the descriptions of these different scoring systems.

For example, DShield.org, a volunteer effort supported by the SANS Institute, was officially launched in November 2000. Since then, it has developed into an Internet attack correlation engine with worldwide coverage. DShield.org uses an Internet Threat Level scoring system in which "ThreatCon" levels of red, yellow, and green (traffic signal colors) are assigned to different attacks to indicate their relative severity.

Cisco Systems uses a metric it calls an Attack Relevance Rating (ARR). The ARR quantifies attacks detected by its IPS. The ARR is then used as a data point to calculate an overall Risk Rating for each intrusion to be dealt with by the Cisco Security Manager, of which the IPS is a component.

MyNetWatchman.com is a service for monitoring Internet activity on behalf of Internet Service Providers (ISPs) that subscribe to the MyNetWatchman service. Each day, MyNetWatchman automatically collects and aggregates firewall logs from a very large number of ISP computers, analyzes these logs for evidence of hacker or worm attacks, and notifies the ISPs of the originations of the attacks are coming from. The two measures generated by the MyNetWatchman service are—

- **Ports Rising in Attack Rates**—Indicates ports on which the number of detected attacks has increased since the previous day's collection and aggregation.
- **Ports Being Attacked Most**—Indicates the absolute metric of number of attacks by Internet port type.

7.5 Vulnerability Assessment and Management

Vulnerability assessments are a longstanding aspect of IA. In fact, many organizations already have some form of vulnerability assessment process in place, ranging from identifying the patches that need to be applied to systems, to performing active vulnerability scans on a regular basis. To this end, vulnerability assessment results can form an important aspect of a CS/IA measurement program.

This section identifies two popular CS/IA measurement approaches employed by DoD and US-CERT that organizations may leverage—either as a whole or as a basis for their own customized CS/IA measures.

7.5.1 IAVA Statistics

DoD publishes and maintains the IAVA database, which aggregates the vulnerability reporting performed by various external organizations (*e.g.*, Bugtraq bulletins, Microsoft bulletins, US-CERT announcements). Because IAVAs require acknowledgement and compliance on the part of IAVA bulletin recipients, DoD can maintain measures on the number of systems that are in compliance with the latest IAVA bulletin.

The Vulnerability Compliance Tracking System provides information on all DISA IT assets that are affected by IAVAs. DISA can generate measures on the current security posture of its IT systems by measuring their compliance status, which can be one of seven states, [142] as shown in Table 7-5.

Table 7-5 DISA Vulnerability Compliance Tracking System Measures

State	Definition
Open	An asset is currently affected by an alert, but mitigations have not been applied
Not Applicable	An asset has been determined to not be affected by the alert
Fixed/In Compliance	The accepted mitigation strategy has been applied
Extension Requested	An extension beyond the 30-day compliance deadline has been filed
Extension Approved	An asset is currently affected by an alert, but the deadline for mitigation has been extended
Extension Denied	An extension has been denied and the mitigation strategy must be implemented immediately
Extension Expired	An extension has expired and the asset is still affected by the alert

By assessing the number of systems in each possible state, DoD can determine how efficiently it is handling a specific alert. In aggregate, DoD can determine how long IAVAs take, on average, to be addressed within the organization, which helps gauge the level of risk posed by open vulnerabilities. Similarly, this information can be used to identify specific "problem systems" that may lag behind the rest of the network in complying with IAVAs.

7.5.2 US-CERT Vulnerability Note

US-CERT maintains what it calls its Vulnerability Notes Database, which is comparable to the NIST National Vulnerability Database and the CVE database.

Each entry in the Vulnerability Notes Database is called a Vulnerability Note. Vulnerability Notes "generally describe vulnerabilities independent of a particular vendor," and include a number of data fields describing the vulnerability [143] and providing information about it. One of these data fields is "Metric," which forms the basis for rating the vulnerability according to its severity.

Similar in intent to a CVSS score, the Metric is, in fact, determined based on a different set of component metrics, which are quantified answers to questions about the vulnerability. The component metrics used to compute the Vulnerability Note Metric include the following—

- Is information about the vulnerability widely available or known?
- Is the vulnerability being exploited?
- Is the Internet Infrastructure at risk because of this vulnerability?
- How many systems on the Internet are at risk from this vulnerability?
- What is the impact of exploiting the vulnerability?
- How easy is it to exploit the vulnerability?
- What are the preconditions required to exploit the vulnerability?

The answer to each question is assigned an approximate numeric value; the value is approximate in recognition of the fact that different sites may assign different values, based on differences in their environment and their perceptions of the vulnerability given that environment. The component metrics are then calculated together to produce an overall numeric metric score for the vulnerability; this is a number from 0-180, with 180 representing the highest possible severity. Vulnerabilities with a metric score of 40 or greater merit issuance of US-CERT Technical Alerts (TA).

Because the component metrics are not all given equal weight (priority), US-CERT warns that composite vulnerability scores should not be considered linear; that is, a vulnerability with a score of 40 should not be considered twice as severe as one with a score of 20.

7.6 Risk Management and Compliance Outputs

"The most significant challenge is validating results from the risk management process. Demonstrating due diligence is key. However, the inadequacy of traditional risk management methodologies make this essentially impossible. Thus, security metrics (in various forms) have become the emerging methodology to assess and demonstrate compliance with industry standard security practices and procedures. The HIPAA Security regulations, ISO 17799, and other similar standards are useful taxonomies to organize a security program;

> *however, these standards do not provide a basis to quantify particular security activities and their results within [an] organization." [144]*

> *"…We need to adopt a risk-based approach in both our operations and our philosophy. Risk management is fundamental to managing the threat, while retaining our quality of life and living in freedom. Risk management must guide our decision-making as we examine how we can best organize to prevent, respond and recover from an attack." [145]*

DHS has developed a range of risk assessment tools for different types of assets, systems, or sectors (*e.g.*, the Maritime Security Risk Analysis Model [MSRAM]). Data from these tool-driven assessments are intended to be used by government and critical infrastructure sector organizations to populate IA risk and compliance metrics, and to show performance improvements.

7.6.1 CNDSP C&A

In early 2001, DoD Directive (DoDD) O-8530.1, "Computer Network Defense (CND)," 8 January 2001, designated a new term Computer Network Defense Services Provider (CNDSP). Implementation of the Directive within DoD began in 2003. This term is used to describe the providers of CND and incident response services in DoD that incorporate services similar to those provided by CERTs and Computer Security Incident Response Teams (CSIRT). Along with this new directive, DoD also published a supporting manual, DoD Manual O-8530.1-M, "Information Assurance Workforce Improvement Program," 19 December 2005, defining a measurement-driven C&A process for evaluating the performance of DoD CNDSPs.

Unlike traditional C&A, which calculates the security risk for a given system and certifies that the security controls in place for that system adequately mitigate that risk, the C&A of a CNDSP assesses the degree to which that provider assures a minimum standard of service to its DoD subscribers.

All general services CNDSPs are held to the same standard of minimum acceptable level of service and assessed using the same set of criteria. These criteria are captured in over 100 metrics that are used to measure the adequacy of the services the CNDSPs provide in four main categories, or "goal areas"—

- **Protect**—Includes vulnerability analysis and assessment, CND red teaming, virus protection, subscriber protection and training, information operations condition implementation, and IA vulnerability management;
- **Monitor, Analyze, and Detect**—Includes network security monitoring and intrusion detection, attack sensing and warning, and indications and warnings and situational awareness;
- **Respond**—Includes incident reporting, response, and analysis;

- **Sustain Capability**—Includes memoranda of understanding and contracts, CND policies and procedures, CND technology development, evaluation, and implementation, personnel levels and training/certification, security administration, and the primary information systems that support the CNDSP.

The metrics used to measure the adequacy of CNDSP services are based on IA best practices, self-assessment tools, and DoD requirements. Some examples of metrics used in the CNDSP assessment include verifying the establishment of policy and procedures for, and the performance of intrusion detection, vulnerability scanning, *etc.*, on subscriber networks.

Since the establishment by DARPA in 1988 of the Computer Emergency Response Team/Coordination Center (CERT/CC) at CMU's Software Engineering Institute, CERT/CC and DoD have worked closely together. CERT/CC that was used as the model for DoD's definition of the CNDSP and many CERT/CC practices have been included in the CNDSP C&A methodology.

The CERT/CC defined a system for prioritizing CNDSP C&A according to the criticality of the services being measured—

1. **Priority I metrics**—Those used to measure adequacy of services critical to an incident management capability.
2. **Priority II metrics**—Those used to measure the adequacy of the next most important services. These metrics address traditional operational concerns.
3. **Priority III and Priority IV metrics**—Those used to measure best practices that support operational effectiveness and quality.

The CERT/CC then applies a scoring system to rate how well the CNDSP is doing with regard to each metric—

- **Not applicable**—The metric does not apply to the organization, so was excluded from the total "score";
- **Not observed**—The metric was not observed during the assessment;
- **Yes**—The metric was met;
- **Partial**—The metric was partially met;
- **No**—The metric was not met.

The assessor's job, then, is to analyze data collected during the CNDSP's initial self-assessment (which precedes the C&A inspection by DISA) and during the C&A inspection to determine—

- Has the CNDSP met the required indicators for each metric?
- Has the metric been satisfied?
- What is the quality of performance for the metric (if this can be determined)?

According to the CERT/CC, the measurement results are intended to (1) enable the calculation of a risk exposure based on the number and prioritization of unmet and partially-met metrics; (2) drive an improvement plan to be undertaken by the CNDSP, with metrics' priorities driving the prioritization of remediations for the unmet and partially-met metrics.

Since the CNDSP C&A program began in 2003, all DoD CNDSP are required to undergo C&A inspection by DISA certifiers every three years; based on their findings during the inspection, the certifiers recommend a certification level to US Strategic Command, which is responsible for making the final accreditation determination. [146]

In 2005, DHS's US-CERT announced its intention to establish a federal CNDSP program, modeled closely on the DoD program, and to include a measurement-based CNDSP performance assessment process using "federalized" metrics adapted from those in DoDD O-8530.1.

For Further Reading

Buzz Walsh and Ralph Ghent. "The Road Ahead for Computer Network Defense Service Providers," in *IAnewsletter,* Volume 6 Number 3, Winter 2003/2004, pp. 6-11. Accessed 11 May 2009 at: *http://iac.dtic.mil/iatac/download/Vol6_No3.pdf*

Audrey Dorofee, Chris Alberts, and Robin Ruefle Carnegie Mellon University CERT/CC. "Evaluating CSIRT Operations," presented at the 18th Annual FIRST Conference, Baltimore, Maryland, 25-30 June 2006. Accessed 11 May 2009 at: *http://www.first.org/conference/2006/program/presentations.html#p210*

7.6.2 NIST FDCC Compliance Metrics Initiative

Initiated by OMB, the Federal Desktop Common Configuration (FDCC) attempts to define a single configuration for all federal government desktop and laptop computers that run some version of Microsoft Windows. By standardizing on a single enterprise-wide configuration, the FDCC is intended to reduce the costs associated with support and application compatibility while also improving security. [147]

The FDCC Compliance Metrics Initiative was undertaken by NIST to provide the guidance and tools needed to support the effective implementation and verification of the FDCC. Publicly accessible FDCC Compliance Metrics resources, including Frequently Asked Questions (FAQ) and an FDCC checklist, are maintained as part of the NIST SCAP program. [148]

Through the FDCC Web site, organizations can identify SCAP-validated tools. [149] Many of these tools are capable of scanning personal computers against FDCC machine-readable checklists. NIST describes an FDCC scanner as "a product with the ability to audit and assess a target system in order to determine its compliance with the FDCC requirements. By default, any product validated as an FDCC Scanner is automatically awarded the

Authenticated Configuration Scanner validation." [150] Using these tools, organizations can automate the process of verifying whether systems meet the organization's configuration requirements.

7.6.3 C&A Risk Measures

Security C&A is a common priority for any IA program. The activity of performing Security Test & Evaluation (ST&E) on systems and program components as part of C&A drives the ability to document the status of security controls, discovered weaknesses, and, ultimately, the Authority to Operate (ATO). Data collected from the process can and is frequently used to calculate CS/IA measures.

The annual FISMA report documents the roll-up of the number and percentage of federal systems that have a C&A. C&A measures can also be found at more detailed levels during the fourth phase of C&A, Enterprise Continuous Monitoring. [151] Examples of these metrics include number and percentage of—

- Systems tested;
- Test results reviewed;
- Scheduled milestones for the relevant FISMA reporting cycle completed on time;
- Security Project Management Officers (SPMO) and system test teams offered training;
- Systems that use mandated methods and formats for testing and reporting;
- Controls selected and tested that are applicable and appropriate;
- Controls that are tested as "In Place";
- Controls that are tested as "Risk Based Decision" or "Not Applicable";
- Systems that have the appropriate level of justification and evidence;
- Program units that enter all appropriate information into the FISMA repository by FISMA reporting deadlines.

Another example of these C&A measures can be found in the Defense Logistics Agency (DLA) document, *How to Perform Information Systems Security C&A within the Defense Logistics Agency (DLA) using Metrics and Controls for Defense-in-Depth (McDiD)*. [152] Metrics for the McDiD approach are based on an assessment or rating that serves as an indicator of compliance with the control. Testing of individual controls is generally defined using the four readiness "C-Levels" with progress toward full compliance with each control noted as follows—

- **C1**—The security control has been fully implemented and the security profile achieved by the control is being actively maintained. Full compliance indicates that only minor IA deficiencies with a negligible impact on mission capabilities may be expected.

- **C2**—The IT organization is in the process of deploying or implementing the security control. This level of compliance indicates that some IA deficiencies with a limited impact on mission capabilities may be expected.
- **C3**—The IT organization is aware of the control and is in a planning phase for compliance. This level of compliance indicates that significant IA deficiencies preventing the performance of some portions of required missions may be expected.
- **C4**—No awareness of the control or progress toward compliance is evident. This level of compliance indicates that major IA deficiencies that preclude satisfactory mission accomplishment may be expected.

7.6.4 Risk Measures from Event-Driven Security Products

Vendors of IDSs, IPSs, data leakage detection systems, anomaly detection systems, firewalls, and other event-driven security products often collect and generate CS/IA measures pertaining to—

- **The findings of their systems**—*e.g.*, quantification and severity rankings of detected security incidents or violations;
- **Potential response(s) to those findings**—Including level of risk associated with various automatic and administrator responses, such as automatic blocking of anomalous traffic, or administrator shutdown of firewall monitoring of certain Internet ports/protocols/IP addresses.

Cisco's Security Manager, for example, generates measures indicating the level of risk (ranked from 1 to 100) associated with the configuration setting of each of the system's Event Action Filters. This risk rating is informed, to a degree, by the attack relevance rating or threat rating that Cisco uses to quantify the significance of various attacks to a particular event action filter. Security Manager also generates measures for the perceived value of the target being protected/monitored; in this case, system rankings are qualitative rather than quantitative (*i.e.*, "low," "medium," "high," "mission critical"). In most cases, these measures are intended to assist the administrator in decision-making when configuring the product or responding to its output.

7.7 Measures Categorization and Taxonomy Efforts

"The arguments over metrics are overstated, but to the extent they are contentious, it is because 'metrics' means different things to different people. For some people, who take a risk-centric view of security, metrics are about estimating risk based on a model…For those with an IT operations background, metrics are what you get when you

> ***measure ongoing activities…And there is a third camp that feels metrics should be all about financial measures…" [153]***

Along with the numerous efforts to define CS/IA measures of various sorts, there have been a number of efforts to categorize or, more formally, taxonomize, the various types of CS/IA measures that can be collected.

Several attempts have been made to define taxonomies of CS/IA measures categories. Some of these taxonomies are extremely simple, while others are extensive and "deep" in terms of levels of hierarchy. What all these taxonomies share is a categorization that accommodates both technical and non-technical measures.

A few of these taxonomies are said by their creators to have been derived from, based upon, or inspired by the implied taxonomy is CS/IA measures proposed at the 2001 WISSSR Workshop.

7.7.1 WISSSR Structure

Participants in the WISSSR Workshop elected to structure their discussion around certain aspects of information security. As a result, this subject matter fell into a categorization that has been interpreted by some of the WISSSR attendees, and others who later read about the outcomes of the workshop, as an implied taxonomy for CS/IA measures—an implied taxonomy that has, in fact, formed the basis for some of the taxonomies described below. The subject matter addressed in the WISSSR Workshop fell into two main categories, as shown in Table 7-6.

Table 7-6 WISSSR Measures

Group	Measures	Description	Additional Information
Organizational Security	IA Program Developmental	Measures the extent to which an organization has effectively implemented IA policies and processes	▶ Policy Management ▶ Process Maturity
	Support	Measures the organization's support for security programs and processes	▶ Personnel ▶ Resource Support
	Operational	Measures the organization's operational readiness and effectiveness in providing IA	▶ Management and Technical Readiness ▶ Operational Practice ▶ Operational Environment
	Effectiveness	Measure how effective the organization's IA program is in actually providing "defense-in-depth assurance"	▶ N/A

Group	Measures	Description	Additional Information
Technical Target of Assessment (TTOA)	Strength Assessment	Measures the strength of the TTOA in terms of its features when used under normal circumstances and under abnormal circumstances, such as attacks and denial of service	▶ Work Factor ▶ Survivability
	Weakness Assessment	Measures the susceptibility of the TTOA to threats, vulnerabilities, risks, and anticipated losses in the face of attack, and any operational limitations	▶ Risk ▶ Operational Limitation

7.7.2 NIST Types of Measures

NIST SP 800-55 Rev. 1 provides an informal taxonomy in Section 3.3, "Types of Measures." The publication identifies three categories of measures shown in Table 7-7.

Table 7-7 NIST Types of Measures

Categories of Measures	Examples of Measures
Implementation measures—Used to demonstrate the organization's progress in implementing information security programs, specific security controls, security of system-level areas, and policies and procedures associated with any of these.	▶ Percentage of information systems with approved system security plans ▶ Percentage of information systems with password policies that are configured as required ▶ Percentage of servers in a system that have been configured to conform with a standard configuration ▶ Percentage of assets identified and prioritized as critical ▶ Existence of documented assurance objectives
Effectiveness/Efficiency measures—Used to determine whether program-level processes and system-level security controls have been implemented correctly, operate as intended, and achieve their intended (desired) outcomes. Effectiveness/efficiency measures reflect two aspects of the results of security control implementation: the robustness of the result itself (*i.e.,* its effectiveness), and the timeliness of the result (*i.e.,* its efficiency).	Examples of effectiveness measures— ▶ Percentage of information security incidents caused by improperly-configured access controls, ▶ Percentage of unexpected and unwarranted events that have been registered. Examples of efficiency measures are— ▶ Percentage of system components that undergo maintenance on schedule ▶ Length of time it took to react to an incident (speed of incident response) ▶ Length of time it took to regain full operational capacity after unscheduled downtime

Categories of Measures	Examples of Measures
Impact measures—Articulate the impact (*i.e.,* business or mission impact) of information security on the organization's ability to accomplish its mission. Depending on the organization's mission, impact measures may quantify such factors as— ▶ Cost savings that result from the information security ▶ Cost of response per incident ▶ Costs incurred by addressing security incidents ▶ Degree of public trust gained or maintained by the information security program ▶ Variance between planned and actual spending on IA training ▶ Return on investment on costs of security protections/countermeasures *vs.* expected losses from security exposures/compromises that would be possible if the target of attack were not protected ▶ Any other mission-related impact of information security	▶ Percentage of the agency's IT budget devoted to security ▶ Number of information security investments reported to OMB in an Exhibit 300

7.7.3 I3P Taxonomy of Security Metrics for Process Control Systems [154]

The purpose of the Institute for Information Infrastructure Protection (13P) taxonomy is to categorize measurement of security of process control systems, *e.g.,* SCADA systems. The developers of this taxonomy used as a starting point three implied IA metrics taxonomies—

- Categorization of CS/IA measurement subject matter at the WISSSR;
- Control objectives in ISO/IEC 17799, *Information technology – Security techniques – Code of practice for information security management;*
- Categories of technologies in American National Standards Institute (ANSI)/International Society of Automation (ISA)-TR99.00.01-2004, *Security Technologies for Manufacturing and Control Systems.*

The I3P taxonomy divides metrics into the three categories: (1) Organizational, (2) Operational, and (3) Technical—then adds two further categories to capture security controls designated in ISO/IEC 17799 and ANSI/ISA-TR99.00.01-2004. The taxonomists suggest that the following measurable aspects of an information security activity or system can be mapped to measures in one or more of the five high-level categories, as depicted in Table 7-8.

Table 7-8 Mapping of Measurable Security Elements to Metrics Categories

	ISO/IEC 17799	ISA TR99.1	Organizational Metrics	Operational Metrics	Technical Metrics
Security Policy	✔		✔	✔	
Vulnerability and Risk Assessment		✔		✔	
Organizational Security	✔		✔		
Asset Clarification and Control	✔		✔		✔
Personnel Security	✔	✔	✔		
Physical and Environmental Security	✔	✔	✔		
Communications and Operations Management	✔			✔	
Access Control	✔	✔		✔	
Systems Development and Maintenance	✔			✔	✔
Business Continuity Management	✔		✔	✔	
Compliance	✔		✔		

I3P had not, at the time of proposing its taxonomy, defined a more complete hierarchy of metrics categories and subcategories, nor had it populated its proposed taxonomy. The I3P researchers had, however, identified an extensive list of potential sources for such metrics, and categorized these within the first three categories of their taxonomy; they had also surveyed and evaluated the potential usefulness of the metrics in each source for measuring security attributes of process control systems.

In doing this survey, the researchers actually implied a more complete taxonomy of relevant security metrics than is indicated by their formally proposed taxonomy. Table 7-9 depicts that implied taxonomy of security metrics.

Table 7-9 I3P Taxonomy of Security Metrics for Process Control Systems

Metric Group	Metrics	Sub Metrics	Description/Examples
Organizational	Security Program		
	Security Process		
	Security Program Maturity		
Operational	Operational Readiness/ Security Posture		
	Measures used in Risk Management	Security Performance	▶ Reflect current/recent system behavior
		Compliance	
		Risk	▶ Describe the threat environment ▶ Support the incident response ▶ Support vulnerability management
	Security Relevant		
Technical	Technology Security Standards, such as the Common Criteria		
	Other Security Products/Services		
	Technical Measures of Risk, such as those generated from DREAD or through implementation OUST		
	Process Control System-specific		▶ Sandia National Laboratories Framework for SCADA Security Policy ▶ NIST's emerging definition of SCADA security controls, based on NIST SP 800-53 ▶ NERC Cyber Security Standards CIP-002 through CIP-009

7.7.4 Department of Public Safety and Emergency Preparedness Canada Taxonomy [155]

This CS/IA measures taxonomy was defined for the Department of Public Safety and Emergency Preparedness to measure results of network assessments. Its measures fall into three categories, with the same three sub-categories within each category, as illustrated in Table 7-10.

Table 7-10 Department of Public Safety and Emergency Preparedness Taxonomy

Security Metrics			Quality of Service Metrics			Availability Metrics		
Technical	Organizational	Operational	Technical	Organizational	Operational	Technical	Organizational	Operational

7.7.5 VTT Technical Research Centre of Finland Security Metrics Taxonomy for R&D Organizations [156]

Researchers at the Valtion Teknillinen Tutkimuskeskus (Government Technical Research Center)—commonly known as the VTT Technical Research Centre—in Otaniemi, Finland, proposed another taxonomy, intended to "bridge the gaps between business management, information security management, and information and communication technology product security measurement practices." The proposed taxonomy is shown in Table 7-11.

Table 7-11 VTT Technical Research Centre of Finland Security Metrics Taxonomy for R&D

Metric Group	Metrics	Sub Metrics	Description
Business Level Security	Security metrics for cost- benefit analysis		
	Trust metrics for business collaboration		
	Security metrics for business-level risk management		
Security metrics for organization's Information Security Management (ISM)	Management Security	▶ ISM Process ▶ ISM-level risk management ▶ Resource and awareness management	
	Operational Security	▶ Susceptibility of operational controls ▶ Effectiveness of operational controls	▶ Reflect current/recent system behavior
	Information System Technical Security	▶ Technical Security ▶ Dependability ▶ Trust ▶ Technical Control, including logs/audit trails	

Metric Group	Metrics	Sub Metrics	Description
Security, Dependability, and Trust Metrics for Products, Systems, and Services	Product/System/Service Life Cycle Management	▶ System conception ▶ System design ▶ System realization ▶ System service	
	Product/System/Service Security Rating or Assurance	▶ Evaluation ▶ Testing ▶ Verification ▶ Certification	
	Product/System/Service Security Engineering	▶ System-level technical security solution	▶ Software/hardware platform design-level technical security solution ▶ Application design-level technical security solution ▶ Network design-level technical security solution ▶ Software/hardware platform implementation-level technical security solution ▶ Application implementation-level technical security solution metrics ▶ Network implementation-level technical security solution
		▶ System-level technical risk management	

7.7.6 Daniel Geer's Balanced Scorecard-based Taxonomy

In his tutorial *Measuring Security,* [157] IA metrics expert Daniel Geer suggests a taxonomy based on the four corners of a balanced scorecard:

1. Financial *vs.* Security,
2. Internal Business Process *vs.* Security,
3. Learning and Growth *vs.* Security,
4. Customer *vs.* Security.

Geer then provides examples of metrics that might fall under each of the four categories in Table 7-12.

Table 7-12 Daniel Geer's Balanced Scorecard Taxonomy with Sample Metrics

Aspects to be Compared Based on Metrics	Metrics to Use for Comparison
Financial *vs.* Security	▶ Cost of security per transaction ▶ Denial of service and other attack-related downtimes ▶ Data flow per transaction and per source ▶ Budget correlation with risk measures ▶ Comparison with similar organizations
Internal Business Process *vs.* Security	▶ Percentage of critical systems addressed in disaster recovery plan ▶ Percentage of systems obeying Policy X ▶ Mean Time-Between-Failure (MTBF) and Mean Time-To-Repair (MTTR) for security incidents ▶ Number of security team consultations ▶ Latency to address X [quantity] change orders
Learning and Growth *vs.* Security	▶ Percentage of job reviews involving security ▶ Percentage of security workers with training ▶ Ratio of business unit security staff to central staff ▶ New system timely security consultations ▶ Percentage of programs with budgeted security
Customer *vs.* Security	▶ Percentage of Service Level Agreements with security standards ▶ Percentage of tested external-facing applications ▶ Number of non-employees with access ▶ Percentage of data that is secure-by-default ▶ Percentage of customer data residing outside the data center

7.8 Quantifying the Economic Value of Security and Assurance

"Metrics provide a mechanism to accurately measure the success of security initiatives and investments in the context of the business." [158]

"Just about every security certification course (SANS, CISSP) talks about ALE, for reasons I cannot fathom…When we focus just on dollars, ALE, and 'security ROI [Return on Investment],' we make things too simple." [159]

A key function of CS/IA measurement can be to quantify economic value of security, such as ROSI and other economic indicators. Through true measurement, monitoring, and verification, IA can be executed accurately, efficiently, and effectively, to create maximum value for every IA investment. CS/IA measurement can help answer the following questions—

- Are the demands of information security capital planning overwhelming?
- Does your organization have an overall strategy to fund information security investments?
- How do I know what to invest in to strengthen the agency's security posture?
- Do your information security investments fail to deliver the benefits you anticipated?

- How can I reasonably estimate information security benefits?
- How can I communicate the value of my investments to decision makers?

Karen Evans, OMB Administrator for Electronic Government and Information Technology, in testimony before the Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, stated—

> ***"There continues to be a failure to adequately prioritize IT function decisions to ensure that remediation of significant security weaknesses are funded prior to proceeding with new development… Agencies must—***
> 1. ***Report security costs for IT investments;***
> 2. ***Document in their business cases that adequate security controls have been incorporated into the lifecycle planning for each IT investment;***
> 3. ***Reflect the agency's security priorities as reported separately in their plans of action and milestones for fixing programs and systems found to have security vulnerabilities;***
> 4. ***Tie those plans of action and milestones for an IT investment directly to the business case for that investment." [160]***

Ms. Evans' comments echo the need to identify and justify the economic value of security through the use of CS/IA measurement. Information security investments should be rank-ordered against security criteria to create a prioritized investment strategy using CS/IA measurement. Once investments are prioritized, business cases can be developed to communicate their value to the agency. The value of the prioritized information security investments can then be communicated in management terms.

NIST SP 800-55 Rev. 1 refers to the value of security through the use of impact measures, which are used to articulate the impact of information security on an organization's mission. For example, the percentage of the agency's information system budget focused toward information security is a key indicator of the organization's probability to protect its mission. Appendix A of NIST SP 800-55 Rev. 1 contains the detail for this CS/IA measure. The document's measures creation process and implementation process facilitate the creation of more value-based and impact measures.

The ultimate value of security is typically measured through breaches, when the security fails or bypassed, and through the resulting economic fallout. Economic models can be applied to calculating the value of security versus the prior and theoretical cost of incidents.

The Burton Group recently published a paper on the measurement of IT's business value. [161] The focus of the article is that IT metrics typically measure activities that are easy to measure, such as project completion, system defects, and operational uptime, but unsuccessfully measure the quality and usefulness of the information that IT systems produce for the business. The paper outlines suggestions for how IT leaders can use metrics to provide a more accurate view of the IT business value.

Another article, "An ounce of prevention *vs.* a pound of cure: how can we measure the value of IT security solutions?," [162] focuses on how the integration of a company's risk profile can be used to determine costs and benefits of IT security solutions. Two crucial concepts of the article are—

- **Incident type**—Refers to the various types of cyber incident that can happen to an organization;
- **Bypass rate of a security solution**—The rate at which an attack results in actual damage to the organization.

The article concluded by proposing to focus on the need for more risk-based structured cost-benefit methods for evaluating and comparing IT security solutions.

A study entitled, "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," [163] goes beyond just identifying the direct costs of breaches to examine the economic effect of information security breaches reported in newspapers or publicly traded US corporations—

> ***"We find limited evidence of an overall negative stock market reaction to public announcements of information security breaches. However, further investigation reveals that the nature of the breach affects this result. We find a highly significant negative market reaction for information security breaches involving unauthorized access to confidential data, but no significant reaction when the breach does not involve confidential information. Thus, stock market participants appear to discriminate across types of breaches when assessing their economic impact on affected firms. These findings are consistent with the argument that the economic consequences of information security breaches vary according to the nature of the underlying assets affected by the breach." [164]***

Quantifying the return of information security investments through traditional ROI justification models is often challenging because these investments provide more benefits than just bottom-line savings. Information security investments do not always lend themselves to ROI calculations because they cannot always be quantified.

Use of models and simulations can help qualitatively and quantitatively measure direct and indirect benefits by assessing the probability of program success, analyzing investment risks, and reasonably predicting outcomes, and focusing on certainty, rather than specificity to provide probability and ranges of outcomes.

The Economics and Security Resource Page [165] is dedicated to this topic and includes links to a number of key papers, conferences, the home pages of active researchers, relevant books, and other resources. These resources can assist in identifying and leveraging useful potential CS/IA measures.

For Further Reading

Ashish Arora, Dennis Hall, C. Ariel Pinto, Dwayne Ramsey, and Rahul Telang. "Measuring the Risk-Based Value of IT Security Solutions," in *IT Professional,* Vol. 6, No. 6, Nov./Dec. 2004, pp. 35–42. Digital Object Identifier: 10.1109/MITP.2004.89 Accessed 7 April 2009 at: *http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F6294%2F30282%2F01390871.pdf&authDecision=-203*

S. Chandra and R.A. Khan. "Object Oriented Software Security Estimation Life Cycle-Design Phase Perspective," in Journal of Software Engineering, Volume 2 Issue 1, 2008, pp. 39–46. Accessed 13 April 2009 at: *http://www.scialert.net/fulltext/?doi=jse.2008.39.46*

Tony Coulson, Jake Zhu, and C.E. Tapie Rohm, California State University-San Bernardino, and Shan Miyuan, Hunan University-Changsha. "The Price of Security: The Challenge of Measuring Business Value Investments in Securing Information Systems," in *Communications of the IIMA,* Volume 5, Issue 4, 2005. Accessed 25 March 2009 at: *http://www.iima.org/CIIMA/8%205.4_Coulson_19_24.pdf*

Tony Coulson, Jake Zhu, Kurt Collins, Walter Stewart, C.E. Tapie Rohm, Jr., California State University-San Bernardino. "Security: Valuing Increased Overhead Costs," in *Proceedings of the 10th Colloquium for Information Systems Security Education,* Adelphi, MD, 5–8 June 2006. Accessed 25 March 2009 at: *http://www.cisse.info/colloquia/cisse10/proceedings10/pdfs/papers/S05P03.pdf*

Raph Levien. "Advogato's trust metric," 22 February 2000. Accessed 6 April 2009 at: *http://www.advogato.org/trust-metric.html*

Raph Levien. "Attack Resistant Trust Metric Metadata HOWTO," 3 July 2002. Accessed 6 April 2009 at: *http://www.levien.com/free/tmetric-HOWTO.html*

Shaun Remnant. "Counting the cost of IT security," in *ITadviser,* Issue 38, July/August 2005. Accessed 25 March 2009 at: *http://www.nccmembership.co.uk/pooled/articles/BF_WEBART/view.asp?Q=BF_WEBART_171149*

Stuart Edward Schechter. "Toward Econometric Models of the Security Risk from Remote Attack," in *IEEE Security & Privacy,* Vol. 3, No. 1, January/February 2005, pp. 40–44. Digital Object Identifier: 10.1109/MSP.2005.30; Earlier version published in *Proceedings of the Third Workshop on Economics and Information Security,* Minneapolis, MN, May 2004, Accessed 25 March 2009 at: *http://www.eecs.harvard.edu/~stuart/papers/eis04.pdf*

Trustcomp Yahoo Group. "Welcome to Trustcomp.org!" Accessed 25 March 25, 2009 at: *http://www.trustcomp.org*

References

125 Gary Hinson, IsecT Ltd. "Seven myths about information security metrics," in *ISSA Journal,* July 2006. Accessed 13 April 2009 at: *http://www.noticebored.com/IsecT_paper_on_7_myths_of_infosec_metrics.pdf*

126 Nadya Bartol. "IA Metrics—Why and How to Measure Goodness of Information Assurance." Presented to ISSEA PSM User's Group Conference, July 2005. Accessed 29 December 2008 at: *http://www.psmsc.com/UG2005/Presentations/15_Bartol_IA_Metrics.pdf*

127 Sandia National Laboratories. "IDART Red Team Metrics Quick Reference Sheet." Accessed 6 January 2009 at: *http://www.idart.sandia.gov/research.html*

128 Michael J. Scroch, Sandia National Laboratories. "IORTA Red Team Metrics 101" (Incomplete Beta Version). Lecture slides for Information Operations Red Team and Assessments Training Program, 19 May 2005.

129 M.S. Ahmed, E. Al-Shaer, L. Khan. "A Novel Quantitative Approach For Measuring Network Security, INFOCOM 2008," in *The 27th Conference on Computer Communications. IEEE,* April 2008 Page(s):1957–1965, Digital Object Identifier 10.1109/INFOCOM.2008.260. NIST National Vulnerability Database Web page. Accessed 25 March 25, 2009 at: *http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=4509855*

130 Glenn Fink and Brett Chappell, Naval Sea Systems Command (NAVSEA) Information Transfer Technology (ITT) Group, B30 Combat Systems Technology Division. "A Metrics-Based Approach to Intrusion Detection System Evaluation for Distributed Real-Time Systems." Accessed 8 February 2009 at: *http://people.cs.vt.edu/~finkga/ids/IDS-Briefing-09Apr02.ppt*

131 Security Metrics, Inc. Accessed 12 February 2008 at: *http://SecurityMetrics.com*

132 Aladdin. "Attack Intelligence Research Center: Security Statistics." Accessed 7 April 2009 at: *http://www.aladdin.com/airc/security-statistics.aspx.*

133 The MITRE Corporation. "Common Vulnerabilities and Exposures (CVE)," *op cit.*

134 The MITRE Corporation. "OVAL FAQ." Accessed 3 February 2009 at: *http://oval.mitre.org/oval/about/faqs.html#a16*

135 Peter Mell and Karen Scarfone, NIST, and Sasha Romanosky, CMU. *CVSS: A Complete Guide to the Common Vulnerability Scoring System Version 2.0.* Accessed 29 January 2009 at: *http://www.first.org/cvss/cvss-guide.pdf*

136 Victor-Valeriu Patriciu, Iustin Priescu, and Sebastian Nicolaescu. "Security Metrics for Enterprise Information Systems," in *Journal of Applied Quantitative Methods (JAQM),* Vol. 1, No. 2, Winter 2006. Accessed 6 January 2009 at: *http://jaqm.ro/issues/volume-1,issue-2/pdfs/patriciu_priescu_nicolaescu.pdf*

137 Chris Wysopal, Veracode, Inc. "Software Security Weakness Scoring." Presented at MetriCon 2.0, Boston, Massachusetts, 7 August 2007. Accessed 16 February 2009 at: *http://www.securitymetrics.org/content/attach/Metricon2.0/Wysopal-metricon2.0-software-weakness-scoring.ppt*

138 Karen Scarfone and Peter Mell. *The Common Configuration Scoring System (CCSS) (DRAFT),* NIST Interagency Report 7502 (Draft), May 2008. Accessed 2 February 2009 at: *http://csrc.nist.gov/publications/drafts/nistir-7502/Draft-NISTIR-7502.pdf*

139 Elizabeth Van Ruitenbeek and Karen Scarfone. *The Common Misuse Scoring System (CMSS) (DRAFT),* NIST Interagency Report 7517 (Draft), February 2009. Accessed 26 March 2009 at: *http://csrc.nist.gov/publications/drafts/nistir-7517/Draft-NISTIR-7517.pdf*

140 National Cyber Security Division (Hosted by The MITRE Corporation.) "CWSS—Common Weakness Scoring System," Common Weakness Enumeration. Accessed 6 April 2009 at: *http://cwe.mitre.org/cwss/index.html*

141 The MITRE Corporation. "Making Security Measurable." Accessed 16 February 2009 at: *http://measurablesecurity.mitre.org*

142 Edgar Sibley, George Mason University. "National Information Assurance Training Standard for System Administrators." Lecture slides for course on IAVA, Summer 2008. Accessed 5 February 2009 at: *http://mason.gmu.edu/~esibley/ISA562SU08/Slide/11%2520cont%25202%2520IAVA%2520.ppt*

143 US-CERT. "Vulnerability Notes Database Field Descriptions." Accessed 4 February 2009 at: *http://www.kb.cert.org/vuls/html/fieldhelp*

144 Robert Hudock. "Why Security Metrics Must Replace Traditional Risk Analysis Methodologies," *Computer Security Law,* 6 March 2008. Accessed 19 January 2009 at: *http://computersecuritylaw.us/2008/03/06/why-security-metrics-must-replace-traditional-risk-analysis-methodologies.aspx*

145 Michael Chertoff, DHS Secretary. Speech at the George Washington University Homeland Security Policy Institute, 16 March 2005. Accessed 7 April 2009 at: *http://www.dhs.gov/xnews/speeches/speech_0245.shtm*

146 Darlene Goodwin, "NCDOC Garners Network Defense Accreditation Milestone," in *INFODOMAIN,* Fall 2008, pg. 7. Accessed 11 May 2009 at: *http://www.netwarcom.navy.mil/pao/infodomain/010-InfoDomain-Fall2008.pdf*

147 NetIQ Corporation, Inc. "SCAP and FDCC." Accessed 8 February 2009 at: *http://www.netiq.com/solutions/regulatory/fdcc/default.asp*

148 NIST NVD program. "Managing Security Risk by Using Common Security Configurations." Accessed 8 February 2009 at: *http://nvd.nist.gov/fdcc/faq-common_security_configurations.cfm*

149 NIST. "Security Content Automation Protocol Validated Products." Accessed 6 April 2009 at: *http://nvd.nist.gov/scapproducts.cfm*

150 NIST. "Security Content Automation Protocol (SCAP) Validation Program." Accessed 6 April 2009 at: *http://nvd.nist.gov/validation.cfm#fdcc_scanner*

151 Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, and George Rogers. NIST. SP 800-53 Rev. 2, *Recommended Security Controls for Federal Information Systems,* December 2007. Accessed 3 April 2009 at: *http://www.csrc.nist.gov*

152 Defense Logistics Agency (DLA). "Certification and Accreditation: the DLA Approach." Accessed 26 March 2009 at: *http://csrc.nist.gov/groups/SMA/fasp/documents/c&a/DLABSP/DLABSP.htm*

153 Christofer Hoff, Rational Security. "Take5 (Episode #6)—Five Questions for Andy Jaquith, Yankee Group Analyst and Metrician…," Rational Survivability Blog, 13 September 2007. Accessed 29 January 2009 at: *http://rationalsecurity.typepad.com/blog/2007/09/take5-episode-6.html*

154 Described in M. Stoddard, *et al.* "An Initial Metrics Taxonomy," in *Process Control System Security Metrics—State of Practice,* I3P Institute for Information Infrastructure Protection Research Report No. 1, August 2005. Accessed 19 January 2009 at: *http://www.thei3p.org/docs/publications/ResearchReport1.pdf*

155 Described in Nabil Seddigh, Peter Pieda, Ashraf Matrawy, Biswajit Nandy, John Lambadaris, and Adam Hatfield. "Current Trends and Advances in Information Assurance Metrics," in *Proceedings of Second Annual Conference on Privacy, Security, and Trust (PST 2004),* Fredericton, NB, Canada, 13–15 October 2004. Accessed 19 January 2008 at: *http://dev.hil.unb.ca/Texts/PST/pdf/seddigh.pdf*

156 Described in: Reijo Savola, VTT Technical Research Centre of Finland. "A Novel Security Metrics Taxonomy for R&D Organisations," in *Proceedings of the Information Security South Africa (ISSA) 2008 Innovative Minds Conference,* Johannesburg, South Africa, 7–9 July 2008. Accessed 2 January 2009 at: *http://icsa.cs.up.ac.za/issa/2008/Proceedings/Full/2.pdf.* Also described in Reijo M. Savola, VTT Technical Research Center of Finland. "Towards a Taxonomy for Information Security Metrics," *Proceedings of ACM Workshop on Quality of Protection (QoP '07),* Alexandria, Virginia, 29 October 2007. DOI: *http://doi.acm.org/10.1145/1314257.1314266*

157 Daniel E Geer. *Measuring Security,* Version 2.1:16x07. Accessed 30 January 2009 at: *http://geer.tinho.net/measuringsecurity.tutorial.pdf*

158 Ayoub, Frost & Sullivan. "Analysis of Business Driven Metrics: Measuring for Security Value," *op cit.*

159 Hoff, "Take5 (Episode #6)—Five Questions for Andy Jaquith, Yankee Group Analyst and Metrician…" *op cit.*

160 Karen Evans, OMB. Testimony before the Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, 16 March 2004. Accessed 22 January 2009 at: *http://www.whitehouse.gov/omb/assets/omb/legislative/testimony/evans/karen_evans031604.pdf*

161 Lyn Robison, The Burton Group. *IT Metrics: Measuring IT's Business Value,* 27 February 2009. Accessed 13 March 2009 at *https://www.burtongroup.com*

162 Ashish Aroral, Dennis Hall, C. Ariel Pinto, Dwayne Ramsey, and Rahul Telang1. *An ounce of prevention vs. a pound of cure: how can we measure the value of IT security solutions,* 2004. Accessed 26 March 2009 at: *http://www.osti.gov/energycitations/product.biblio.jsp?osti_id=842753*

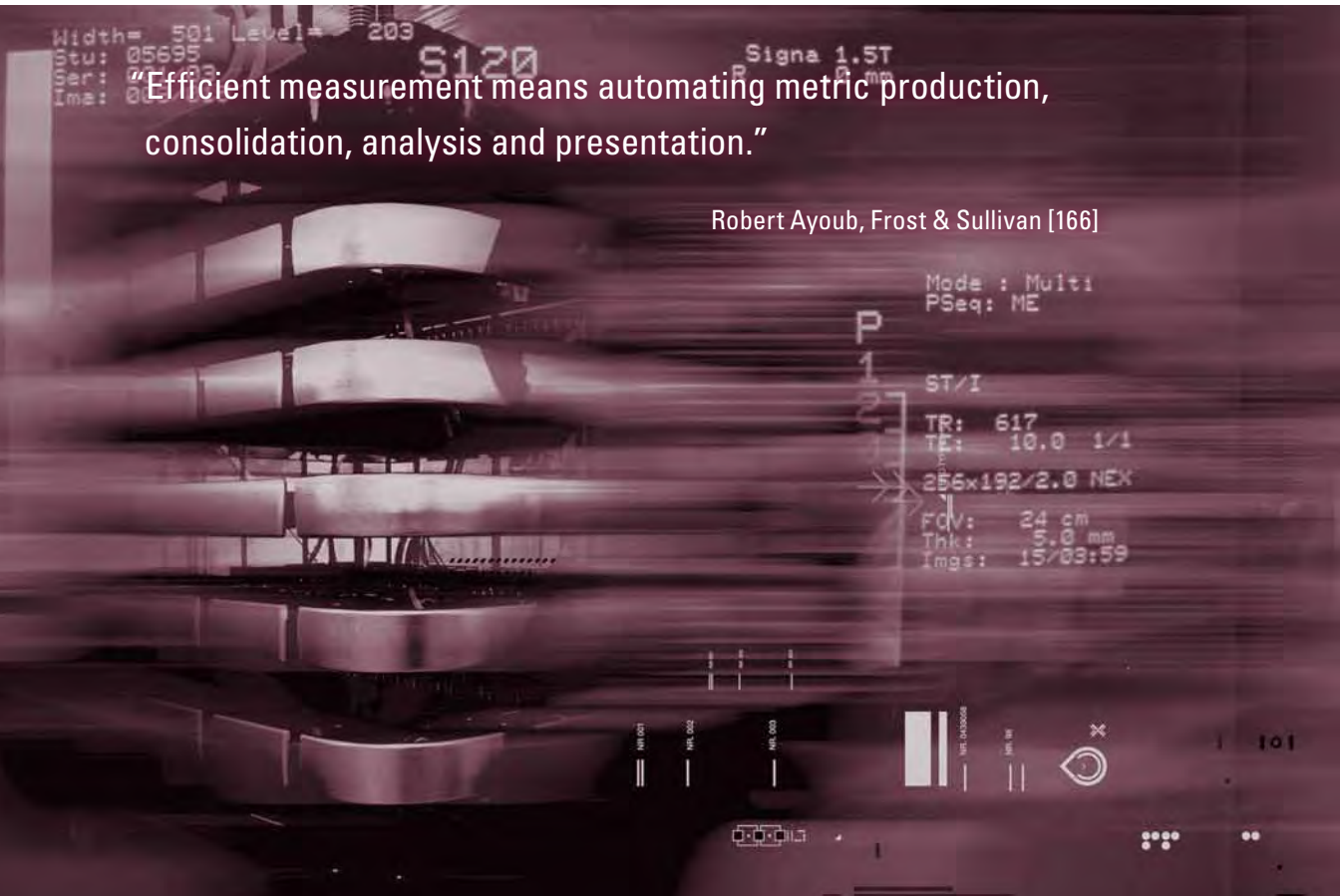
163 Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," in *Journal of Computer Security Archive,* Volume 11, Issue 3 (March 2003), Table of Contents IFIP 2000, Pages: 431 to 448, 2003, ISSN:0926-227X. Accessed 26 March 2009 at: *http://portal.acm.org/citation.cfm?id=876669*

164 *Ibid.*

165 Ross Anderson, University of Cambridge Computer Laboratory. "Economics and Security Resource Page." Accessed 26 March 2009 at: *http://www.cl.cam.ac.uk/~rja14/econsec.html*

8

Tools and Technologies



"Efficient measurement means automating metric production, consolidation, analysis and presentation."

Robert Ayoub, Frost & Sullivan [166]

There is much information posted on the Web on the topics of IA measurement methodologies, lessons learned, sound measurement practices, and examples. However, there is little public information regarding CS/IA measurement tools.

Few COTS software products are being marketed as CS/IA measurement tools, although some compliance and analytical tools note CS/IA measurement as a component of the tools' functionality.

Most tools that serve this purpose are homegrown government off-the-shelf (GOTS) applications, using existing vendor technologies, created to meet organizations' needs to respond to compliance legislation, such as FISMA, and other directives, such as the President's Management Agenda (PMA). Examples and components of CS/IA measurement tools typically fall into the following four groups—

- Integration (frameworks/platforms),
- Collection/storage,
- Analysis/assessment,
- Reporting.

When building or selecting a CS/IA measurement tool, it is important to perform requirements, gap, and selection processes to see which tool would best fit the organization or even to see if the organization already owns a tool that could be leveraged.

For CS/IA measurement tools to be successful, the following sound measurement practices should be considered—

- Tools and dashboards should be vetted through all appropriate approval channels.

- Policy, procedures, and risk priorities should be used to derive measurable performance goals and objectives prior to selection and implementation of tools.
- Tools should allow CS/IA measures to be more quantitatively focused to increase the objectivity and validity of data.
- Tools should enable CS/IA measurement data to be easily collected, accessed, and stored.
- Tools and process should be repeatable with the ability to identify performance trends over time.
- Tools should display CS/IA measurement results in the appropriate format to the appropriate stakeholder level.
- Tools should enable CS/IA measures to be useful to stakeholders and yield information that is important in the decision-making process.

This section does not aim to provide a comprehensive view of the tools available for generating and processing CS/IA measures. Instead, it provides the reader with a sampling of tools that can serve as a starting point for any organization intending to acquire or deploy CS/IA measurement tools.

8.1 Integration

For CS/IA measures to be successful, some infrastructure should be leveraged for the integration, sharing, and publishing of CS/IA measurement results using tools like the ones identified in Table 8-1. CS/IA measurement data should be stored in a secure shared network space for appropriate protection.

Table 8-1 CS/IA Measurement Integration (Frameworks/Platforms) Tools

Name	Description	For More Information
Microsoft Sharepoint	Browser-based collaboration and a document-management that provides a platform for CS/IA measures collection, sharing, and storage	*http://www.microsoft.com/Sharepoint/default.mspx*
Plumtree Portal	Modular portal in which portlets can be used to store and display CS/IA measures	*http://www.plumtree.com*
Opensims	Framework for linking open source tools together for security management into a common infrastructure with real-time CS/IA measures	*http://www.opensims.org*
Symbiot Security	Risk Metrics Appliances—dynamic, real-time, interactive interface displaying CS/IA measurement output from its appliances used with virtually any Web browser on any platform	*http://www.symbiot.com/riskmetricsolutions.html*
OpenService	Collects, stores, and scores CS/IA measures from a wide range of devices and events	*http://www.openservice.com*

Name	Description	For More Information
Intellitactics SAM Tool	Provides CS/IA measures that dynamically update with the enterprise specific data	*http://www.intellitactics.com/int*
NetIQ Risk and Compliance Center	Aligns CS/IA measures gathered from IT systems to demonstrate compliance with IT-related policies and regulations and displays them in a customizable dashboard	*http://www.netiq.com/products/rcc/default.asp*
Elemental Security, Inc.	Elemental Security Platform is integrated system for enterprise policy and risk management	*http://www.elementalsecurity.com*

8.2 Collection/Storage

It is common for organizations to be using Microsoft Excel or Access to collect and store CS/IA measurement data.

Table 8-2 lists examples of automated tools that emerged since 2000 to handle a variety of IA compliance activities. Though the tool examples described in Table 8-2 can perform additional functions, they are focused primarily on collection and storage of CS/IA data.

Table 8-2 CS/IA Measurement Collection/Storage Tools

Name	Description	For More Information
CSAM and ASSERT OMB Security Line of Business Solutions	Allow users to browse the catalog of security controls, display the controls in selected views, and export information from the database into a variety of popular data formats that may be needed for automated tool support	*http://csrc.nist.gov/groups/SMA/fisma/support_tools.html*
Trusted Agent FISMA (TAF)	Enables users to automate, document, and report information security performance through relational database and Web interfaces to demonstrate FISMA compliance	*http://www.trustedintegration.com*
Prosight	This portfolio management software solution can be used to capture and track IA assets, and derive data that can be used to calculate CS/IA measures	*http://www.primavera.com/products/prosight/index.asp*
Splunk	Enables compliance with explicit requirements to monitor, review, and retain audit trails; demonstrate compliance across all other information protection controls; and capture and retain IT data for extended periods, per NIST standards	*http://www.splunk.com/article/2307*
IBM/Tivoli	TCIM's FISMA Management Module maintains the security of federal information systems, and facilitates compliance with FISMA requirements by proactively monitoring access to sensitive data and reporting on IT security policy enforcement	*http://www-01.ibm.com/support/docview.wss?uid=swg21300129*

Name	Description	For More Information
Telos/Xacta	Enables continuous monitoring and managing information security risks, and automates and enforces processes for governance, risk, and compliance	*http://www.telos.com/solutions/information%20assurance*
MASE Consulting Ltd. Information Security Metrics Spreadsheets	Developed to record and track the Information Security (IS) Program measures listed in the Information Security Objectives and Metrics document, and detailed in the IS program strategy	*http://www.maseconsulting.com/Metrics-Road-Map-s/6.htm*

8.3 Analysis/Assessment

Security analysis and assessment tools are directed at a variety of capabilities, including finding vulnerabilities in networks and code, analysis of log-based data, assessing the overall status of CS/IA, evaluating IA risks, or IA compliance. Some of these analysis tools are described in Table 8-3.

Table 8-3 CS/IA Measurement Analysis and Assessment Tools

Name	Description	For More Information
Coverity	Coverity offers a suite of tools to perform security analysis of software architecture, code and running applications. The Coverity Integrity Center can provide organization with measures based on the results of the Coverity suite to aid in determining the risk associated with their applications.	*http://www.coverity.com/products/*
Klocwork Insight	Klocwork Insight performs source code analysis to identify vulnerabilities within an organization's source code. Insight offers reporting capabilities that generate measures based on the results of the tool, including the number of vulnerabilities detected and fixed on the developers' desktops, and comparisons of the number of defects over time.	*http://www.klocwork.com/products/insight.asp*
Ounce Suite	Ounce Labs provides a suite of tools for scanning the source code of applications and providing measures based on the number and severity of vulnerabilities identified. The Ounce Portfolio Manger provides measures at an organizational level based on the results of Ounce Las Tools.	*http://www.ouncelabs.com/products*
Fortify Suite	The Fortify suite of tools supports scanning the source code and performing run-time analysis of applications, allowing organizations to compare the health of their applications over time. Fortify offers a Web portal that organizations can use to disseminate the results from Fortify-based tools.	*http://www.fortify.com/products/detect*

Name	Description	For More Information
BogoSec	BogoSec is an open source tool that scans code using three popular open source code scanning tools and generates security measures based on the results.	*http://bogosec.sourceforge.net*
MOPS	MOPS is an example of a static (compile-time) analysis tool, which can check whether the program violates specified security properties. The security properties that MOPS checks are temporal, properties that are required to perform certain security-related operations in a certain order. While the primary function of these tools is not measures, the properties being checked are relevant to security and the data points can be used to populate a measure.	Hao Chen, Drew Dean, and David Wagner. "Model checking one million lines of C code," *Proceedings of the 11th Annual Network and Distributed System Security Symposium, 2004,* pp 171–185. Accessed on 7 April 2009 at: *http://www.cs.ucdavis.edu/~hchen/paper/ndss04.pdf*
Daikon	Daikon performs dynamic invariant detection, which runs a program, observes the values that the program computes, and then reports properties that were true over the observed executions. Dynamic invariant detection is a machine learning technique that can be applied to arbitrary data. The Daikon system detects invariants in code-based programs and in data sources. The output of the system has been used for predicting incompatibilities in component integration, generating test cases, repairing inconsistent data structures, and checking the validity of data streams, and could be seen as a data source for populating CS/IA measures.	Michael D. Ernst, Jeff H. Perkins, Philip J. Guo, Stephen McCamant, Carlos Pacheco, Matthew S. Tschantz, and Chen Xiao. "The Daikon system for dynamic detection of likely invariants." Science of Computer Programming, vol. 69, no. 1–3, Dec. 2007, pp. 35–45.
Cenzic Hailstorm	Cenzic Hailstorm performs a scan of organization's Web applications to detect vulnerabilities. Organizations may generate reports from the tool that generate measures based on the results of Hailstorm scans over time and across multiple systems within an organization, providing a high level overview of the organization's security posture.	*http://www.cenzic.com/products/overview*
HP WebInspect	HP WebInspect performs a scan of organization's Web applications to detect vulnerabilities. Organizations may generate reports from the tool that generate measures based on the results of WebInspect scans over time and across multiple systems within an organization, providing a high-level overview of the organization's security posture.	*https://h10078.www1.hp.com/cda/hpms/display/main/hpms_content.jsp?zn=bto&cp=1-11-201-200^9570_4000_100__*
LogLogic Compliance Suites	Provides a real-time view of adherence to multiple regulations and standards using Log data	*http://www.loglogic.com/products/compliance-management/compliance.php* (accessed 25 March 2009)

Name	Description	For More Information
The Bug Isolation Project	A research effort designed to monitor a collective of software applications, record behavior while they run, and report back how they work (or how they fail to work) in the hands of real end-users. The monitoring is transparent, low overhead with minimal impact on application behavior or performance, and the system is engineered to protect your privacy and ensure the security of the data collected. Data values and decisions within the application are scanned periodically and tested to see if unusual patterns are discovered. The instrumentation is not active all the time and turns on and off randomly while applications run. The approach is called statistical debugging, which is finding bugs in programs *via* automated statistical analysis instead of laborious manual inspection. This approach could be applied to security and also used as a data source for populating CS/IA measures.	Benjamin R Liblit. Cooperative Bug Isolation, University of California, Berkeley, PhD Thesis, December 2004
vsRisk	vsRisk is a risk assessment tool that measures compliance against ISO 27001:2005, assessing confidentiality, integrity and availability for each of business, legal, and contractual aspects of information assets	*http://www.itgovernance.co.uk/products/744*
OCTAVE	The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) project provides tools, techniques and methods for performing security evaluations.	*http://www.cert.org/octave*
MSAT	Microsoft Security Assessment Tool (MSAT) aids organizations in assessing the weaknesses in their current IT security environment. MSAT provides a Business Risk Profile (BRP) that measures the risks associated with their business while the Defense-in-Depth Index (DiDI) describes how the organization's security measures are deployed. The tool uses this information to calculate risk.	*http://technet.microsoft.com/en-us/security/cc185712.aspx*
DISA IA Portal	The DISA IA Portal provides access to IA assessment and analysis tools that are available throughout DoD, including anti-virus software, host-based security systems, compliance validation, and other tools.	*http://iase.disa.mil/tools/index.html*
Information Security Assessment Tool for State Agencies	The Assessment Tool for State Agencies aids agencies in determining the degree to which they have implemented an information security program or framework at the strategic level within their agency.	*http://www.oispp.ca.gov/government/documents/docs/RA_Tool_State_Agencies.doc*

Name	Description	For More Information
I3P Tools for Assessing SCADA/Control Systems Security	I3P developed a number of tools, including Risk-to-Mission Assessment Process (RiskMAP), PCS Security Technology Evaluation Tool (P-STET), 21 Steps Security Metrics Tool for performing security assessments of SCADA/Control System deployments. Their paper also identifies a number of commercially available assessment tools, including Control System Cyber Security Self Assessment Tool (CS2SAT), the I3P Security Metrics Starter Kit, the Skybox View Suite, and the ClearPoint Metrics Accelerator.	*http://www.thei3p.org/docs/publications/ResearchReport12.pdf*
CIS-CAT	Center for Internet Security—Configuration Audit Tool (CIS-SAT) reports the configuration status of individual systems against to the configuration settings defined in CIS Benchmark XML files, which are available for a large number of operating systems and applications.	*http://www.cisecurity.org/hgtoolmembers.html*
VMinformer	VMinformer assesses the security of VMware environments based on VMware's security recommendations, the DISA STIG for VMware ESX Server, and the CIS VMware guide, providing organizations with an indication of how well their ESX deployment complies with these available best-practices.	*http://www.vminformer.com*
NRAT	The Network Risk Assessment Tool (NRAT) is an analysis tool prototype developed through IATAC that considers the architecture, protection strategy, and attacks that a system may be affected by. NRAT assesses how attacks to the system would compromise the confidentiality, integrity and availability of the system and determines the effectiveness of the protections build into the information system.	*http://iac.dtic.mil/iatac/download/Vol11_No1.pdf*

8.4 Reporting

Collected and stored CS/IA measurement data provide the information necessary to populate security dashboards and other reports enabling "near real-time" status monitoring of the organization's security posture. When selecting dashboards formats, organizations should allow for information in the security repositories to be accessed, reused, displayed, and refreshed quickly and efficiently.

Examples of CS/IA measures reporting tools are described in Table 8-4.

Table 8-4 CS/IA Measures Reporting Tools

Name	Description	For More Information
IBM/Cognos	High-volume production reports, individual *ad hoc* queries, widely distributed business reports, and centrally authored reports with self-service customization that can be used to report CS/IA measures	*http://www.cognos.com*
Business Objects/ Crystal Reports/ Xcelsius	Complete report management solutions, and dynamic and customizable data visualization software to report CS/IA measures	*http://www.businessobjects.com/product*
Oracle/Hyperion	Balanced scorecard collaborative certified application that helps companies clearly articulate strategy and goals	*http://www.oracle.com/appserver/business-intelligence/hyperion-financial-performance-management/hyperion-performance-scorecard.html*
Corda	Real-time access to enterprise data, *via* performance dashboards from any location	*http://www.corda.com*
MicroStrategy	Enterprise reporting engine with fully integrated reporting, analysis, and monitoring, allowing business users to interact with the tool and design reports in familiar and intuitive ways	*http://www.microstrategy.com/Software/Products/Service_Modules/Report_Services*
Clear Point Metrics	Security Performance Manager is an integrated software and best practices content solution that enables IT and security executives and their teams to successfully measure, monitor, and communicate the state, quality, and effectiveness of their information security investments.	*http://www.clearpointmetrics.com*
Security Executive Council Performance Dashboard Tool	The Security Executive Council tool, available to members, aids in the presentation of measures data to senior management within an organization. Security program data is fed into a "dashboard dial" that provides indicators of success based on enterprise risk concerns.	*https://www.securityexecutivecouncil.com/knowledge/index.html?mlc=507*
Balanced Scorecard Designer	Security Metrics Balanced Scorecard is a tree of security metrics useful in designing an IT security measurement scorecard.	*http://www.strategy2act.com/solutions/IT_security_metrics.htm*

Dashboards are especially critical to CS/IA measurement programs as they are the visualization of the CS/IA measurement results.

Supporting evidence of security activities should also be collected, analyzed, and stored using the other activities documented in case of audit.

Security data and documentation produced from all planning, evaluation, and reporting activities should be maintained in a centralized repository. This coordinated recordkeeping enables security management, auditors, future assessment teams, and system owners to cross-reference raw and analyzed security data, findings, and subsequent mitigation

recommendations from the variety of sources creating such information. Such a repository mitigates the risks of "stove piping," which risks data loss through scattered organization and duplicative data calls—

> ***"Efficient measurement means automating metric production, consolidation, analysis and presentation. Dashboards provide a fast way to promote security measures, and easy to understand measurement can be quickly achieved using popular dashboard technology." [167]***

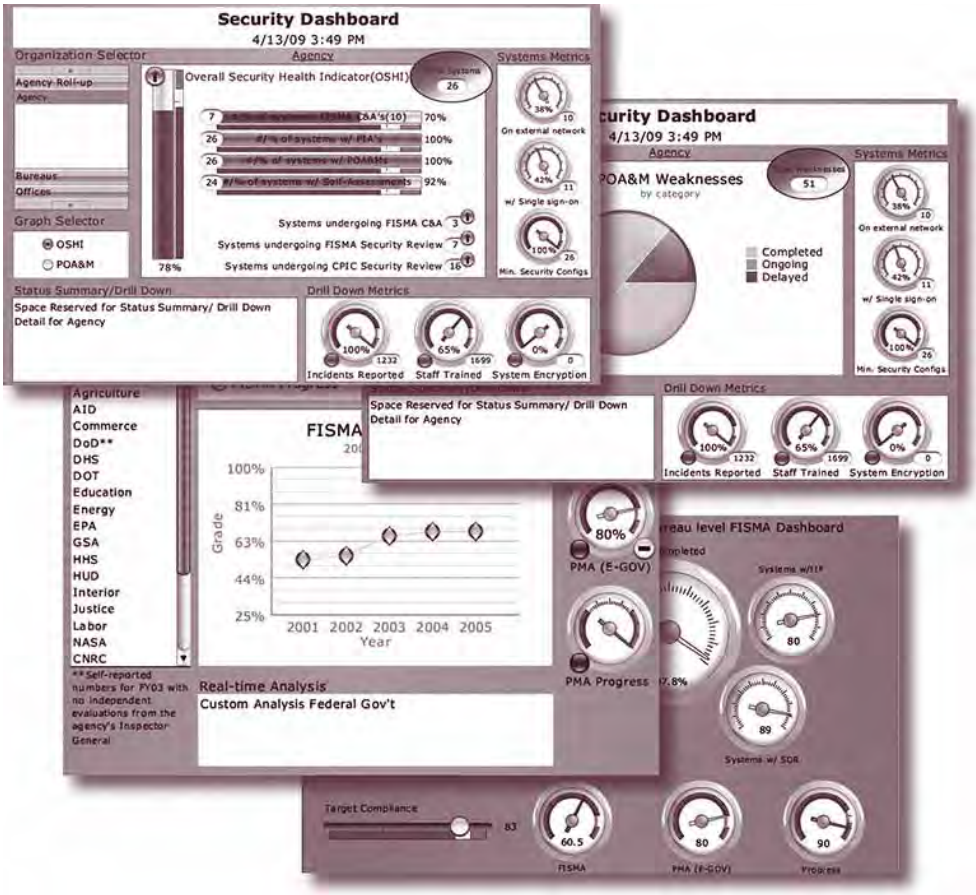
Robust security assessment and monitoring capabilities allow for greater access to data and more accurate reporting. Such capabilities provide the information necessary to populate security dashboards and other analytical tools. Mature programs have the capability to deliver these kinds of information, utilizing innovative and interactive security dashboards that can be published to multiple media formats in "near real-time."

As the organization works to improve/maintain its security performance, a customized dashboard, tailored to organizational concerns as well as to FISMA baselines, allows the identification of areas that require work, improving the ability to properly allocate resources. Flexible dashboard technology provides the ability to rapidly transform any data into meaningful, visually intuitive, and interactive business intelligence.

The initial status contained in the dashboard should include all of the required FISMA/Privacy Act compliance measures along with any available security data necessary to respond to any request for status on an as required basis.

Figure 8-1 is a sample of interactive security dashboards that can be used to visualize CS/IA measures. [168]

Figure 8-1 Security Dashboard Example [169]



References

166 Robert Ayoub, Frost & Sullivan. "Analysis of Business Driven Metrics: Measuring for Security Value," in *DM Review,* March 2006. Accessed 10 December 2008 at: *http://www.dmreview.com/white_papers/2290613-1.html* (requires online registration to download)

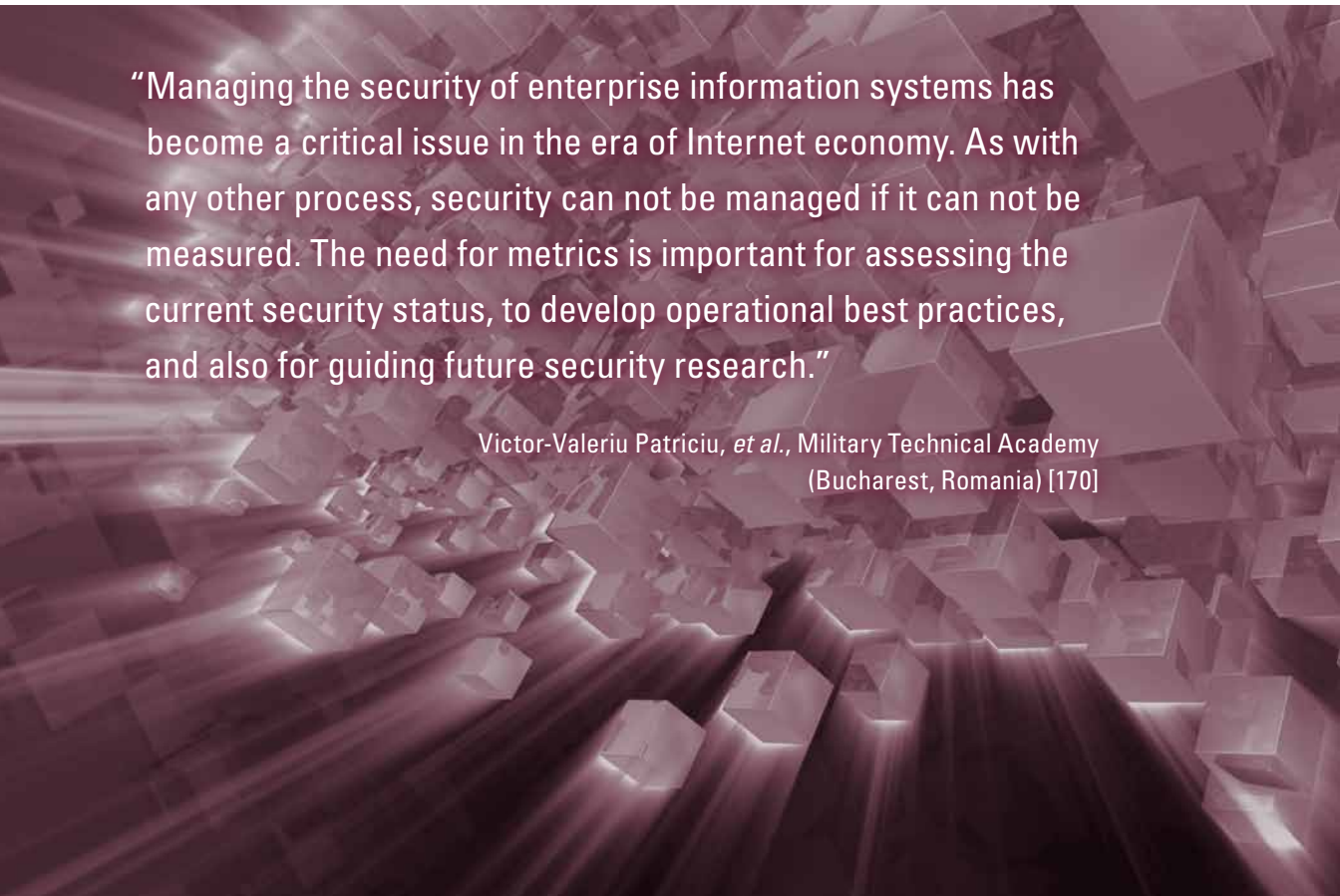
167 Ayoub, Frost & Sullivan. "Analysis of Business Driven Metrics: Measuring for Security Value," *op cit.*

168 Nadya Bartol and Brian Bates, Booz Allen Hamilton. "FISMA & beyond: Collection, analysis, and reporting on the status of information security at the executive level," in *Lessons Learned in Security Measurement,* 27 December 2008. Annual Computer Security Applications Conference (ACSAC), December 2008. Accessed 7 April 2009 at: *http://www.acsac.org/2008/program/case-studies/Bartol_Bates.pdf*

169 *Ibid.*

9

Recommendations



"Managing the security of enterprise information systems has become a critical issue in the era of Internet economy. As with any other process, security can not be managed if it can not be measured. The need for metrics is important for assessing the current security status, to develop operational best practices, and also for guiding future security research."

Victor-Valeriu Patriciu, *et al.*, Military Technical Academy (Bucharest, Romania) [170]

This section identifies common expectations that exist in the CS/IA stakeholder community regarding the value that CS/IA measures can provide. It also summarizes the gaps that were identified during the research conducted for this SOAR, and recommends several approaches for closing these gaps by either leveraging existing CS/IA measures techniques and approaches or through additional research.

9.1 Stakeholder Expectations

Authors of this report identified a number of stakeholder expectations that contribute to the mixed success of many CS/IA measurement efforts. These expectations center around the feasibility and expected value from CS/IA measurement efforts, based on the research conducted for this report and the authors' experience implementing CS/IA measures for multiple federal and commercial organizations. Understanding these expectations and moving forward in addressing the expectations can help organizations embarking on CS/IA measurement efforts achieve success.

Common stakeholder expectations that present challenges for successful CS/IA measurement efforts are illustrated in Table 9-1.

Table 9-1 Common CS/IA Measurement Stakeholder Expectations

Common Expectation	Associated Challenge
CS/IA measures are a finite effort that will be completed within a short time period.	CS/IA measures are most effective when they are a part of continual improvement efforts aimed at monitoring and improving IA status and posture long term. Short-term expectations are counterproductive to CS/IA measures success.
Data to support CS/IA measures exist in the form that is conducive to measurement; therefore, minimal investment is required to collect the data.	To be useful, data supporting CS/IA measures need to be identified, collected, stored, and leveraged for analysis in specific formats that are rarely available from existing data sources. Expectations of minimal changes to data collection and analysis processes will undermine the quality of data needed to support CS/IA measures and, therefore, undermine the ability of CS/IA measures to provide useful information for decision making.

Common Expectation	Associated Challenge
Setting unrealistic goals for CS/IA measures, such as identifying outcome measures when an organization does not have mature IA processes, and sufficient data to support outcome measures. "How soon will I see the return from CS/IA measures?" is a common stakeholder question.	The gap between stakeholder expectations and what can realistically be delivered creates adverse conditions for CS/IA measures success.
Desire to automate measures to become self-calculating too early in the life cycle of CS/IA measurement program.	"How soon can I automate my measurement process?" is a common question. Automating measurement to self-calculate too early in the life cycle can be a counterproductive activity until measures have been tested, and been proven to be reliable and successful. CS/IA measures need to be correctly designed with accurate data and thoroughly tested to trust the automated process to achieve the desired results.
Measures should help ensure the maximum ROI of CS/IA, and generate a timely return on their cost. Senior level executives typically want to leverage measures to measure ROI of their security programs.	A common hurdle in doing so is the lack of emphasis placed on the other foundational types of measures, such as implementation and efficiency/effectiveness. Measuring impact or outcome is not usually a simple calculation and requires a mature measurement program to be in place before these measures can be produced with a high degree of accuracy.

These expectations can be managed and overcome by educating organizations on the success factors for CS/IA measurement, and by focusing on small successes, progressing toward identified long-term objectives.

9.2 Success Factors

A number of success factors are critical for meeting stakeholder expectations on what CS/IA measurement efforts will deliver. Understanding the following expectations and moving forward in addressing the expectations can help organizations embarking on CS/IA measurement efforts achieve success—

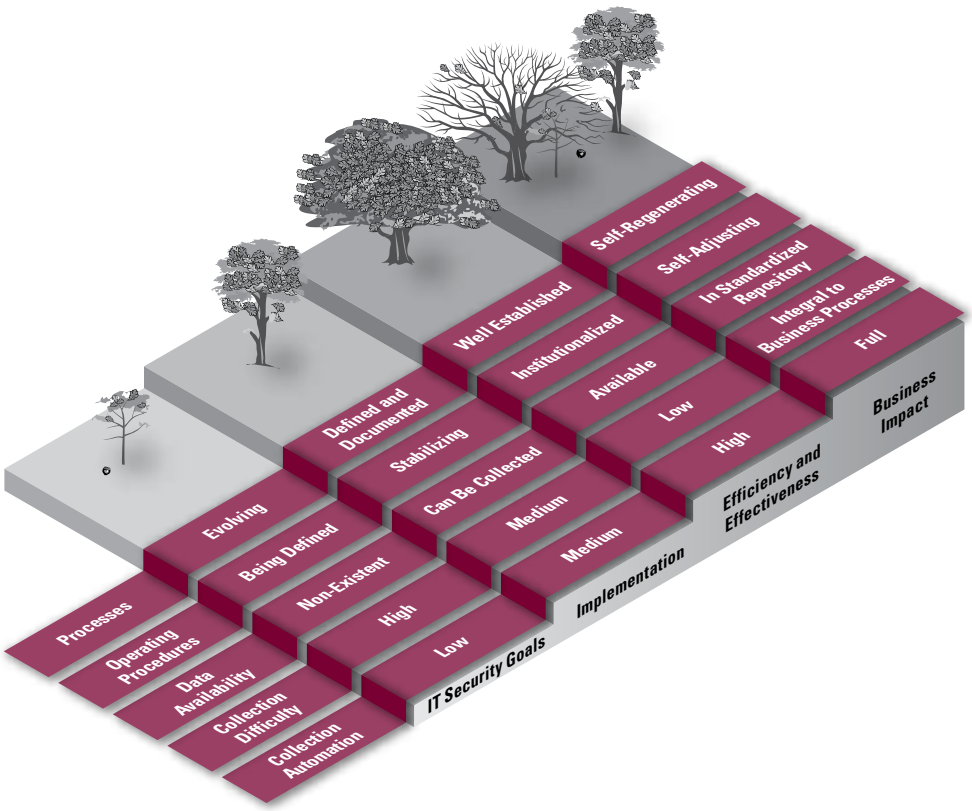
1. *Management commitment* is often the primary driver behind successful CS/IA measurement programs. Measurement programs have a higher rate of success when they are supported by a management commitment, combined with achievable expectations. As measurement programs are never "done," and are a critical component in organizations' efforts to improve information assurance, management commitment must be reaffirmed regularly to ensure continued success.
2. *Availability of solid data* is the second primary driver of successful CS/IA measurement programs. Without good data, measurement programs are unreliable and are not able to satisfy stakeholder expectations.
3. *Easy to use measures* that are easy to understand are a key success factor. Easy to use and understandable CS/IA measures require use of a common data collection, analysis, and reporting methodology; and the presence of aware and educated stakeholders who create, use,

and refine these measures. Complex and cumbersome measures are often created when the reality of how the measures will be used or calculated is not properly considered early in the CS/IA measures development process.

4. *Proactive and preventative measures* that can be used to predict the future are challenging, because most measurement data is based in the recent past. The ability to proactively determine a course of action of prevent adverse events, based on CS/IA measures, depends on the organization's ability to process and analyze CS/IA measurement data and extrapolate meaning.

Figure 9-1 shows the maturity path that should be followed to truly achieving the full benefits of CS/IA measurement.

Figure 9-1 Information Security Measurement Program Maturity Path [171]



9.3 Methodology Gaps

CS/IA measurement efforts could benefit by addressing the following gaps—

1. **Standardized set of minimum measures**—Adopting a minimum tailorable set of measures that should be used as a starting point for CS/IA measurement efforts. Standardized statistics, like those for major sports, could be applied for this purpose and would generate a new level of interest in CS/IA measurement. New measures can and would be added over time, but the core list of measures could remain fixed if created in a fashion to surmount technology changes.
2. **Number-driven risk measures "'fundamentally broken'"**—[172] As risk is an inherent and crucial component of CS/IA programs, this specific gap is thoroughly outlined in a recent article that described why numerical risk measures are no longer functioning as designed. Former National Cyber Security Division Director Amit Yoran is quoted in the article that—

   "'When you try to boil down complex network traffic into a traffic light or some number to present to management—which understands only traffic lights—you're driving organizations toward bad metrics versus the task at hand,' Yoran said. 'We're struggling to present number-driven metrics to people who struggle to understand all this complexity.'" [173]

   By having organizations refocus energy on measuring the impact of data loss, versus a singular focus on systems or infrastructure security, organizations will be able to understand the impact and value of personally identifiable data, intellectual property or other business critical data.
3. **Sustaining and maintaining CS/IA measurement efforts**—The sustainability of a CS/IA measurement program is typically linked to the organization's leadership. As long as a strong proponent of the program remains in charge, the CS/IA measurement program will be healthy. Maintenance is another aspect that can impact the health of measurement efforts. Stagnant measurement programs that are not refreshed on a continual basis are not operating at optimal performance. The CS/IA measurement maintenance plan should be documented as part of the organization's SOPs and/or performance management plan.
4. **Definitions and Vocabulary**—The CS/IA industry is moving toward consensus for what CS/IA measures mean, including a common set of definitions and vocabulary. However, more work needs to be done to increase the level of consensus and common understanding among CS/IA practitioners. Broad agreement to adopt existing standards

and definitions (*i.e.,* NIST SP 800-55 Rev.1, ISO/IEC 27004, DHS SwA Framework) would provide much-needed consistency among a variety of CS/IA measurement efforts.

5. **Combining existing approaches to create a solution**—A number of approaches and measurement methodologies described in this SOAR can be used to facilitate progress in CS/IA measurement. None of these approaches is complete, but many have merit. Exploring the combination of existing approaches with additional features that have not yet been identified could help advance the progress in solving the puzzle of CS/IA measurement, and would help the community improve the quality of existing and emerging CS/IA measures implementations. Achieving consensus regarding common definition and broad awareness of existing measurement methodologies and solutions is key for addressing this gap.
6. **Creating measures case studies that demonstrate how to roll up individual pieces of data into consistent executive-level measures**—ISO/IEC 15939 and ISO/IEC 27004 provide useful models for rolling up individual data points to compose indicators that can be described in plain English for a variety of audiences. Using these models for creating examples that pertain to hard questions that can be answered by measurement will provide help for many in the industry who do not know how to start their CS/IA measurement efforts, as well as articulate dependencies among CS/IA activities that impact CS/IA posture.

9.4 Technology Gaps

Bridging the technology gap is critical for achieving the next generation of stable CS/IA measures. Addressing the gaps discussed below would help improve the efficiency, effectiveness, and impact of CS/IA measures programs on improving CS/IA posture of systems and networks throughout the community—

1. **Real-time and/or self-healing measures**—Modern professionals thrive on instant feedback and immediate diagnostics. Providing real-time measures has been elusive in the CS/IA industry, except in heavily funded environments. “Self-healing” measures is a new term for measures that would cause an improvement action to be performed automatically, based on the current or projected value registered by an automated tool.
2. **Improving commonality of data formats provided by the COTS vendors**—Encouraging the industry to design and sell commercial products that collect and compile data in standard formats would be conducive to the creation and comparison of measures originating from different systems and organizations. Such solutions would facilitate flexible reporting that would provide CISA practitioners

increasingly useful insight into the state of systems and networks. The US Government and industry are moving in this direction through the SCAP program and other efforts. Further research as well as incentives are required to facilitate success in this area.

3. **Investing in data modeling of CS/IA measures and measurable outcomes associated with CS/IA activities**—Few organizations have sufficient resources to invest in long-term projects to test cause and effect theories about CS/IA that can be proven through measurement. For example, it appears that, after IA training, users would be more diligent in selecting better passwords (*i.e.,* passwords that comply with the password policy and are more difficult to crack with a password cracker). Correlating the data from awareness training statistics, help desk calls, and password-cracking tools could prove or disprove this hypothesis. Many similar hypothesis require modeling to demonstrate what really works and what does not.

9.5 Knowledge Base Gaps

A number of actions that could help bridge the gaps listed in the previous three sections are focused on increasing the knowledge base of CS/IA measurement practitioners by—

1. **Leveraging measurement expertise and lessons learned from other industries**—Common expectations, challenges, and success factors, articulated in Sections 9.1 and 9.2, are not unique to the CS/IA industry. While many challenges are specific to CS/IA, many are of an organizational nature. Measurement experts in other industries have successfully managed and overcome many of these challenges. Knowledge that exists within other industries can increase the cost-effectiveness and success rate of CS/IA measurement efforts.
2. **Creating a skilled/trained labor force dedicated to CS/IA measures**—Building the CS/IA measurement knowledge base and resource pool is critical to the success of CS/IA measurement efforts. The current workforce is knowledgeable about IA or about measurement, but it is rare that both skill sets are present. Investing in training IA practitioners in measurement methods and techniques would increase cost-effectiveness and success ratio of current and future CS/IA measurement efforts.

References

170 Victor-Valeriu Patriciu, Iustin Priescu, and Sebastian Nicolaescu. "Security Metrics for Enterprise Information Systems," in *Journal of Applied Quantitative Methods (JAQM),* Vol. 1, No. 2, Winter 2006. Accessed 6 January 2009 at: *http://jaqm.ro/issues/volume-1,issue-2/pdfs/patriciu_priescu_nicolaescu.pdf*

171 Chew, *et al. Performance Measurement Guide for Information Security, op cit.*

172 Michael S. Mimoso, Editor. "Number-driven risk metrics 'fundamentally broken'," in *Information Security,* 12 March 2009. Accessed March 26, 2009 at: *http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1350658,00.html#*

173 *Ibid.*

A

Abbreviations, Acronyms, and Definitions

Acronym	Definition
ACSAC	Annual Computer Security Applications Conference
ActSec	Actual Security
AES	Advanced Encryption Standard
AFCA	Air Force Communication Agency
AFIT	Air Force Information Technology
AG	Attack Group
ALE	Annualized Loss Expectancy
AMBER	Assessing, Measuring, and Benchmarking Resilience
AmI	Ambient Intelligence
ANSI	American National Standards Institute
ARO	Annualized Rate of Occurrence
ARO	Army Research Office
ARR	Attack Relevance Rating
AS&W	Attack Sensing and Warning
ASVS	Application Security Verification Standard
AT/SPI	Anti-Tamper/Software Protection Initiative
ATO	Authorization to Operate
BAR	Business Adjusted Risk
BJS	Bureau of Justice Statistics
BOF	Birds of a Feather

BRM	Business Reference Model
C&A	Certification and Accreditation
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CCE	Common Configurations Enumeration
CCSS	Common Configurations Scoring System
CHACS	Center for High Assurance Computer Systems
CI/KR	Critical Infrastructure and Key Resources
CCTL	Common Criteria Testing Laboratories
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CIS	Center for Internet Security
CISO	Chief Information Security Officer
CISWG	Corporate Information Security Working Group
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CMM	Capability Maturity Models
CMMI	Capability Maturity Model Integration
CMSS	Common Misuse Scoring System
CMU	Carnegie Mellon University
CMVP	Cryptographic Module Validation Program
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
CNO	Computer Network Operations
CNRS-LAAS	Université de Toulouse Centre Nationale de la Recherche Scientifique Laboratoire d'Analyse et d'Architecture Systemès
COTS	Commercial Off the Shelf
CPE	Common Platform Enumeration
CR/TA	Critical Review/Technology Assessment
CS/IA	Cyber Security and Information Assurance
CSIS	Center for Secure Information Systems
CSO	Chief Security Officer
CSR	Critical Security Rating
CSS	Computer Security Survey
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerabilities Common Scoring System
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
DARPA	Defense Advanced Research Projects Agency
DEPEND	Design and Validation of Reliable Networked Systems
DESEREC	Dependability and Security by Enhanced ReConfigurability
DHS	Department of Homeland
DIACAP	Defense Information Assurance Certification and Accreditation Process

DIAP	Defense-wide Information Assurance Program
D-IART	Defense-Information Assurance Red Team
DISA	Defense Information Systems Agency
DITSCAP	Defense Technology Security Certification and Accreditation
DLA	Defense Logistics Agency
DoD	Department of Defense
DON	Department of Navy
DON CIO	Department of Navy Chief Information Officer
DREAD	Damage potential, Reproducibility, Exploitability, Affected users, Discoverability
DRM	Data Reference Model
DRM	Digital Rights Management
DSS	Data Security Standard
DTIC	Defense Technical Information Center
EAL	Evaluation Assurance Levels
ENST	Telecom ParisTech
EPRI	Electric Power Research Institute
ERIM	Erasmus Research Institute of Management
ESOPE	Evaluation de la Sécurité Operationnelle
ESM	Evaluator's Scoring Metrics
EU	European Union
FAQ	Frequently Asked Questions
FBI	Federal Bureau of Investigation
FCD	Final Committee Draft
FDCC	Federal Desktop Common Configuration
FEA	Federal Enterprise Architecture
FIPS	Federal Information Processing Standard
FIRST	Forum of Incident Response and Security Teams
FISMA	Federal Information Security Management Act
FITSAF	Federal Information Technology Security Assessment Framework
FWP	Sixth Framework Program
FWP7	Seventh Framework Program
GIAP	GIG IA Portfolio program
GMU	George Mason University
GNOSC	Global Network Operation and Security Center
GOTS	Government Off the Shelf
GP	Generic Practices
GPRA	Government Performance Results Act
GQIM	Goal, Question, Indicator, Methodology
HIPAA	Health Insurance Portability and Accountability Act
I3P	Institute for Information Infrastructure Protection

IA	Information Assurance
IA-CMM	IA Capability Maturity Model
IAM	INFOSEC Assessment Methodology
IASET	Information Assurance Science and Engineering Tools
IASM	Information Assurance and Security Management
IATAC	Information Assurance Technical Analysis Center
IATRP	INFOSEC Assurance Training and Rating Program
IAVA	Information Assurance Vulnerability Alert
ICT	Information and Community Technologies
IDART	Information Design Assurance Red Team
IDS	Intrusion Detection Systems
IEC	International Electrotechnical Commission
IG	Inspector General
INFOSEC	Information Security
INFRES	Institut TELECOM Computer Science and Networking Department
IORTA	Information Operational Red Team Assessment
IPS	Intrusion Protection Systems
IRC	Information Security Research Council
ISA	International Society of Automation
ISECOM	Institute for Security and Open Methodologies
ISMS	Information Security Management Systems
ISO	International Organization for Standardization
ISOT	Information Security and Object Technology
ISP	Internet Service Provider
ISSA	Information Systems Security Association
ISSEA	International System Security Engineering Association
ISSRR	Information Security System Rating and Ranking
IT	Information Technology
ITSEC	Information Technology Security Evaluation Criteria
ITUA	Intrusion Tolerance by Unpredictable Adaption
JCIAC	Joint Council on Information Age Crime
JMRR	Joint Monthly Readiness Reports
JPL	Jet Propulsion Laboratory
JQRR	Joint Quarterly Readiness Reports
KGI	Key Goal Indicators
KPI	Key Performance Indicators
JTF-GNO	Joint Task Force Global Network Operations
LC	Loss Controls
LOE	Level of Effort
McDiD	Metrics and Controls for Defense-in-Depth
MAIS	Major Automated Information Systems
MDAP	Major Defense Acquisition Programs

METF	Mean Effort to Security Failure
MHS	Military Health System
MOA	Memorandum of Agreement
MSRAM	Maritime Security Risk Analysis Model
MTBF	Mean Time-Between-Failure
MTTR	Mean Time-to-Repair
NASA	National Aeronautics and Space Administration
NCSD	National Cyber Security Division
NCSS	National Computer Security Survey
NDIA	National Defense Industrial Association
NII	Network and Information Integration
NIPP	National Infrastructure Protection Program
NIST	National Institute of Standards and Technology
NMCI	Navy Marine Corps Internet
NRL	Naval Research Laboratory
NSA	National Security Agency
NSF	National Science Foundation
NSTAC	National Security Telecommunications Advisory Committee
NVD	National Vulnerabilities Database
OASD	Office of the Assistant Secretary of Defense
OECD	Organization for Economic Cooperation and Development in Europe
OJP	Office of Justice Programs
OMB	Office of Management and Budget
OpSec	Operational Security
OSD	Office of the Secretary of Defense
OSSTMM	Open Source Security Testing Methodology Manual
OVAL	Open Vulnerability and Assessment Language
OVAL-ID	Open Vulnerability and Assessment Language Identifier
OWASP	Open Web Application Security Project
PA	Process Areas
PEPA	Performance Evaluation Process Algebra
PERFORM	Performability Engineering Research Group
PLA	Protection Level Agreements
POA&M	Plan of Action and Milestones
PP	Protection Profile
PRM	Performance Reference Model
PSM	Practical Software and Systems Measurement Support Center
QoS	Quality of Service
QUERIES	Quantitative Evaluation of Risk for Investment Efficient Strategies
RAI	Resiliency Assurance Index

RASQ	Relative Attack Surface Quotient
RAV	Risk Assessment Value
R&D	Research and Development
RDX	R&D Exchange
ReSIST	Resilience for Survivability in IST
ROI	Return on Investment
ROSI	Return on Security Investment
RTWF	Red Team Work Factor
SAMATE	Software Assurance Metrics and Tool Evaluation
SANS	SysAdmin, Audit, Network, Security
SCADA	Supervisory Control and Data Acquisition
SCAP	Secure Content Automation Protocol
SCARE	Source Code Analysis Risk Evaluation
SDLC	Software Development Life Cycle
SEAS	Structured Evidential Argumentation System
SecLab	Security Lab
SecMet	Security Metrics Consortium
SEPG	Software Engineering Process Group
SERENITY	System Engineering for Security and Dependability
SG	Security Group
SIG	Special Interest Groups
SLA	Service Level Agreement
SLE	Single Loss Expectancy
SM	Security Management
SOAR	State of the Art Report
SOP	Standard Operational Procedures
SP	Special Publication
SPMO	Security Project Management Officers
SPP	Security and Privacy Profile
SQUALE	Security, Safety, and Quality Evaluation for Dependable Systems
SRD	SAMATE Reference Dataset
SRM	Service-Component Reference Model
SSAA	System Security Authorization Agreement
SSE CMM	System Security Engineering Capability Maturity Model
S&T	Science and Technology
ST	Security Target
ST&E	Security Test and Evaluation
STEM	Security Testing and Engineering Using Metrics
S-Vector	Scoring Vector
SwA	Software Assurance (SwA)
TA	Technical Alerts
TAF	Trusted Agent FISMA

TCSEC	Trusted Computer System Evaluation Criteria
TMA	TRICARE Management Activity
T-MAP	Threat Modeling framework based on Attack Path Analysis
TOE	Target of Evaluation
TRM	Technology Reference Model
TSABI	Top Secret and Below Information
TSF	Tolérance aux Fautes et Sûreté de Fonctionnement Informatique
TTOA	Technical Target of Assessment
UK	United Kingdom
UML	Unified Modeling Language
USAF	United States Air Force
US-CERT	United States Computer Emergency Response Team
USMC/MCNOSC	United States Marine Corps/Marine Corps Network Operations and Security Command
USSTRATCOM/ JTF-GNO	United States Strategic Command/Joint Task Force Global Network Operations
VA/RM	Vulnerability Assessment/Risk Management
VFT	Value-Focused Thinking
VMS	Vulnerability Management System
VPN	Virtual Private Network
VTT	Valtion Teknillinen Tutkimuskeskus
WISSSR	Workshop on Information Security System Scoring and Ranking
WG	Working Group
XCCDF	Extensible Configuration Checklist Description Format
YTD	Year to Date

B

Resources

B.1 Materials Used in Developing this SOAR

M.S. Ahmed, E. Al-Shaer, L. Khan. "A Novel Quantitative Approach For Measuring Network Security, INFOCOM 2008," in *The 27th Conference on Computer Communications. IEEE*, April 2008 Page(s): 1957 – 1965, Digital Object Identifier 10.1109/INFOCOM.2008.260.

Aladdin Knowledge Systems Ltd. "Attack Intelligence Research Center: Security Statistics." Accessed 7 April 2009 at: http://www.aladdin.com/airc/security-statistics.aspx

Dave Aland, Johns Hopkins APL (supporting OSD DOT&E Deputy Director of Naval and C4ISR Systems). "Metrics Lessons Learned from Conducting Operational Assessments of Networks," in *Proceedings of the MORS Workshop on Transforming IA for Netcentric Operations: Providing Assured Information for National Security*, Laurel, Maryland, March 2007. Accessed 10 December 2008 at: http://www.mors.org/meetings/2007_tia/pres/aland.pdf

John I. Alger. "On Assurance, Measures, and Metrics: Definitions and Approaches," in *Proceedings of the Workshop on Information Security System Scoring and Ranking Information System Security Attribute Quantification or Ordering (commonly but improperly known as Security Metrics)*, Williamsburg, Virginia, 21-23 May 2001 (commonly referred to as the Workshop on Information Security System Scoring and Ranking [WISSRR]). Accessed 8 April 2009 at: http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf

Ross Anderson, University of Cambridge Computer Laboratory. "Economics and Security Resource Page." Accessed 26 March 2009 at: http://www.cl.cam.ac.uk/~rja14/econsec.html

Applied Computer Security Associates and The MITRE Corporation. *Proceedings of the Workshop on Information Security System Scoring and Ranking Information System Security Attribute Quantification or Ordering (Commonly but improperly known as "Security Metrics")*, Williamsburg, Virginia, 21-23 May 2001 (commonly referred to as the Workshop on Information Security System Scoring and Ranking [WISSRR]). Accessed 8 April 2009 at: http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf

Army Global Network Operations and Security Center (GNOSC). Accessed 7 April 2009 at: https://gnosc.army.mil

Ashish Aroral, Dennis Hall, C. Ariel Pinto, Dwayne Ramsey, and Rahul Telang, Lawrence Berkeley National Laboratory. *An ounce of prevention vs. a pound of cure: how can we measure the value of IT security solutions*. Paper LBNL-54549, November 2004. Accessed 26 March 2009 at: http://repositories.cdlib.org/lbnl/LBNL-54549

-also-

13 April 2009 at: http://www.courant.nyu.edu/ComplexSystems/literature/Arora,etal.pdf

Robert Ayoub, Frost & Sullivan. "Analysis of Business Driven Metrics: Measuring for Security Value," in *DM Review*, March 2006. Accessed 10 December 2008 at: http://www.dmreview.com/white_papers/2290613-1.html (requires online registration to download)

Nadya Bartol, Booz Allen Hamilton. "IA Metrics—Why and How to Measure Goodness of Information Assurance." Presented to ISSEA Ninth Annual PSM Users' Group Conference: Measurement in Support of System and Process Integrity, Keystone, Colorado, 18-22 July 2005. Accessed 29 December 2008 at: http://www.psmsc.com/UG2005/Presentations/15_Bartol_IA_Metrics.pdf

Nadya Bartol and Brian Bates, Booz Allen Hamilton. "FISMA and beyond: Collection, analysis, and reporting on the status of information security at the executive level," *in Proceedings of the 24th Annual Computer Security Applications Conference (ACSAC 24)*, Anaheim, California, 27 December 2008. Accessed 7 April 2009 at: http://www.acsac.org/2008/program/case-studies/Bartol_Bates.pdf

Nadya Bartol and Joyce Richardson. "Measuring Capability-Based Assurance," in *Proceedings of the Fifth Annual Information System Security Engineering Association (ISSEA) Conference*, Arlington, Virginia, 13-15 October 2004

Lawrence E. Bassham III., NIST Information Technology Laboratory Computer Security Division. "Advanced Encryption Standard Algorithm Evaluation Suite (AESAVS)." 15 November 2002. Accessed 4 February 2009 at: http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf

Jennifer L. Bayuk. "Information Security Metrics: An Audited-based Approach." NIST and CSSPAB Workshop, Washington, D.C., 14 June 2000.

Steven M. Bellovin, Columbia University. "On the Brittleness of Software and the Infeasibility of Security Metrics." Keynote presentation at Metricon 1.0, Vancouver, BC, Canada, 1 August 2006 (slides revised 21 November 2006). Accessed 10 December 2008 at: http://www.cs.columbia.edu/~smb/talks/brittle-metricon.pdf

-also-

Original version, accessed 7 January 2009 at: http://www.securitymetrics.org/content/Wiki.jsp?page=Metricon1.0Keynote#section-Metricon1.0Keynote-OnTheBrittlenessOfSoftwareAndTheInfeasibilityOfSecurityMetricsStevenBellovinColumbiaUniversity

Scott Berinato. "A Few Good Metrics," in *CSO Magazine*, 1 July 2005. Accessed 13 April 2009 at: http://www.csoonline.com/article/220462/A_Few_Good_Information_Security_Metrics

Paul Bicknell. "Security Assertions, Criteria and Metrics Developed for the IRS," MITRE Technical Report, May 2001. Accessed 13 April 2009 at: http://www.mitre.org/work/tech_papers/tech_papers_01/bicknell_security/index.html

D.J. Bodeau, "Information assurance assessment: Lessons-learned and challenges," in *Proceedings of the 1st Workshop on Information-Security-System Rating and Ranking (WISSSR)*, Williamsburg, Virginia, 21-23 May 2001. Full proceedings accessed 13 April 2009 at: http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf

BNET Business Wire. "CIOview Delivers SecurityNOW!: Provides Financial Transparency for IT Security; Increases Security Auditor Productivity 90%," 14 September 2004. Accessed 30 January 2009 at: http://findarticles.com/p/articles/mi_m0EIN/is_/ai_n6193303

Pauline Bowen, Joan Hash, and Mark Wilson. NIST Special Publication 800-100, *Information Security Handbook: A Guide for Managers*, October 2006. Accessed 13 April 2009 at: http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

W. Krag Brotby, IT Governance Institute. *Information Security Governance: Guidance for Boards of Directors and Executive Management*, 2nd Edition. (Rolling Meadows, Ilinois: ISACA, 2006).

Adam R. Bryant, Capt. USAF. *Developing a Framework for Evaluating Organizational Information Assurance Metrics Programs.* Master of Science Thesis for Air Force Institute of Technology. AFIT/GIR/ENV/07-M5, March 2007. Accessed 11 December 2008 at: https://www.afresearch.org/skins/rims/q_mod_be0e99f3-fc56-4ccb-8dfe-670c0822a153/q_act_downloadpaper/q_obj_217f0dc1-baf2-47c8-a458-60956d23bc05/display.aspx?rs=enginespage

Peter Burris and Chris King. "A Few Good Security Metrics." METAGroup, Inc. audio, 11 Oct. 2000. URL: http://www.metagroup.com/metaview/mv0314/mv0314.html (10 July 2001).

Christian Byrnes, Gartner Group. "Security Metrics." Podcast of presentation made to Gartner IT Security Summit, 4-6 June 2007.

Linda Tracy, Jamie K. Guevara, Oliver Harcourt, and Eric Stegman, The Gartner Group. *IT Key Metrics Data 2008: Key Information Security Measures: Spending & Staffing Excluding Disaster Recovery*, 10 December 2007.

George K Campbell. "Measures and Metrics in Corporate Security: Communicating Business Value." CSO Executive Council, 2006. Accessed 13 April 2009 at: https://www.csoexecutivecouncil.com/content/Metrics_Mini_Update_060706.pdf

Katherine Campbell, Lawrence A. Gordon, Martin P. Loeb, and Lei Zhou. "The economic cost of publicly announced information security breaches: empirical evidence from the stock market," in *Journal of Computer Security Archive*, Volume 11 Issue 3, March 2003, pp. 431-448.

CDT. "Evaluating DRM: Building a Marketplace for the Convergent World," Version 1.0, September 2006. Accessed 19 January 2009 at: http://www.cdt.org/copyright/20060907drm.pdf

David A. Chapin and Steven Akridge. "How Can Security be Measured?," in *Information Systems Control Journal,* Volume 2, 2005. http://www.isaca.org/Template.cfm?Section= Home&Template=/ContentManagement/ContentDisplay.cfm&ContentID=24173. Also: http://www.isaca.org/Content/ContentGroups/Journal1/20058/How_Can_Security_Be_Measured_.htm

Hao Chen, Drew Dean, and David Wagner. "Model checking one million lines of C code," in *Proceedings of the 11th Annual Network and Distributed System Security Symposium*, 2004, pp. 171—185. Accessed 7 April 2009 at: http://www.cs.ucdavis.edu/~hchen/paper/ndss04.pdf

Michael Chertoff, DHS Secretary. Speech at the George Washington University Homeland Security Policy Institute, 16 March 2005. Accessed 7 April 2009 at: http://www.dhs.gov/xnews/speeches/speech_0245.shtm

Elizabeth Chew, Marianne Swanson, Kevin Stine, Nadya Bartol, Anthony Brown, and Will Robinson. NIST SP 800-55 Rev. 1, *Performance Measurement Guide for Information Security*, July 2008. Accessed 13 April 2009 at: http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf

CIS. *The CIS Security Metrics*, May 2009.

K. Clark, J. Dawkins, and J. Hale. "Security Risk Metrics: Fusing Enterprise Objectives and Vulnerabilities," in *Proceedings of the 2005 IEEE Workshop on Information Assurance and Security*, West Point, New York, 2005. Digital Object Identifier: 10.1109/IAW.2005.1495978.

CIO Council, Federal Information Architecture Program Management Office. *FEA Security and Privacy Profil*e, Version 2.0, 1 June 2006. Accessed 9 April 2009 at: http://www.cio.gov/documents/Security_and_Privacy_Profile_v2.pdf

Vivian A. Cocca, OSD(NII). "DoD's Approach to IA Metrics." Presented at PSM Technical Working Group meeting, 23 March 2005. Accessed 28 December 2008 at: http://www.psmsc.com/Downloads/TWGMarch05/05_Cocca_DoD_Metrics_Initiative.pdf

Center for Internet Security (CIS). "Security Metrics Initiative." Accessed 13 April 2009 at: http://members.cisecurity.org/kb/category.php?id=24

CIS. *The CIS Security Metrics*, April 2009.

ComputerWorld Security Knowledge Center. "Security Statistics," 9 July 2001. Accessed 7 April 2009 at: http://www.computerworld.com/securitytopics/security/story/0,10801,62002,00.html

Corporate Information Security Working Group. "Report of the Best Practices and Metrics Team," 17 November 2004 (Revised 10 January 2005). Accessed 3 February 2009 at: http://infotech.aicpa.org/NR/rdonlyres/9C87179C-7F68-4EA0-8FA6-1B8A2EF2768A/0/CISWG_Report_of_best_practices_and_metrics_teams.pdf (also at: http://educause.edu/ir/library/pdf/CSD3661.pdf)

James P. Craft. "Metrics and the USAID Model Information Systems Security Program." NIST and CSSPAB Workshop, Washington, DC, 14 June 2000.

CSO. "The Security Metrics Collection," Security Leadership. 27 October 2008. Accessed 13 April 2009 at: http://www.csoonline.com/article/455463/The_Security_Metrics_Collection

Department of Public Safety and Emergency Preparedness Canada. "Information Assurance Metrics for Security, QoS, and Availability," in *Proceedings of the Second Annual Conference on Privacy, Security, Trust*, New Brunswick, Canada, 13-15 October 2004. Accessed 11 December 2008 at: http://dev.hil.unb.ca/Texts/PST/pdf/seddigh.pdf

DHS. "Guidance for Developing Sector-Specific Plans as input to the National Infrastructure Protection Plan," 2 April 2004. Accessed 4 February 2009 at: http://cees.tamiu.edu/covertheborder/TOOLS/SSAGuidance.pdf

Department of the Navy Chief Information Officer blog. Accessed 1 April 2009 at: http://www.doncio.navy.mil/tagresults.aspx?ID=28

Dreamland Technologies. "OSSTMM: measurable security." Corporate brochure. Accessed 30 January 2009 at: http://www.dreamlab.net/download/documents/dlt_OSSTMM_engl.pdf

Cezar Drugescu and Rafael Etges. "Maximizing the Return on Investment of Information Security Programs: Program Governance and Metrics," in *Information Systems Security Journal*, December 2006. Accessed 13 April 2009 at: http://www.ist-llc.com/joomla/pdfs/industry-articles/information-security-roi.pdf

Irene Eusgeld, Felix C. Freiling, and Ralf Reussner, Editors. *Dependability Metrics: Advanced Lectures* (specifically: Introduction to Section III, "Security Metrics"). (Berlin/Heidelberg, Germany: Springer-Verlag, 2008).

Karen Evans, OMB. Testimony on FISMA Reporting before the Committee on Government Reform, Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, 16 March 2004. Accessed 22 January 2009 at: http://www.whitehouse.gov/omb/assets/omb/legislative/testimony/evans/karen_evans031604.pdf

S. Evans, S. Bush, and J. Hershey. "Information Assurance through Kolmogorov Complexity," in *Proceedings of the DARPA Information Survivability Conference and Exposition II (DISCEX-II-2001)*, Anaheim, California, 12-14 June 2001. Accessed 13 April 2009 at: http://www.research.ge.com/~bushsf/ia/discex.pdf

Glenn Fink and Brett Chappell, Naval Sea Systems Command (NAVSEA) Information Transfer Technology (ITT) Group, B30 Combat Systems Technology Division. "A Metrics-Based Approach to Intrusion Detection System Evaluation for Distributed Real-Time Systems." Accessed 8 February 2009 at: http://people.cs.vt.edu/~finkga/ids/IDS-Briefing-09Apr02.ppt

Federal Information Security Management Act of 2002 (FISMA), 44 USC. § 3541, et seq., enacted as Title III of the E-Government Act of 2002 (Pub.L. 107-347, 116 Stat. 2899). Accessed 13 April 2009 at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

Diane Frank. "Agencies Seek Security Metrics," in *Federal Computer Week*. 19 June 2000. URL: http://www.fcw.com/article70756 (16 June 2006).

Felix C. Freiling. "Introduction to Security Metrics," in *Dependability Metrics* (Lecture Notes in *Computer Science*, Volume 4909/2008), pp. 129-132 (Berlin/Heidelberg, Germany: Springer-Verlag, 2008). Digital Object Identifier: 10.1007/978-3-540-68947-8

Daniel E Geer. "Measuring Security," Version 2.1:16x07. Accessed 30 January 2009 at: http://geer.tinho.net/measuringsecurity.tutorial.pdf

Daniel Geer, Kevin Soo Hoo, and Andrew Jaquith. "Information security: Why the future belongs to the quants," in *IEEE Security and Privacy*, Volume 1 Issue 4, July/August 2003, pp. 24-32. Digital Object Identifier: 10.1109/MSECP.2003.1219053

Larry Gordon, Ph.D. University of Maryland. "Empirical Research Related to Economic Aspects of Cyber/Information Security." Accessed 15 April 2009 at: http://www.rhsmith.umd.edu/faculty/lgordon/cybersecurity/Gordon,%20Slides%20for%20Panel%20Presentation%20on%20Empirical%20Research%20at%20WESII,%20October%202006.ppt

Kelly J. Harris and Todd G. Shipley, SEARCH, The National Consortium for Justice Information and Statistics (for the US Department of Justice Office of Community Oriented Policing Services). *Law Enforcement Tech Guide for Information Technology Security* (specifically, Chapter 6, "Phase IV - Measure Your Security Controls"), 2006. Accessed 13 April 2009 at: http://www.cops.usdoj.gov/files/RIC/Publications/e01071252_itsecurity.pdf

Todd Heberlein, Senthil Ebina, Melissa Danforth, and Tye Stallard, University of California at Davis. *Attack Graphs: Identifying Critical Vulnerabilities within An Organization*. Seminar presented by University of California-Davis Computer Security Lab, 10 March 2004. Accessed 6 February 2009 at: http://seclab.cs.ucdavis.edu/seminars/AttackGraphs.pdf

Arthur Hecker, TELECOMParisTech (ENST). "On System Security Metrics and the Definition Approaches," in *Proceedings of the Second International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE '08)*, Cap Esterel, France, 23-31 August 2008, pp.412-419. DOI Bookmark: http://doi.ieeecomputersociety.org/10.1109/SECURWARE.2008.37

Debra S. Hermann, US Nuclear Regulatory Commission. *Complete Guide to Security and Privacy Metrics* (Boca Raton, Florida: Auerbach Publications, 2007).

S.O.S. Herrera. "Information security management metrics development," in *Proceedings of the 39th Annual 2005 International Carnahan Conference on Security Technology (CCST '05)*, 11-14 October 2005, pp. 51-56 Digital Object Identifier: 10.1109/CCST.2005.1594818

Pete Herzog, ISECOM. "Calculating Risk Assessment Values." ISECOM Whitepaper. Accessed 29 January 2009 at: http://isecom.securenetltd.com/RAVs.pdf

Gary Hinson, IsecT Ltd. "Seven myths about information security metrics," in *ISSA Journal*, July 2006. Accessed 13 April 2009 at: http://www.noticebored.com/IsecT_paper_on_7_myths_of_infosec_metrics.pdf

Christofer Hoff, Rational Security. "Take5 (Episode #6) - Five Questions for Andy Jaquith, Yankee Group Analyst and Metrician...." Rational Survivability Blog, 13 September 2007. Accessed 29 January 2009 at: http://rationalsecurity.typepad.com/blog/2007/09/take5-episode-6.html

Michael Howard. "Attack Surface: Mitigate Security Risks by Minimizing the Code You Expose to Untrusted Users," in *MSDN Magazine*, November 2004. Accessed 30 January 2009 at: http://msdn.microsoft.com/en-us/magazine/cc163882.aspx

Robert Hudock. "Why Security Metrics Must Replace Traditional Risk Analysis Methodologies," in *Computer Security Law*, 6 March 2008. Accessed 19 January 2009 at: http://computersecuritylaw.us/2008/03/06/why-security-metrics-must-replace-traditional-risk-analysis-methodologies.aspx

A. Hunstad, J. Halberg, and R. Andersson, "Measuring IT security—a method based on common criteria's security functional requirements," in *Proceedings of the Fifth IEEE Systems, Man and Cybernetics (SMC) Information Assurance Workshop*, West Point, New York, 9-14 June 2004, pp. 226-233. Digital Object Identifier: 10.1109/IAW.2004.1437821

IATAC. *IAnewsletter*, Volume 7 Number 3, Winter 2004. Accessed 2 February 2006 at: http://iac.dtic.mil/iatac/IA_newsletter.html

IATAC. *IA Metrics* Critical Review and Technology Assessment (CR/TA) Report, 2000. May be requested from .mil and .gov domains at: http://iac.dtic.mil/iatac/reports.jsp#CR/TA

IATAC. *State-of-the-Art Report (SOAR): Software Security Assurance*, 31 July 2007. Accessed 1 April 2009 at: http://iac.dtic.mil/iatac/download/security.pdf

INFOSEC Assurance Training and Rating Program. "INFOSEC Vulnerabilities Technical and Non-Technical Solutions." Accessed 8 February 2009 at: http://www.iatrp.com/infosec.php

Information Technology Association of America. Federal Information Security Resources. Accessed 13 April 2009 at: http://www.itaa.org/policy/infosec/policy.cfm?ID=86.

ISACA. Accessed 10 February 2009 at: www.isaca.org

ISECOM. *Open Source Security Testing Methodology Manual (OSSTMM).* Accessed 2 April 2009 at: http://www.isecom.org/osstmm/

ISO/IEC 15408-1:2005(E), *Information technology – Security techniques – Evaluation criteria for IT Security.* May be downloaded at no cost from the Common Criteria Portal at: http://www.commoncriteriaportal.org/thecc.html (accessed 10 February 2009).

ISO/IEC 21827:2008, *Information technology – Systems security engineering – Capability Maturity Model Capability Maturity Model*® (SSE-CMM®). Accessed 1 April 2009 at: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44716

ISSA, UK Chapter IT Advisory. "Is Security Awareness Wasted on End Users?" 13 March 2008, pg. 12. Accessed 29 January 2009 at: http://www.issa-uk.org/downloads/Security%2520awareness%2520presentation.pdf

Andrew Jaquith. *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. (Indianapolis, IN: Addison-Wesley Professional, 2007).

JCIAC. "Computer-Related Crime Impact: Measuring the Incidence and Cost." White Paper, January 2004. Accessed 25 March 2009 at: http://www.jciac.org/JCIAC%20docs/Computer-Related%20Crime%20 Impact%20010904.pdf

Joe Jarzombek, Director for Software Assurance, National Cyber Security Division, DHS. "Considerations in Advancing the National Strategy in Cyberspace." Presentation at DHS Software Assurance Measurement Workshop, 18 July 2006. Accessed 13 April 2009 at: http://www.psmsc.com/UG2006/Presentations/11_ DHS_SwA_Overview_for_PSM.pdf

George Jelen. "SSE-CMM Security Metrics." NIST and CSSPAB Workshop, Washington, D.C., 13-14 June 2000. URL: http://csrc.nist.gov/csspab/june13-15/jelen.pdf

(US Department of) Justice, Bureau of Justice Statistics. "National Computer Security Survey." Accessed 10 March 2009 at: http://www.ojp.usdoj.gov/bjs/survey/ncss/ncss.htm

Erkan Kahraman, DSV SU/KTH, Institutionen for Data-och Systemvetenskap. *Evaluating IT security performance with quantifiable metrics*. Stockholm University and Royal Institute of Technology Master of Science Thesis, February 2005. Accessed 15 April 2009 at: http://www.dsv.su.se/en/seclab/pages/pdf-files/2005-x-245.pdf

Khalid Kark and Paul Stamp. "Defining an Effective Security Metrics Program," 16 May 2007. Accessed 29 December 2008 at: http://www.scribd.com/doc/2935458/best-practices-defining-an-effective-security-metrics-program

Khalid Kark, Forrester Research. "Best Practices: Security Metrics," July 22, 2008. Accessed 8 February 2009 at: http://www.forrester.com/Research/Document/Excerpt/0,7211,45787,00.html (Executive summary; full access to articles available only to Forrester Research clients.)

Khalid Kark and Chris McClean, Forrester Research. "The Forrester Wave: Security Consulting, Q3 2007," 25 September 2007. Accessed 2 February 2009 at: http://www.wipro.com/analyst_reports/pdf/Forrester_Security_Consulting_Wave_07.pdf (Executive summary; full access to articles available only to Forrester Research clients.)

C.W. Kirkwood. Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets. (Belmont, California: Duxbury Press, 1997).

Abe Kleinfeld, nCircle. "Measuring Security," in *IT Backbones: Computer Security News*, 28 November 2006. Accessed 15 April 2009 at: http://www.itbsecurity.com/pr/11424

Ahmet H. Koltuksuz, Izmir Institute of Technology. "On Defining Security Metrics for Information Systems," in *Proceedings of the International Conference of Computational Methods in Sciences and Engineering (ICCMSE 2005)*, Crete, Greece, 21-26 October 2005. Accessed 29 December 2008 at: http://wireless.iyte.edu.tr/documents/ahmetkoltuksuz_text.pdf

KoreLogic, Inc. "Information Security Metrics." Presented to Central Virginia Chapter of ISSA, 11 October 2006. Accessed 15 April 2009 at: http://www.issa-centralva.org/documents/SecurityMetricISSA_101106.pdf

Clint Kreitner, CIS. "The CIS Security Metrics and Benchmarking Service." Presented at Metricon 3.0, San Jose, California, 29 July 2008. Accessed 30 January 2009 at: http://www.securitymetrics.org/content/attach/Metricon3.0/metricon3-kreitner.pdf

B.S. Littlewood, *et al.* "Towards Operational Measures of Computer Security." Accessed on 13 April 2009 at: http://www.csr.city.ac.uk/people/bev.littlewood/bl_public_papers/Measurement_of_security/Quantitative_security.pdf

Robert D. Materna and Peter S. Greis. *Assessing the Value of Information Technology: Creating Value*. (Dayton, Ohio: NCR Corporation Strategic Consulting Group, March 1992).

Johnny Mathisen. *Measuring Information Security Awareness*. Gjøvik University College Master of Science Thesis, 17 June 2004. Accessed 30 January 2009 at: http://www.dsv.su.se/en/seclab/pages/pdf-files/2005-x-213.pdf

Johnny Mathisen. "Measuring the effect of an information security awareness drive." M.Sc. Project Plan, December 2003.

Dennis McCallam. "The case against numerical measures for information assurance," in *Proceedings of the First Workshop on Information Security System Rating and Ranking (WISSRR)*, Williamsburg, Virginia, 23 May 2001. Accessed 8 January 2009 at: http://www.seeeach.com/doc/189512_Position_Paper_The_Case_Against_Numerical_Measures_for_Information_. The entire WISSRR Proceedings can be downloaded from: http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf (Accessed 20 January 2009).

James McCurley, Software Engineering Institute; John Zebrow, Software Engineering Institute; and Carol Dekkers, Quality Plus Technologies, Inc. "Measures and Measurement for Secure Software Development." Accessed 15 April 2009 at: https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/measurement/227-BSI.html

John McHugh, "Quantitative measures of assurance: Prophecy, process, or pipedream?," in *Proceedings of the 1st ISSRR Workshop, ACSAC*, May 2001.

John McHugh, Carnegie Mellon University Center for Survivable Systems. "Information Assurance Metrics: Prophecy, Process, or Pipedream?," in *Proceedings of the 23rd National Information Systems Security Conference*, Baltimore, Maryland, 16-19 October 2000. Accessed 20 January 2009 at: http://csrc.nist.gov/nissc/2000/proceedings/papers/201.pdf

Miles McQueen, Wayne Boyer, Sean McBride, Marie Farrar, Zachary Tudor. *Measurable Control System Security through Ideal Driven Technical Metrics*, January 2008. Presented at SCADA Security Scientific Symposium, January 23, 2008. Accessed 6 April 2009 at: http://www.inl.gov/technicalpublications/Documents/3881671.pdf

Peter Mell and Karen Scarfone, NIST, and Sasha Romanosky, CMU. CVSS: *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*. Accessed 29 January 2009 at: http://www.first.org/cvss/cvss-guide.pdf

R.T. Mercuri, "Analyzing security costs," in *Communications of the ACM*, Vol. 46, pp. 15 – 18, June 2003.

Metrics Center. *Metrics Catalog Project*. Accessed 5 February 2009 at: http://www.metricscenter.org (Log-in required)

Michael S. Mimoso, Editor. "Number-driven risk metrics 'fundamentally broken'," in *Information Security*, 12 March 2009. Accessed March 26, 2009 at: http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1350658,00.html

securitymetrics.org. Metrics Catalog Project Page. Accessed 15 April 2009 at: http://www.securitymetrics.org/content/Wiki.jsp?page=MetricsCatalogProject

The MITRE Corporation. "Common Configuration Enumeration (CCE)." Accessed 26 March 2009 at: http://cce.mitre.org

The MITRE Corporation. "Common Platform Enumeration (CPE)." Accessed 26 March 2009 at: http://cpe.mitre.org

The MITRE Corporation. "Common Vulnerabilities and Exposures (CVE)." Accessed 26 March 2009 at: http://cve.mitre.org

The MITRE Corporation. "Making Security Measurable." Accessed 16 February 2009 at: http://measurablesecurity.mitre.org/

The MITRE Corporation. "OVAL Open Vulnerability and Assessment Language." Accessed 26 March 2009 at: http://oval.mitre.org

The MITRE Corporation. "OVAL FAQ." Accessed 3 February 2009 at: http://oval.mitre.org/oval/about/faqs.html#a16

Mozilla Security Metrics Project. http://blog.mozilla.com/security/2008/07/02/mozilla-security-metrics-project/ (12/22/08)

John Murdoch, Computer Science Department, University of York. *Security Measurement White Paper*, 13 January 2006. Accessed 3 April 2009 at: http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper_v3.0.pdf

B. Nandy, P. Pieda, N. Seddigh, J. Lambadaris, A. Matrawy, and A. Hatfield. "Current Trends and Advances in Information Assurance Metrics." Technical Report prepared for the Canadian Federal Government Department of Public Safety and Emergency Preparedness Office of Critical Infrastructure Protection and Emergency Preparedness (OCIPEP), March 2004. Accessed 15 April 2009 at: http://dev.hil.unb.ca/Texts/PST/pdf/seddigh.pdf

National Cyber Security Division (hosted by The MITRE Corporation.) "CWSS—Common Weakness Scoring System," Common Weakness Enumeration. Accessed 6 April 2009 at: http://cwe.mitre.org/cwss/index.html

Native Intelligence, Inc. "Security Awareness Program Metrics." Accessed 30 January 2009 at: http://www.nativeintelligence.com/ni-programs/ni-program-metrics-4pg.pdf

(Department of the) Navy. *CHIPS - The Department of the Navy Information Technology Magazine*. Accessed 2 April 2009 at: https://www.chips.navy.mil/archives/06_Jul/web_pages/FISMA.htm

David B. Nelson, NASA. "Performance Measures for Information Security: NASA Case Study," in *SecurIT*, Spring 2002 (22 April 2002).

NetIQ Corporation, Inc. "SCAP and FDCC." Accessed 8 February 2009 at: http://www.netiq.com/solutions/regulatory/fdcc/default.asp

Fran Nielsen. "Approaches to Security Metrics." NIST and CSSPAB Workshop, Washington, D.C., 13-14 June 2000.

DLA. "Certification and Accreditation: the DLA Approach." Accessed 26 March 2009 at: http://csrc.nist.gov/groups/SMA/fasp/documents/c&a/DLABSP/DLABSP.htm

NIST. "CND Data Strategy and Security Configuration Management." September 2008. Accessed 26 March 2009 at: http://nvd.nist.gov/scap/docs/2008-conf-presentations/day1/CM-and-Data-Strategy-Brief-NIST-2008-SCAP-Conf-Final-Slides.pdf

NIST. "The Information Security Automation Program and The Security Content Automation Protocol." Accessed 26 March 2009 at: http://nvd.nist.gov/scap.cfm

NIST. "National Vulnerability Database." Accessed 25 March 2009 at http://nvd.nist.gov

NIST. "NIST Mission, Vision, Core Competencies, and Core Values." Accessed 2 April 2009 at: http://www.nist.gov/public_affairs/nist_mission.htm

NIST. *Security Requirements for Cryptographic Modules* (Federal Information Processing Standards Publication [FIPS PUB] 140-2). 25 May 2001. Accessed 4 February 2009 at: http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf

NIST. *Security Requirements for Cryptographic Modules* (FIPS PUB 140-3 (DRAFT); will supersede FIPS PUB 140-2, 2001 May 25). Accessed 9 February 2009 at: http://csrc.nist.gov/publications/fips/fips140-3/fips1403Draft.pdf

NIST. "NVD Common Vulnerability Scoring System Support v2." Accessed 26 March 2009 at: http://nvd.nist.gov/cvss.cfm

NIST. "Security Content Automation Protocol Validated Products." Accessed 6 April 2009 at: http://nvd.nist.gov/scapproducts.cfm

NIST. "Security Content Automation Protocol (SCAP) Validation Program." Accessed 6 April 2009 at: http://nvd.nist.gov/validation.cfm#fdcc_scanner

NIST. "XCCDF - The Extensible Configuration Checklist Description Format." Accessed 26 March 2009 at: http://nvd.nist.gov/xccdf.cfm

NIST NVD program. "Managing Security Risk by Using Common Security Configurations." Accessed 8 February 2009 at: http://nvd.nist.gov/fdcc/faq-common_security_configurations.cfm

NIST SAMATE program. "Metrics and Measures." Accessed 6 January 2009 at: https://samate.nist.gov/index.php/Metrics_and_Measures

NSTAC."Research and Development (R&D) Exchange Workshop September 28 - September 29, 2000 Tulsa, Oklahoma." Accessed 2 February 2009 at: http://www.ncs.gov/nstac/rd/nstac_rdexchange_ok.html

Arne R. Nygard. "Security Metrics in SCADA Networks." Thesis proposal, 2003.

Arne R. Nygard. "Metrics for Software Resistance Against Trojan Horse Attacks." Project proposal, Norwegian Information Security Laboratory, 2003.

OMB. "FY07 Budget Formulation: FEA Consolidated Reference Model Document," Version 2.3, October 2007. Accessed 8 April 2009 at: http://www.whitehouse.gov/omb/assets/fea_docs/FEA_CRM_v23_Final_Oct_2007_Revised.pdf

OMB. "Fiscal Year 2007 Report to Congress on Implementation of The Federal Information Security Management Act of 2002." Accessed 3 February 2009 at: http://www.whitehouse.gov/omb/inforeg/reports/2007_fisma_report.pdf

OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," 26 September 2003. Accessed 15 April 2009 at: http://www.whitehouse.gov/omb/memoranda/m03-22.html

OSD DOT&E Deputy Director of Naval and C4ISR Systems. "Metrics Lessons Learned from Conducting Operational Assessments of Networks." Accessed 11 December 2008 at: http://www.mors.org/meetings/2007_tia/pres/aland.pdf

OWASP. Accessed 25 March 2009 at: http://www.owasp.org/index.php/Main_Page

OWASP. "OWASP Application Security Metrics Project." Accessed 13 January 2008 at: http://www.owasp.org/index.php/Category:OWASP_Application_Security_Metrics_Project

OWASP. "Types of Application Security Metrics." Accessed 15 April 2009 at: http://www.owasp.org/index.php/Types_of_application_security_metrics

J. Pamula, P. Ammann, S. Jajodia, George Mason University; and V. Swarup, The MITRE Corporation. "A weakest-adversary security metric for network configuration security analysis," in *Proceedings of the 2nd ACM Quality of Protection Workshop—Security Measurements and Metrics (QoP'06)*, Alexandria, Virginia, 30 October-3 November 2006. Accessed 15 April 2009 at: http://portal.acm.org/citation.cfm?id=1179494.1179502&coll=GUIDE&dl=GUIDE&type=series&idx=SERIES320&part=series&WantType=Proceedings&title=CCS&CFID=30508145&CFTOKEN=96888592

Victor-Valeriu Patriciu, Iustin Priescu, and Sebastian Nicolaescu. "Security Metrics for Enterprise Information Systems," in *Journal of Applied Quantitative Methods (JAQM)*, Vol. 1, No. 2, Winter 2006. Accessed 6 January 2009 at: http://jaqm.ro/issues/volume-1,issue-2/pdfs/patriciu_priescu_nicolaescu.pdf

Shirley C. Payne. "A Guide to Security Metrics," in *ISACA Newsletter*, November 2006. Accessed 13 April 2009 at: http://www.sans.org/reading_room/whitepapers/auditing/a_guide_to_security_metrics_55?show=55.php&cat=auditing

Gunnar Peterson and Elizabeth Nichols. "Web Application Security Metrics Framework," in *IEEE Security & Privacy*, March/April 2007.

Nguyen Pham, Loic Baud, Patrick Bellot, and Michel Riguidel, Telecom ParisTech. "A Near Real-time System for Security Assurance Assessment," in *Proceedings of the Third International Conference on Internet Monitoring and Protection (ICIMP 2008)*. Bucharest, Romania, 29 June-5 July 2008. Accessed 1 April 2009 at: http://www.infres.enst.fr/~bellot/publis/ICIMP2008.pdf

John P. Pironti. "Developing Metrics for Effective Information Security Governance," in *Information Systems Control Journal,* Volume 2, 2007. Accessed 2 April 2009 at: http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=35913&TEMPLATE=/ContentManagement/ContentDisplay.cfm

PSM Safety and Security Technical Working Group. "Security Measurement Whitepaper," Version 3.0, 13 January 2006. Accessed 2 February 2008 at: http://www.psmsc.com/Downloads/TechnologyPapers/SecurityWhitePaper

Deb Radcliff. "Government Vertical: Is FISMA Working?," in *SC Magazine,* 1 November 2007. Accessed 3 February 2009 at: http://www.scmagazineus.com/Government-vertical-Is-FISMA-working/article/58396

RAND Corporation. "DOJ/DHS National Computer Security Survey." Accessed 10 March 2009 at: http://www.ncss.rand.org/index.html

"Research and Development (R&D) Exchange Workshop October 28 - October 29, 2004 Monterey, California." Accessed 2 February 2009 at: http://www.ncs.gov/nstac/rd/nstac_04_bos.html

Lyn Robison, The Burton Group. *IT Metrics: Measuring IT's Business Value*, 27 February 2009. Accessed 13 March 2009 at: https://www.burtongroup.com

G. Rogers and B. Stauffer. "An approach to InfoSec program metrics," *in Proceedings of the 1st ISSRR Workshop, ACSAC*, March 26 2001.

Ron Ross, Stu Katzke, Arnold Johnson, Marianne Swanson, Gary Stoneburner, and George Rogers. NIST SP 800-53 Rev. 2, *Recommended Security Controls for Federal Information Systems*, December 2007. Accessed 3 April 2009 at: http://www.csrc.nist.gov

K. Rudolf, Native Intelligence, Inc. "Security Awareness Metrics: Measure What Matters." Accessed 29 January 2009 at: http://www.nativeintelligence.com/ni-programs/metrics-01.asp_v3.0.pdf

Elizabeth Van Ruitenbeek and Karen Scarfone. *The Common Misuse Scoring System (CMSS) (DRAFT)*, NIST Interagency Report 7517 (Draft), February 2009. Accessed 26 March 2009 at: http://csrc.nist.gov/publications/drafts/nistir-7517/Draft-NISTIR-7517.pdf

Sandia National Laboratories. "IDART Red Team Metrics Quick Reference Sheet." Accessed 6 January 2009 at: http://www.idart.sandia.gov/research.html

Reijo Savola, VTT Technical Research Centre of Finland. "A Novel Security Metrics Taxonomy for R&D Organisations," in *Proceedings of the Information Security South Africa (ISSA)* 2008 *Innovative Minds Conference*, Johannesburg, South Africa, 7-9 July 2008. Accessed 2 January 2009 at: http://icsa.cs.up.ac.za/issa/2008/Proceedings/Full/2.pdf. Also described in Reijo M. Savola, VTT Technical Research Center of Finland. "Towards a Taxonomy for Information Security Metrics," in *Proceedings of ACM Workshop on Quality of Protection (QoP '07)*, Alexandria, Virginia, 29 October 2007. DOI: http://doi.acm.org/10.1145/1314257.1314266

Karen Scarfone and Peter Mell. *The Common Configuration Scoring System (CCSS) (DRAFT)*, NIST Interagency Report 7502 (Draft), May 2008. Accessed 2 February 2009 at: http://csrc.nist.gov/publications/drafts/nistir-7502/Draft-NISTIR-7502.pdf

E.A. Schneider, "Measurements of system security," in *Proceedings of the 1st ISSRR Workshop, ACSAC*, May 2001.

Stuart Edward Schechter. *Computer Security Strength & Risk: A Quantitative Approach*. Harvard University Ph.D. Thesis, May 2004. Accessed 13 April 2009 at: http://www.eecs.harvard.edu/~stuart/papers/thesis.pdf

Michael J. Scroch, Sandia National Laboratories. "IORTA Red Team Metrics 101" (Incomplete Beta Version). Lecture.

Michael J. Scroch, J. McHugh, and J.M. Williams. "Information Assurance Metrics: Prophecy, Process or Pipedream." Panel Workshop, National Information Systems Security Conference (NISSC 2000), Baltimore, Maryland, October 2000.

Securitymetrics.org. Accessed 13 April 2009 at: http://www.securitymetrics.org/content/Wiki.jsp

Nabil Seddigh, Peter Pieda, Biswajit Nandy, and John Lambadaris, Solana Networks; and Ashraf Matrawy and Adam Hatfield, Department of Public Safety and Emergency Preparedness Canada. "Current Trends and Advances in Information Assurance Metrics." Accessed 10 December 2008 at: http://dev.hil.unb.ca/Texts/PST/pdf/seddigh.pdf

Nabil Seddigh, Peter Pieda, Ashraf Matrawy, Biswajit Nandy, John Lambadaris, and Adam Hatfield. "Current Trends and Advances in Information Assurance Metrics," in *Proceedings of Second Annual Conference on Privacy, Security, and Trust (PST 2004)*, Fredericton, NB, Canada, 13-15 October 2004. Accessed 19 January 2008 at: http://dev.hil.unb.ca/Texts/PST/pdf/seddigh.pdf

Nicholas Sheble, ISA. "Control system security occupies time, cyberspace," *InTech*, 15 October 2008. Accessed 11 December 2008 at: http://www.isa.org/InTechTemplate.cfm?Section=Industry_News&template=/ContentManagement/ContentDisplay.cfm&ContentID=72373

Edgar Sibley, George Mason University. "National Information Assurance Training Standard for System Administrators." Lecture slides for course on IAVA, Summer 2008. Accessed 5 February 2009 at: http:// mason.gmu.edu/~esibley/ISA562SU08/Slide/11%2520cont%25202%2520IAVA%2520.ppt

Daniel J. Solove, Marc Rotenberg, and Paul M. Schwartz. *Privacy, Information, and Technology* (New York, New York: Aspen Publishers, 2006)

-and-

Joel Rosenblatt. "Security Metrics: A Solution in Search of a Problem," in *EDUCAUSE Quarterly*, Vol. 31, No. 3, July-September 2008. Accessed 22 December 2008 at: http://connect.educause.edu/Library/EDUCAUSE+Quarterly/SecurityMetricsASolutioni/47083

Kevin Soo Hoo, PacketMotion. Economic Incentives & Metrics of Cybersecurity. Lecture slides for Stanford University course on US National Cybersecurity, 2 November 2006. Accessed 19 January 2009 at: http://www.stanford.edu/class/msande91si/slides/lecture_6_soohoo.pdf

Derek Slater. "Security Budget Benchmarks: Inside the Sausage Factory," in *CIO*, 9 December 2002. Accessed 13 April 2009 at: http://www.cio.com/article/217728/Security_Budget_Benchmarks_Inside_the_Sausage_Factory

M. Stoddard, *et al*. "An Initial Metrics Taxonomy," in *Process Control System Security Metrics—State of Practice*, I3P Institute for Information Infrastructure Protection Research Report No. 1, August 2005. Accessed 19 January 2009 at: http://www.thei3p.org/docs/publications/ResearchReport1.pdf

Marianne Swanson, Nadya Bartol, John Sabato, Joan Hash and Laurie Graffo. NIST Special Publication 800-55, *Security Metrics Guide for Information Technology Systems*, July 2003. Accessed 26 March 2009 at: http://webharvest.gov/peth04/20041027033844/csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf

Software Assurance Community Resource and Information Clearinghouse Measurement Working Group. Accessed 1 April 2009 at: https://buildsecurityin.us-cert.gov/swa/measwg.html

SSE-CMM. "Systems Security Engineering Capability Maturity Model (SSE-CMM), Version 3." Accessed 1 April 2009 at: http://www.sse-cmm.org/model/model.asp

SwA Measurement Working Group. *Practical Measurement Framework for Software Assurance and Information Security*, Version 1.0, October 2008. Accessed 7 April 2009 at: https://buildsecurityin.us-cert.gov/swa/downloads/SwA_Measurement.pdf

US-CERT. "Vulnerability Notes Database Field Descriptions." Accessed 4 February 2009 at: http://www.kb.cert.org/vuls/html/fieldhelp

United States Congress. *Federal Information Security Act*, DON CIO Website H.R. 2458–48. Accessed 1 April 2009 at: http://csrc.nist.gov/groups/SMA/fisma/index.html

Rayford B. Vaughn and Ambareen Siraj, Mississippi State University, and Ronda Henning, Harris Corporation, Government Communications Systems Division. "Information Assurance Measures and Metrics—State of Practice and Proposed Taxonomy," *Proceedings of the 36th Hawaii International Conference on System Sciences (HICSS-36)*, 6-9 January 2003. Accessed 19 January 2008 at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.71.184

R. B. Vaughn, "Are measures and metrics for trusted information systems possible?," in *Proceedings of the 1st ISSRR Workshop*, ACSAC, May 2001.

Rayford B. Vaughn, Ambareen Siraj, and David A. Dampier, Mississippi State University. "Information Security System Rating and Ranking," in *CrossTalk: The Journal of Defense Software Engineering*, May 2002. Accessed 19 January 2009 at: http://www.stsc.hill.af.mil/crosstalk/2002/05/vaughn.html

Chenxi Wang and William A. Wulf, University of Virginia. "Towards a Framework for Security Measurement." *Proceedings of the National Information Systems Security Conference (NISSC)*, Baltimore, Maryland, 7-10 October 1997. Accessed 8 January 2009 at: http://csrc.nist.gov/nissc/1997/proceedings/522.pdf

Lingyu Wang, Tania Islam, Tao Long, Anoop Singhal, and Sushil Jajodia. "An attack graph-based probabilistic security metric," in *22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, London, UK, 13-16 July 2008

Lingyu Wang, Anoop Singhal, and Sushil Jajodia. "Measuring the overall security of network configurations using attack graphs," in *Data and Applications Security XXI* (Berlin/Heidelberg, Germany: Springer Verlag, 2007), pp. 98–11.

Mark Wilson and Joan Hash. NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*. October 2003. Accessed 30 January 2009 at: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf

G. Wold. "Is use of security metrics expedient to measure performance of an implemented organizational security policy?" M.SC. Project Plan, Dec. 2003.

Carol Woody, CMU SEI CERT/CC. "Strengthening Ties between Process and Security," on DHS National Cyber Security Division's BuildSecurityIn Web portal, 1 Aug 2008. Accessed 2 April 2009 at: https://buildsecurityin.US-CERT.gov/daisy/bsi/articles/knowledge/sdlc/1049-bsi.html#dsy1049-bsi_harm

Carol Woody. "Process Improvement Should Link to Security: SEPG 2007 Security Track Recap." Technical Note CMU/SEI-2007-TN-025, September 2007. Accessed 6 April 2009 at: http://www.sei.cmu.edu/publications/documents/07.reports/07tn025.html

Chris Wysopal, Veracode, Inc. "Software Security Weakness Scoring." Presented at MetriCon 2.0, Boston, Massachusetts, 7 August 2007. Accessed 16 February 2009 at: http://www.securitymetrics.org/content/attach/Metricon2.0/Wysopal-metricon2.0-software-weakness-scoring.ppt

B.2 Additional Print Sources of Information for Suggested Reading

Richard B. Cole. *Measuring Security Performance and Productivity.* (Alexandria, Virginia: ASIS International, 2003).

Lisa Witzig Davidson, Advanced Performance Consulting Group. "US Department of State's Overseas Wireless Program: Measuring Performance, Measuring Security," in *Proceedings of the 5th International Command and Control Research and Technology Symposium (ICCRTS)*, Canberra, Australia, October 2000. Accessed 7 February 2009 at: http://www.dodccrp.org/events/5th_ICCRTS/papers/Track6/033.pdf

Dieter Gollmann, Fabio Massacci, and Artsiom Yautsiukhin, Editors. Quality of Protection: Security Measurements and Metrics (City, Country: Springer-Verlag, 2006).

Debra S. Hermann. *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI* (Boca Raton, Florida: Auerbach Publications, 2007).

Andrew Jaquith. *Security Metrics: Replacing Fear, Uncertainty, and Doubt* (City, State: Addison-Wesley Professional, 2007).

Gerald L. Kovacich and Edward Halibozek. *Security Metrics Management: How to Manage the Costs of an Assets Protection Program* (Oxford, England: Butterworth-Heinemann, 2006).

Timothy P. Layton. *Information Security: Design, Implementation, Measurement, and Compliance* (Boca Raton, Florida: Auerbach Publications, 2006)

Overseas Economic Co-operation and Development (OECD) Directorate for Science, Technology, and Industry. "Measuring Security and Trust in the Online Environment: A View Using Official Data." OECD Digital Economy Paper No. 140, DSTI/ICCP/IIS(2007)4/FINAL, 29 January 2008. Accessed 7 February 2009 at: http://www.sourceoecd.org/10.1787/230551666100

B.3 Additional Online Sources of Information for Further Reading

Ashish Arora, Dennis Hall, C. Ariel Pinto, Dwayne Ramsey, and Rahul Telang. "Measuring the Risk-Based Value of IT Security Solutions," in *IT Professional*, Vol. 6 No. 6, November/December 2004, pp. 35-42. Digital Object Identifier: 10.1109/MITP.2004.89 Accessed 7 April 2009 at: http://ieeexplore.ieee.org/Xplore/login.jsp?url=http%3A%2F%2Fieeexplore.ieee.org%2Fiel5%2F6294%2F30282%2F01390871.pdf&authDecision=-203

Nadya Bartol. "IA Metrics—Why and How to Measure Goodness of Information Assurance." Presented to ISSEA PSM User's Group Conference, July 2005. Accessed 29 December 2008 at: metrics http://www.psmsc.com/UG2005/Presentations/15_Bartol_IA_Metrics.pdf

Blake Causey. "Why Application Security Metrics are broken." 22 December 2008 on the "Hancock"/Attack Vectors blog. Accessed 2 February 2009 at: http://attackvectors.com/~/blog/index.php?m=12&y=08&entry=entry081222-141210

S. Chandra and R.A. Khan. "Object Oriented Software Security Estimation Life Cycle-Design Phase Perspective", in *Journal of Software Engineering*, Volume 2 Issue 1, 2008, pp. 39-46. Accessed 13 April 2009 at: http://www.scialert.net/fulltext/?doi=jse.2008.39.46

Tony Coulson, Jake Zhu, and C.E. Tapie Rohm, California State University-San Bernardino; and Shan Miyuan, Hunan University-Changsha. "The Price of Security: The Challenge of Measuring Business Value Investments in Securing Information Systems," in *Communications of the IIMA*, Volume 5, Issue 4, 2005. Accessed 25 March 2009 at: http://www.iima.org/CIIMA/8%205.4_Coulson_19_24.pdf

Tony Coulson, Jake Zhu, Kurt Collins, Walter Stewart, C.E. Tapie Rohm, Jr., California State University-San Bernardino. "Security: Valuing Increased Overhead Costs," in *Proceedings of the 10th Colloquium for Information Systems Security Education*, Adelphi, MD, 5-8 June 2006. Accessed 25 March 2009 at: http://www.cisse.info/colloquia/cisse10/proceedings10/pdfs/papers/S05P03.pdf

DHS. "Measurement," in *DHS BuildSecurityIn*. Accessed 3 April 2009 at: https://buildsecurityin.us-cert.gov/daisy/bsi/articles/best-practices/measurement.html

DON CIO, *Department of the Navy Federal Information Security Management Act (FISMA) Guidance*, March 2006. Accessed 1 April 2009 at: http://www.doncio.navy.mil/Download.aspx?AttachID=294

DON CIO Blog. Accessed 1 April 2009 at: http://www.doncio.navy.mil/tagresults.aspx?ID=28

Government Accountability Office (GAO) Report to Congressional Addressees. *Information Technology: DOD Needs To Ensure That Navy Marine Corps Intranet Program Is Meeting Goals And Satisfying Customers*, December 2006. Accessed 1 April 2009 at: http://www.gao.gov/new.items/d0751.pdf

Fred Hall. "Measurement of Security Processes." Presentations from workshop presented at PSM Technical Working Group Meeting, Herndon, Virginia, March 2006. Accessed 2 February 2009 at: http://www.psmsc.com/Downloads/TWGMarch06/3%20-%20Measurement%20of%20Security%20Processes.Hall.zip

Michael Howard, Microsoft Corporation; and Jon Pincus and Jeannette M. Wing, Carnegie Mellon University. "Measuring Relative Attack Surfaces," in *Proceedings of Workshop on Advanced Developments in Software and Systems Security*, Taipei, December 2003. Accessed 29 January 2009 at: http://www.cs.cmu.edu/~wing/publications/Howard-Wing03.pdf

Vivian Cocca (OSD/NII), Steven Skolochenko, and Jonathan Smith. "The Importance of High Quality IA Metrics," in *IAnewsletter*, Volume 7 Number 2, pg. 22. Accessed 13 April 2009 at: http://iac.dtic.mil/iatac/download/Vol7_No3.pdf

Cheryl Jones, USA. "Making Measurement Work," in *CrossTalk: The Journal of Defense Software Engineering,* January 2003. Accessed 2 February 2009 at: http://www.stsc.hill.af.mil/Crosstalk/2003/01/jones.html

Cheryl Jones, CIV USA AMC, and John Murdoch, University of York. "Security Measurement: Applying PSM Principles." Presented at Practical Software and Systems Measurement Users' Group Conference, 14-18 July 2008, Mystic, CT. Accessed 3 February 2009 at: http://www.psmsc.com/UG2008/Presentations/14%20-%20Murdoch-Security%20Measurement-17Jul08.pdf

Raph Levien. "Advogato's trust metric," 22 February 2000. Accessed 6 April 2009 at: http://www.advogato.org/trust-metric.html

Raph Levien. "Attack Resistant Trust Metric Metadata HOWTO," 3 July 2002. Accessed 6 April 2009 at: http://www.levien.com/free/tmetric-HOWTO.html

(United States) Marine Corps. *Initial Capabilities Document (ICD) for Marine Corps Enterprise Information Technology Services (MCEITS)*, Version 3.4, 20 May 2005. Accessed 1 April 2009 at: http://www.mceits.usmc.mil/docs/05-05-20_MCEITS_ICD_(v3.4).pdf

(Secretary of the) Navy. *Federal Managers' Financial Integrity Act. FY 2008 Statement of Assurance*, 28 August 2008. Accessed 1 April 1, 2009 at: www.fmo.navy.mil/mic/docs/SOA_Final_WEB.pdf

securitymetrics.org, Community Web site for Security Practitioners. Accessed 9 April 2009 at: http://www.securitymetrics.org/content/Wiki.jsp

Andy Ozment, University of Cambridge. "Software Security Growth Modeling: Examining Vulnerabilities with Reliability Growth Models," in *Quality of Protection: Security Measurements and Metrics* (Dieter Gollman, Fabio Massacci and Artsiom Yautsiukhin, editors). Accessed 3 April 2009 at: http://www.cl.cam.ac.uk/~jo262/papers/qop2005-ozment-security_growth_modeling.pdf

SecurityStats.com. Latest Computer Security News. Accessed 9 April 2009 at: http://www.securitystats.com

Shaun Remnant. "Counting the cost of IT security," in *ITadviser*, Issue 38, July/August 2005. Accessed 25 March 2009 at: http://www.nccmembership.co.uk/pooled/articles/BF_WEBART/view.asp?Q=BF_WEBART_171149

SANS Institute. "Twenty Most Important Controls and Metrics for Effective Cyber Defense and Continuous FISMA Compliance." Accessed 15 April 2009 at: http://www.sans.org/cag

Lora Shinn. "Instituting Security Metrics," in *Inc. Technology*, June 2008. Accessed 13 April 2009 at: http://technology.inc.com/security/articles/200806/metrics.html

John Steven and Gunnar Peterson. "A Metrics Framework to Drive Application Security Improvement," in *Building Security In*, IEEE Security and Privacy, 2007. Accessed 25 March 2007 at: http://www.arctecgroup.net/pdf/0703-OWASPMetrics.pdf

Trustcomp Yahoo Group. "Welcome to Trustcomp.org!" Accessed 25 March 25, 2009 at: http://www.trustcomp.org

US-CERT. "Briefings from Workshop on Assurance with CMMI," August 2007, in *BuildSecurityIn*. Accessed 10 February 2009 at: https://buildsecurityin.us-cert.gov/swa/procresrc.html

B.4 Publicly Available CS/IA Measures Lists

A number of CS/IA measures lists are available from books, guidelines, articles, and other sources. The following is a representative list of those sources:

NIST SP 800-55 Rev. 1, *Performance Measurement Guide for Information Security, Appendix A, Candidate Measures*

SwA Measurement Working Group. *Practical Measurement Framework for Software Assurance and Information Security*

CIS. *The CIS Security Metrics*

Debra S. Hermann, *Complete Guide to Security and Privacy Metrics*

Andrew Jaquith. *Security Metrics: Replacing Fear, Uncertainty, and Doubt.*

ISSA, UK Chapter. *Is Security Awareness wasted on End Users?,*

Gary Hinson, *Seven myths about information security metrics, in ISSA Journal*

K. Rudolf, *Security Awareness Metrics: Measure What Matters.*

C

CS/IA Measurement Before 2000

This Appendix describes some leading CS/IA measures that were defined prior to the period addressed in this SOAR.

C.1 Background

In the outbrief of its third R&D Exchange (RDX) Workshop in October 1998, the President's National Security Telecommunications Advisory Committee (NSTAC), a component of the National Communications System, identified and discussed the need for research in the area of CS/IA measurement. Five years later, at NSTAC's 2003 RDX Workshop, "technical metrics that measure the strength of security" was again identified as recommended Cyber Security Research focus that deserved funding by the Office of Science and Technology Policy. The 2003 RDX outbrief at RDX 2004 specifically called for development and verification of "security metrics for use on a national level." [174]

Significant work on the definition of CS/IA measures and measurement techniques began in the mid-late 1990s. In their presentation, "A Report on the Information System Information System Security Rating and Ranking Workshop," at the 14th Annual Software Technology Conference (Salt Lake City, Utah, 29 April–2 May 2002), Ray Vaughn of Mississippi State University and Ronda Henning of Harris Corporation, identified a number of "renowned existing IA metrics," many of which emerged during that period. These metrics are listed in Table C-1.

Table C-1 Renowned Existing CS/IA Measures

Defining Organization	Initiative Title
Air Force Communications Agency (AFCA)	Information Protection Metrics and Measurement Program
CVE Editorial Board and Advisory Council	Common Vulnerabilities and Exposures (CVE) Vulnerability Scanner Coverage Metric (expressed as number of CVE entries)
DISA	Information Assurance Vulnerability Alerts (IAVA) metrics
DoD	Defense Technology Security Certification and Accreditation Process (DITSCAP) Certification Levels (now Defense Information Assurance Certification and Accreditation Process [DIACAP] Certification levels)
ESC/DIW	IA Vulnerability Assessment/Risk Management (VA/RM) metrics
Federal CIO Council/NIST	Federal Information Technology Security Assessment Framework (FITSAF)
Information Systems Security Engineering Association (ISSEA)	System Security Engineering Capability Maturity Model (SSE-CMM)
Intelligence Community Top Secret and Below Information (TSABI) Initiative	INFOSEC Risk Management metrics
ISO/IEC	Common Criteria Evaluation Assurance Level
LAAS-CNRS	Attacker success measures
Lincoln Labs (for DARPA)	Intrusion Detection algorithm performance metrics
Logicon	Resiliency Assurance Index
The MITRE Corporation (for OSD(C3I)/I&IA)	Defense-Information Assurance Red Team (D-IART)
Sandia National Laboratories	Information Design and Assurance Red Team (IDART) metrics (see Section 7.1.1.1)
SANS	SANS Institute Certification Levels
Sparta	IA Risk Metric Tree
SRI (for DARPA)	Red Team Work Factor (RTWF)

A number of these efforts are still in active use or under development; these are discussed elsewhere in this document. Of those that appear to be obsolete, a representative sampling is described below.

C.2 Annualized Loss Expectancy as a CS/IA Measure

Until the late 1990s, the main measures used by traditional security risk analysis methodologies was Annualized Loss Expectancy (ALE). While it is not specifically an CS/IA measure *per se*, ALE was used by risk analysts to express the level of security risk posed to an organization in terms of potential monetary loss accruing from a security incident. Specifically, ALE was the result of the calculation of the expected monetary loss that would result from an asset being lost in a security incident. This monetary loss was expressed in terms of a Single Loss Expectancy (SLE) measure. The SLE

measure was then multiplied by a second measure, the Annualized Rate of Occurrence (ARO), which expressed the probability of the security incident occurring within a given one year period, [175] as follows:

SLE * ARO = ALE

The ALE was intended to provide the basis for estimating the reasonable annualized cost of the countermeasure(s) (*e.g.*, security product, architecture, policy) that could mitigate the risk (of loss posed by the security incident); the cost of mitigation was considered reasonable if it was less than or equal to the ALE.

The credibility of ALE as a meaningful measure for CS/IA has been increasingly questioned. On his "Practical Risk Management" blog, security consultant Bryan Fish neatly summed up ALE skeptics' concerns:

> ***"ALE is fundamentally wrong for information security. I'll concede that ALE can be useful as a simple conceptual model for risk because it requires us to think about both of the factors that generally influence risk: Likelihood and Impact. But literal use of ALE for information security decisions is problematic to say the least.***
>
> ***The problem with ALE is that the numbers we plug into that formula are so baseless that the resulting calculation has no credibility.... How does one calculate the financial impact of a security breach? Here's a hint: the amount of money you paid for the server that was just compromised is wrong. There's a whole bunch of things that go into it: the cost of employees and consultants to restore order after the breach, the potential legal liability, the cost of business you may have lost when the system went down, the opportunity cost of things you couldn't do because you had to spend time and resources responding to the incident, and the impact of lost goodwill and reputation damage that you suffer in the market. All of these factors are either immeasurable or unpredictable, which makes them poor candidates for mathematical calculations.***
>
> ***How does one calculate the likelihood of a security breach? The spectrum of threats is too broad and too unpredictable to have any hope of doing this. If you were just hacked by an outsider, or fell victim to a disgruntled employee, or made a simple mistake and exposed a bunch of sensitive information on a Web site, chances are you never saw it coming, and sure couldn't have sat at your desk six months ago and said 'there's a 20% chance that this will happen in the next year'." [176]***

C. 3 DARPA IASET Measures of Assurance Research: Value-Focused Thinking

Defense Advanced Research Projects Agency (DARPA) ISO's Information Assurance Science and Engineering Tools (IASET) Program undertook management of several research projects to "develop quantifiable measures of assurance."

The goal of IASET's measures research was to first identify measures that are measurable, testable, and useful for the quantification and comparison of IA components over time, for the comparison between similar systems, for the comparison of systems to requirements, and for measuring the utility of a system in a particular environment. The ultimate objective was to produce useful measures for designers, assessors, planners, and users.

DARPA's priority was for as many of these measures as possible to be quantitative, but also recognized that qualitative measures were unavoidable; therefore, their meaning must be consistent and defined. IASET promoted the development of a common frame of reference and language for measures to ensure they would be universally understood by designers, assessors, and operators.

DARPA was also interested in the definition of benchmarks or touchstones for IA, recognizing the limitations of measures which, while they could provide standards of measure, might not provide insight that humans could readily understand and use. DARPA's measures research focused also on the development of comparative benchmark measures, measurable against a standard scale, in recognition that absolute measures are not available.

In summary, IASET sought to develop an integrated environment for measures by defining their purpose, meaning, units, range of values, inherent taxonomies, and relationship to other measures and calculations for IA.

Among the most promising research efforts funded by the DARPA/IO/IASET Program was the Value-Focused Thinking (VFT) methodology, developed by researchers at the Air Force Institute of Technology. Adapted from a methodology described by Kirkwood, [177] VFT was formulated as an analytical framework for facilitating development and evaluation of IA strategies. The framework enabled the analyst to evaluate the merits of alternative IA strategies (a "strategy" being the collection of technical—hardware, software, firmware—and non-technical—policies, procedures—countermeasures used to achieve IA objectives), based on the analysis and comparison of the perceived quantified value of each strategy in terms of its effectiveness in achieving a desired (or required) level of assurance while imposing the least possible operational impact, at the most reasonable cost.

The VFT framework included several sets of measures that allocated values to the IA, operational capability, and resource factors that must be considered to—

- Measure the attainment of IA objectives,

- Determine the meaningful balance between a required/desired level of IA against the operational and resource costs associated with attaining that level of assurance.

Using these measures, the AFIT researchers defined three different value models—

- An IA model,
- An Operational Capability model,
- A Resource Costs model.

Each model quantifies the values of the strategy's various components (the methodology providing a technique for balancing the relative value "weights" of each model). In this way, the analyst can compare the values of multiple candidate strategies to determine which of them provides the greatest overall value.

Building upon concepts described by Materna, [178] the AFIT researchers produced a Microsoft Excel-based decision support tool that enabled the user to define the value models and provide them the necessary inputs, evaluation measures, and weighting criteria *via* a semi-automated input process implemented by Visual Basic macros, which are also used to generate the tool's summary of the analysis results.

C.4 RAI

Researchers at Logicon felt that numerical "measures of merit," such as "80% secure," "95% secure," "99% secure," *etc.*, were of dubious value for quantifying levels of IA protection or gauging the true security posture of a system.

To address their concern, the Logicon researchers developed a quantitative (10-level) Resiliency Assurance Index (RAI) [179] for use in rating the ability of a system to resist, contain and minimize damage, and recover from an attack.

The Logicon researchers failed, however, to clarify why they believed that a 10-level system of resilience ratings produced more meaningful measures than a system that assigned percentage ratings to a system's perceived security strength.

C.5 D-IART

Developed at the end of the 1990s for the Office of the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence/Information Assurance (OSD(NII)), the Defense-Information Assurance Red Team Methodology (D-IART) is a red teaming methodology based on red teaming best practices from across DoD and within The MITRE Corporation.

The methodology was designed to guide red teamers through the specific steps required to organize, tailor, and conduct red team activities, and to aid in after-action analysis. Recognizing that lessons learned from read teaming activities are maximized if the red team results can be quantified and used as a basis of comparison, the methodology also provides measures for data collection and analysis.

C.6 SM Framework [180]

Developed by researchers at University of Virginia, the Security Measurement (SM) framework applies the theory and practice of formal measurements to assist the user in defining adequate security measures, then to determine the values of such measurements. The SM framework comprises—

- A definition of computer security (*i.e.*, the thing to be measured, derived from the TCSEC);
- An approach for selection of units and scales of measurement;
- A specification of an estimation methodology;
- An approach for formal validation of the defined measures.

References

174 NSTAC. "Research and Development (R&D) Exchange Workshop September 28 - September 29, 2000 Tulsa, Oklahoma." Accessed 2 February 2009 at: *http://www.ncs.gov/nstac/rd/nstac_rdexchange_ok.html*

-and-

"Research and Development (R&D) Exchange Workshop October 28 - October 29, 2004 Monterey, California." Accessed 2 February 2009 at: *http://www.ncs.gov/nstac/rd/nstac_04_bos.html*

175 Robert Hudock. "Why Security Metrics Must Replace Traditional Risk Analysis Methodologies," in Computer Security Law Updates, 6 March 2006. Accessed 30 January 2009 at: *http://computersecuritylaw.us/2008/03/06/why-security-metrics-must-replace-traditional-risk-analysis-methodologies.aspx?ref=rss*

176 Bryan Fish, Securityworks. "Is Risk-Based Security Really Possible?," Practical Risk Management Blog, 21 July 2008. Accessed 30 January 2009 at: *http://www.security-works.com/blog/labels/risk.html*

177 As described in C.W. Kirkwood. Strategic Decision Making: Multiobjective Decision Analysis with Spreadsheets. (Belmont, California: Duxbury Press, 1997).

178 As described in Robert D. Materna and Peter S. Greis. Assessing the Value of Information Technology: Creating Value. (Dayton, Ohio: NCR Corporation Strategic Consulting Group, March 1992).

179 Dennis McCallam. "The case against numerical measures for information assurance," in Proceedings of the First Workshop on Information Security System Rating and Ranking (WISSR), Williamsburg, Virginia, 23 May 2001. Accessed 8 January 2009 at: *http://www.seeeach.com/doc/189512_Position_Paper_The_Case_Against_Numerical_Measures_for_Information_*. The entire WISSR Proceedings can be downloaded from: *http://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf* (Accessed 20 January 2009).

180 Chenxi Wang and William A. Wulf, University of Virginia. "Towards a Framework for Security Measurement." Proceedings of the National Information Systems Security Conference (NISSC), Baltimore, Maryland, 7-10 October 1997. Accessed 8 January 2009 at: *http://csrc.nist.gov/nissc/1997/proceedings/522.pdf*

D

Conferences and Workshops

A number of conferences on IA, cyber security, application security, and related disciplines have included tracks on measures and measurement. However, an emerging trend has been "specialist" conferences and workshops that focus on the problems associated with definition and use of CS/IA measures and measurement techniques and tools.

The following are conferences and workshops that devoted predominantly or entirely to CS/IA measurement.

D.1 Workshop on Information Security System Scoring and Ranking (WISSSR)

Also referred to as: 1st Workshop on Information Security System Rating and Ranking (ISSRR) Workshop. Williamsburg, Virginia, 21-23 May 2001. Co-sponsored by Applied Computer Security Associates and The MITRE Corporation.

The goals of the workshop were to characterize the information security measurement problem domain, identify "good practices," focus needs, and determine potential research directions. Common themes that emerged included—

- No single information security measure will successfully quantify the assurance of a system. Multiple measures will be needed and will need to be refreshed frequently.

- Software and systems engineering (*e.g.,* 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 an imperfect way of generating measurable data and is, to some extent, non-repeatable.
- Government and commercial sectors have different agendas: the former is policy-driven, the latter is profit-driven. Thus, the two sectors may place different values on security measures.
- Measuring defense in depth and breadth is a critical area that warrants further research.
- Past attempts to quantify and obtain partial ordering of systems' security attributes (*e.g.,* TCSEC, Common Criteria) have been unsuccessful to a large degree.

Processes, procedures, tools, and people all interact to produce assurance in systems. Measures need to incorporate all of these aspects.

For more information: http://www.acsac.org/measurement (Accessed 3 February 2009)

D.2 Fourth Workshop on Assurance Cases for Security "The Metrics Challenge"

Edinburgh, Scotland, June 2007. Sponsored by International Working Group on Assurance Cases (for Security).

The focus of this workshop was on metrics for assurance cases for security.

For more information: http://www.csr.city.ac.uk/AssuranceCases/dsn2007workshop.html (Accessed 3 February 2009)

D.3 Workshop on "Measuring Assurance in Cyberspace"

Monterey, California, 26 June 2003. Sponsored by IFIP Working Group 10.4.

The stated challenges to be addressed at the workshop included—

- Inability to quantify how assured systems and networks are;
- Inability to quantify the ability of protective measures to keep intruders out;
- Difficulty characterizing capabilities of intrusion detection systems in detecting novel attacks;
- Inability to measure benefits of novel response mechanisms comparatively or absolutely.

The goals of this one-day workshop were to—

- Assess the state of the art for quantifying system assurance;
- Discuss recent research results;
- Formulate the challenges that obstruct forward movement;

- Formulate potential new technical approaches to address the challenges above.

For more information: http://www2.laas.fr/IFIPWG/Workshops&Meetings/44 (Accessed 3 February 2009)

D.4 MetriCon and Mini-MetriCon

Recurring, semi-annually (MetriCon: usually co-located with USENIX Security; Mini-MetriCon: usually co-located with RSA Conference). Sponsored by Securitymetrics.org.

The focus of this workshop was on metrics for security assurance cases. The workshop was divided into four presentations on security assurance cases and security metrics followed by two talks on the topic and an afternoon of discussion.

According to its Web site, "The workshop reported on some progress on assurance cases but, for this organiser at least, its value was in highlighting the enormous gaps in our ability to measure, model and communicate security risks. Progress on assurance cases for security will require more rigorous work on the underlying problems."

For more information: http://www.securitymetrics.org (Accessed 3 February 2009)

D.5 International Workshop on Quality of Protection "Security Measurements and Metrics"

Recurring. Sponsored by the Association for Computing Machinery (ACM).

The goal of the QoP Workshop is to help security research progress toward a notion of Quality of Protection in Security comparable to the notion of Quality of Service in Networking, Software Reliability, or measures in Empirical Software Engineering.

Information Security has gained numerous standards, industrial certifications, and risk analysis methodologies. However, the field still lacks the strong, quantitative, measurement-based assurance found in other fields. For example—

- Networking researchers have created and utilize Quality of Service (QoS), SLAs, and performance evaluation measures.
- Empirical Software Engineering has made similar advances with software measures: processes to measure the quality and reliability of software exist and are appreciated in industry.
- Even a fairly sophisticated standard, such as ISO17799, has an intrinsically qualitative nature. Notions, such as Security Metrics, Quality of Protection (QoP) and Protection Level Agreements (PLA), have surfaced in the literature, but they still have a qualitative flavor. Furthermore, many recorded security incidents have a non-IT cause.

> As a result, security requires a much wider notion of "system" than do most other fields in computer science. In addition to the IT infrastructure, the "system" in security includes users, work processes, and organizational structures.

For more information: http://qop-workshop.org (Accessed 3 February 2009)

E

Research and Emerging Methods Summary

Table E-1 provides an extensive listing of current CS/IA measurement research activities. Excluded from this table are research activities about which conference papers were published, but about which no additional information (*e.g.,* sponsorship of the research) could be discovered. This table should not be interpreted as an exhaustive listing of research, but rather as representative of the types of research activities that have been underway in the years 2000 to 2008.

Table E-1 CS/IA Measurement Research

Institution	Project/Program	Description	URL or Reference
Air Force Research Laboratory Anti-Tamper/Software Protection Initiative (ATSPI) Technology Office	A Threat-Driven, System Design/Assessment Hypothesis for Cyber Security: The Three Tenets Algorithm	Developed based on a heuristic secure system development algorithm used by the ATSPI Technology Office for the last seven years, the Three Tenets Algorithm is based on a framework in which all system threats are decomposed into the following three elements: (1) susceptibilities (logical and physical system access points); (2) accessibility by threats to those access points ("threat" being defined as the user in a given use case); (3) ability of the threat to exploit those access points. The Three Tenets, which are applied during system design to address these three elements of the threat decomposition, are: (1) Include only mission-essential functions, thereby minimizing inherent susceptibilities, and enumerate critical security controls for those mission functions. (2) Logically and/or physically move data/processes for essential mission elements and their associated security controls "out-of-band" to eliminate threat access to those data/processes and their associated controls; (3) Employ detection, reaction, and adaptation technologies that use automatic/autonomic system response to mitigate threat exploitation attempts. Adherence to the Three Tenets is expected to result in (1) ability to assemble secure systems from commercial components (the Three Tenets hold promise as an algorithm to assist in secure system composability), and (2) superior mitigation of nation state class threats. Extensive research and experimentation (including simulations using QuERIES, "black hatting," and red teaming) are underway to detect and examine conditions that invalidate the either of these expected results, and to identify which Tenets are necessary but not sufficient on their own to mitigate nation state threats. Quantitative measurements of adherence to the Three Tenets are being refined; these measurements are applicable both during the system design phase and during after-the-fact system assessments.	http://spi.dod.mil/tenets.htm

Institution	Project/Program	Description	URL or Reference
AMBER Consortium (Faculdad de Ciencias e Tecnologia da Universidade de Coimbra, Budapest University of Technology and Economics, City, Chalmers University of Technology, University of Florence, University of Newcastle upon Tyne, ResilTech S.R.L. Sponsored under European Union Information and Communication Technologies (ICT) Seventh Framework Program (FWP 7) ICT-2007.1.4 "Secure, Dependable and Trusted Infrastructures Research Area"	Assessing, Measuring, and Benchmarking Resilience (AMBER)	Define measurement and benchmarking techniques and metrics for comparatively evaluating the resilience and determining the trustworthiness of computer systems, networks, information infrastructures, and their components.	AMBER project Web page. Accessed 7 February 2009 at: http://amber.dei.uc.pt/index.php

Institution	Project/Program	Description	URL or Reference
ATSPI Technology Office, Air Force Research Laboratory, Wright-Patterson Air Force Base, Ohio.	A Threat Driven, System Design/Assessment Hypothesis for Cyber Security: The Three Tenets Algorithm.	A threat driven, secure system design/assessment hypothesis has been developed based on a heuristic algorithm used by the ATSPI Technology Office in secure system development for the last seven years. First, a three-part system oriented threat decomposition is defined as: (1) system susceptibilities (axiomatically described as logical and physical system access points); (2) threat accessibility to those access points (threat =user for a given use case); and (3) threat capability to exploit those access points. This decomposition is used as the threat framework for the Three Tenets. During secure system design, the Three Tenets are applied individually to target the three elements of the threat decomposition. The Three Tenets: (1) zealously focus on including only mission essential functions in the system under development to minimize inherent susceptibilities and enumerate critical security controls associated with those mission functions; (2) move data/processes for the essential mission elements and especially security controls associated with those functions 'out-of-band' either logically, physically, or both (eliminate threat access for a given use case); and, finally (3) employ detect, react, and adapt technologies that mitigate threat exploitation attempts *via* automatic/autonomic system response. The hypothesis is that adherence to the Three Tenets results in secure systems that are compatible with the enterprise, can be built from commercial components, and result in superior nation state class threat mitigation. Quantitative measurements of Tenet adherence are being refined that can be applied in either the system design phase or after the fact in a system assessment process. Extensive research and experimentation (including simulations such as QuERIES, black hatting, and red teaming) are underway to look for conditions that invalidate the hypothesis. Investigations into which tenets are necessary, but not sufficient conditions for nation/state threat mitigation, are ongoing. The Three Tenets also hold promise as an algorithm to assist in secure system composability.	ATPSI. "The Three Tenets of Cyber Security." Accessed 20 April 2009 at: http://spi.dod.mil/tenets.htm

Institution	Project/Program	Description	URL or Reference
Carleton University Department of System and Computer Engineering (funded by Solana Networks and CITO)	Quantitative Evaluation of Network Security	This project investigates the evaluation of network security using quantitative metrics. The main contribution is the experimental study carried out with real network traffic. The study is based on our Hierarchical Quantitative Metrics (HQM) model that enables the representation of important aspects of network security using quantitative metrics. The HQM model was experimentally demonstrated through an example set of Intrusion Detection metrics.	F. El-Hassan, A. Matrawy, N. Seddigh, and B. Nandy. "Experimental Evaluation of Network Security through a Hierarchical Quantitative Metrics Model", in *Proceedings of the International Conference on Communication, Network, and Information Security,* Cambridge, Massachusetts, October 2006.
Carnegie Mellon University (Pratyusa K. Manadhata and Jeannette M. Wing) Sponsored by Army Research Office (ARO), National Science Foundation (NSF), and CMU Software Engineering Institute	Attack Surface Measurement	Extend CMU's work on Microsoft RASQ to produce a metric to determine whether one version of a software system is more secure than another with respect to the system's attack surface (defining the attack surface of a system in terms of the system's attackability along three abstract dimensions: method, data, and channel). Unlike RASQ, this Attack Surface Metric will not require explicit identification of attack vectors. Formally define and generalize relative attack surface metric across multiple software systems using entry and exit points instead of root attack vectors to identify the resources that contribute to software attack surface. Produce a semi-formal mathematical model with little subjective analysis as the basis for producing a metric that is consistent across multiple types of software. Delivery to date: plug-in for the Eclipse IDE that performs majority of the calculations required for the new metric. The researchers expect to the metric to demonstrate what appears intuitive: the larger the attack surface, the more likely the system will be attacked, and hence the more insecure it is.	CMU Attack Surface Measurement project Web page. Accessed 29 January 2009 at: http://www.cs.cmu.edu/~pratyus/as.html *-and-* Pratyusa K. Manadhata and Jeannette M. Wing, CMU. An Attack Surface Metric. Technical Report CMU-CS-05-155, July 2005. Accessed 29 January 2009 at: http://reports-archive.adm.cs.cmu.edu/anon/2005/CMU-CS-05-155.pdf *-and-* Manadhata, Pratyusa K. and Jeannette M. Wing, CMU. An Attack Surface Metric. *Proceedings of the USENIX Security Workshop on Security Metrics (MetriCon),* Vancouver, British Columbia, Canada, August 2006. Accessed 29 January 2009 at: http://www.cs.cmu.edu/~pratyus/metricon.pdf *-and-* Pratyusa K. Manadhata, Yuecel Karabulut, and Jeannette M. Wing. "Measuring the Attack Surfaces of Enterprise Software," in *Proceedings of the International Symposium on Engineering Secure Software and Systems,* Leuven, Belgium, February 2009.

Institution	Project/Program	Description	URL or Reference
Carnegie Mellon University Software Engineering Institute	Enterprise Security Metrics	Define requirements for enterprise security metrics, to include: (1) They should identify the 'secure state' of the enterprise. (2) They should indicate whether the security strategy is aligned with organizational drivers. (3) They should indicate whether there is an equilibrium between requirements, efforts, asset values and controls. (4) They should reveal whether risk management is driving decisions. (5) They should reveal whether internal controls are supporting security strategy. (6) They should reveal whether residual risk is in line with risk tolerance. Example metrics include: number of assets for which risk assessments have been conducted; number of violations by staff who have taken security training; number of personnel with performance criteria related to IA; number of investigated security incidents; number of unmitigated vulnerabilities present in key systems.	James F. Steven and Bradford Willke, Carnegie Mellon University Software Engineering Institute. "Enterprise Security Metrics: Taking a Measure of What Matters." Presented at Third Annual Information Technology and Network Security Conference (SecureIT 2005), San Diego, California, 19-22 April 2005 (presentation revised April 2006). http://www.secureitconf.com/OLD/2005/presentations/Enterprise%20Security.pdf
Catholic University of Leuven (Louvain, Belgium) Sponsored by the Flemish government's SoBeNet project	Measuring Framework for Software Security Properties	Define a structured framework of properties adapted from the list of security principles and measurement practices in G. Stoneburner's, C. Hayden's, and A. Feringa's "Engineering principles for information technology security," NIST SP 800-27 Rev A (June 2004), M. Graff's and K. van Wyk's *Secure coding: principles and practices* (O'Reilly, 2003), SSE-CMM, and ISO 17799. Map the derived principles to the corresponding Software Development Life Cycle (SDLC) process phases to which they apply. Analyze the security principles that are relevant to the measurement of software security properties, and propose suitable metrics to measure them. This work falls under SoBeNet's Software Security for Network Applications project.	Riccardo Scandariato, Bart De Win, and Wouter Joosen, Katholieke Universiteit Leuven. "Towards a Measuring Framework for Security Properties of Software," in *Proceedings of the 2nd ACM Workshop on Quality of Protection (QOP 2006),* Alexandria, Virginia, 30 October 2006. Accessed 8 January 2009a at: http://www.cs.kuleuven.be/~riccardo/uploads/docs/qop2006.pdf

Institution	Project/Program	Description	URL or Reference
Catholic University of Leuven (Thomas Heyman and Christophe Huygens)	Metrics Associated with Security Patterns	Investigate ways in which security metrics can be directly associated with software security patterns to measure the effectiveness of those patterns in securing the software system. The security patterns under consideration describe software security functionality, so it is likely that the defined metrics will measure effectiveness of those security functions in terms of policy enforcement and/or intrusion/compromise prevention.	Thomas Heyman, Riccardo Scandariato, Christophe Huygens, and Wouter Joosen, Catholic University of Leuven. "Using Security Patterns to Combine Security Metrics," in *Proceedings of the Third International IEEE Conference on Availability, Reliability, and Security,* Barcelona, Spain, 4-7 March 2008, pp. 1156-1163. Digital Object Identifier: 10.1109/ARES.2008.54 *-and-* Thomas Heyman, Christophe Huygens, and Wouter Joosen, Catholic University of Leuven. "Developing secure applications with metrics in mind." Presented at Metricon 2.0, Boston, Massachusetts, 7 August 2007. Accessed 16 February 2009 at: http://www.securitymetrics.org/content/attach/Metricon2.0/heyman-metricon2-print.pdf *-also-* http://www.sintef.no/upload/IKT/9013/security/heyman-secse08.pdf
Colorado State University (O.H. Alhazmi, Y.K. Malaiya, I. Ray)	Predictive Undiscovered Vulnerability Density Metric	Adapt quantitative reliability metrics to prediction of vulnerability density in future software releases. Analyze data on vulnerabilities found in popular operating systems to determine whether "vulnerability density" is even useful as a metric and, if so, whether it is possible to pinpoint the fraction of all software defects that have security implications. Produce a "vulnerability discovery rate" metric *that quantifies* discovered vulnerabilities, and extrapolate from this a metric for estimating the number of undiscovered (*i.e.,* hypothetical) vulnerabilities in future software.	O. H. Alhazmi, Y.K. Malaiya, and I. Ray. Colorado State University. "Security Vulnerabilities in Software Systems: A Quantitative Perspective." http://web.archive.org/web/20070609151527 *-and-* http://www.cs.colostate.edu/~malaiya/635/IFIP-10.pdf

Institution	Project/Program	Description	URL or Reference
Crispin Cowan Sponsored by DARPA	Relative Vulnerability Metric	Develop a metric that compares the ratio of exploitable vulnerabilities in a system's components to those mitigated by security extensions, thereby calculating the percentage of vulnerabilities that are protected by those extensions and quantifying the effectiveness of a particular security extension/solution. This metric is only applicable to security extensions in that it measures relative improvements over the base (unprotected) systems.	Crispin Cowan. "Relative Vulnerability: An Empirical Assurance Metric." Presented at the Workshop on Measuring Assurance in Cyberspace, 44th IFP Working Group, June 2003. Accessed 3 February 2009 at: http://www2.laas.fr/IFIPWG/Workshops&Meetings/44 *-also-* http://www.homeport.org/~adam/shmoocon/shmoocon-cowan.pdf
Erasmus Research Institute of Management (ERIM), Erasmus University Rotterdam	Privacy Metrics	Define a set of qualitative and quantitative privacy metrics (quantitative and qualitative) pertaining to the relationships between the privacy protector and the information gatherer. The metrics should (1) enable the assessment and comparison of user scenarios and their differences; (2) define a notion of a privacy boundary encompassing a given set of information, behaviors, actions, and processes to be covered by a privacy agreement between the privacy protector and the information gatherer; (3) characterize the contribution of privacy enhancing technologies (PET). The researchers have developed a use case wherein the qualitative and quantitative privacy metrics are used to evaluate the Cisco Inc. privacy agreement.	Louis F. Pau. "Privacy Metrics and Boundaries." Published by Erasmus Research Institute of Management (ERIM) of Erasmus University Rotterdam, 4 March 2005. Accessed 11 December 2008 at: http://repub.eur.nl/publications/index/783244873 *-also-* Accessed 06 February 2009 at: http://publishing.eur.nl/ir/repub/asset/1935/ERS%202005%20013%20LIS.pdf
Foundstone (Pravir Chandra)	Flaw Severity Metrics and Severity-to-Complexity Metrics	Research a set of metrics for: (1) rating severity of reported software flaws (critical, high, medium, low); (2) determining whether flaw reports affect a product's market share, and if so whether reports of low severity flaws reduce market share less than reports of high severity flaws; (3) determining whether it is it possible to directly correlate number and severity of detected flaws and vulnerabilities with the complexity of the code that contains them.	Pravir Chandra. "Code Metrics." MetriCon 1.0. Accessed 20 April 2009 at: http://www.securitymetrics.org/content/attach/Welcome_blogentry_010806_1/software_chandra.ppt

Institution	Project/Program	Description	URL or Reference
Gjøvik University College (Gjøvik, Norway) Norwegian Information Security laboratory (NISlab)	Security Reporting	Investigate how reporting security indicators to management can contribute to reduction of vulnerabilities in critical infrastructure. Model/ prototype a security metrics Balanced Scorecard that can "continuously" validate the security level of Process Control Systems and SCADA networks. Describe a model or prototype of such a Scorecard for security metrics in a SCADA network. Create a toolkit of CI/KR security metrics from risk management, laws, regulations, *etc.*, related to information security in the chosen area of CI/KR. Establish a metrics library, a tool for setting up a metrics program, strategies for automated collection of parameters, indicators, and metrics, and strategies for representing the metrics in tables, graphs, figures, and Scorecards. Organize, analyze, and use data to validate the usefulness of these strategies, tool, and library. Define strategies for validating the accuracy of metrics and for utility company remediation to mitigate risk.	Finn Olav Sveen, Jose M. Sarriegi, Eliot Rich, and Jose J. Gonzalez, Gjøvik University College. "Toward viable information security reporting systems," in *Information Management and Computer Security,* Vol. 15 Issue 5, 2007, pp. 408-419. Digital Object Identifier: 10.1108/09685220710831143 *-and-* NISlab Security Reporting project Web page. Accessed 3 April 2009 at: http://www.nislab.no/research/projects/hig43706/live
I3P Sponsored by DHS and NIST	I3P Process Control Systems Security Research Project	Investigate ways to advance the security of process control systems (PCS), including through development of security metrics for PCS security by: (1) identifying existing metrics and standards that are or can be immediately applied to oil and gas industry PCS; (2) defining specific metrics requirements for PCS security metrics; (3) developing metrics tools that satisfy these requirements for use by the oil and gas industry	Institute for Information Infrastructure Protection (I3P). "Process Control Systems Security Research Project." Accessed 22 December 2008 at: *-and-* Martin Stoddard, Cliff Glantz, and James Shaw, Pacific Northwest National Laboratory, Deborah Bodeau, The MITRE Corporation, Rolf Carlson, Sandia National Laboratories, and Yacov Haimes, Chenyang Lian, and Joost Santos, University of Virginia. "Process Control System Security Metrics—State of Practice." I3P Research Report No. 1, 31 August 2005. Accessed 3 April 2009 at: http://stuweb.ee.mtu.edu/~ssmoily/section_4.pdf

Institution	Project/Program	Description	URL or Reference
Idaho National Laboratory, Sandia National Laboratory, Securicon, George Mason University Sponsored by DHS NCSD	Security Metrics for Process Control Systems	Determine the applicability of metrics to control systems, develop a metrics taxonomy that builds on the Automated Systems Reference Model (ASRM) to clarify difficult aspects of what types of metrics are useful and where they should be applied, and address the use of metrics to benchmark control systems security.	Ron Halbgewachs and Annie McIntyre, Sandia National Laboratories. "Security Metrics for Control Systems," presented at 2006 National SCADA Test Bed Visualization and Controls Program Peer Review. Accessed 11 December 2008 at: http://www.oe.energy.gov/DocumentsandMedia/Security_Metrics_for_Control_Systems_Halbgewachs.pdf *-and-* McIntyre, Annie, Blair Becker, Ron Halbgewachs, Sandia National Laboratories. "Security Metrics for Process Control Systems." Sandia Report SAND2007-2070P, September 2007. Accessed 11 December 2008 at: http://www.sandia.gov/scada/documents/McIntyre-SAND2007-2070P.pdf
Institute for Information Infrastructure Protection (I3P)	Better Security through Risk Pricing	Extends scoring metrics used in risk-based markets, CMMI, and ISO standards that show the effectiveness of technologies that reduce attack likelihood and organizational response capabilities.	Better Security through Risk Pricing project Web page. Accessed 7 February 2009 at: http://www.thei3p.org/research/risk_pricing.html

Institution	Project/Program	Description	URL or Reference
ISECOM	Source Code Analysis Risk Evaluation (SCARE) security complexity metric for measuring the security complexity of source code	Create a security complexity metric that will analyze source code and provide a realistic and factual representation of the potential of that source code to create a problematic binary by flagging code for a particular interaction type or control and allowing the developer to understand which Operational Security (OpSec) holes are not protected. The goal of this study is to apply the research findings to use OpSec ("holes" in the layers of protection), Controls (mitigations for those holes), and Limitations (problems/failures within OpSec and Controls) to calculate a SCARE value, that is comparable to a RAV, which reflects the degree (percentage) of equilibrium existing between OpSec holes, Controls, and lack of Limitations. The SCARE is intended to work with code in any programming language, but has only been demonstrated against C source code.	Accessed 29 January 2009 at: http://www.isecom.info/mirror/SCARE.0.3.pdf *-and-* Pete Herzog. SCARE - The Source Code Analysis Risk Evaluation. Accessed 29 January 2009 at: http://www.isecom.org/research/scare.shtml
MASTER Consortium (ATOS Origin Sociedad Anónima Española, SAP, Università di Trento, Engineering Ingegneria Informatica S.p.A., British Telecom, ETH, University of Stuttgart, LERO, ANECT, Deloitte, IBM, CESCE, Fondazione San Rafaele, Stiftelsen SINTEF) Sponsored under European Union Information and Communication Technologies (ICT) Seventh Framework Program (FWP 7) ICT-2007.1.4 "Secure, dependable and trusted infrastructures Research Area"	Managing Assurance, Security and Trust for sERvices (MASTER)	Develop methodologies and infrastructures to facilitate monitoring, enforcement, audit of quantifiable assurance and security indicators, protection and regulatory models, model transformations, business process assessment method, and verification tools for use with dynamic service oriented architectures (SOA); objective: to assure the security levels, trust levels, regulatory compliance of those SOAs. Results of this research: a strategic component of European Technology Platform NESSI Security and Trust pillar.	MASTER project Web page. Accessed 7 February 2009 at: http://www.master-fp7.eu/

Institution	Project/Program	Description	URL or Reference
Naval Research Laboratory (NRL) Center for High Assurance Computer Systems (CHACS) (John McDermott)	Quantitative Attack Potential Based Survivability Modeling for High Consequence Systems	Define a methodology for using Performance Evaluation Process Algebra (PEPA) to mathematically model and quantify the survivability of a software-based system to what he terms "human sponsored" (rather than stochastic) faults. Quantification is achieved using mean time to discovery of a vulnerability as the metric, *i.e.,* the longer a vulnerability goes undiscovered due to lack of activation of the associated fault, the longer the software system is considered to have survived in the undetected presence of that fault.	John McDermott, NRL CHACS. "Attack-Potential-based Survivability Modeling for High-Consequence Systems," in *Proceedings of the Third International Information Assurance Workshop,* March 2005, 119–130. Accessed 31 July 2007 at: http://chacs.nrl.navy.mil/publications/CHACS/2005/2005mcdermott-IWIA05preprint.pdf
Office of the Deputy Under Secretary Defense (Science & Technology) Anti-Tamper/Software Protection Initiative (AT/SPI)	Quantitative Evaluation of Risk for Investment Efficient Strategies (QuERIES)	Develop an adaptable methodology for quantitative cyber security risk assessment, using quantitative techniques from computer science, game theory, control theory, and economics. Initial testing of QuERIES has been performed in small-scale but realistic read teaming, black hat analysis, and cyber security risk assessment scenarios focused on protection of high-value DoD intellectual property (*e.g.,* weapons system and chip designs, complex software designs) for which a single loss would be catastrophic.	Lawrence Carin, Duke University, George Cybenko, Dartmouth College, and Jeff Hughes, Air Force Research Laboratory (AFRL). "Quantitative Evaluation of Risk for Investment Efficient Strategies in Cybersecurity: The QuERIES Methodology." AFRL/WS-07-2145, September 2007 Accessed 16 February 2009 at: http://www.securitymetrics.org/content/attach/Metricon3.0/metricon3-cybenko%20article.pdf
Pennsylvania State University, Polytechnic University, SAP	Security Scoring Vector (S-Vector) for Web Applications	Develop "a means to compare the security of different applications, and the basis for assessing if an application meets a set of prescribed security requirements." The S-vector measure will rate a Web application's implementation against its requirements for: (1) technical capabilities (*i.e.,* security functions); (2) structural protection (*i.e.,* security properties); (3) procedural methods (*i.e.,* processes used in developing, validating, and deploying/configuring the application). Together these ratings will be used to produce an overall security score (*i.e.,* the S-vector) for the application.	Russel Barton, William Hery, and Peng Liu. "An S-vector for Web Application Security Management." Penn State University. Accessed 9 February 2009 at: http://www.smeal.psu.edu/cdt/ebrcpubs/res_papers/2004_01.pdf

Institution	Project/Program	Description	URL or Reference
Politecnico di Torino (Italy), Wroclaw University of Technology (Poland), Stiftung Secure Information and Communication Technologies (Austria), Vodafone Omnitel NV (Italy), Bull SA (France), Saint Petersburg (Russia) Institute for Informatics and Automation of the Russian Academy of Sciences, Ministero della Giustizia (Italy), Universidad de Murcia (Spain), PRESECURE Consulting GmbH (Germany), BearingPoint INFONOVA GmbH (Germany; until 2005 Sponsored by the European Commission	Policy-based Security Tools and Framework (POSITIF)	A major aspect of POSITIF's research focuses on defining and using formal models, attack graphs, and simulations to enable security measurement.	POSITIF Project Overview. Accessed 16 February 2009 at: http://www.positif.org

Institution	Project/Program	Description	URL or Reference
St. Petersburg Institute for Informatics and Automation (SPIIRAS) Computer Security Research Group Sponsored by Russian Foundation of Basic Research, 2004-2006	Modeling of information security processes in computer networks in adversarial environment: formal framework, mathematical models, multi-agent architecture, software prototype and experimental evaluation	Research results include: (1) development of models of computer attacks and malefactor, attack tree formation and an estimation of computer network security level; (2) development of supporting automated technique and software tool for detailed analysis of computer network security based on the malefactor models.	Igor Kotenko and Mikhail Stepashkin. "Attack Graph Based Evaluation of Network Security", in *Proceedings of the 10th IFIP Conference on Communications and Multimedia Security (CMS 2006),* Heraklion, Greece, 19-21 October 2006, pp. 216-227. Accessed 13 April 2009 at: http://comsec.spb.ru/en/papers/31/getfile *-and-* Igor Kotenko and Mikhail Stepashkin. "Network Security Evaluation Based on Simulation of Malefactor's Behavior," in *Proceedings of the International Conference on Security and Cryptography (SECRYPT 2006),* Portugal, 7-10 August 2006, pp. 339-344. Accessed 13 April 2009 at: http://stepashkin.com/pubs/2006/secrypt-06-paper.pdf *-also-* http://comsec.spb.ru/en/papers/67/getfile *-and-* Igor Kotenko and Mikhail Stepashkin. "Analyzing network security using malefactor action graphs," in *International Journal of Computer Science and Network Security,* Volume 6 Number 6, June 2006, pp. 226-235. Accessed 13 April 2009 at: http://comsec.spb.ru/en/papers/36/getfile

Institution	Project/Program	Description	URL or Reference
Sandia National Laboratories	National SCADA Test Bed Visualization and Controls Program: Security Metrics for Control Systems	Develop an approach to security metrics as they pertain to control systems, including development of a metrics taxonomy and guidelines for using metrics. This approach is targeted at the organizational level for an audience of asset owners and control systems management. For asset owners, this means there should be a way to measure and determine their current security posture and the improvements that will be attained upon implementation of standards for those control systems. The final products of this project included the taxonomy, a report, and a presentation to stakeholders (if required). It is anticipated asset owners will use these products to assist in arriving at a security plan that involves identification of critical areas within the architecture, the selection of applicable best practices, and the definition and application of relevant metrics in those areas.	Annie McIntyre, Blair Becker, and Ron Halbgewachs, Sandia National Laboratories. "Security Metrics for Process Control Systems." Sandia Report SAND2007-2070P, September 2007. Accessed 7 February 2009 at: http://www.sandia.gov/scada/documents/McIntyre-SAND2007-2070P.pdf

Institution	Project/Program	Description	URL or Reference
SERENITY Consortium (Athens Technology Center, ATOS, City University of London, Deep Blue, Engineering Ingegneria Informatica S.p.A, Fraunhofer SIT, *Catholic University of Leuven,** Telefonica I+D, SAP, Security Technology Competence Centre, Strategies Telecoms & Multimedia, Thales, *University of Trento,** University of Aegean, University of Malaga) Sponsored under European Commission IST 6th Framework Programme * *known to be engaged in SERENITY metrics-related research*	System Engineering for Security and Dependability (SERENITY)	SERENITY aims at providing security and dependability in Ambient Intelligence systems (AmI). Work package 1.5 of the project focuses on Identification of Security & Privacy threats, risks, and metrics for patterns in high-level business, management, and organizational policies for privacy and security at enterprise level. Another research activity focused on extending a model-based approach to security management to include concepts and methods that enable quantitative assessments based on security metrics aggregated within the framework of the underlying model. Specifically, the metrics are derived by measuring numbers of attacks by certain threats, then estimating their likelihood of propagation along the dependencies in the underlying model. This approach enables the identification of which threats have the greatest impact on business security objectives, and how various security controls differ in their effectiveness mitigating these threats. Another research activity focused on investigating ways in which security metrics can be directly associated with software security patterns to measure the effectiveness of those patterns in securing the software system. The security patterns under consideration describe software security functionality, so it is likely that the defined metrics will measure effectiveness of those security functions in terms of policy enforcement and/or intrusion/compromise prevention. Also within this activity is an effort to define a quantitative approach to assessing the security of a pattern-based software architecture, with security patterns used to measure the extent to which the architecture is protected against relevant threats. Threat coverage metrics are associated with the security patterns, and an aggregation algorithm is used to compute an overall security indicator for the software design. With such indicators applied to different pattern-based designs, the approach aids in comparing the security of design alternatives.	SERENITY project. Accessed 7 February 2009 at: http://www.serenity-project.org *-and-* Breu, Ruth, Frank Innerhofer–Oberperfler, Fabio Massacci, and Artsiom Yautsiukhin. "Quantitative assessment of enterprise security system," in *Proceedings of the 1st International Workshop on Privacy and Assurance (WPA-2008)*, Barcelona, Spain, 4-7 March 2008. Accessed 7 February 2009 at: http://www.dit.unitn.it/~evtiukhi/Resources/BREU-08-WPA.pdf *-and-* Artsiom Yautsiukhin, Thomas Heyman, Riccardo Scandariato, Fabio Massacci, and Wouter Joosen. "Towards a quantitative assessment of security in software architectures," in *Proceedings of the 13th Nordic Workshop on Secure IT Systems (NordSec 2008)*, Copenhagen, Denmark, 9-10 October 2008. Accessed 7 February 2009 at: http://www.dit.unitn.it/~evtiukhi/Resources/YAUT-08-NordSec.pdf
Solana Networks and Sombra Labs Sponsored by Deptartment of Public Safety and Emergency Preparedness Canada (PSEPC)	Network Security Metrics	A state of the art report (ca 2004) of IA metrics. Proposed a new definition of Information Assurance that includes security, quality of service, and availability. Evaluated current IA taxonomies and proposed a new taxonomy along with a metric that represents the health of an organization's network.	Nabil Seddigh, Peter Pieda, Matrawy Ashraf, Biswajit Nandy, John Lambadaris, Adam Hatfield. "Current Trends and Advances in Information Assurance Metrics." Second Annual Conference on Privacy, Security and Trust. http://dev.hil.unb.ca/Texts/PST/pdf/seddigh.pdf

Institution	Project/Program	Description	URL or Reference
SRI International Sponsored by DARPA	Critical Security Rating (CSR); Global Measure of Assurance	SRI International worked to define a "global measure," referred to as a Critical Security Rating (CSR), for inclusion in the Assurance Argument. The CSR reflects a calculation from numerous "local" IA measures captured for the system under consideration, *i.e.,* measures of particular, specific aspects of the system's IA; a local measure might, in fact, pertain only to a single subsystem or component of the system overall. The CSR, then, was intended to provide a single, easy-to-calculate, system-relevant, and easily and widely comprehensible measure of the assurance for the system. Through experimentation, the SRI team refined the CSR by limiting the local measures from which it was calculated to those that were (mostly) probabilistic (being "like" measures, these could be more easily combined in a calculation of overall system IA), and by other adjustments. While initially conceived as a data point for inclusion in Assurance Arguments generated by the SRI-developed Structured Evidential Argumentation System (SEAS), SRI was one of several "seedling performers" identified by DARPA, which evaluated the CSR in the context of its Measuring Assurance in CyberSpace program. Another Measuring Assurance in CyberSpace "seedling performer," BBN Technologies, chose the CSR as the measure for quantifying adversary impact in the red team models they developed in their research.	Victoria Stavridou, Bob Riemenschneider, and Steve Dawson, SRI International. "Systematic Information Assurance Assessment." Presented at the 44th IFIP Working Group 10.4 Workshop on Measuring Assurance in Cyber Space, Monterey, California, 26 June 2003. Accessed 6 February 2009 at: http://www.laas.fr/IFIPWG/Workshops&Meetings/44/W1/08-Stavridou.pdf

Institution	Project/Program	Description	URL or Reference
Stockholm University/KTH	Security metrics for evaluation of information systems security	Examine a framework that can be used to develop Common Criteria Protection Profiles by applying various established measurement methodologies, including Federal Bridge Certification Authority certificate policy assurance levels for public key certificates (Rudimentary, Basic, Medium, High); International Systems Security Engineering Association (ISSEA) SSE-CMM process area metrics for measuring organization secure system engineering maturity; Common Criteria (CC) assurance levels for rating assurance of evaluated security products; and a social-technical model. Use the Common Criteria to identify security functions of an X.509 certificate/PKI-enabled application, and associate one or more metrics with each function identified. These metrics may fall into the following categories: (1) Impact metrics, for measuring impact to the organization when a security function is compromised; (2) Risk impact and risk likelihood metrics; (3) Security service/security function assurance levels; (4) Policy metrics; (5) Human factors metrics to (a) delineate early, late, and last adopters of information systems technology; (b) measure what people consider to be ethical on unethical in regard to computer misuse and crime.	Kevin Clark, Ethan Singleton, Stephen Tyree, and John Hale, Chaula, Job Asheri, Louise Yngström, and Stewart Kowalski. "Security Metrics and Evaluation of Information Systems Security," in *Proceedings of Information Security South Africa Enabling Tomorrow Conference (ISSA 2004)*, Midrand, South Africa, 30 June 2004-2 July 2004. Accessed 29 December 2008 at: http://icsa.cs.up.ac.za/issa/2004/Proceedings/Research/048.pdf

Institution	Project/Program	Description	URL or Reference
Thales Communications, S.A. Sponsored under European Union Information and Communication Technologies (ICT) Sixth Framework Program (FWP 6) IST-2004-2.4.3 "Towards a global dependability and security framework"	DEpendability and Security by Enhanced REConfigurability (DESEREC) Project	DESEREC involves development of approaches and tools to design, model, simulate, and plan critical infrastructures to dramatically improve their resilience, integration of various detection mechanisms to ensure fast detection of severe incidents but also to detect complex ones, and definition of a framework for computer-aided countermeasures to respond in a quick and appropriate way to a large range of incidents and rapidly mitigate the threats to dependability through reconfiguration and other system/network survivability mechanisms. Specific metrics-related work under DESEREC includes the use of attack graphs to compute an "attackability metric" for static evaluation, and implementation of a security assurance assessment system (the "Security Cockpit") to generate the real world equivalents of the identified static metrics.	Nguyen Pham, Loïc Baud, Patrick Bellot, and Michel Riguidel, Telecom Paris École Nationale Supérieure des Télécommunications. "A Near Real-time System for Security Assurance Assessment," in *Proceedings of the Third International Conference on Internet Monitoring and Protection (ICIMP 2008),* Bucharest, Romania, 29 June–5 July 2008. Accessed 8 January 2007 at: http://www.infres.enst.fr/~bellot/publis/ICIMP2008.pdf *-and-* Nguyen Pham, Loic Baud, Patrick Bellot, and Michel Riguidel, Telecom Paris École Nationale Supérieure des Télécommunications. "Towards a Security Cockpit," in *Proceedings of the Second International Conference on Information Security and Assurance (ISA 2008),* Busan, Korea, 24-26 April 2008. Accessed 8 January 2009 at: http://www.infres.enst.fr/~bellot/publis/543.pdf *-and-* DESEREC Web pages. Accessed 4 February 2009 at: http://www.deserec.eu

Institution	Project/Program	Description	URL or Reference
Université de Toulouse Centre National de la Recherche Scientifique Laboratoire d'Analyse et d'Architecture des Systèmes (CNRS-LAAS) Groupe Tolérance aux fautes et Sûreté de Fonctionnement informatique (TSF) Sponsored under European Commission IST 6th Framework Programme	Security, Safety, and Quality Evaluation for Dependable Systems (SQUALE) Resilience for Survivability in IST (ReSIST) Other EC-sponsored projects	In work that began in the late 1990s under the European Commission-sponsored SQUALE project, continued under a variety of EC-sponsored research projects, and now continues under the umbrella of the EC-sponsored ReSIST project, CNRS-LAAS (also a "seedling performer" under the DARPA Measuring Assurance in CyberSpace program), has since developed an approach to computation of meaningful vulnerability/attacker effort correlation measures. Based on an understanding of the security policy, and algebraic models of operational system vulnerabilities and attack processes, measures were computed for individual attacker-target couples in the models, including (1) Mean Effort To security Failure (METF), Shortest Path (Mean Effort required to go through shortest path to the target node), and Number of Paths from the attacker to the target node. They also developed the Évaluation de la Sécurité OPErationnelle (ESOPE) tool set to automate the definition of security policy, the modeling of vulnerabilities into privilege graphs (based on analysis of real vulnerabilities in a UNIX system) and attackers, and computation of measures based on those data. Through experimentation, qualitatively validate these measures and models, and adjust automated modeling approach by using honeynets as data source for use in building the vulnerability and attack models, thereby improving accuracy and significance of the calculated measures. The larger ReSIST program is developing a Resilient Computing Curriculum and Resilience Knowledge Base for use by academics and researchers.	Yves Deswarte and Mohamed Kaâniche, Université de Toulouse CNRS-LAAS. "Towards Quantitative Security Evaluation." Presented at the 44th IFIP Working Group 10.4 Workshop on Measuring Assurance in Cyber Space, Monterey, California, 26 June 2003. Accessed 6 February 2009 at: http://www.laas.fr/IFIPWG/Workshops&Meetings/44/W1/11-Deswarte.pdf *-and-* Geraldine Vache, CNRS-LAAS, Université de Toulouse (France). "Towards Information System Security Metrics," in *Proceedings of the Seventh European Dependable Computing Conference (EDCC-7)*, Kaunas, Lithuania, 7-9 May 2008 -and- ReSIST project Web page. Accessed 7 February 2009 at: http://www.resist-noe.org *-and-* SQUALE project Web page. Accessed 7 February 2009 at: http://research.cs.ncl.ac.uk/cabernet/www.laas.research.ec.org/squale
University of Illinois at Champaign-Urbana Design and Validation of Reliable Networked Systems (DEPEND) group Sponsored by DARPA	Measurement-based characterization of networked system dependability and security	Apply ANALYZE-NOW monitoring and data gathering tool to monitoring and measuring the dependability and security of networked systems and, ultimately, the Internet. This work includes the implementation of metrics to describe reliability of Internet network hosts.	University of Illinois/Champaign-Urbana DEPEND group. Security and Performance Modeling: An Environment and Tools for Measurement-based Evaluation of the Availability of Field Systems project Web page. Accessed 6 February 2009 at: http://www.crhc.illinois.edu/DEPEND/projects/security/security.html

Institution	Project/Program	Description	URL or Reference
University of Illinois at Champaign-Urbana PERFORM group Sponsored by NSF	Möbius	Apply ITUA work on survivability measures in Möbius, a software tool developed by the PERFORM group for modeling the behavior of complex systems. Originally developed for studying the reliability, availability, and performance of computer and network systems, Möbius' use expanded to modeling of a broad range of discrete-event systems, ranging from biochemical reactions within genes to the effects of malicious attackers on secure computer systems. One of the key features of Möbius is its support for customized measures for measuring system properties (*e.g.,* reliability, availability, performance, security) by enabling users to construct detailed expressions that measure the exact information desired about the system, with the defined measurements conducted at specific points in time, over periods of time, or whenever the system reaches a steady state.	University of Illinois-Champaign/Urbana PERFORM group. Möbius project Web Page. Accessed 6 February 2009 at: http://www.mobius.uiuc.edu/
University of Illinois at Champaign-Urbana PERFORM group Sponsored by DARPA	Compiler-Enabled Model- and Measurement-Driven Adaptation Environment for Dependability and Performance	Apply earlier survivability measurement research to developing a "Compiler-Enabled Model- and Measurement-Driven Adaptation Environment for Dependability and Performance," which uses error and performance measurement techniques to characterize system error behavior, enable early error detection, guide online adaptation models, and improve compiler-based error detection and tolerance. A particular focus of this research has been use of measurements in operational systems to characterize real-world issues in the field, such as correlated errors and error propagation—issues that often escape current detection mechanisms.	University of Illinois-Champaign/Urbana PERFORM group. A Compiler-Enabled Model- and Measurement-Driven Adaptation Environment for Dependability and Performance (NSF CNS-0406351) project Web page. Accessed 6 February 2009 at: http://perform.csl.illinois.edu/projects/newNSFNGS.html
University of Illinois at Champaign-Urbana Performability Engineering Research group (PERFORM) Sponsored by DARPA	Intrusion Tolerance by Unpredictable Adaptation (ITUA)	As part of architecture for adding intrusion tolerance *via* middleware to information systems, define probabilistic measures that could be used to measure system survivability in the face of attacks and intrusions in aid of validation of intrusion tolerance as a viable approach to information security.	William H. Sanders, University of Illinois at Champaign-Urbana. "Probabilistic Quantification of Survivability Properties." Presented at the 44th IFIP Working Group 10.4 Workshop on Measuring Assurance in Cyber Space, Monterey, California, 26 June 2003. Accessed 6 February 2009 at: http://www.laas.fr/IFIPWG/Workshops&Meetings/44/W1/07-Sanders.pdf

Institution	Project/Program	Description	URL or Reference
University of Mannheim Laboratory for Dependable Distributed Systems	Dependability Metrics	Among the quantitative dependability measurement approaches under development includes "a practical approach which allows to assess the security of a system using a qualitative effort-based metric." The approach is based on the notion of security testing (also known as penetration testing).	Dependability Metrics project page. Accessed 13 April 2009 at: http://pi1.informatik.uni-mannheim.de/index.php?pagecontent=site%2FResearch.menu%2FProjects.page%2FDepandability_Metrics.page
University of Nevada at Reno Database and Security Lab	Adaptive Security Metrics for Computer Systems	To overcome the system-specificity of most metric systems by defining metrics "that are portable adaptable to any particular type of system," developing a matrix-based mathematical model for evaluating predefined security metrics of a particular computer system, then tailoring those metrics to reflect the unique security factors of another system by adding, deleting, or modifying the security and integrity factors captured by the matrix.)	Gregory L. Vert and Satish Baddelpeli, University of Nevada at Reno. "Adaptive Security Metrics for Computer Systems," in *Proceedings of the 2006 International Conference on Security and Management (SAM 2006)*. Las Vegas, Nevada, 26-29 June 2006, pp. 351-356. Accessed 7 January 2009 at: http://ww1.ucmss.com/books/LFS/CSREA2006/SAM8020.pdf *-also-* Vert, Gregory and Phanid Dogiparthi, University of Nevada at Reno. "A Generic Metric for Evaluation of Database Security," in *Proceedings of the 2007 International Conference on Security and Management (SAM 2007)*. Las Vegas, Nevada, USA, 25-28 June 2007, pp. 298-305

Institution	Project/Program	Description	URL or Reference
University of Pennsylvania Computer and Information Science Department	Quantitative Denial of Service research	The measurement-related objectives of this research included establishment of better metrics of security, examples of which included: (1) a denial of service workfactor-like formulation that is a composite of a variety of measurements with imprecise but meaningful weights; (2) quantification of the relative security of systems and software to support informed tradeoffs between security and overhead *vs*. features and convenience; (3) statistically based models that quantitatively capture rules of thumb regarding salient properties of software packages.	Michael B. Greenwald, Carl A. Gunter, B. Knutsson, Andre Scedrov, Jonathan M. Smith, and S. Zdancewic, "Computer Security is Not a Science (but it should be)," in the *Large-Scale Network Security Workshop,* Landsdowne, VA, 13-14 March 2003. http://www.cis.upenn.edu/~mbgreen/papers/lns03-security-science-whitepaper.pdf *-also-* http://www.cis.upenn.edu/~stevez/papers/GGKS03.pdf
University of Southern California Center for Systems and Software Engineering	Security Economics and Threat Modeling for IT Systems - A Stakeholder Value Driven Approach	Devised a quantitative model, the Threat Modeling framework based on Attack Path analysis (T-MAP), to measure and prioritize security threats by calculating the total severity weights of relevant attacking paths for IT systems. Compared to value-neutral approaches, T-MAP is dynamic and sensitive to system stakeholder value priorities and IT environment. It distills the technical details of more than 23,000 known software vulnerabilities into management-friendly numbers at a high-level. T-MAP has also been demonstrated to aid in prioritizing and estimating the cost-effectiveness of security investments, specifically the cost-effectiveness of security improvements attained through system patching, user account control, and firewall deployment.	Security Economics and Threat Modeling for IT Systems project. Accessed 7 February 2009 at: http://csse.usc.edu/csse/research/COTS_Security/

Institution	Project/Program	Description	URL or Reference
University of Tulsa	Security Risk Metrics; Strata-Gem	Define a risk assessment methodology that synthesizes high-level enterprise assessment with detailed technical analysis to generate security metrics. Increase methodology scalability by automating the identification of critical states and vulnerabilities. Increase usefulness with a means to differentiate between likely and unlikely attacks based on multi-stage attack trees and fault tree analysis for rating risks associated with various types of adversaries, likely attack scenarios. Develop a risk assessment framework that uses mission trees to link organizational objectives to their implementing IT assets, thereby identifying critical states that an attacker can reach to affect the organization's mission. Using these states, attack and fault trees can be created and analyzed to determine the likelihood of attack.	Clark, Kevin, Jerald Dawkins, and John Hale. "Security Risk Metrics: Fusing Enterprise Objectives and Vulnerabilities," in *Proceedings of the IEEE Workshop on Information Assurance and Security (IAW '05),* United States Military Academy, West Point, NY, 15-17 June 2005. Accessed 7 February 2009 at: http://serv1.ist.psu.edu:8080/viewdoc/download;jsessionid=F57FE1A9C334ECA823A2289464B8D9FA?doi=10.1.1.93.3272&rep=rep1&type=pdf *-and-* Clark, Kevin, Ethan Singleton, Stephen Tyree, and John Hale, University of Tulsa. "Strata-Gem: risk assessment through mission modeling," in *Proceedings of the 4th ACM Workshop on Quality of Protection,* Alexandria, Virginia, 2008, pp. 51-58.
University of Victoria Information Security and Object Technology (ISOT) Research Lab (British Columbia, Canada)	Security Testing and Engineering using Metrics (STEM)	Identify, develop and validate mathematically and empirically a family of metrics that can be used to guide efficiently the software security engineering process. Propose a set of design metrics that allow for measurement of basic security attributes such as confidentiality, integrity, and availability. Extend this metrics suite to other measurement of software security attributes. Define an axiomatic framework for rigorous evaluation of software security metrics, and develop a benchmark for empirical evaluation of these metrics. Develop a toolkit (STEM) that will assist developers in generating and interpreting the metrics from Unified Modeling Language (UML) models.	STEM project Web page. Accessed 7 February 2009 at: http://www.isot.ece.uvic.ca/projects/stem/index.html

Institution	Project/Program	Description	URL or Reference
California State University San Bernardino Information Assurance and Security Management (IASM) Center	Value of information security investments	Assess existing approaches for measuring the normative, real, and perceived value of investments in information security.	Tony Coulson, Jake Zhu, and C.E. Tapie Rohm, California State University-San Bernardino; and Shan Miyuan, Hunan University-Changsha. "The Price of Security: The Challenge of Measuring Business Value Investments in Securing Information Systems," in *Communications of the IIMA*, Volume 5 Issue 4, 2005. Accessed 25 March 2009 at: http://www.iima.org/CIIMA/8%20 5.4_Coulson_19_24.pdf *-and-* Tony Coulson, Jake Zhu, Kurt Collins, Walter Stewart, C.E. Tapie Rohm, Jr., California State University-San Bernardino. "Security: Valuing Increased Overhead Costs," in *Proceedings of the 10th Colloquium for Information Systems Security Education,* Adelphi, MD, 5-8 June 2006. Accessed 25 March 2009 at: http://www.cisse.info/colloquia/cisse10/ proceedings10/pdfs/papers/S05P03.pdf
Carnegie Mellon University H. John Heinz III School of Public Policy and Management	Economics of Information and Software Security	Measurement of risk-based return on investment for information security and software security. Measurement of business impact of software vulnerability disclosure.	Ashish Arora, Dennis Hall, C. Ariel Pinto, Dwayne Ramsey, and Rahul Telang. "Measuring the Risk-Based Value of IT Security Solutions," IT Professional, Vol. 6 No. 6, Nov./Dec. 2004, pp. 35-42. Digital Object Identifier: 10.1109/MITP.2004.89

Institution	Project/Program	Description	URL or Reference
University of Maryland-College Park Department of Mechanical Engineering Center for Risk and Reliability Sponsored by NSF	Probabilistic Evaluation of Computer Security Based on Experimental Data	Propose a new approach for evaluating the security of a computer network based on experimental data. The results obtained from this project will allow security practitioners to quantify the security of a computer network. This research includes the development of different tools and large data collections on vulnerabilities and attackers.	Gerry Sneeringer and Michel Cukier. Quantification of Security: Some Case Studies. Presented at University of Maryland Department of Mechanical Engineering Research Review Day, 19 March 2007. Accessed 25 March 2009 at: http://www.enme.umd.edu/events/RRD/2007/Presentations/SecuritySneeringerCukier.pdf
Colorado State University Software Assurance Laboratory	Security Measurement	Definition of metrics for security vulnerabilities, design tradeoffs involving security	Omar H. Alhazmi, Yashwant K. Malaiya, and Indrakshi Ray. "Measuring, Analyzing and Predicting Security Vulnerabilities in Software Systems," in *Computers and Security Journal,* Volume 26 Issue 3, May 2007, pp. 219-228. Accessed 25 March 2009 at: http://www.cs.colostate.edu/~malaiya/pub/com&security_darticle.pdf *-and-* O. H. Alhazmi. Assessing Vulnerabilities in Software Systems: A Quantitative Approach. Ph.D. Dissertation, Colorado State University Computer Science Department, 6 November 2006. Accessed 25 March 2009 at: http://www.cs.colostate.edu/~malaiya/pub/omar_dissertation.pdf

Institution	Project/Program	Description	URL or Reference
University of Victoria (British Columbia, Canada) Information Security and Object Technology (ISOT) Research Lab	Security Testing and Engineering Using Metrics (STEM)	Proposed collection of design metrics that allow measurement of basic security attributes such as confidentiality, integrity, and availability. Definition of an axiomatic framework for rigorous evaluation of software security metrics. Extension of proposed metrics suite to measure other software security attributes. Development of a benchmark for empirical evaluation of the proposed metrics. Development of a STEM toolkit to assist developers in generating and interpreting the metrics from UML models.	http://www.isot.ece.uvic.ca/projects/stem/index.html
Stockholm University and Royal Institute of Technology Deptartment of Computer and Systems Sciences Information Systems Security Lab (SecLab)	Security Metrics	Identification of Key Performance Indicators underpinning ROI estimations for security investments	Job Asheri Chaula, Louise Yngström, and Stewart Kowalski. "Security Metrics Evaluation of Information System Security," in *Proceedings of Information Security South Africa*, 30 June-2July 2004, Midrand, South Africa. Accessed 25 March 2009 at: http://icsa.cs.up.ac.za/issa/2004/Proceedings/Research/048.pdf *-and-* Erkan Kahraman. "Evaluating IT security performance with quantifiable metrics." Masters Thesis for Stockholm University and Royal Institute of Technology, 1 February 2005. Accessed 25 March 2009 at: http://dsv.su.se/research/seclab/pages/pdf-files/2005-x-245.pdf
Electric Power Research Institute (EPRI)	Security Metrics for Energy Management Centers	EPRI, in partnership with Dyonyx and Lumina Systems, is developing a tool that will provide quantitative estimates of the value of security activities for Energy Management Centers. A prototype version of the tool has been produced that is based on Lumina Systems' Analytica product.	Madhava Sushilendra, Electrical Power Research Institute. "Roadmap to Secure Control Systems in the Energy Sector." Presented at the Energy Sector Control Systems Working Group ieRoadmap Workshop, Chicago, IL, 28-29 May 2008. Accessed 25 March 2009 at: http://www.controlsystemsroadmap.net/pdfs/17%20Security%20Metrics%20for%20EMS.pdf

Institution	Project/Program	Description	URL or Reference
Telecom ParisTech (ENST) Institut TELECOM Computer Science and Networking Department (INFRES)	Vers un cockpit de sécurité (Towards a Security Cockpit)	Development of a "security cockpit" tool to help assess large, networked, IT-driven systems and determine their overall security assurance levels. The tool uses attack graphs to compute an attackability metric value for the system, and to define other metrics for anomaly detection that further support assessment of both static and dynamic views of the system.	Nguyen Pham, Loic Baud, Patrick Bellot, Michel Riguidel. "Towards a Security Cockpit," in *Proceedings of the International Conference on Information Security and Assurance (ISA 2008),* Busan (Pusan), South Korea, 24-26 April 2008, pp. 374-379. http://www.infres.enst.fr/~bellot/publis/743.pdf *-and-* Pham, Nguyen, Loic Baud, Patrick Bellot, Michel Riguidel. "Near Real-time System for Security Assurance Assessment," in *Proceedings of the Third International Conference on Internet Monitoring and Protection (ICIMP '08),* Bucharest, Romania, 29 June-5 July 2008, pp. 152-160. Accessed 25 March 2009 at: http://www.infres.enst.fr/~bellot/publis/ICIMP2008.pdf

F

Why is CS/IA Measurement Challenging

The government research community has publicly acknowledged the importance of CS/IA measurement. The community has also acknowledged the challenges involved in achieving the measures and measurement techniques that will yield meaningful assessments and quantifications of information, system, and network security assurance, effectiveness of technical and non-technical security measures, process security, *etc.*

The two excerpts below, from the INFOSEC Research Council's (IRC) "Hard Problems List of 2005" [181] (the last time IRC published such a list) and the National Science and Technology Council Interagency Working Group on Cyber Security and Information Assurance's Federal Plan for Cyber Security and Information Assurance Research and Development of April 2006, are representative of this government research community's views.

F.1 IRC Hard Problem No. 8 Enterprise-Level Security Metrics Definition:

Along with the systems and component-level metrics that have been mentioned in the preceding "hard problems," and the technology-specific metrics that are continuing to emerge with new technologies year after year, it is essential to have a macro-level view of security within an organization.

What happens when all the systems, processes, and tools are turned on? Today, government decision makers and corporate leaders do not have answers to such important questions as—

- How secure is my organization?
- Has our security posture improved over the last year?
- To what degree has security improved in response to changing threats and technology?
- How do we compare with our peers?
- How secure is this product or software that we are purchasing?
- How does it fit into the existing systems and networks?
- What is the marginal change in our security, given the use of a new tool or practice?

Most organizations view the answers to these questions in the short term from a financial mind-set and make a cost-benefit trade analysis. The decisions resulting from this analysis will frequently be to the detriment of significant improvements in security in the long term, which may require costly new development.

Threat

One of the most insidious threats to security metrics lies in the metrics themselves. The mere existence of a metric may encourage its purveyors to over-endow the significance of the metric. A common risk is that analyses may be based on spurious assumptions, inadequate models, and flawed tools, and that the metrics themselves are inherently incomplete—often a one-dimensional projection of a multidimensional situation.

Furthermore, a combination of metrics in the small (*e.g.,* regarding specific attributes of specific components) typically do not compose into metrics in the large (*e.g.,* regarding the enterprise as a whole).

Motivation

Without answers to these important questions, management is mired in a quandary without meaningful direction. The dearth of metrics and decision-making tools places the determination of information security risk to the enterprise on the judgment of IT security practitioners. The gathering and sharing of information about threats, vulnerabilities, and attacks is critical to establishment of a scientific approach to managing these risks.

Metrics and a risk management framework must guide decision makers—

- First, recent events (like 9/11 and its economic impacts), along with intelligence reporting, have shown the existence of considerable threats to the critical infrastructures of the United States.
- Second, financial restrictions require explicit understanding of how funds invested in security will affect an organization.

- Last, regulations, such as FISMA and the Public Company Accounting and Investor Protection Act, require the government and private sector firms to become accountable in the area of IT security.

These factors support the need for decision makers to have sound metrics and a decision-making framework that embraces risk management principles.

As technology continues to advance into every facet of society, societal dependence on technology grows. This dependence has increased unabated. Technologies are at risk not only from highly publicized hackers, but also from more deceptive and dangerous nation-states and terrorists.

In addition, systems that are poorly designed, implemented, and maintained tend to fall apart on their own, without any attacks.

Organizations need a metric-based approach built on qualitative and quantitative risk management principles for the effective allocation of IT security resources, in addition to empirical methods.

Challenges

Many challenges still exist in this area—

- First, in a world where technology, threats, and users change so quickly, tomorrow's risks may be quite different from yesterday's risks, and historical data is not a sufficiently reliable predictor of the future.
- Second, organizations are reluctant to share information, thus making data on emerging threats difficult to collect. Even when network owners are aware of threats, the constant barrage and high volume of low-level threats (*e.g.,* phishing attacks and spam) distract many organizations from defending against potentially devastating attacks representing more serious threats.
- Third, risk management is complicated by a dearth of adequate information on capabilities and intentions of threat agents, such as terrorists and hostile nations. To estimate the potential costs of downtime, loss, or impairment of tangible and intangible assets across an entire organization for previously unseen events is almost impossible.
- Finally, complete security is unattainable at any price, and security is not simply a matter of technology.

Many factors complicate the statistical foundations of any approach to predict the likelihood of attacks for a range of impacts. Better protection for some resources often merely increases the likelihood of other resources being attacked. Attackers will shift their focus from more protected resources to less well-protected resources.

Furthermore, IT security technology is often bought through a principle of adverse selection: Groups that are the most lucrative targets will buy the most defensive technology, and although those defenses may decrease attacks, those organizations may still be attacked more than their peers that are less lucrative targets. This creates a misperception that defenses draw attacks.

Amplifying this perception, the best defended groups often have the best sensors, catching and reporting more successful attacks than other groups. This leads to the imprecise conclusion that funds spent on defenses have allowed the number of successful attacks to rise, when in reality, the number of successful attacks may have fallen, although the fraction being detected may have risen.

Also, even as the fraction of attacks detected rises, that fraction is never known, because "you never know what you don't know."

IT security also experiences self-falsification through a set of moral hazards similar to the claim that "seatbelts cause accidents"—in that such protection can lower users' risk aversion, causing them to operate systems less cautiously.

These factors make formal metrics for IT security difficult.

Approaches

Many disciplines operate in environments of decision making under uncertainty, but most have proven methods to determine risk. Examples include: financial metrics and risk management practices; balanced scorecard, six-sigma, insurance models; complexity theory; and data mining.

The field of finance, for example, has various metrics that help decision makers understand what is transpiring in their organizations. These metrics provide insight into liquidity, asset management, debt management, profitability, and market value of a firm. Capital budgeting tools, such as net present value and internal rate of return, allow insight in the return that can be expected from an investment in different projects.

In addition, the financial industry relies on decision-making frameworks, such as the Capital Asset Pricing Model and Options Pricing Model, that link risk and return to provide a perspective of the entire portfolio.

These frameworks have demonstrated some usefulness and can be applied across industries to support decision making. A possible analog for IT security would be sound systems development frameworks that support an enterprise view of an organization's security.

Metrics

The IRC supports the Computing Research Association's finding that an excellent goal or "Grand Challenge" for this area would be that, within 10 years, quantitative information-systems risk management should be at least as good as quantitative financial risk management.

However, a caveat is needed. This goal has serious pitfalls based on some inherent differences between the more or less continuous mathematics of multidimensional econometric and financial models on one hand, and the more or less discrete nature of computers on the other hand. For example, a one-bit change in a program or piece of data may be all that is required to transform something that is extremely secure to something that is completely insecure.

Metrics for the validity of metrics for security need to be taken with a grain of salt. Indeed, metrics about metrics always seem to be speculative.

F.2 NSTC IWG on Cyber Security and Information Assurance Federal Plan for Cyber Security and Information Assurance Research and Development

Findings and Recommendations—

Finding 8: Develop and apply new metrics to assess cyber security and IA.

Finding

It is widely acknowledged in the IT industry and the national research community that a major research challenge is posed by the lack of effective methods, technologies, and tools to assess and evaluate the level of component, system, and network security. The baseline analysis of federal investments found that, while the technical topic of software testing and assessment tools is both funded and ranked as a top R&D priority, the topic of metrics is not in either the top funding or top priority rankings.

Recommendation

As part of roadmapping, federal agencies should develop and implement a multi-agency plan to support the R&D for a new generation of methods and technologies for cost-effectively measuring IT component, system, and network security. As more exacting cyber security and IA metrics, assessment tools, and best practices are developed through R&D, these should be adopted by agencies and applied in evaluating the security of federal systems, and should evolve with time. [182]

References

181 INFOSEC Research Council (IRC). Hard Problems List, November 2005. Accessed 11 December 2008 at: *http:// www.cyber.st.dhs.gov/docs/IRC_Hard_Problem_List.pdf*

182 *Federal Plan for Cyber Security and Information Assurance Research and Development,* April 2006. Accessed 31 March 2009 at: *http://nitrd.gov/pubs/csia/csia_federal_plan.pdf*

This State-of-the-Art Report is published by the Information Assurance Technology Analysis Center (IATAC). IATAC is a DoD-sponsored Information Analysis Center, administratively managed by the Defense Technical Information Center (DTIC), and the Director, Defense Research and Engineering (DDR&E).