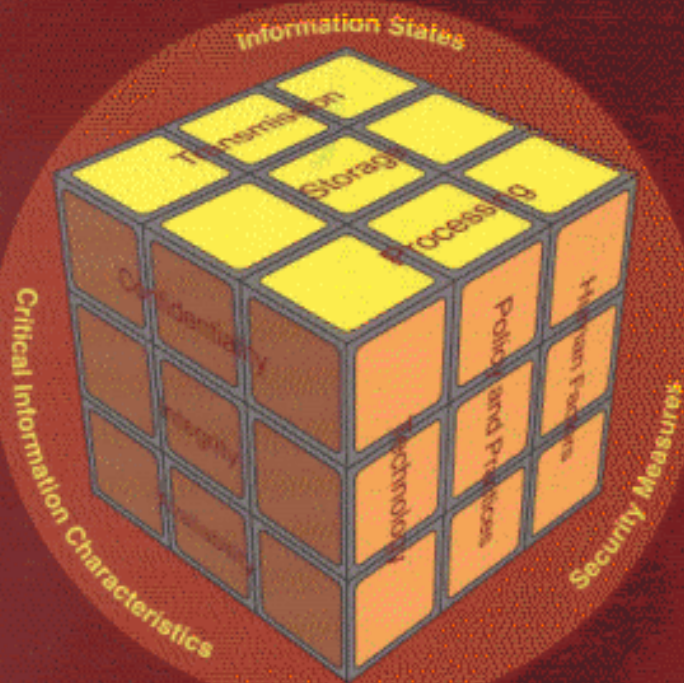


Assessing and Managing Security Risk in IT Systems

A Structured Methodology



John McCumber



CONTENTS

SECTION I SECURITY CONCEPTS

1	Using Models.....	3
	Introduction: Understanding, Selecting, and Applying Models	3
	Understanding Assets.....	4
	Layered Security	6
	Using Models in Security	8
	Security Models for Information Systems	11
	Shortcomings of Models in Security.....	15
	Security in Context	19
	Reference	22
2	Defining Information Security.....	23
	Confidentiality, Integrity, and Availability	23
	Information Attributes.....	26
	Intrinsic versus Imputed Value	28
	Information as an Asset	30
	The Elements of Security	32
	Confidentiality.....	32
	Integrity	36
	Availability.....	38
	Security Is Security Only in Context.....	40
3	Information as an Asset	41
	Introduction	41
	Determining Value	44
	Managing Information Resources	50
	References.....	55
4	Understanding Threat and Its Relation to Vulnerabilities	57
	Introduction	57
	Threat Defined	58
	Analyzing Threat.....	63

Assessing Physical Threats	64
Infrastructure Threat Issues	66
5 Assessing Risk Variables: The Risk Assessment Process	71
Introduction	71
Learning to Ask the Right Questions about Risk	76
The Basic Elements of Risk in IT Systems	83
Information as an Asset	83
Defining Threat for Risk Management	84
Defining Vulnerabilities for Risk Management	86
Defining Safeguards for Risk Management	89
The Risk Assessment Process	90

SECTION II THE McCUMBER CUBE METHODOLOGY

6 The McCumber Cube.....	99
Introduction	99
The Nature of Information	101
Critical Information Characteristics	102
Confidentiality	102
Integrity	103
Availability	103
Security Measures	104
Technology	105
Policy and Practice	105
Education, Training, and Awareness (Human Factors)	106
The Model	107
Overview	107
Use of the Model	108
References	110
7 Determining Information States and Mapping Information Flow	111
Introduction	111
Information States: A Brief Historical Perspective	112
Automated Processing: Why Cryptography Is Not Sufficient	115
Simple State Analysis	116
Information States in Heterogeneous Systems	119
Boundary Definition	122
Decomposition of Information States	122
Step 1: Defining the Boundary	123
Step 2: Make an Inventory of All IT Resources	125
Step 3: Decompose and Identify Information States	126
Developing an Information State Map	127
Reference	129
8 Decomposing the Cube for Security Enforcement	131
Introduction	131

A Word about Security Policy.....	133
Definitions	134
The McCumber Cube Methodology	135
The Transmission State.....	137
Transmission: Confidentiality.....	137
Transmission: Integrity	139
Transmission: Availability.....	139
The Storage State	140
Storage: Confidentiality	140
Storage: Integrity	142
Storage: Availability	144
The Processing State.....	145
Processing: Confidentiality.....	147
Processing: Integrity	148
Processing: Availability.....	150
Recap of the Methodology.....	150

9 Information State Analysis for Components and Subsystems	153
Introduction	153
Shortcomings of Criteria Standards for Security Assessments.....	154
Applying the McCumber Cube Methodology for Product Assessments	156
Steps for Product and Component Assessment	157
Information Flow Mapping	158
Define the Boundary	158
Take an Inventory of Information Resources and Components.....	158
Decompose and Identify All Information States	158
Cube Decomposition Based on Information States	159
Call Out the Information State Column	159
Decompose Blocks by Attribute	160
Identify Existing and Potential Vulnerabilities	160
Develop Security Architecture	161
Describe Required Safeguards.....	161
Cost Out Architecture Components and Enforcement Mechanisms.....	162
Recap of the Methodology for Subsystems, Products, and Components.....	162
References.....	163
10 Managing the Security Life Cycle.....	165
Introduction	165
11 Safeguard Analysis	177
Introduction	177
Technology Safeguards	178
Procedural Safeguards	179
Human Factors Safeguards.....	180

Vulnerability–Safeguard Pairing	181
Hierarchical Dependencies of Safeguards	182
Security Policies and Procedural Safeguards	185
Developing Comprehensive Safeguards: The Lessons of the Shogun	186
Identifying and Applying Appropriate Safeguards	189
Comprehensive Safeguard Management: Applying the McCumber Cube	191
The ROI of Safeguards: Do Security Safeguards Have a Payoff?	192

12 Practical Applications of McCumber Cube Analysis.....197

Introduction	197
Applying the Model to Global and National Security Issues.....	198
Programming and Software Development.....	200
Using the McCumber Cube in an Organizational Information Security Program	200
Using the McCumber Cube for Product or Subsystem Assessment	203
Using the McCumber Cube for Safeguard Planning and Deployment ...	204
Tips and Techniques for Building Your Security Program	205
Establishing the Security Program: Defining You	205
Avoiding the Security Cop Label	207
Obtaining Corporate Approval and Support	207
Creating Pearl Harbor Files.....	210
Defining Your Security Policy	214
Defining What versus How.....	215
Security Policy: Development and Implementation.....	218
Reference	219

SECTION III APPENDICES

Appendix A — Vulnerabilities	223
Appendix B — Risk Assessment Metrics	235
Appendix C — Diagrams and Tables.....	245
Appendix D — Other Resources	251
Index.....	255