National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

An Introduction to Computer Security: The NIST Handbook

Special Publication 800-12

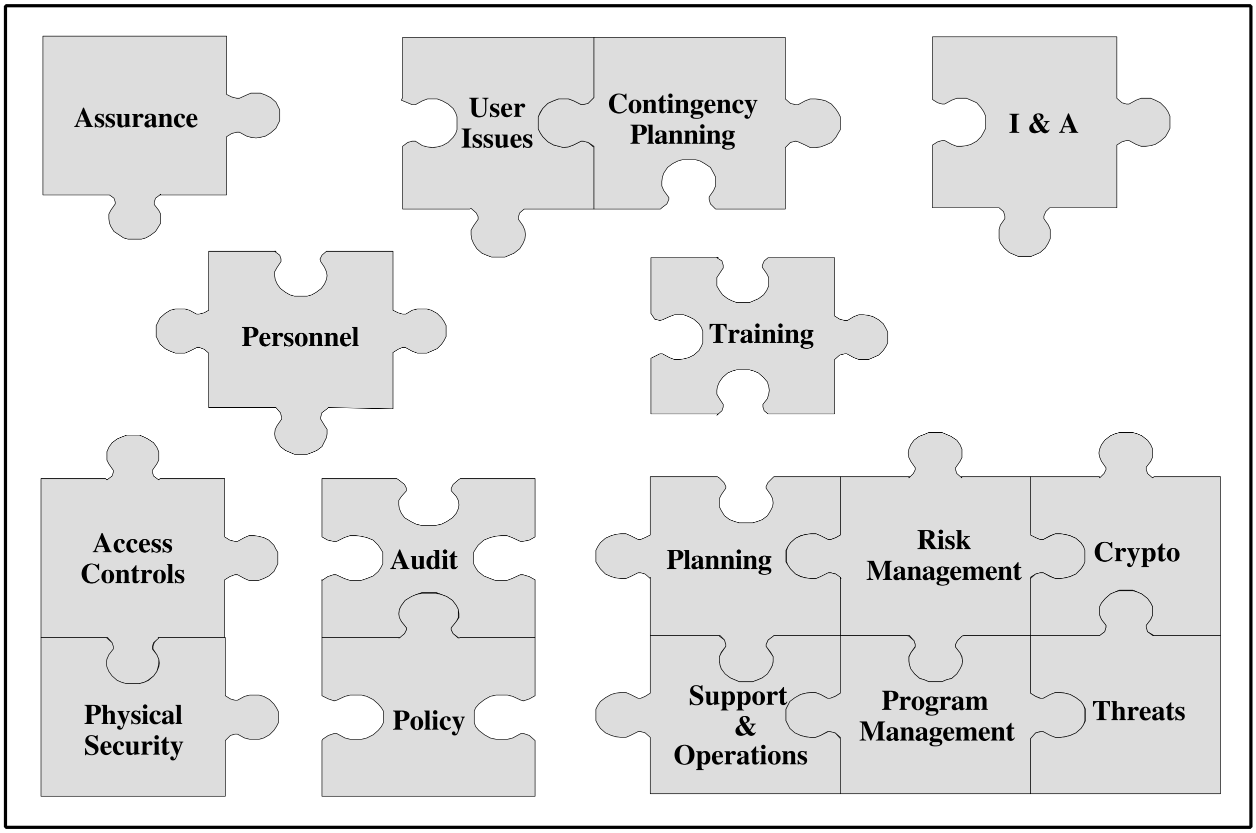

Table of Contents

I. INTRODUCTION AND OVERVIEW

Chapter 1

INTRODUCTION

1.1 Purpose 3
1.2 Intended Audience 3
1.3 Organization 4
1.4 Important Terminology 5
1.5 Legal Foundation for Federal Computer Security Programs . 7

Chapter 2

ELEMENTS OF COMPUTER SECURITY

2.1 Computer Security Supports the Mission of the Organization. 9
2.2 Computer Security is an Integral Element of Sound Management. 10
2.3 Computer Security Should Be Cost-Effective. 11
2.4 Computer Security Responsibilities and Accountability Should Be Made Explicit. 12
2.5 Systems Owners Have Security Responsibilities Outside Their Own Organizations. 12
2.6 Computer Security Requires a Comprehensive and Integrated Approach. 13
2.7 Computer Security Should Be Periodically Reassessed. 13
2.8 Computer Security is Constrained by Societal Factors. 14

Chapter 3

ROLES AND RESPONSIBILITIES

3.1 Senior Management 16
3.2 Computer Security Management 16
3.3 Program and Functional Managers/Application Owners 16
3.4 Technology Providers 16
3.5 Supporting Functions 18
3.6 Users 20

Chapter 4

COMMON THREATS: A BRIEF OVERVIEW

4.1 Errors and Omissions 22
4.2 Fraud and Theft 23
4.3 Employee Sabotage 24
4.4 Loss of Physical and Infrastructure Support 24
4.5 Malicious Hackers 24
4.6 Industrial Espionage 26
4.7 Malicious Code 27
4.8 Foreign Government Espionage 27
4.9 Threats to Personal Privacy 28

II. MANAGEMENT CONTROLS

Chapter 5

COMPUTER SECURITY POLICY

5.1 Program Policy 35
5.2 Issue-Specific Policy 37
5.3 System-Specific Policy 40
5.4 Interdependencies 42
5.5 Cost Considerations 43

Chapter 6

COMPUTER SECURITY PROGRAM MANAGEMENT

6.1 Structure of a Computer Security Program 45
6.2 Central Computer Security Programs 47
6.3 Elements of an Effective Central Computer Security Program 51
6.4 System-Level Computer Security Programs 53
6.5 Elements of Effective System-Level Programs 53
6.6 Central and System-Level Program Interactions 56
6.7 Interdependencies 56
6.8 Cost Considerations 56

Chapter 7

COMPUTER SECURITY RISK MANAGEMENT

7.1 Risk Assessment 59
7.2 Risk Mitigation 63
7.3 Uncertainty Analysis 67
7.4 Interdependencies 68
7.5 Cost Considerations 68

Chapter 8

SECURITY AND PLANNING
IN THE COMPUTER SYSTEM LIFE CYCLE

8.1 Computer Security Act Issues for Federal Systems 71
8.2 Benefits of Integrating Security in the Computer System Life Cycle 72
8.3 Overview of the Computer System Life Cycle 73

Click here to download full PDF material