Introduction to Information Security

Ms Sundus Latif

Department of Computer Science

Part I

(Overview, Access, Control, Cryptography, Risk Analysis)

Part II

(Business Continuity Planning, Data Classification, Security Awareness, Computer and System Security)

Part III

(Telecommunications Security, Organization Architecture, Legal Regulatory Investigation)

Part IV

(Investigation, Application program Security, Physical Security, Operations Security)

Part V
(Information Ethics, Policy Development)

Computer Security Act of 1987 Requires:

- Sensitive systems and data must be identified
- Plans for ensuring security and control of such systems must be created
- Personnel training programs must be developed and in place

Development of Security Program

- Objectives
- Policies
- Connectivity, Corporate Structure, and Security
- Plans
- Responsibilities

Security Policy Goals

- Avoidance
- Deterrence
- Detection
- Correction

Risk Analysis

- Identify sensitivity of data
- Determine value of systems and information
- Assess threats and vulnerabilities (sabotage, environment, errors)

Purposes of Risk Analysis

- No significant intentional or accidental threat is overlooked
- Assure that cost-benefit analysis is reasonable

Contingency Plan

- Purpose: Protect, detect, recover
- Criticality: Formulated, communicated to ALL employees, tested regularly

Legal Issues

- Licenses
- Fraud/Misuse
- Privacy
- Copyright
- Trade Secrets
- Employee Agreements

Access Control

Collection of mechanisms to restrain or prohibit use of information and systems

Includes: Functions, implementation, good practices, environmental constraints

Considerations

- Ownership of Data
- Custodian of Data
- Accountability
- Reconciliation
- Rule of Least Privilege

User Authentication and Password Management

- Access Control
- Knowledge-Based Authentication
- Token-Based Authentication
- Characteristic-Based Authentication
- Password Management

Access Control

- Policies
- Procedures
- Standards
- Control

Cryptography

Definition: Use of secret codes to provide integrity/confidentiality of information during transfer and storage

Considerations:

-Complexity

-Secrecy

- Characteristics of key

Definition:

Encryption: plaintext to ciphertext

Decryption: From ciphertext to plaintext

Key Management

- Public vs. Private
- Selecting Key
- Management of the Keys
- Protection of Keys
- Testing of Keys
- Updating Keys
- Error Detection

Risk Management

Includes ideas, models, methods, techniques to control risk

Includes:

-Assessment

-Reduction

-Protective measures

-Risk Acceptance

-Insurance

Considerations of Risk Assessment

- Annual Loss Expectancy(ALE)
- Asset Valuation/Inventory
- Types of Attacks/Threats
- Availability of Resources/Denial of Service
- Detection
- Exposure
- Passive Threats
- Perils
- Prevention
- Analysis/Assessment/Management of Risk
- Data Valuation

Classification of People/Assets

Should Include:

-People

-Procedures

-Data/Information

-Software

-Hardware

Threat and Exposure Assessment

- Density/Volume of Information
- Accessibility of Systems
- Complexity
- Electronic Vulnerability
- Media Vulnerability
- Human Factors

Safeguards and Counter Measures

- Prevent Exposures
- Detect Attempted Threats
- Correct the Causes of Threats

Business Continuity Planning (1)

- Planning and Analysis Methods
- Rates of Occurrence of Disabling Events
- Availability and Use of Planning Tools/Aids
- Identification of Business Success factors(BSF) and Critical capabilities(Critical or Key Success Factors (CSF/KSF)

Business Continuity Planning (2)

- Alternative Sources of Supply
- Legal and Regulatory Requirements

Backups and Procedures

- Importance for Recovery
- Data Value
- Manuals and Documentation
- Back Up Frequency
- On-Line Systems
- Equipment

The Three C’s

-Catastrophe

-Contingency

-Continuation

BE PREPARED!!!

Off-site Backups and Storage
Two Control Points:

1. When backup material is being transferred to/from the site
2. When backup material is stored at the site

(also consider in-house storage)

Data Classification

- Elements and Objectives of a Classification Scheme
- Criteria used to Classify Data
- Procedures to be Used
- Differences Between Government and Commercial Programs
- Limitations
- Program Implementation

To Be Included:

- Distinguish Between Classification and Sensitivity
- Classified vs. Sensitive
- Data Elements
- Handling of Data
- Identify Criteria
- Classification Schemes
- Rule of Users Managers
- Effect of Data Aggregation on Classification
- Techniques for Avoiding Disclosure

Security Awareness Include:

- Corporate Policies, Procedures, Intentions
- Areas Where Remedial Actions are Needed
- Assessment of Threats and Vulnerabilities
- Technology Trends
- Behaviors to be Encouraged
- User Motives
- Applicable Laws and Regulation
- Available/Applicable Communication Channels/Media

Administrative/Organizational Controls

- Policies
- Awareness
- Employee Non-Disclosure Considerations
- Employee Training
- Telecommuting Considerations
- Effects of Technological Changes/Updates

Personnel Considerations

- Human Motives for Criminal Action
- Employee Selection
- Professional Certificates
- Working Environment
- Technological Updates (Effect on Users)
- Employee Separation

Computer and System Security

Professionals Should Understand:

- Computer Organizations, Architectures, Designs
- Source and Origin of Security Requirements
- Advantages/Disadvantages of Various Architectures
- Security Features/Functions of Various Components
- Choices to be Considered When Selecting Components

Common Flaws and Penetration Methods

- Operating Systems Flaws
- Penetration Techniques(Trojan Horses, Virus, Salami Attack, Deception)

Viruses

- Design
- Protection
- Recovery
- Prevention
- Counter Measures

Telecommunications Security

- Objectives
- hazards and Exposures
- Effects of Topology, Media, Protocols, Switching
- Hazards and Classes of Attack
- Defenses and Protective Measures

Methods

- Aborted Connection
- Active Wiretapping
- Between - The - Lines Entry
- Call Back
- Emanations
- Covert Channel
- Cross-Talk
- Eavesdropping
- Electronic Funds Transfer(EFT)
- Handshaking

Considerations

- Transmission Technologies
- Bandwidth
- Connectivity Potential
- Geographical Scope
- Noise Immunity
- Security
- Applications
- Relative Cost

System Security Officer

- Organizational Knowledge (Structural and Behavioral)
- Technical Knowledge
- Accounting/Audit Concepts
- Personnel Administration Matters
- Laws/Legislation
- Strategic/Tactical Planning
- Labor/Negotiation/Strategies/Tactics

Computer Security Incidence Response

- Goals
- Constituency
- Structure
- Management Support/Funding
- Charter
- Handbook of Operations
- Staffing

Legal/Regulatory

- Federal Laws/Regulations
- State Laws/Regulations
- International Issues
- Organizational/Agency Considerations
- Personal Behavior
- Remedies to Constituents
- Civil vs. Criminal Law
- Pending Legislation

Computer Crime

- Fraud
- Embezzlement
- Unauthorized Access
- “White Collar” Crime
- Theft of Hardware/Copying Software
- Physical Abuse
- Misuse of Information
- Privacy/Confidentiality Violations
- Intellectual Property
- Negligence
- License Agreements

Investigation

- Legal Requirements for Maintaining a Trail of Evidence
- Interrogation Techniques
- Legal Limits on Interrogation Methods Permitted

Application Program Security

- Distribution of Controls Between Application and System
- Controls Specific to Key, Common, or Industry Applications
- Criteria for Selection and Application
- Tests for Adequacy
- Standards for Good Practice

Software Controls

- Development
- Maintenance
- Assurance
- Specification and Verification
- Database Security Controls
- Accounting/Auditing

Physical Security

- Site/Building Location
- External characteristics/Appearance
- Location of Computer Centers
- Construction Standards
- Electrical Power(UPS)
- Water/Fire Considerations
- Traffic/Access Control
- Air Conditioning/Exhaust
- Entrances/Exits
- Furnishings
- Storage of Media/Supplies

Operations Security

- Resources to be Protected
- Privileges to be Restricted
- Available Control Mechanisms
- Potential for Abuse of Access
- Appropriateness of Controls
- Acceptable Norms of Good Practice

Information Ethics
Doing the Right Thing!!

- Privacy/Confidentiality
- Common Good
- Professional Societies
- Professional Certifications

Policy Development Considerations:

- Have Longevity
- Be Jargon Free
- Be Independent of Jobs, Titles, or Positions
- Set Objectives
- Fix Responsibility
- Provide Resources
- Allocate Staff
- Be Implemented Using Standards and Guidelines

That’s All Folks
(and not a minute too soon!!)

I’m Looking Forward to working With You!!!!