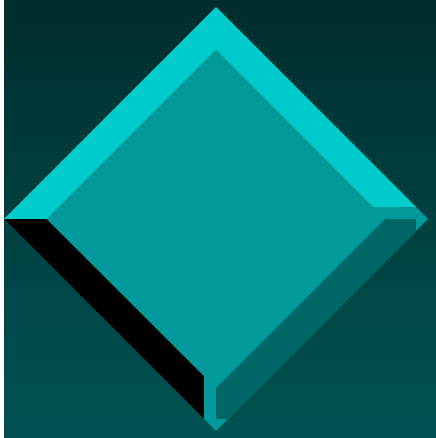


Information Security Fundamentals for Business

By
Dr. Andrew M. Colarik

Presentation Overview

- What is Information Security?
- Security Services & Mechanisms
- Managing Information Security
- Helpful Things to Remember

What is Information Security?

- "The concepts, techniques, technical measures, and administrative measures used to protect information assets from deliberate or inadvertent unauthorized acquisition, damage, disclosure, manipulation, modification, loss, or use" [McDaniel 94].

What is Information Security?

- Primarily directed around:
  - Organizational Issues
    - Proper procedures for handling security issues
  - Hardware and Software Systems
    - Protocols, firewalls, smart cards, locks, cameras, etc.
  - People
    - Hiring, training, managing and discharging

What is Information Security?

- Prevent
  - Security Mechanisms
  - Policies and Procedures
  - Training
- Detect
  - Intrusion Detection
  - Monitoring and Auditing Transactions and Traffic
- Response
  - Incident Response Plan

What is Information Security?

- There is no such thing as 'complete security' in a usable system.
- Security is not a static end state, it is an interactive process.
- Concentrate on known and probable threats.
- Nature of threats are ever-changing.
- You can't detect what you aren't monitoring.
- Security is a path, not a destination.

Security Services & Mechanisms

- Confidentiality
  - Keeping data or information secret from unauthorized users or systems.
    - Secret Key and Public / Private Key
    - Secure Socket Layer (SSL)
    - Transport Layer Security (TLS)
    - IPv6
    - Internet Protocol Security (IPSec)

Security Services & Mechanisms

- Integrity
  - Keeping data or information whole and/or unmodified unless authorized to do so.
    - Hash Product (MD5, SHA-1, RIPEMD-160)
    - Digital Certificate
    - IPv6

Security Services & Mechanisms

- Availability
  - Making data or information available to authorized users or systems.
    - Capacity Planning / Scalable Bandwidth
    - Server / Site Mirroring
    - Packet Filtering and Blocking
    - Distributive Operations

Security Services & Mechanisms

- Authentication
  - Confirmation of an authorized user or system's credentials.
    - Public Key Infrastructure and X.509
    - Kerberos
    - Global Directory Services (X.500)
    - Tokens

Security Services & Mechanisms

- Access Control
  - Controlling the access to resources of an authorized user or system.
    - Reference Monitor
    - Access Control Lists
      - Server Domains
      - Routers
      - Switches
      - Etc.

Security Services & Mechanisms

- Non-repudiation
  - The ability to provide non-refutable evidence that an activity took place and by whom/what.
  - Proof of origin, original content, delivery and original content received
    - PKI
    - Digital Certificates
    - HMAC

Security Services & Mechanisms

- Auditing
  - The process of recording database activity and access to database objects as it occurs in the database.
    - Intrusion Detection Systems
    - Highly developed Non-Repudiation systems
    - Server transaction logs
    - Database transaction logs
    - Certificate Authorities

Managing Information Security

- Risk Management
  - Identification
  - Analysis
  - Control

Managing Information Security

- Security Policy
  - Identity Infrastructure
  - Permission Infrastructure
  - User Management
  - Secure Communication
  - Isolation Infrastructure
  - Threat Management
  - Configuration Management
  - Conformance Monitoring

Managing Information Security

- Physical / Environmental Security
  - Physical Intrusion
    - Protection against unauthorized persons
    - Protection against theft
    - Protection against physical destruction
    - Protection against unauthorized reading
  - Physical Security Issues
    - Knowledge of facility location
    - Physical security parameter
    - Physical entry controls
    - Working in secured areas
    - Isolated delivery & loading areas
    - Protecting equipment from external disturbances
    - Protection against eavesdropping

Managing Information Security

- Asset Classification and Control
  - Inventory of all company assets
  - Having a system for maintaining this list
    - Acquisition
    - Usage
    - Upgrades
    - Replacements
    - Disposals

Managing Information Security

- Communication and Operating Management
  - Security mechanisms
  - Internal and external information storage and exchange policy
  - Protective systems
  - Software and Update management
  - Vulnerability assessments

Managing Information Security

- Access Control
  - Unauthorized Access Attempts
    - System Alerts & Failures
    - Interceptions
  - Proper Identification
    - Personal Knowledge, Something Possessed
    - Biometric Verification
  - Authentication Methods
    - Tokens & Cryptocards
  - Network Access
    - Internal & External Policies and Systems

Managing Information Security

- Personnel Security and Awareness Training
  - Hiring and Training Staff
  - Security Clearance
  - Training
  - Termination Procedures
  - Security Screening Firms

Managing Information Security

- Business Continuity Management
  - Procedures for the activation of the emergency procedures
    - A procedure related to a particular emergency / accident type.
  - Escalation procedures including moving the essential services to a backup location.
  - After the danger has passed, there must be plans for returning to normal operations.
  - Training of the staff for handling the emergencies.
  - The methods of introduction and verification of updates to the plan.
  - Listing of the people and positions that are responsible.

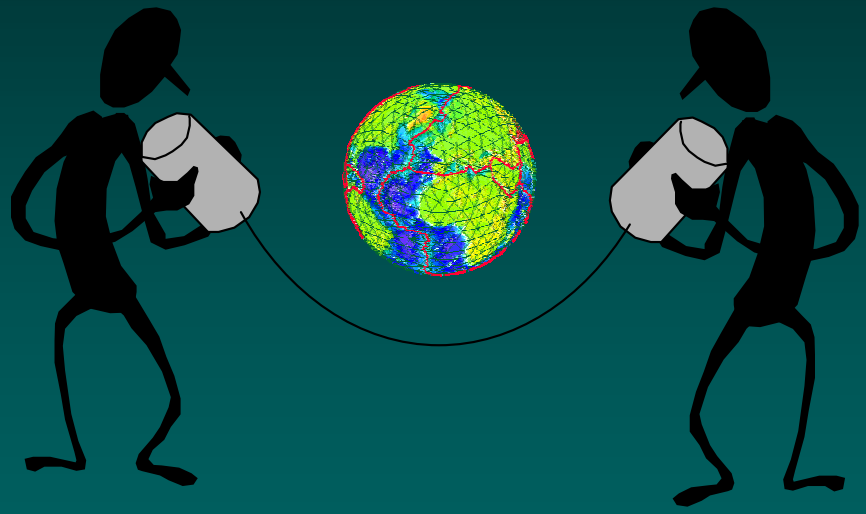
Managing Information Security

- Legal Compliance
  - Safeguarding Organizational Records
  - Misuse of IT Facilities
  - Collection & Storage of Evidence
  - Intellectual Property Rights

Helpful Things to Remember

- Understand that everything in security starts with people and then systems
  - Policies and Procedures
  - Security Training
  - Everything revolves around trust
- Stay Current
  - Hardware and Software
  - Skill Sets
  - Outside Resources
- Maintain Alternative Backup Strategies
  - It’s the information and its usage that is important, and not necessarily your computer assets

Questions?



Contact Details

Phone: (330) 220-8355

E-mail: acolarik@hotmail.com

Website: www.AndrewColarik.com