CISSP 2007 Training by Shon Harris/Logical Security

- **Course Number:** CISSP07
- **Length:** 6 Day(s)

Certification Exam

This course will help you prepare for the following exams:

- **CISSP**

Course Overview

Certified Information Systems Security Professional (CISSP) is the highest certification that may be attained by an IT security professional. This course focuses not only on the areas necessary for the CISSP examination, but also on a more detailed and practical perspective that will give you competitive skills in the real world as well. Our objective is to not just prepare you for CISSP Certification, but to also provide you with the practical, detailed understanding and knowledge of security topics that will be of valued use to you and your company.

Prerequisites

At least 4 years of experience in the information security field or 3 years of experience and a college degree (or equivalent life experience).

Audience

The CISSP is geared towards IT security professionals with at least 4 years of experience in the information security field.

Course Outline

- Domain 1 - Information Security and Risk Management
- Information Security and Risk Management
- Mainframe Days
- In the Good Old Days –Who Knew?
- Today's Environment
- Security Definitions
- Vulnerabilities
- Examples of Some Vulnerabilities that Are Not Always Obvious
- Risk – What Does It Really Mean?
- Relationships
- Who Deals with Risk?
- Overall Business Risk
- Who?
- AIC Triad
- Availability
- Integrity
- Confidentiality
- Who Is Watching?
- Social Engineering
- What Security People Are Really Thinking

- Security Concepts
- Security?
- The Bad Guys Are Motivated
- If Not Obscurity – Then What?
- Open Standards
- Common Open Standards
- Without Standards
- “Soft” Controls
- Logical Controls
- Physical Controls
- Are There Gaps?
- Understanding Drivers
- Holistic Security
- Not Always So Easy
- What Is First?
- Different Types of Law
- How Is Liability Determined?
- Examples of Due Diligence
- Examples of Due Care
- Prudent Person Rule
- Prudent Person
- Taking the Right Steps
- Regulations
- Why Do We Need Regulations?
- Risk Management
- Why Is Risk Management Difficult?
- Necessary Level of Protection Is Different for Each Organization
- Security Team/Committee
- Risk Management Process
- Planning Stage – Team
- Analysis Paralysis
- Planning Stage – Scope
- Planning Stage – Analysis Method
- Risk Management Tools
- Defining Acceptable Levels
- Acceptable Risk Level
- Collecting and Analyzing Data Methods
- What Is a Company Asset?
- Data Collection – Identify Assets
- Data Collection – Assigning Values
- Asset Value
- Data Collection – Identify Threats
- Data Collection – Calculate Risks
- Scenario Based – Qualitative Risk Approach
- Qualitative Analysis Steps
- Want Real Answers?
- Qualitative Risk Analysis Ratings
- Qualitative Risks
- Quantitative Analysis Steps
- Quantitative Analysis
- How Often Will This Happen?
- ARO Values and Their Meaning

- Calculate ALE
- ALE Value Uses
- Relationships
- Calculate Risks – ALE Example
- Your Turn!
- ALE Calculation
- Can a Purely Quantitative Analysis Be Accomplished?
- Risk Types
- Examples of Types of Losses
- Delayed Loss
- Cost/Benefit Analysis
- Cost of a Countermeasure
- Cost/Benefit Analysis Countermeasure
- Criteria
- Calculating Cost/Benefit
- Controls
- Control Selection Requirements
- Quantitative Analysis
- Quantitative Analysis Disadvantages
- Qualitative Analysis Approach
- Qualitative Analysis Disadvantages
- Can You Get Rid of All Risk?
- Calculating Residual Risk
- Uncertainty Analysis
- Dealing with Risk
- Management's Response to Identified Risks
- Risk Acceptance
- Risk Analysis Process Summary
- Components of Security Program
- A Layered Approach
- In Security, You Never Want Any Surprises
- Building Foundation
- Security Roadmap
- Functional and Assurance Requirements
- Building Foundation
- Most Organizations Silo Security Structure
- Islands of Security Needs and Tools
- Get Out of a Silo Approach
- Security Is a Process
- Approach to Security Management
- Result of Battling Management
- Industry Best Practices Standards
- ISO/IEC 17799
- Pieces and Parts
- Numbering
- New ISO Standards
- COBIT
- Inside of COBIT
- COBIT – Control Objectives
- Measurements
- Information Technology Infrastructure Library
- Security Governance

- Security Program Components
- Policy Framework
- Policy Types
- Organizational Policy
- Policy Approved – Now What?
- Issue-Specific Policies
- ASP Policy Example
- System-Specific Policies
- Standards
- Standard Example
- Baseline
- Data Collection for Metrics
- Guidelines
- Procedures
- Tying Them Together
- Program Support
- Entity Relationships
- Senior Management's Role
- Security Roles
- Custodian
- Auditor
- Access
- Information Classification
- Information Classification Program
- Data Leakage
- Do You Want to End Up in the News?
- Types of Classification Levels
- Data Protection Levels
- Classification Program Steps
- Information Classification Components
- Procedures and Guidelines
- Classification Levels
- Information Classification Criteria
- Criteria Example
- Or Not
- Information Owner Requirements
- Clearly Labeled
- Testing Classification Program
- Who Is Always Causing Problems?
- Employee Management
- Employee Position and Management
- Hiring and Firing Issues
- A Few More Items
- Unfriendly Termination
- Security Awareness and Training
- Training Characteristics
- Awareness
- Security Enforcement Issues
- Answer This Question
- Domain 1 Review
- Domain 2 - Access Control Domain Objectives
- Agenda 1

- Definitions
- Access Control Mechanism Examples
- Technical Controls
- Administrative Controls
- Access Control Characteristics
- Preventive Controls
- Preventive - Administrative Controls
- Preventive – Physical Controls
- Preventive - Technical Controls
- Control Combinations
- Detective - Administrative Control
- Detective Examples
- Administrating Access Control
- OS, Application, Database
- Administrating Access Control
- Authorization Creep
- Accountability and Access Control
- Trusted Path
- Fake Login Pages Look Convincing
- Who Are You?
- Identification Issues
- Authentication Mechanisms
- Characteristics
- Strong Authentication
- Fraud Controls
- Internal Control Tool: Separation of Duties
- Authentication Mechanisms in Use Today
- Biometrics Technology
- Biometric Devices
- Example
- Verification Steps
- What a Person Is
- Why Use Biometrics?
- Biometric Type
- Identification or Authentication?
- Iris Sampling
- Iris
- Finger Scan
- Hand Geometry
- Facial Recognition
- Comparison
- Biometrics Verification
- Issues
- Downfalls to Biometric Use
- Biometrics Error Types
- Crossover Error Rate
- Biometric System Types
- Passwords
- Password Generators
- Password “Shoulds”
- Support Issues
- Password Attacks

- Attack Steps
- Many Tools to Break Your Password
- Rainbow Table
- Passwords Should NOT Contain…
- What's Left?
- Countermeasures for Password Cracking
- Cognitive Passwords
- One-Time Password Authentication
- Synchronous Token
- One Type of Solution
- Synchronous Steps
- Administrator Configures
- Challenge Response Authentication
- Asynchronous Token Device
- Asynchronous Steps
- Challenge Response Authentication
- Cryptographic Keys
- Passphrase Authentication
- Key Protection
- Memory Cards
- Memory Card Characteristics
- Smart Card
- Characteristics
- Card Types
- Smart Card Attacks
- Software Attack
- Side Channel Attack
- Side Channel Data Collection
- Microprobing
- Identity Management
- How Are These Entities Controlled?
- Some Current Issues
- Management
- Typical Chaos
- Different Identities
- Identity Management Technologies
- Directory Component
- Enterprise Directory
- Directory Responsibilities
- Authoritative Sources
- Meta Directory
- Directory Interactions
- Web Access Management
- Web Access
- Password Management
- Legacy Single Sign-On
- Account Management Systems
- Provisioning Component
- Provisioning
- Not Just Computers
- Profile Update
- Working Together

- Enterprise Directory
- Identity Management Solution Components
- Right for Your Company
- What you need to know
- Federated Identity
- Identity Theft
- Fake Login Tools
- How Do These Attacks Work?
- Attempts to Get Your Credentials
- How Do These Work?
- Instructional Emails
- Knowing What You Are Disposing of Is Important
- Other Examples
- Another Danger to Be Aware of… Spyware
- Is Someone Watching You?
- What Does This Have to Do with My Computer?
- Sometimes You Know that Software Is Installing on Your System
- New Spyware Is Being Identified Every Week
- Spyware Comes in Many Different Forms
- How to Prevent Spyware
- Different Technologies
- Single Sign-on Technology
- Single Sign-on
- Directory Services as a Single Sign-on Technology
- Active Directory
- Some Technologies Can Combine Services
- Security Domain
- Domains of Trust
- Domain Illustration
- Thin Clients
- Example
- Kerberos as a Single Sign-on Technology
- Kerberos Components Working Together
- Pieces and Parts
- More Components of Kerberos
- KDC Components
- Kerberos Steps
- Tickets
- Ticket Components
- Authenticators
- Steps of Validation
- Kerberos Security
- Why Go Through All of this Trouble?
- Issues Pertaining to Kerberos
- Kerberos Issues
- SESAME as a Single Sign-on Technology
- SESAME Steps for Authentication Combo
- Models for Access
- Access Control Models
- Discretionary Access Control Model
- ACL Access
- File Permissions

- Enforcing a DAC Policy
- Security Issues
- Mandatory Access Control Model
- MAC Enforcement Mechanism – Labels
- Formal Model
- Software and Hardware
- Software and Hardware Guards
- Where Are They Used?
- SELinux
- MAC Versus DAC
- Role-Based Access Control
- RBAC Hierarchy
- RBAC and SoD
- Acquiring Rights and Permissions
- Rule-Based Access Control
- Firewall Example
- Access Control Matrix
- Capability Tables
- User Capability Tables
- Temporal Access Control
- Access Control Administration
- Access Control Methods
- Centralized Approach
- Remote Centralized Administration
- RADIUS
- RADIUS Steps
- RADIUS Characteristics
- TACACS+ Characteristics
- Diameter Characteristics
- Diameter Protocol
- Mobile IP
- Diameter Architecture
- Two Pieces
- AVP
- Decentralized Access Control Administration
- Controlling Access to Sensitive Data
- Protecting Access to System Logs
- Accountability = Auditing Events
- Agenda 2
- IDS
- IDS Steps
- Network IDS Sensors
- Host IDS
- Combination
- Types of IDSs
- Signature-Based Example
- Behavior-Based IDS
- Statistical Anomaly
- Statistical IDS
- Protocol Anomaly
- What Is a Protocol Anomaly?
- Protocol Anomaly Issues

- Traffic Anomaly
- IDS Response Mechanisms
- Responses to Attacks
- IDS Issues
- Intrusion Prevention System
- Differences
- Vulnerable IDS
- Trapping an Intruder
- Domain 2 Review
- Domain 3 - Cryptography Objectives
- Services Provided by Cryptography
- Cryptographic Definitions
- Cipher
- Cryptanalysis
- A Few More Definitions
- Need Some More Definitions?
- Now This Would be Hard Work
- Symmetric Cryptography – Use of
- Secret Keys
- Historical Uses of Symmetric
- Cryptography – Hieroglyphics
- Scytale Cipher
- Substitution Ciphers
- Simple Substitution Cipher Atbash
- Simple Substitution Cipher Caesar Cipher
- Caesar Cipher Example
- Simple Substitution Cipher ROT13
- Historical Uses
- Polyalphabetic Cipher – Vigenere Cipher
- Polyalphabetic Substitution
- Vigenere Algorithm
- Enigma Machine
- U-Boats had Enigma Machines
- Code Book
- Historical Uses of Symmetric
- Cryptography – Running Key and
- Concealment
- Agenda 1
- Transposition Ciphers
- Key and Algorithm Relationship
- Does Size Really Matter?
- It Does with Key Sizes
- Key space
- Ways of Breaking Cryptosystems – Brute Force
- Brute Force Components
- Ways of Breaking Cryptosystems – Frequency Analysis
- Strength of a Cryptosystem
- Do You Know What You are Doing?
- Developing Cryptographic Solutions In-House
- Characteristics of Strong Algorithms
- Open or Closed More Secure?
- Agenda 2

- Types of Ciphers Used Today
- Type of Symmetric Cipher – Block Cipher
- S-Boxes Used in Block Ciphers
- Binary Mathematical Function 1
- Type of Symmetric Cipher – Stream Cipher
- Symmetric Characteristics
- Initialization Vectors
- Security Holes
- Strength of a Stream Cipher
- Let’s Dive in Deeper
- Symmetric Key Cryptography
- Out-of-Band Transmission
- Symmetric Key Management Issue
- Symmetric Algorithm Examples
- Symmetric Downfalls
- Why?
- Asymmetric Cryptography
- Key Functions
- Public Key Cryptography Advantages
- Asymmetric Algorithm Disadvantages
- Confusing Names
- Symmetric versus Asymmetric
- Asymmetric Algorithm Examples
- Questions 1
- When to Use Which Key
- Using the Algorithm Types Together
- Encryption Steps
- Receiver's Public Key Is Used to Encrypt the Symmetric Key
- Receiver’s Private Key Is Used to Decrypt the Symmetric Key
- Digital Envelope
- E-mail Security
- Secret versus Session Keys
- Asymmetric Algorithms We Will Dive Into
- Asymmetric Algorithm – Diffie-Hellman
- Diffie-Hellman
- Key Agreement Schemes
- Asymmetric Algorithm – RSA
- Factoring Large Numbers
- RSA Operations
- RSA Key Size
- El Gamal
- ECC
- ECC Benefits
- Asymmetric Mathematics
- Asymmetric Security
- Mathematics
- Symmetric Ciphers We Will Dive Into
- Symmetric Algorithms – DES
- Block Cipher
- Double DES
- Evolution of DES
- Modes of 3DES

- Encryption Modes
- Block Cipher Modes – CBC
- IV and CBC
- CBC Example
- Different Modes of Block Ciphers –ECB
- ECB versus CBC
- Block Cipher Modes – CFB and OFB
- CFB and OFB Modes
- Counter Mode
- Modes Summary
- Symmetric Cipher – AES
- IDEA
- RC4
- RC5
- Agenda 3
- Data Integrity
- Hashing Steps
- Protecting the Integrity of Data
- Hashing Algorithms
- Data Integrity Mechanisms
- Hashing Strength
- Question 1
- Weakness in Using Only Hash Algorithms
- More Protection in Data Integrity
- MAC
- HMAC – Sender
- HMAC – Receiver
- Another Look
- What Services
- Authentication Types
- CBC-MAC
- MAC Using Block Ciphers
- Integrity?
- What Services?
- Question 2
- Digital Signatures
- One More Look 1
- U.S. Government Standard
- What is…
- Not Giving up the Farm
- Zero Knowledge Proof
- Message Integrity Controls
- Security Issues in Hashing
- Example of a Birthday Attack
- Birthday Attack Issues
- Key Management
- Key Backup
- Key Management (Cont.)
- Key Usage
- Cryptoperiod
- M-of-N
- Key Types

- Agenda 4
- Why Do We Need a PKI?
- PKI and Its Components
- Components of PKI
- PKI
- PKI Steps
- RA Roles
- CA
- Let’s Walk Through an Example
- Digital Certificates
- Certificate
- Signing the Certificate
- Verifying the Certificate
- Trusted CA’s
- Non-Trusted CA
- One More Look 2
- What Do You Do with a Certificate?
- Components of PKI, Repository, and
- CRLs
- Revoked?
- CRL Process
- Different Uses for Certificates
- Lifecycle of a Certificate
- Cross Certification
- PKI and Trust
- Agenda 5
- Historical Uses of Symmetric Cryptography – Vernam Cipher
- Binary Mathematical Function 2
- One-Time Pad in Action
- One-Time Pad Characteristics
- Steganography
- Steganography Utilities
- Digital Watermarking
- Link versus End-to-End Encryption
- End-to-End Encryption
- Encryption Location
- Email Standards
- You Decide
- Non-Hierarchical
- Secure Protocols
- SSL Connection Setup
- Example - SSL
- Validating Certificate
- Secure Protocols (Cont.)
- SSL and the OSI Model
- E-Commerce
- How Are You Doing?
- Hard the First Times Through
- Secure Email Standard
- Agenda 6
- Network Layer Protection
- IPSec Key Management

- IPSec Handshaking Process
- VPN Establishment
- SAs in Use
- Key Issues Within IPSec
- Configuration of SA Parameters
- IPSec Configuration Options
- IPSec Is a Suite of Protocols
- AH and ESP Modes
- IPSec Modes of Operation
- VPN Establishment (Cont.)
- Review
- Questions 2
- Attack Types
- Attacks on Cryptosystems
- Known-Plaintext Attack
- Chosen-Plaintext Attack
- Chosen-Ciphertext Attack
- Adaptive Attacks
- Side Channel Attacks
- Domain 3 Review
- Domain 4 - Physical Security Objectives
- Physical Security – Threats
- Different Types of Threats
- Categories of Threats
- Wake Up Call
- Not Just Hacking
- Number One Priority
- Legal Issues
- Planning Phase
- Physical Security Program Goals
- Measurable Results
- Planning Process
- Risk Assessment Needs to be Carried Out
- Deterrence
- Deterrence Options
- Delay
- Another Delay Approach
- Layered Defense Model
- Layers of Defense
- Detection
- Assessment
- Response
- Weak Link in the Chain
- Part of the Overall Security Program Controls with the Same Goals
- Agenda 1
- Threat Categories
- Crime Prevention through Environmental Design
- Crux of Approach
- Protection Built In
- CPTED Examples
- Natural Access Control
- Access Control

- CPTED Main Strategies
- Target Hardening
- Access Barriers
- Facility Site Selection
- Urban Camouflage
- Facility Construction
- Earthquake Protection
- Construction Materials
- Rebar Encased in Concrete
- Pentagon with Reinforcements
- Fire Resistance Walls
- Data Center
- Data Center Protection
- Designing a Secure Site
- Levels of Protection
- Door Types
- Hollow-Core Doors
- Solid Core Doors
- Bullet Proof Door
- Door Component
- Door Lock Types
- Window Types
- Controlling Access
- Sensitive Areas
- Possible Threats
- Security Zones
- Various Sensors
- Lock Types
- Controlling Keys
- Smart Locks
- Lock Picking
- Entry Access Control
- Facility Access
- Wireless Proximity Devices
- Device Types
- Piggybacking
- Entrance Protection
- Mantraps
- Door Configurations
- External Boundary Protection
- Perimeter Protection – Fencing
- Detection Fencing
- Detecting Intruders
- Fencing Characteristics
- Fencing Issues
- Gates
- What Level of Protection is Needed?
- Bollards
- Perimeter Protection – Lighting
- Properly Laid Out
- Lighting Issues
- Perimeter Security – Security Guards

- Guard Tasks
- Security Guards
- Monitoring
- Level of Detail that is Required
- CCTV
- Items to Consider about CCTVs
- CCTV Components
- CCTV Lens Types
- CCTV Components (Cont.)
- Agenda 2
- Types of Physical Intrusion
- Detection Systems
- Intrusion Detection Characteristics
- Electro-Mechanical Sensors
- Volumetric Sensors
- Alarm Systems
- Securing Mobile Devices
- Stolen Laptops (partial list..)
- Agenda 3
- HVAC Attributes
- Environmental Considerations
- Who's Got Gas?
- Documentation of Procedures
- Electrical Power
- Backup Power
- Problems with Steady Power Current
- Power Interference
- Disturbances
- Protection Against Electromagnetic Discharge
- Definitions
- Power Preventive Measures
- Device Protection
- Consistent Power Flow
- Static Electricity
- Agenda 4
- Fire Prevention
- Not Allowed
- Components of Fire
- Fire Sources
- Automatic Detector Mechanisms
- Fire Detection
- Fire Suppression Agents
- Fire Types
- Emergency Power Off Switch
- Employees Need to be Trained
- Fire Suppression Systems
- Fire Extinguishers
- Emergency Procedures
- Drills and Testing
- Water Detectors
- Full Program
- Domain 5 - Security Architecture and Design Objectives

- Agenda 1
- Computer Architecture
- Central Processing Unit (CPU)
- Registers
- Arithmetic Logic Unit
- Control Unit
- Processing Data
- Register Types
- Program Status Word (PSW)
- Trust Levels
- Process
- Memory Segment Assignment
- Threads
- Process and Thread
- Process States
- Agenda 2
- Interrupts
- Interrupt Masking
- Process Table
- Moving Information
- Stacks
- Buses
- Processor and Buses
- 32-Bit versus 64-Bit
- Working Together
- Multiprocessing
- Multiprocessor
- System Functionality
- Multitasking Types
- Multitasking
- Deadlock
- Agenda 3
- Memory Types
- Cache Types
- Read Only Memory
- Virtual Memory
- Swapping
- Types of Memory
- Architecture Components
- Memory Manager Responsibilities
- Memory Protection
- Memory Manager Responsibilities (Cont.)
- Memory Addressing
- Base and Limit Addresses
- Shared Memory
- Memory Protection (Cont.)
- Memory Leaks
- Agenda 4
- CPU and OS
- System Protection – Levels of Trust
- Trust Levels (Cont.)
- System Protection - Protection Rings

- What Does It Mean to Be in a Specific Ring?
- System Protection – Layering
- System Call Interfaces
- API Application Programming Interface
- System Protection - Application Program Interface
- Process Protection
- Process Isolation
- Virtual Mapping
- Process ID
- Virtual Machines
- VMWare
- Input/Output Devices
- I/O Addressing
- Device Types
- Device Drivers
- Security Issues
- Software Complexity
- Types of Compromises
- Agenda 5
- Trusted Computing Base
- TCB
- Hardened Kernel
- Execution Domains
- Simple Definition
- Main Functions of TCB
- Process Activation
- Execution Domain Switching
- Security Perimeter
- Evaluation
- System Protection - Reference Monitor
- Security Kernel Requirements
- Tying Concepts Together
- Agenda 6
- Security Levels
- MAC Modes
- Modes of Operation
- MAC Modes (Cont.)
- Agenda 7
- Enterprise Architecture
- Objectives
- Without an Enterprise Security Architecture
- Can’t Just Wing It
- Just Right
- Breaking Down the Components
- Strategic Alignment
- Business Enablement
- Process Enhancement
- Process Enhancement Requires…
- Security Foundation
- Security Effectiveness
- Are We Doing it Right?
- Integration of Components

- How Do We Do All of This?
- Security Enterprise Architecture
- Industry Model
- Security Roadmap
- Trust Zones
- Infrastructure Level
- Application Layer
- Component Layer
- Business Process Layer
- Holistic Security
- Agenda 8
- Access Control Models
- Policy versus Model
- State Machine
- Information Flow
- Information Flow Model
- Bell-LaPadula
- Rules of Bell-LaPadula
- Rules Clarified
- Tranquility Types
- Biba
- Definition of Integrity
- Biba Access Rules
- Clark-Wilson
- Goals of Model
- Clark Wilson Components
- Clark-Wilson (Cont.)
- Clark-Wilson Model
- Non-Interference Model
- Lattice-Based Access Control
- Lattice Approach
- Understanding Lattice
- Access Control Matrix Model
- Access Control Matrix
- Brewer and Nash Model – Chinese Wall
- Brewer and Nash
- Take-Grant Model
- Graham-Denning Model
- Agenda 9
- Trusted Computer System Evaluation Criteria (TCSEC)
- TCSEC
- TCSEC Rating Breakdown
- Evaluation Criteria - ITSEC
- ITSEC Ratings
- ITSEC – Good and Bad
- Common Criteria
- Common Criteria Standard
- Security Functional Requirements
- Security Assurance Requirements
- Common Criteria Components
- Common Criteria Requirements
- Package Ratings

- Common Criteria Outline
- Certification Versus Accreditation
- Domain 5 Review
- Domain 6 - Law, Investigation and Ethics
- Objectives
- Not Just Fun and Games
- Examples of Computer Crimes
- Who Perpetrates These Crimes?
- Types of Motivation for Attacks
- A Few Attack Types
- Dumpster Diving
- Telephone Fraud
- Privacy of Sensitive Data
- Privacy Issues – U.S. Laws as Examples
- European Union Principles on Privacy
- Routing Data Through Different Countries
- Employee Privacy Issues
- Agenda 1
- Civil Law
- Criminal Law
- Administrative Law
- U.S. Federal Laws
- Trade Secret
- Copyright
- More Intellectual Property Laws
- Software Licensing
- Software Piracy
- Digital Millennium Copyright Act
- Agenda 2
- Computer Crime and Its Barriers
- Countries Working Together
- Worldwide Cybercrime
- Security Principles for International Use
- Determine if a Crime Has Indeed Been Committed
- Bringing in Law Enforcement
- Citizen versus Law Enforcement Investigation
- Investigation of Any Crime
- Role of Evidence in a Trial
- Evidence Requirements
- Chain of Custody
- How Is Evidence Processed?
- Hearsay Evidence
- Hearsay Rule Exception
- Agenda 3
- Preparing for a Crime Before It Happens
- Incident Handling
- Evidence Collection Topics
- Computer Forensics
- Hidden Secrets
- Trying to Trap the Bad Guy
- Companies Can Be Found Liable
- Sets of Ethics

- (ISC)2
- Computer Ethics Institute
- Internet Architecture Board
- Domain 6 Review
- Domain 7 - Telecommunications and Networking
- Agenda 1
- OSI Model
- OSI Layers
- Networking Communications
- An Older Model
- Data Encapsulation
- Application Layer
- OSI – Application Layer
- Presentation Layer
- OSI – Presentation Layer
- OSI – Session Layer
- Client/Server Model
- Client/Server Session Layer
- Transport Layer
- Transport Layer Analogy
- Transport Protocols
- OSI – Network Layer
- Here to There
- Network Layer
- OSI – Data Link
- Data Link
- Sublayers
- OSI – Physical Layer
- Physical Layer
- Layers Working Together
- Protocols at Each Layer
- Devices Work at Different Layers
- Types of Networks
- Network Topologies – Physical Layer
- Topology Type – Bus
- Topology Type – Ring
- Topology Type – Star
- Network Topologies – Mesh
- Mesh Topologies
- Summary of Topologies
- Agenda 2
- LAN Media Access Technologies
- Media Access
- One Goal of Media Access Technologies
- Collision Domain
- Back Off, Buddy
- Carrier Sense Multiple Access
- CSMA/Collision Avoidance (CSMA/CA)
- Media Access Technologies – Ethernet
- Media Access Technologies – Token Passing
- Token’s Role
- Other Technologies

- Media Access Technologies – Polling
- Agenda 3
- Cabling Types – Coaxial
- Coaxial
- Cabling Types – Twisted Pair
- Cable Types
- Types of Cabling – Fiber
- Multimode vs. Single Mode
- Signal and Cable Issues
- Signaling Issues
- Transmission Types – Analog and Digital
- Transmission Types – Synchronous
- Asynchronous
- Transmission Types – Baseband
- Transmission Types – Broadband
- Cabling Issues – Plenum-Rated
- Transmission Types – Number of Receivers
- Internet Group Management Protocol
- Multicasting
- Network Technologies
- Extranet
- Network Technologies (Cont.)
- EDI Evolution
- Networking Devices
- Network Device – Repeater
- Network Device – Hub
- Networking Device – Bridge
- Forwarding Table Example
- Network Devices – Switch
- Virtual LAN
- VLAN
- Interfaces and VLANs
- Sniffers
- Networking Devices – Router
- Hops
- Routers
- Bridges Compared to Routers
- Network Devices – Gateway
- Agenda 4
- Port and Protocol Relationship
- Client Ports
- Conceptual Use of Ports
- TCP/IP Suite
- UDP versus TCP
- TCP Segment
- SYN Flood
- Teardrop Attack
- Source Routing
- Source Routing Types
- IP Address Ranges
- IPv6
- Protocols

- Protocols – ARP
- IP to MAC Mapping
- How ARP Works
- ARP Poisoning
- ICMP Packets
- A Way Hackers Use ICMP
- Ping Steps
- Protocols – SNMP
- SNMP in Action
- SNMP
- SNMP Output
- POP3 and SMTP
- Protocols – SMTP
- Mail Relay
- Protocols – FTP, TFTP, Telnet
- Protocols – RARP and BootP
- DHCP – Dynamic Host Configuration
- Protocol
- Agenda 5
- Networking Device – Bastion Host
- Network Configurations
- DMZ Configurations
- Firewall Comparisons
- Network Devices – Firewalls
- Firewall Types – Packet Filtering
- Packet Filtering Firewall
- Packet Filtering Firewall Weaknesses
- Packet Filtering
- Rule Set Example
- Firewall Types – Proxy Firewalls
- Firewall Types – Circuit-Level Proxy
- Firewall
- Circuit-Level Proxy
- Firewall Types – Application-Layer Proxy
- Application-Layer Proxy Advantages
- Application-Layer Proxy Disadvantages
- Dedicated Proxy Servers
- Firewall Types – Stateful
- State Table
- Compare
- Firewall Types – Kernel Proxies
- Firewall based VPN Devices
- Best Practices
- Firewall Placement
- Packet Filtering (Cont.)
- Screened Host
- Firewall Architecture Types – Multi- or Dual-Homed
- Screened Subnet
- Agenda 6
- Dial-Up Protocols and Authentication Protocols
- Dial-Up Protocol – SLIP
- Dial-Up Protocol – PPP

- PPP
- PPP versus SLIP
- Authentication Protocols – PAP
- Authentication Protocols – CHAP
- Authentication Protocol – EAP
- Data Inspection
- Virtual Private Network Technologies
- What Is a Tunneling Protocol?
- Analogy
- Examples
- Tunneling Protocols – PPTP
- Tunneling Protocols – L2TP
- L2TP Encapsulation
- Tunneling Protocols – IPSec
- IPSec Basic Features
- IPSec Transport Mode
- IPSec Tunnel Mode
- Security Associations (SAs)
- Combining Sas
- Iterated Tunnelling
- Agenda 7
- SDLC and HDLC
- Layer 3 at Layer 2
- MPLS
- Multiprotocol Label Switching
- Quality of Service (QoS)
- QoS Services
- Autonomous Systems
- Routing Protocols
- Routing
- Routing Protocols (Cont.)
- OSPF
- OSPF Packet Values
- IGRP
- BGP
- Routing Protocol Attacks
- Metropolitan Area Network Technologies
- MAN Technologies – FDDI
- FDDI
- SONET Rings
- MAN Technologies – SONET
- Connecting Networks
- Network Services
- Network Service – DNS
- DNS Server Structure
- Name Resolving Steps
- Split DNS
- Host Name Resolution Attacks
- Network Service – NAT
- Types of NAT
- PAT
- NIS

- Storing Data
- NIS+ Authentication
- Agenda 8
- WAN Technologies Are Circuit or Packet Switched
- PSTN
- Connecting to the PSTN
- Circuit Switching
- Steps of Connections
- Multiplexing
- Types of Multiplexing
- TDM Process
- Statistical Time Division
- Multiplexing
- FDM
- FDM Process
- Packet Switching
- Circuit versus Packet Switching
- WAN Technologies – Packet Switched
- WAN Technologies – X.25
- X.25
- WAN Technologies – Frame Relay
- WAN Example
- Frame Relay
- PVC and SVC
- WAN Technologies – ATM
- Cell Switching
- Wide Area Network Technologies
- Dedicated Lines
- WAN Technologies – ISDN
- On-Demand
- ISDN Service Types
- WAN Technologies – DSL
- DSL
- ADSL
- SDSL
- WAN Technologies – Cable Modem
- Cable Modems
- Cable Network
- Satellites
- Hybrid Connection
- Satellite Coverage
- Satellite Supplying Different
- Subscribers
- Network Perimeter Security
- Complexity only Increases
- A Layered Approach
- Agenda 9
- Traditional Voice Network
- PSTN (Cont.)
- Private Branch Exchange
- PBX Vulnerabilities
- PBX Best Practices

- IP Telephony
- Voice Over IP
- Combination of Old and New
- IP Telephony Components
- Media Gateways
- PBX and VoIP
- Voice over…
- IP Telephony Issues
- Telephony Protection Mechanisms
- Telephony Security
- IP Telephony with Wireless
- IP Phones Security
- Mobile Technology Generations
- Mobile Phone Security
- Mobile Device Security
- Cell Phone
- Agenda 10
- Wireless Technologies – Access Point
- Wireless Frequencies
- Alphabet Soup of Standards
- Spread Spectrum
- OFDM
- Where does Spread Spectrum Work?
- 802.11n
- Wireless Technologies – Access Point (Cont.)
- Architectures
- Wireless Technologies – Service Set ID
- Authenticating to an AP
- 802.11 Authentication
- Wireless Technologies – WEP
- WEP Problems
- Wireless Technologies – More WEP Woes
- Lack of Integrity
- WEP Security Issues
- Domain 8 - Business Continuity Objectives

- Needs for BCP
  Is Your Organization Prepared?
  Is Your Company Prepared?
  9/11 Changed Mentalities About BCP
  Disaster affected Many
  America is Rebuilding
  Partial FEMA Disaster List for 2005
  Do We have a Plan?
  DRP Focus
  BCP Focus
  Comparing the Two
  What is the Purpose of a BCP?
  More Reasons to have Plans in Place
  Framework
  BCP is a Core Component of Every Security Program
  Steps of BCP Process
  Different BCP Model

Documentation
Documentation and Approval
BCP Policy Outlines
BCP Policy Sample
Who is In Charge and Who Can We Blame?
What's Needed in a Team?
BCP Development Team
Project Sizing
Properly Determining Scope is Important
BCP Risk Analysis Steps
BIA Steps
Data Gathering
Information from Different Sources
Analysis
Critical Functions
How to Identify the Most Critical Company Functions
Interdependencies
Well, of course an Organization Knows How it Works!
Business Silos
Understanding the Enterprise
BIA Steps (Cont.)
Identifying Functions' Resources
Who Connects to Who?
BIA Steps (Cont..)
Maximum Tolerable Downtime
MTD
Example
MTD Definitions
BIA Steps (Cont...)
Range of Threats to Consider
Thinking Outside of the Box What if….
Biological Threats
BIA Steps (Cont….)
Potential Disasters
Risk Approach
Ranking by Risk Level
Potential Losses
Include all RISK Components
What Have We Completed Up to Now?
BIA Steps (Cont…..)
Recovery Strategies
Alternate Business Process Procedures
Business Process Reconstruction
Recovery Strategies (Cont.)
Facility Recovery
Facility Backups – Hot Site
Facility Backups – Warm Site
Facility Backups – Cold Site
Compatibility Issues with Offsite Facility
Tertiary Sites
Subscription Costs
Multiple Processing Centers

Location, Location, Location
Choosing Site Location
Other Offsite Approaches
Security does Not Stop
More Options
Rolling Hot Site
Recovery Strategies (Cont..)
Supply and Technology Recovery
VoIP
Equipment Replacement
What Items Need to Be Considered?
Priorities
Anything Else?
Replacements
Executive Succession Planning
Recovery Strategies (Cont...)
User Environment Recovery
Recovery Strategies (Cont….)
Data Recovery Technologies
Co-Location
Data Recovery
Backup Redundancy
Recovering Data
Automated Backup Technologies
Tape Vaulting
Data Recovery (Cont.)
Clustering for Fault Tolerance
Clustering
Disk or Database Shadowing
Which Option to Use
Cost Effective Measures
Resources, Time, Solutions
Determining Recovery Solutions
Cost and Recovery Times
Proactive
BIA Steps (Cont…...)
Recovery Solutions
Preventative Measures
Reviewing Insurance
Results from the BIA
Now Ready to Develop the Plan
Basic Structure of BCP
Products That Can Help
Plan Components
Teams to Be Developed
External Groups
Policy Components
Activation Phase
Damage Assessment
Notifying Personnel
Plan Activation
Emergency Response

Policy Components (Cont.)
Next Phases
Recovery Procedures
Documentation of Recovery Steps
Policy Components (Cont..)
Reconstitution Phase
Reconstitution Items
Returning to Original Facility
Who goes First?
Disaster Hit – Now What?
Termination of BCP
Life Cycle
Who has the Plan?
Backup of the Backup Plan
Results
Types of Tests to Choose From
Test Objectives
Training Requirements
Lessons Learned
What Is Success?
Out of Date?
BCP Plans Commonly and Quickly Become Out of Date
Keeping it Current
Change Control
Resulting Plan Should Contain…
Phases of the BCP
Domain 8 Review

- Domain 9 - Application Security
- How Did We Get Here?

Why Are We Not Improving at a Higher Rate?
Usual Trend of Dealing with Security
Where to Implement Security

- Agenda 1
- Software Development Tools

CASE Tools
New Paradigm of Coding
Security Issues
Language Types
Turn into Machine Code
New and Old
Object-Oriented Programming
Classes and Objects
Objects
Object Characteristics
Functions and Messages
Encapsulation
Modularity of Objects
Object-Oriented Programming Characteristic
Polymorphism
Another Characteristic of OOP
Module Characteristics
Low Cohesion

Levels of Cohesion
Coupling

- Agenda 2
- Distributed Computing
  Distributed Computing – ORBs
  Common Object Request Broker Architecture
  COM Architecture
  DCOM Architecture
  Enterprise Java Beans
  J2EE Platform Example
  Linking Through COM
  Mobile Code with Active Content
  World Wide Web OLE
  ActiveX Security
  Java and Applets
  Sandbox
  Java and Bytecode
- Agenda 3
- Database Systems
  Database Model
  Timeline
  Hierarchical Database
  Network Database
  Object-Oriented Database
  Benefits of OO Database Model
  Object Relational Database
  Relational Database
  Database Models – Relational Components
  Relational Database Entities
  Primary Key
  Foreign Key
  Database Integrity
  Different Modeling Approaches
  Database Access Methods
  Accessing Databases
  ODBC
  OLE DB
  OLE DB Database Access
  ActiveX Data Objects (ADO)
  Java Database Connectivity
  Database Connectivity
  eXtensible Markup Language
  XML Database
- Agenda 4
- Database Security Mechanisms
  Databases are Busy Beasts
  Rollback Control
  Checkpoint Control
  Checkpoint Protection
  Lock Controls
  Deadlock Example
  Two-Phase Commit

Lock Controls Help to Provide ACID
Inference Attack
Database View Control
Common Components

- Agenda 5
- Data Warehousing
  Warehouse Creation
  Using a Data Warehouse
  Metadata
  Database Component
  Data Mart
  Potential Malicious Traffic Tunneling through Port 80
  URL Interpretation
  Common Database Attacks
- Agenda 6
- OLTP
  Online Transaction Processing
  OLTP Requirements
  Online Analytical Processing
  Knowledge Management
  Knowledge Components
  HR Example
  Knowledge Discovery in Databases
  Data Mining
  Approaches to Knowledge Management
  Expert Systems
  Expert System Components
  Artificial Neural Networks
  Data, Information, Knowledge
  Comparing Types
- Agenda 7
- Software Development Models
  System Life Cycle
  Project Development – Phases I and II
  Project Development – Phases III and IV
  Phase V
  Project Development – Phases VI and VII
  Testing Types
  Levels of Tests
  Data Contamination Controls
  Best Practices for Testing
  Test for Specific Threats
  Verification versus Validation
  Evaluating the Resulting Product
- Agenda 8
- Controlling How Changes Take Place
  Change Control Process
  Administrative Controls
- Agenda 9
- Common Information Flow
  Vulnerabilities at Different Layers
  Tier Approach and Communication Components

Tiered Network Architectures
Sensitive Data Availability
Cookies
Find Out Where You Have Been
Pulling Data
Web Server Error Pages
Steps of Interaction
Provide the Hackers with Tools
Common Web Server Flaws
Improper Data Validation
Uniform Resource Locator (URL)
Directory Traversal
Buffer Overflow
Cross-Site Scripting Attack
Common SQL Injection Attack
Attacking Mis-configurations
CGI Information
Logging Activities
Are ALL Patches Applied?
Microsoft Example Best Practices
Authorize Access
Isolation for Protection
Authentication
Protecting Traffic
Maintain Server Software
Common Issues
Best Practices

- Agenda 10
- Rolling ‘em Out

Patching Issues

- Agenda 11
- Virus

Boot Sector Invasion
Few Other Types
Types of Viruses
How Do They Work?
More Malware
Trojans
Blended Malware
A Back Orifice Attack!
NetBus
Hoaxes

- Agenda 12
- Malware Protection Types

Signature Scanning
Monitoring Activities
Monitoring for Changes
More Bad Stuff
Attack Characteristics
Disclosing Data in an Unauthorized Manner
Covert Storage Channel
Covert Timing Channel

Circumventing Access Controls
Attacks
TOC/TOU Examples
Attack Type – Race Condition
Attacking Through Applications
How Buffers and Stacks Are Supposed to Work
How a Buffer Overflow Works
Watching Network Traffic
Traffic Analysis
Functionally Two Different Types Of Rootkits
Examples of Trojaned Files
Domain 9 Review

- Domain 10 - Operations Security Objectives
- Computer Operations

Operations Security Involves
What Do We Have?
Hardware Protection
Licensing Issues
Software Installation
ITIL – Problem Management
Problem Management
Areas of Problem Management
Problem Management Procedures for Processing Problems
Higher Level Look
Data Output Controls
Administrative Controls Personnel Controls
Non-Employees
Security Operations Personnel
Change Control
Configuration Management
Another Example

- Agenda 1
- Resource Protection

Library Maintenance
Media Labels
Media Controls
Software Escrow
Media Reuse
Weak Link
Liabilities of Insecure Disposal of Information
Devastating to the Company
Results of Data Leakage
Object Reuse
Safe Disposal
Degaussing
Zeroization
Physical Destruction
Remaining Data
Purging
Why Not Just Delete the Files?
Formatting Media
Mainframes

- Agenda 2
- Different Types of Backups
  Backups
  HSM
  Off-Line
  Backup Types
  Incremental Backup
  Incremental
  Differential Backup
  Differential
  Backup Protection
  Continuous Threat
- Agenda 3
- Devices Will Fail
  Mean Time Between Failure
  Mean Time to Repair
  Single Point of Failure
  Countermeasures
  Redundant and Fault Tolerance
  Mirroring Data
  Disk Duplexing
  Direct Access Storage Device
  Redundant Array of Independent Disks
  Massive Array of Inactive Disks (MAID)
  Redundant Array of Independent Tapes (RAIT)
  Serial Advanced Technology Architecture
  SAN
  Fault Tolerance
  Network Redundancy
  Mesh Network
  Redundancy Mechanism
  Backup Configuration Files
  Some Threats to Computer Operations
  Trusted Recovery of Software
  After System Crash
  Security Concerns
- Agenda 4
- Contingency Planning
- Agenda 5
- Remote Access Security
  Authentication
  Remote Access
  Administering Systems Remotely
  Facsimile Security
  Securing Data in Motion
  Support Systems
- Agenda 6
- Before Carrying Out Vulnerability Testing
  Testing for Vulnerabilities
  Vulnerability Assessments
  Security Testing Issues
  Vulnerability Scanning

Basic Scanner
More Functionality
Data Leakage – Keystroke Logging
Looking at Keystrokes
Password Cracking
One of Many Tools
War Dialing
PhoneSweep
Wardialing Output
Detailed PhoneSweep Output
War Driving
Wireless Reconnaissance Output
Wireless Reconnaissance
Wireless Attacks
MAC Filtering
Penetration Testing
Testing Steps
Testing Methodology
Automated Pen Testing Tools Canvas Operation
Penetration Testing
Automated Pen Testing Tools Core Impact Operation
Post-Testing and Assessment Steps
Penetration Testing Variations
Types of Testing
Protection Mechanism – Honeypot
Log Reviews