Fairway Markers

This report shows a list of fairway markers by Exam and Cert Obj for the period between 06/18/2009 and 06/18/2009.

Exam 'GSLC Exam'

802.11

The manager will have an understanding of the misconceptions and risks of 802.11 wireless networks and how to secure them.

Fairway Marker
Securing and Protecting wireless best practices
Security Technologies (WPA, 802.11i, 802.1x, and EAP)
WEP Weaknesses
Wireless attacks (Eavesdropping, Wardriving, Masquerading, DoS, Rogue AP, Airborne Viruses)

Access Control and Password Management

The manager will understand the fundamental theory of access control and the role of passwords in controlling access to systems

Fairway Marker
Access control models (DAC, MAC, RBAC)
Best Practices (implicit deny, least privilege, separation of duties, job rotation)
Centralized Access Control Technologies (Active directory, RADIUS)
Fundamentals of Biometrics
Jerome Kerviel case
Password cracking
Passwords, Hashes and limitations of windows hashes
Terminology (identity, authentication, authorization, least privilege, need to know, separation of duties, rotation of duties, data owner, single sign on)
The use and importance of strong password policies

Advanced Reconnaissance and Vulnerability Scanning

The manager will understand additional methods attackers use to gather network and perimeter information, how to do a vulnerability scan and how to identify specific vulnerabilities.

Fairway Marker
CISecurity.org
Fundamentals of Core Impact
How to conduct a vulnerability scan
How to use Metasploit effectively

Fairway Marker
How to use Nessus effectively
How to use Nmap effectively
Internal and external views of a network
P2P and IM dangers and controls
Social Engineering

Building a Security Awareness Program

The manager will demonstrate an understanding of the critical elements of creating and managing a Security Awareness Program.

Fairway Marker
General approach to training
Know what NIST SP 800 - 50 is
Metrics for Security Awareness Programs
Security Awareness Goals (changing user behavior)

Business Situational Awareness

The manager will be familiar with the concept of situational awareness and the fundamental sources of information that lead to business situational awareness.

Fairway Marker
Budgeting Approaches (top down, bottom up, negotiated, devolving)
Ensuring accountability
Follow the money closely
Maximizing the benefits from investments in security
Time Management

Change Management and Security

The manager will be able to identify the signs of poor change management, understand the risks to the organization, and develop a program to improve operations.

Fairway Marker
Implementing change management
Indicators of change management problems
Relationship between undocumented changes and network instability
Repeatable builds
Tracking unplanned work

Computer and Network Addressing

The manager will understand how computers have a variety of names and addresses on a network and this must be managed.

Fairway Marker
Broadcast addresses
CIDR Addressing
IP addresses and Subnet masks (network and host portion)
MAC Addresses and OUIs (MACs built into NIC, only last for one hop)
Public and Private Addresses

Cryptography Algorithms and Concepts

The manager will be introduced to several crypto algorithms and the concepts behind secure ciphers.

Fairway Marker
Concepts in crypto (computational complexity, intractable problems, public scrutiny)
Crypto Attacks (known plaintext, chosen plaintext, adaptive chosen plaintext, ciphertext only, chosen ciphertext, chosen key)
DES (56 bit key space considered insecure, symmetric block cipher)
ECC usage and vulnerabilities
Quantum cryptography concepts
RSA Factoring Large Primes
RSA vs. DES (asymmetric vs. Symmetric) characteristics

Cryptography Applications, VPNs and IPSec

The manager will understand how cryptography can be used to secure a network and be introduced to VPNs and IPSec

Fairway Marker
IPSEC Headers (AH and ESP)
IPSEC modes (transport and tunnel)
PPP Basics
VPN components and placement issues
VPN technologies (SSL, SSH)
VPN types (site to site, client VPN)

Cryptography Fundamentals

The manager will have a basic understanding of the fundamental concepts of cryptography.

Fairway Marker
History of Cryptography
Key management is weakest link
ROT-13
Stream and block cipher characteristics
Types of ciphers (substitution, permutation, etc.)
Why cryptography is the last line of defense

Fairway Marker
XOR operations

Defense-in-Depth

The manager will be introduced to the terminology and concepts of Risk and Defense-in-Depth including threats and vulnerabilities.

Fairway Marker
Information-centric DiD
Protected Enclaves DiD
Role Based Access Control
Terminology (risk, threat, attack surface)
Uniform Protection DiD (least important type)
Vector Oriented DiD

Defensive OPSEC

The manager will understand what OPSEC is and the techniques used in defensive Operational Security.

Fairway Marker
3 key laws of OPSEC
Employee issues (monitoring, screening, agreements, need to know, least privilege)
OPSEC Defined
Sensitive information (labeling, handling, and access)

Disaster Recovery / Contingency Planning

The manager will learn how to lead the BCP/DRP team and realistically plan for Business Continuity and Disaster Recovery.

Fairway Marker
BCP (definition and components)
Business Impact Analysis
DRP (definition and components)
Key Elements of continuity planning
Top BCP/DRP Planning Mistakes

DNS

The manager will understand how the Domain Name System (DNS) works, common attacks against DNS, and what can be done to defend against those attacks.

Fairway Marker
Cache Poisoning - dangers of attacker controlling namespace
Cybersquatting

Fairway Marker
Domain Hijacking -- procedural and technical controls to prevent
gethostby name and gethostbyaddr
Hierarchy
Nslookup forward and reverse lookups
Protecting Domain Names
Recursion
Uses and misuses of the HOSTS table

Facilities, Safety, and Physical Secuirty

The manager will be able to articulate the needs of the information technology and security program to the parts of the organization responsible for physical safety and security.

Fairway Marker
Detection of unauthorized access
Evacuation preparation and procedures
Heating and Cooling Basics
Lock types (traditional, cipher lock, magnetic cards, smart cards, biometric)
Physical Security basics
Power Basics
Protecting facilities from explosives
Smoke and Fire basics - detective and suppressive controls
Ventilation Basics

Fraud Management

The manager will be familiar with the common types of fraud and how to detect them.

Fairway Marker
Indicators of Fraud
Types of Fraud (internal, customer, credit card, accounting, telecom)

General Types of Cryptosystems

The manager will have a high level understanding of the three general types of cryptosystems.

Fairway Marker
Goals of each type of crypto system (CIA + non-repudiation)
One way hash functions
Public Key Crypto (Asymmetric/two key crypto)
Secret Key Crypto (symmetric/one key crypto)

Honeypots and Honeynets

The manager will understand basic honeypot techniques and common tools used to set up honeypots.

Fairway Marker
Advantages and disadvantages of using honeypots
Honeypots defined and types (host, network, service, honey token)
How LaBrea 1 tarpits work
Legal Issues
Low Interaction vs High Interaction Honeypots
Technologies (Virtualization, honeynet project, labrea tarpit)

Incident Handling and the Legal System

The manager will be introduced to the basic legal issues in incident and evidence handling.

Fairway Marker
Chain of Custody
Evidence collection (real, direct, best, relevant, reliable, integrity, sign and seal)
Search and Seizure (with and without a warrant)
Types of laws (regulatory, criminal, civil)
US Title 18 Section 30

Incident Handling Foundations

The manager will understand the concepts of incident handling and the six-step incident handling process.

Fairway Marker
Common Incident Handling Mistakes
Containment Phase - how to contain the incident in detail (make a backup)
Detecting and recognizing incidents
Identification Phase - steps to recognize an incident in detail
Incident Handling and Incidents defined
Preparation Phase - how to in detail
Six Step Incident Handling Process Defined

Information Warfare

The manager will be familiar with the theory and techniques of information warfare.

Fairway Marker
Asymmetry
Goals of Information Warfare
Perception Management
Predictable Response

IP Terminology and Concepts

The manager will understand the terminology and concepts of IP protocols and how they support the Internet and will gain the ability to assess the knowledge of current and prospective network engineers.

Fairway Marker
Encapsulation
Fragmentation (defeats security devices, never on Ethernet)
ICMP characteristics (and how it can be abusesd/misused)
ICMP Ping
IP characteristics (how to determine embedded protocols)
Sniffers (sniffer policy)
TCP characteristics and session establishment (3-way handshake)
UDP characteristics - connectionless, unreliable, fast

Malicious Software

The manager will understand and be able to articulate what malicious code is and how it propagates and why it is such an expensive problem.

Fairway Marker
Malicious Browser Content and Hybrid Threats
Malware Defense Techniques
Propagation techniques
Trojan Horse characteristics
Virus types and characteristics
Worm characteristics

Managerial Wisdom

The manager will learn some of the most effective business techniques from the most acclaimed books.

Fairway Marker
Key Concepts from Good to Great (First Who, then What, Hedgehog Concept, Flywheel, Level 5 leader)
Know the 7 Habits of Highly Effective People

Managing Ethics

The manager will be familiar with ethical issues and guidelines pertaining to IT security.

Fairway Marker
48 laws of power (concept of amorality: win at any cost)
Ethical Discrepancies
Ethical Leadership (managers)
Ethics Terminology (Ethics, Morals, Policy, Laws, Culture)

Managing Globally

The manager will understand key factors affecting globalization including international shipping and value added tax (VAT)..

Fairway Marker
Potential barriers to global communication and business
Value Added Tax (defined and benefits)

Managing Intellectual Property

The manager will learn how to identify and protect intellectual property and intangible assets.

Fairway Marker
Attacks on IP (insider threats, cybersquatting)
Copyrights (defined, fair use, attacks, defenses)
Digital Rights Management (Sony XCP, CSS)
DMCA
How to protect IP (NDA, non-compete, need-to-know, control publicly released info, label information, monitor outgoing traffic, watermarks, Internet searches, best practices)
Intellectual Property Valuation
IP defined
Patents
Trade secrets and know how (defined, how to identify)
Trademarks and Service marks (defined, registration, attacks)

Managing IT Business and Program Growth

The manager will understand the fundamental principles to managing an IT business and achieving sustainable growth.

Fairway Marker
Customer Satisfaction and Angry Customers
Four Ps of Marketing (product, price, promotion, position)
Key Business Concepts (continuous process improvement, strategic and disruptive innovation)
Location (physical and virtual)
Three Cs (customer, cost, community)

Managing Legal Liability

The manager will understand how to use due diligence to manage an organization's legal liability with emphasis on IT issues.

Fairway Marker
Best Practices for Managing Liability
Common Damages
Downstream liability and contributory negligence
Judge Hand Negligence ruling

Managing Negotiations

The manager will be familiar with guidelines to sound negotiation practices.

Fairway Marker
Negotiation Keys (internalization, change, authority, price vs value, speed, walking away)
Distributive Bargaining (BATNA, ZOPA, claiming value, anchoring point)
Good negotiation is win-win.
Integrative Bargaining (principled, mutual gains, win-win)

Managing Privacy

The manager will be familiar with the privacy concerns that customers typically have and solutions that can be used to improve their customers' privacy.

Fairway Marker
OECD Privacy Principles
Personally Identifiable Information (PII)
Privacy Certifications (TRUSTe, WebTrust, BBB Online Privacy Seal)

Managing Security Policy

The manager will learn how to assess current policy, identify overall security posture of organization, ensure that existing policy is applicable to organization's needs and modify policy as required.

Fairway Marker
Issue-specific policy
Policy Benefits
Policy development tools (standards, guidelines, frameworks, mission statement)
Security Posture and Culture

Managing Software Security

The manager will demonstrate the ability to build security into the software development process.

Fairway Marker
Best Practices (safe defaults, modular code, user accountability, error handling)
Code Review (Manual, Automated, Hybrid, SDLC Integration)
Understand basics of common implementation flaws at a high level

Managing Technical People

The manager will understand techniques that can be used to communicate with and manage technical staff.

Fairway Marker
E-mail (business record, retention policy, when to use other comms)
Encouraging Closure of projects
Integrity

Fairway Marker
Listening to and understanding technical people
Meeting best practices
Understand the power dynamic between technical staff and management
Value of Metrics

Managing the Mission

The manager will understand how mission statements and policy keep organizations on track, and how security relates to the mission.

Fairway Marker
COBIT (fundamentals and phases)
ISO 27002 / ISO 17799 defined
Mission Statement (definition and characteristics)
Sales Cycle
Selling A Security Program to upper management
Understand how security relates to the organization
Vision Statement (definition and characteristics)

Managing the Procurement Process

The manager will demonstrate knowledge of the management responsibility for vendor selection through the primary phrases of the procurement process and learn how to provide oversight into requirements analysis, price paid, and analysis of ROI at the one year point.

Fairway Marker
Analytical Hierarchy Process (and steps)
Difference between price and value
Negotiating with vendors (vendor honesty and key negotiating points)
Ricochet response
Vendor and Product Selection

Managing the Total Cost of Ownership

The manager will understand how to apply TCO to analyze proposed solutions over their entire life cycle as well as be able to identify main areas of cost for a given project.

Fairway Marker
Direct costs and Indirect costs
Depreciation (straight line, sum of years)
SDLC disposal phase (grave costs)
TCO (defined, how to calculate)

Methods of Attack

The manager will be introduced to the most common attack methods and the basic strategies used to mitigate those threats.

Fairway Marker
Browsing, Enumeration, and Traffic Analysis
Buffer Overflow key concepts
Denial of Service (centralized p2p, distributed, physical) (basic forms: resource exhaustion , unexpected value, physical disruption, configuration disruption)
Google hacking database and Goolag
Logic bombs and the Duronio case
Malicious Code (Trojan horses and trapdoors)
MITM and Replay attacks
Phishing and spear phishing
Physical Attacks
Race conditions (timing attacks)
Rootkits
SPAM and e-mail flooding

Mitnick-Shimomura

The manager will be familiar with the details of the famous Mitnick-Shimomura attack.

Fairway Marker
IP address spoofing
DoS
Sequence number prediction

Offensive OPSEC

The manager will understand OPSEC principles by learning offensive OPSEC techniques.

Fairway Marker
Competitive intel tools and features (whitepages.com, whois.net, nslookup, tracert, geobytes, wayback machine, Dun and Bradstreet)
Controlling publicly available info (email and web)
Differentiate between espionage and competitive intelligence
Info on Individuals (google, intelius, credit reporting)
Key Google searching techniques (ext, intitle, site, link, cache, related, inanchor, info)
Sources for researching corporate information
Using press releases

Offensive Vulnerability Scanning

The manager will understand common approaches used to gather network intelligence from organizations using commonly available tools and methods used to mitigate or protect against these techniques and other common high risk points of attack.

Fairway Marker
Difference between a vulnerability scanner and exploitation tool
fingerprinting with p0f
Inside view, outside view, user view
Port scan from a spoofed address with hping
Scanning techniques (port, stealth, tcp/udp, passive)
Threat Concerns
Threat Vectors - relation to DiD

PGP and PKI

The manager will understand how Pretty Good Privacy (PGP) works and be introduced to Public Key Infrastructure (PKI).

Fairway Marker
Client and Server side certificate uses
Encrypting mail with PGP (which key encrypts, decrypts)
Key management (public key distribution, private key storage)
PKI CA Hierarchy
PKI problems/challenges
Web of Trust (can apply to linkedin or facebook, or people you know)

Project Management For Security Leaders

The manager will be familiar with the terminology, concepts and five phases of project management.

Fairway Marker
Closing out
Dependencies
Monitor, Control, Conflict Resolution, Change Management
Phases of project management
Staying on top of execution is key to bringing tasks to close

Risk Management and Auditing

The manager will understand how to evaluate and manage risk.

Fairway Marker
Acceptable Risk (who decides)
Acting on the risk (accept, mitigate, transfer, avoid)
Analysis types (SWOT, Cost Benefit, Weakness Gap, Threat Gap)
Best Practices (templates, group policy, hotfixes, www.cisecurity.org, etc.)
Calculating Annualized Loss Expectancy (ALE)
Calculating Single Loss Expectancy (SLE)

Fairway Marker
Difference between qualitative and quantitative approaches
Terminology (Risk, threat, vulnerability, SDLC)
Types of Risk

Security and Organizational Structure

The manager will understand how security integrates into organizational structure and be familiar with guidelines for recruiting and hiring IT staff.

Fairway Marker
Capacity analysis and methods for increasing capacity
Employee discipline and termination
Employee performance (measuring, diagnosing causes of failure)
Employee retention, compensation, and promotion
Filling positions (requirements, hiring, interviews, 1099)
Potential conflict of interest for CISO/CSO to report to CIO

Steganography

The manager will understand the concepts and techniques behind steganography and be introduced to steganographic tools and defensive techniques.

Fairway Marker
Differences between steganography and cryptography and why detection is more difficult
Methods (injection, substitution, file generation)
Steganalysis

The Intelligent Network

The manager will demonstrate an understanding of the differences between a typical traditional network design and the new components that are part of an intelligent network.

Fairway Marker
Basic troubleshooting (troubleshooting UTM)
Data Normalization
Firewall types and the default rule
HIPS and NIPS basics
Ingress/Egress filtering
IPS and IDS basics, alert types, and importance of detection
Managing NIDS Costs (deployment and maintenance)
Signature Analysis, Anomaly Analysis, and Application/Protocol Analysis
Unified Threat Management (features, drawbacks, selection criteria)

The Network Infrastructure

The manager will understand and be able to communicate the fundamental technologies and concepts that describe LAN and WAN network infrastructure.

Fairway Marker
Ethernet
Logical and physical topologies
Network segmentation
TCP Model
The OSI Model
VLANs and how they support Defense In Depth
VOIP Basics, Security Implications, availability issues, and threats

Web and Communications Security

The manager will be introduced to web application communications, security issues, and defenses.

Fairway Marker
CGI and State/Cookie basics
Cross Site Scripting
HTTPS security misconceptions
Protocol basics (HTTP, HTTPS, and FTP)
Proxy modification of cookies
SOA (Exposes business logic)
SQL Injection (stored procedures and input validation to mitigate)

Wireless Advantages and Bluetooth

The manager will understand the advantages that make wireless technology ubiquitous and be introduced to Bluetooth wireless technology.

Fairway Marker
Attacks (bluesnarf, bluejack, sniffing)
Bluetooth defenses (non-discoverable mode, auditing, pairing in trusted environment, strong PINS)
Bluetooth protocol fundamentals (PIN, discovery mode)
Wireless Advantages