Cyber Security

Length: 2 Days

COURSE CONTENT

ACCESS CONTROL

- Effectiveness
- Attacks

TELECOMMUNICATIONS AND NETWORK SECURITY

- Network architecture and design
- Communication channels
- Network components
- Network attacks

INFORMATION SECURITY GOVERNANCE AND RISK MANAGEMENT

- Security governance and policy
- Information classification/ownership
- Contractual agreements and procurement processes
- Risk management concepts
- Personnel security
- Security education, training and awareness
- Certification and accreditation

SOFTWARE DEVELOPMENT SECURITY

- Systems development life cycle (SDLC)
- Application environment and security controls
- Effectiveness of application security

CRYPTOGRAPHY

- Encryption concepts
- Digital signatures
- Cryptanalytic attacks
- Public Key Infrastructure (PKI)
- Information hiding alternatives

SECURITY ARCHITECTURE AND DESIGN

- Fundamental concepts of security models
- Capabilities of information systems (e.g. memory protection, virtualization)
- Countermeasure principles
- Vulnerabilities and threats (e.g. cloud computing, aggregation, data flow control)

OPERATIONS SECURITY

- Resource protection
- Incident response
- Attack prevention and response
- Patch and vulnerability management

BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

- Business impact analysis
- Recovery strategy
- Disaster recovery process
- Provide training