# Introduction to Cyber Security

**ITShare's Introduction to Cyber Security course is designed to give you a foundational look at today's cyber security landscape and how to evaluate and manage security protocol in information processing systems. You will learn about information security concepts and technologies, the principles behind security architecture, how to mitigate vulnerabilities and threats to your systems, and how to implement risk and incident management to protect your infrastructure from cyber attack.**

**Who should enroll in this program?**

The course is ideal for professionals in any organizational role who wish to learn the fundamentals of cyber security and pursue a career in this booming field. The course also caters to CxO level and middle management professionals who want to gain awareness of and address cyber risks.

**Introduction to Cyber Security Course Outcomes:**

Upon completion of this course, you will become familiar with cyber security methodologies and be able to:

- Leverage an enhanced awareness of cybersecurity principles and concepts
- Analyze appropriate types of controls to counteract various threats
- Combat social engineering attacks such as phishing, malware, spyware, adware, ransomware, and Bluetooth attacks
- Determine and analyze software vulnerabilities and security solutions to reduce the risk of exploitation
- Comprehend and execute risk management processes, risk treatment methods, and key risk and performance indicators
- Develop and manage an information security program

## Program Features:

- Four hours of online self-paced learning
- Lifetime access to self-paced learning
- Industry-recognized course completion certificate
- Industry examples and case studies

## Program Description:

### Lesson 01 - Cybersecurity Fundamentals

**Fundamentals of Cybersecurity**

- Introduction to Cyber Security (What and Why)
- Difference between Information Security and Cyber Security
- Cyber Crime Statistics
- Factors Affecting Cybersecurity
- CIA Triad
- Governance, Risk Management, and Compliance
- Cybersecurity Roles
- Approaches to Cyber Security
- Key Terms - Cybersecurity
- Iliustration - Basics of Cybersecurity

**Threat Actors, Attacks and Mitigation Threat Actors, and Categories**

- Threats to a System
- Malware and its types
- Worms, Virus, and Trojan Horse, Backdoor, Rootkits, and logic Bombs, spyware and Adware, Ransomware
- Malware Attacks
- Denial of Service Attack
- Distributed Denial of Service Attack
- Recent DOS/DDOS Attacks

- Application-layer Attacks
- Software Codes and Security
- Software testing methods
- Security Attacks
- Social Engineering
- Social Engineering Attacks Categories
- Social Engineering Attack: Ethereum Classic

**Security Policies and Procedures**

- Security Management Plan
- Types of Security Management Plans
- Security Policy and Types
- Security Policy Framework: Standard/Baseline/Guideline/Procedure
- Due Care and Due Diligence

**Cybersecurity Mitigation Methods**

- Controls or Countermeasures
- Control Types - Implementation Categories
- Control Types - Based on Functionality
- Defense in Depth  or Layered Approach
- Identity Management
- Components of Identity Management
- Identification and Authentication
- Authorization and accountability
- Auditing and Monitoring
- Patch Management
- System Hardening
- System Hardening Activities
- Change Control
- Change control Flow
- Asset Inventory Management
- Asset inventory Management Life Cycle

- Data Management and Stages of Data
- Data LifeCycle
- Data Classification
- Data Protection: Encryption
- Encryption
- Cryptography
- Effective encryption system depends on
- Types of Encryption
- Symmetric Encryption
- Asymmetric Encryption
- Incident Response
- Security Training and Awareness

## Lesson 02 - Enterprise Architecture and Components

### Secure Architecture

- Enterprise Network Architecture
- Basics of Network architecture
- Types of Network architecture
- OSI Model and Seven layers
- Types of Networks
- Data Communication Systems
- Computer Based Information System
- Business Information System
- Hardware Failures
- Hardware Monitoring Procedures
- Host Based Security and its controls

### Wireless networks

- Wireless Networks

- Wireless Attacks and Countermeasure
- Case Study: Wireless Attack
- Virtual Private Network and its types
- VPN Risks and its controls
- Wireless Network Example: Bluetooth
- Bluetooth Attacks and Countermeasure
- Bluetooth Vulnerability - Blueborne
- Radio-Frequency Identification (RFID)
- RFID Risks and Controls
- Case Study: RFID Hack
- Emanation Security

**Network Security Controls**

- Network-based security
- Network attack categories
- Firewall and its features
- UTM - Unified Threat Management
- Web Application Firewalls
- Intrusion Detection System, components, categories
- Intrusion Prevention System
- Network Admission Control
- HoneyPots

**Cloud, Virtualization, BYOD, and IOT Security**

- Virtualization
- Hypervisor
- Case Study - Hypervisor Attack
- Cloud Computing
- Cloud computing characteristics
- Categorization of Cloud: Service and Deployment Categories
- Cloud Security Challenges
- Bring your own Device

- Bring your own Device - Security
- IOT - Internet of Things, Challenges

**Security Testing**

- Vulnerability Scanning, goals
- Penetration testing
- Types of Penetration testing
- Security Audits, types

## Lesson 03 - Information System Governance and Risk Assessment

**Information Security Governance**

- Information Security Governance
- IT Governance Focus Areas
- Business Goals, Objective, and Drivers of Information Security Governance
- Enabling Technology
- Enablers for Governance, Categories
- Effective Information Security Governance
- Information Security Governance Outcomes
- Management support
- Establish reporting and communication Channels
- Performance Management
- IT Balance Score Card
- Capability Maturity Levels
- Smart Metric

**Risk Management**

- Introduction to Risk Management
- Factors to consider in risk management
- Risk Mangement Process

- Risk Management Approach - Quantitive
- Risk Management Approach - Qualitative
- Risk Management Methods
- Key Risk Indicator and Key performance indicator KPI and KRI
- Risk IT Framework

**Information Security Programs**

- Information System Programs
- IS Program Components
- IS Program Objectives
- IS Program Charter
- Information Security Management Framework
- COBIT, five principles
- ISO 27001:2013, Domains
- IS Program Roadmap
- Outcomes of IS program
- Supply Chain, Supply chain management, SCRM
- Supply Chain Risks and countermeasures
- Supplier Management Controls
- Personnel Management
- Case Study: AWS Outage
- Common Information Security Program Challenges

## Lesson 04 - Incident Management

**Developing an Incident Management and Response System**

- Basic Definitions: Incident, Incident management, Incident response, Incident response plan
- Incident Management Stages
- Incident Response Metrics
- Incident Management Team (IMT)
- Gap Analysis

**Digital Forensics**

- Digital Forensics, Goal
- Forensic Investigation Process
- Forensic process best practices
- Forensic Investigative Assessment Types
- Digital Evidence
- Digital Evidence - Admissible in court
- Evidence Life Cycle
- Chain of Custody

**Business Continuity and Disaster Recovery**

- Business Continuity Planning and Disaster Recovery
- Seven Phases of a Business Continuity Plan
- Basic Terms of BCP and DR
- Business Impact Analysis
- Disaster Recovery Sites and Types
- DR Testing and Types