Understanding the Roles and Responsibilities of a CISO

A presentation by the International CISO Advisory Board
What does a CISO do?

- Security Operations
- Business Enablement
- Governance
- Digital Leadership
- Identity Management
- Project Delivery
- Risk Management
- DevSecOps
- HR & Compliance
- Audit & Regulatory
- Security Architecture
Digital Leadership

- Cyber Security Leader
- Negotiating
- Cyber security vision
Project Delivery

- Requirements
- Plan & Design
- Operational Support
- Certification & Accreditation
- Security Testing
Security Architecture

- Network Segmentation
- Application Security
- Defense-in-depth
- Remote Access
- Zero Trust Model
- Industry 4.0
- Encryption Technologies
- Network Virtualization
- Software-Defined Networking
- Cloud Security
- Back-up & Recovery Plans
- Data Security/Protection
Risk Management

1. Physical Security
2. Ongoing Risk Assessment/Pen Testing
3. Integration to Project Delivery
4. Code reviews
5. Risk Assessment Methodology & Framework
6. Policies & Procedures
7. Phishing & Associate Awareness
8. Third Party Risk Assessment
9. Data-Centric Approach
   1. Data Discovery
   2. Data Classification
   3. Access Control
   4. Data Loss Prevention
   5. Partner Access
   6. Encryption/Masking
   7. Monitoring & Alerting
Security Operations

Threat Prevention
1. Network Security
2. Vulnerability Management
   - Identify
   - Classify
   - Mitigation
   - Measure
3. Application Security
4. Identity & Access Management
5. IS Policy
6. Security Health Checks
7. Cyber Threat Intelligence

Threat Detection
1. SIEM
2. SOC Operations
3. AI & Data Analytics
4. Red Team/Blue Team
5. Cyber Threat Intelligence

Incident Management
1. Incident Handling/Response
2. Digital Forensics

Disaster Recovery/Business Continuity
Know more about starting your CISO journey.

Visit - ciso.eccouncil.org