CISO Job

Last Update - October 7, 2016
Twitter: @rafeeq_rehman
Version 8

- Security Operations
  - Threat Prevention
    - Network/Application Firewalls
    - Vulnerability Management
      - Scope
        - Operating Systems
        - Network Devices
        - Applications
        - Databases
        - Code Review
        - Physical Security
        - Cloud
        - Mobile Devices
      - Identify
        - Periodic
        - Comprehensive
      - Classify
        - Risk Based Approach
        - Prioritize
      - Mitigation
        - Fix
        - Verify
      - Measure
        - Baseline
        - Metric
        - Use Awareness Program as a tool
    - Application Security
      - Application Development Standards
      - Secure Code Training and Review
      - Application Vulnerability Testing
      - Change Control File Integrity Monitoring
      - Web Application Firewall
      - Integration to SDLC and Project Delivery
    - IPS
    - Identity Management
    - Information Security Policy
    - DLP
    - Anti Malware, Anti-spam
    - Proxy/Content Filtering
    - Patching
    - DDoS Protection
    - Hardening guidelines
    - Desktop security
    - Encryption, SSL
    - PKI
    - Security Health Checks
  - Threat Detection
    - Log Analysis/correlation/SIEM
    - Alerting (IDS/IPS, FIM, WAF, Antivirus, etc)
    - NetFlow analysis
    - DLP
    - Threat hunting
    - MSSP integration
    - SOC Operations
      - SOC Resource Mgmt
      - Shift management
      - SOC procedures
      - SOC Metrics and Reports
      - SOC and NOC Integration
      - SOC Tech stack management
      - Threat Intelligence Feeds and proper utilization
      - SOC DR exercise
      - Partnerships with ISACs
  - Incident Management
    - Incident Response
    - Media Relations
    - Incident Readiness Assessment
    - Forensic Investigation
    - Data Breach Preparation
      - Update and Test Incident Response Plan
      - Set Leadership Expectations
      - Media Relations
      - Business Continuity Plan
      - Forensic and IR Partner
      - Insurance Policy
      - Adequate Logging
      - Breach exercises (e.g. simulations)
- Budget
  - Security Projects
  - Business Case Development
  - ROSI
  - Alignment with IT Projects
  - FTE and contractors
  - Balancing budget for People, Trainings, and Tools/Technology
- Business Enablement
  - Mergers and Acquisitions
    - Acquisition Risk Assessment
    - Integration Cost
    - Identity Management
  - Cloud Computing
    - Cloud architecture
    - Strategy and Guidelines
    - Cloud risk evaluation
    - Compliance
    - Ownership/Liability/Incidents
    - SaaS Strategy
      - Vendor's Financial Strength
      - SLAs
      - Infrastructure Audit
      - Proof of Application Security
      - Disaster Recovery Posture
      - Application Architecture
      - Integration of Identity Management/Federation/SSO
      - SaaS Policy and Guidelines
    - Log integration
    - VIrtualized security appliances
  - Mobile Technologies
    - Policy
    - Technology
    - Lost/Stolen devices
    - BYOD
    - Mobile Apps Inventory
  - Processes
    - HR/On Boarding/Termination
    - Business Partnerships
  - Business Continuity and Disaster Recovery
  - Understand industry trends (e.g. retail, financials, etc)
  - Eveluating Emerging Technologies (e.g. SDN, Virtual Reality etc)
  - IOT
    - IOT Frameworks
    - Devices
    - IOT Communication Protocols
    - Device Auth and Integrity
    - Over the Air updates
    - IOT Use cases
      - Track and Trace
      - Condition Based Monitoring
      - Customer Experience
      - Smart Grid
      - Smart Cities / Communities
      - Others ...
  - Data Analytics
  - Virtual Reality
  - Crypto currencies/Blockchain
- Project Delivery Lifecycle
  - Requirements
  - Design
  - Security Testing
  - Certification and Accreditation
- Security Architecture
  - Network Segmentation
  - Application protection
  - Defense-in-depth
  - Remote Access
  - Encryption Technologies
  - Backup/Replication/Multiple Sites
  - Cloud/Hybrid/Multiple Cloud Vendors
  - Software Defined Networking
  - Network Function Virtualization
- Compliance and Audits
  - PCI
  - SOX
  - HIPAA and HITECH
  - Regular Audits
  - SSAE 16
  - NIST/FISMA
  - Other compliance needs
- Legal and Human Resources
  - Data Discovery
  - Vendor Contracts
  - Investigations/Forensics
  - Attorney-Client Privileges
  - Integrating into IDM processes
  - Data Retention and Destruction
- Risk Management
  - Physical Security
  - Vulnerability Management
  - Ongoing risk assessments/pen testing
  - Integration to Project Delivery (PMO)
  - Code Reviews
  - Risk Assessment Methodology
  - Policies and Procedures
  - Associate Awareness
  - Data Centric Approach
    - Data Discovery
    - Data Classification
    - Access Control
    - Data Loss Prevention - DLP
    - Partner Access
    - Encryption/Masking
    - Monitoring and Alerting
  - IoT Technologies
  - Operational Technologies
    - Industrial Controls Systems
    - PLCs
    - SCADA
    - HMIs
- Identity Management
  - Credentialing
  - Account Creation/Deletions
  - Single Sign On (SSO, Simplified sign on)
  - Repository (LDAP/Active Directory)
  - Federation
  - 2-Factor Authentication
  - Role-Based Access Control
  - Ecommerce and Mobile Apps
  - Password resets/self-service
  - HR Process Integration
  - Integrating cloud-based identities
  - IOT device identities
- Governance
  - Strategy and business alignment
  - Risk Mgmt/Control Frameworks
    - COSO
    - COBIT
    - ISO
    - ITIL
    - NIST
  - Resource Management
  - Roles and Responsibilities
  - Data Ownership
  - Conflict Management
  - Metrics and Reporting
    - Operational Metrics
    - Executive Metrics and Reporting
    - Validating effectiveness of metrics
- Selling InfoSec (Internal)
  - Aligning with Corporate Objectives
  - Continuous Mgmt Updates
  - Innovation and Value Creation
  - Expectations Management