

CISO MindMap 2025

What do Security Professionals Really do?

Managing Security Projects

Business Case Development
Balancing budget for People, Training, and Tools/Techology/hardware, travel, conferences
Consulting and outsourcing
Contract management
Technology amortization
Better returned & utilized tools
Recruiting, performance & retention
Staff burnout prevention
Balance FTE and contractors
Staff training and skills update

Acquisition Due Assessment
Network/Application/Cloud Integration Cost
JAM integration
Security tools rationalization
Multi-Cloud architecture
Strategy and Guidelines
Cloud Security Posture Management (CSPM)
Diversification/Liability/Compliance
Vendor's Financials
SLA's
Infrastructure Audit
Proof of Application Security
Disaster Recovery Posture
Data ownership, compliance
Integration Management/Federated/SOLO
SaaS Policy and Guidelines

Cloud Integration/PA
Virtual machine security incident
Cloud-native app security
Containers-to-container communication security
Service mesh, micro services
Serverless computing security
Technology advancements

Last/Bottom devices
BYOD and MDM (Mobile Device Management)
Mobile Apps Inventory
HDD/Board/Termination
Business Partnership
Agility, Business Continuity and Disaster Recovery
Understand industry trends (e.g., retail, financials, etc.)
Evaluating Emerging Technologies (e.g., Blockchain, AI/ML, GenAI, etc.)

IOT Frameworks
Hardware/Devices security features
IOT Communication Protocols
Device Identity, Auth and Identity
Over the Air updates
Track and Trace
Customer Experience
Smart Grid / Communities
Others...
IOT Gateways
Augmented and Virtual Reality
Edge Computing

AI Governance, Policies, Transparency
LLMs, Chatbots, Agents, RAG
Safe and ethical uses of GenAI
Secure AI/GenAI models
Protecting Intellectual Property
Identify Good and Bad data
Securing training and test data
Advanced threat detection
AI enabled security tools, threat detection
Train threat teams on AI technologies
NIST AI Risk Mgmt Framework
Use of GenAI in risk automation
AI/GenAI testing tools
OWASP Top 10 LLM and GenAI risk

Embedding security in Project Requirements
Threat modeling and Design reviews
Security Testing
Certification and Accreditation
Traditional network Segmentation
Micro segmentation strategy
Application protection
Data loss prevention
Remote Access
Encryption Technologies
Backup/Replication/Multiple Sites
Cloud/Hybrid/Multiple Cloud Vendors
Software Defined Networking
Network traffic prioritization
Zero trust models and roaming
SASE/SDSE strategy, vendors
Overlay networks, secure enclosures
CCPA, GDPR & other data privacy laws
HIPAA and HITRUST
Regular Audits
SSAE 18
NIST/ISMS
CMIC
HITRUST
GDPR
SEC notification requirements
Other compliance needs

Data Discovery and Data Ownership
Vendor Contracts
Investigations/Forensics
Attorney-Client Privileges
Data Retention and Destruction
Physical Security
Vulnerability Management
Ongoing risk assessment and testing
Code Reviews, SAST
Use of Risk Assessment Methodology and Framework
Policies and Procedures
Phishing and Associate Awareness
Data Discovery
Data Classification
Access Control
Data Loss Prevention - DLP
Customer and Partner Access
Encryption/Masking
Monitoring and Alerting
Industrial Controls
PLCs
SCADA
HMI's
Third party risk management (TRM) information
Cyber Risk Quantification (CRQ)
Maintain Centralized Risk Register
Loss, Fraud prevention

Managing Security Projects

Business Case Development
Balancing budget for People, Training, and Tools/Techology/hardware, travel, conferences
Consulting and outsourcing
Contract management
Technology amortization
Better returned & utilized tools
Recruiting, performance & retention
Staff burnout prevention
Balance FTE and contractors
Staff training and skills update

Acquisition Due Assessment
Network/Application/Cloud Integration Cost
JAM integration
Security tools rationalization
Multi-Cloud architecture
Strategy and Guidelines
Cloud Security Posture Management (CSPM)
Diversification/Liability/Compliance
Vendor's Financials
SLA's
Infrastructure Audit
Proof of Application Security
Disaster Recovery Posture
Data ownership, compliance
Integration Management/Federated/SOLO
SaaS Policy and Guidelines

Cloud Integration/PA
Virtual machine security incident
Cloud-native app security
Containers-to-container communication security
Service mesh, micro services
Serverless computing security
Technology advancements

Last/Bottom devices
BYOD and MDM (Mobile Device Management)
Mobile Apps Inventory
HDD/Board/Termination
Business Partnership
Agility, Business Continuity and Disaster Recovery
Understand industry trends (e.g., retail, financials, etc.)
Evaluating Emerging Technologies (e.g., Blockchain, AI/ML, GenAI, etc.)

IOT Frameworks
Hardware/Devices security features
IOT Communication Protocols
Device Identity, Auth and Identity
Over the Air updates
Track and Trace
Customer Experience
Smart Grid / Communities
Others...
IOT Gateways
Augmented and Virtual Reality
Edge Computing

AI Governance, Policies, Transparency
LLMs, Chatbots, Agents, RAG
Safe and ethical uses of GenAI
Secure AI/GenAI models
Protecting Intellectual Property
Identify Good and Bad data
Securing training and test data
Advanced threat detection
AI enabled security tools, threat detection
Train threat teams on AI technologies
NIST AI Risk Mgmt Framework
Use of GenAI in risk automation
AI/GenAI testing tools
OWASP Top 10 LLM and GenAI risk

Embedding security in Project Requirements
Threat modeling and Design reviews
Security Testing
Certification and Accreditation
Traditional network Segmentation
Micro segmentation strategy
Application protection
Data loss prevention
Remote Access
Encryption Technologies
Backup/Replication/Multiple Sites
Cloud/Hybrid/Multiple Cloud Vendors
Software Defined Networking
Network traffic prioritization
Zero trust models and roaming
SASE/SDSE strategy, vendors
Overlay networks, secure enclosures
CCPA, GDPR & other data privacy laws
HIPAA and HITRUST
Regular Audits
SSAE 18
NIST/ISMS
CMIC
HITRUST
GDPR
SEC notification requirements
Other compliance needs

Data Discovery and Data Ownership
Vendor Contracts
Investigations/Forensics
Attorney-Client Privileges
Data Retention and Destruction
Physical Security
Vulnerability Management
Ongoing risk assessment and testing
Code Reviews, SAST
Use of Risk Assessment Methodology and Framework
Policies and Procedures
Phishing and Associate Awareness
Data Discovery
Data Classification
Access Control
Data Loss Prevention - DLP
Customer and Partner Access
Encryption/Masking
Monitoring and Alerting
Industrial Controls
PLCs
SCADA
HMI's
Third party risk management (TRM) information
Cyber Risk Quantification (CRQ)
Maintain Centralized Risk Register
Loss, Fraud prevention

Last update: March 31, 2025
Expiration date: September 30, 2026
Twitter: @rafeeq_rehman
Downloads: <http://rafeeqrehman.com>

InfoSec Professionals Responsibilities

Artificial Intelligence and Generative AI (GenAI)

Project Delivery Lifecycle

Security Architecture

Compliance and Audits

Legal

Risk Management

Security Team Branding

Remote Work

Automation and Analytics

Governance

Identity Management

Security Operations

Focus Areas for 2025-26

1. It is time for securing GenAI
2. Consolidate and rationalize security tools
3. Identify and manage security debt
4. Ransomware and Cyber resilience
5. Create meaningful metrics
6. Improve Cyber Hygiene

© Copyright 2012-2025 - Rafeeq Rehman