DATA SECURITY: STRATEGIES, BEST PRACTICES & EMERGING TRENDS

(Sunday) 20th April 2025 (1 Day)
09:00AM - 03:00PM
In-person @ UIC premises
Arabic/material in English

FEES FOR UIC MEMBERS
KWD 95

FEES FOR NON-MEMBERS
KWD 125

Roland Abi Najem

Training Objectives:

1. Understand the fundamentals of data security and its importance in modern business.
2. Identify key threats, risks, and vulnerabilities in data security.
3. Learn about cybersecurity frameworks, best practices, and compliance regulations.
4. Explore different data protection technologies, including encryption, firewalls, and access controls.
5. Understand strategies for detecting and responding to security breaches.
6. Develop an action plan to strengthen data security in their organization.

Target Audience:

- IT Managers & System Administrators
- Compliance Officers & Legal Counsel
- Risk Management Professionals
- Business Leaders & Executives
- Project Managers & Team Leads

DATA SECURITY: STRATEGIES, BEST PRACTICES & EMERGING TRENDS

Outline:

Module 1: Introduction to Data Security

- What is Data Security?
- Importance of Data Protection in Organizations
- Key Principles of Data Security: Confidentiality, Integrity, Availability (CIA Triad)
- Case Study: Real-World Data Breaches & Their Impact

Module 2: Understanding Threats & Vulnerabilities

- Types of Cyber Threats: Malware, Ransomware, Phishing, Insider Threats
- Vulnerabilities in IT Systems & Human Factors
- Attack Vectors: Network, Cloud, IoT, Social Engineering
- Risk Assessment Frameworks (NIST, ISO 27001, etc.)

Module 3: Data Security Technologies & Best Practices

- Encryption Techniques (AES, RSA, SSL/TLS)
- Firewalls, Intrusion Detection & Prevention Systems (IDS/IPS)
- Endpoint Security & Zero Trust Architecture
- Access Control & Multi-Factor Authentication (MFA)

Module 4: Regulatory Compliance & Legal Aspects

- Overview of Data Protection Laws: GDPR, CCPA, HIPAA, ISO 27001
- Compliance Requirements & Consequences of Non-Compliance
- Privacy by Design & Data Governance Best Practices
- Discussion: How Regulations Impact Different Industries

Module 5: Data Security Strategy & Risk Management

- Building a Data Security Strategy
- Implementing Risk-Based Security Measures
- Security Audits & Penetration Testing
- Workshop: Conducting a Risk Assessment in Your Organization

Module 6: Incident Response & Business Continuity Planning

- Cyber Incident Lifecycle: Identification, Containment, Eradication, Recovery
- Building an Effective Incident Response Plan
- Backup & Disaster Recovery Strategies
- Case Study: Handling a Major Data Breach

Module 7: Emerging Trends & Future of Data Security

- AI & Machine Learning in Cybersecurity
- Blockchain for Secure Data Transactions
- Quantum Computing & Its Impact on Encryption
- Cybersecurity in the Age of IoT & Cloud Computing

Module 8: Action Plan & Final Discussion

- Best Practices for Strengthening Data Security in Organizations
- Interactive Q&A & Troubleshooting Security Challenges
- Developing a Personalized Data Security Roadmap
- Course Wrap-Up & Key Takeaways

DATA SECURITY: STRATEGIES, BEST PRACTICES & EMERGING TRENDS

Expert's Profile: Roland Abi Najem

Roland Abi Najem Founder and CEO of Revotips – Expert Tech Consultants and Solutions. He was the IT & Cyber Security Consultant at the Ministry of Information – Kuwait and the Personal Consultant for the Minister of Information From 2014 till 2016.

Certified Trainer & Content Developer by ISTD (International Society For Trainers & Developers) He holds a Master's in Business Administration (MBA), Focus on M.I.S Management Information Systems.

Technical Consultant and Information Security Expert with the Mohammed Al Jassim Group for Lawyer and Legal Consultation and specialized in Cyber Crimes.

Roland is the Chairman at several seminars and conferences in the region and also Keynote speaker & Panelist.