Amity Institute of Training and Development

Leading Cybersecurity Change: Building a Security-Based Culture

CONTEXT

Digitalization and the growing networking of machines and industrial systems also mean an increase in the risk of cyberattacks. Appropriate protective measures are imperative, especially for critical infrastructure facilities. An approach that covers all levels simultaneously – from the operational to the field level and from access control to copy protection – is essential for comprehensively protecting industrial facilities against internal and external cyberattacks.

This course is for business leaders, general managers, and executives looking to build an action plan for a more cyber resilient organization.

KEY BENEFITS

After attending this program, participants will be able to:

- To select and use the right frameworks to enhance cybersecurity decision-making in your organization
- To assess risk, improve defences, and reduce vulnerabilities in your organization
- To speak the language of cybersecurity to enable informed conversations with your technology teams and colleagues, and ensure your organization is as cybersecure as possible
- To plan and build a Security based culture in an organization.
- To compare and select the right frameworks to enhance cybersecurity of the organization.
- To assess risk, improve defences, and reduce vulnerabilities in an organization.

PROGRAM CONTENT

MODULE 1	MODULE 2	MODULE 3
Cyber Security Fundamentals	**Enterprise Infrastructure Security**	**Enterprise Network Security**
• Introduction to Cyber Security • Cyber Security Attacks- Passive and Active Attacks • Cyber Security Services: Confidentiality,	• Sources of security threats, Motives & Target Assets • Consequence of Security Threats • Enterprise Cyber Security Threats: E-mail Threats,	• Introduction to Cryptography • Public Key Encryption Algorithms & Public-key Infrastructure • Cryptographic Protocols

Authentication, Non-Repudiation, Integrity, Access Control, Availability, • Point of Vulnerability, • Model for Internetwork Security • Internet Standards and RFCs	Web threats, Hacking, Intruders, Insider threats • Current Trends of Cyber Crimes: Cyber Squatting, Cyber Stalking, Crime of deception, Content Oriented Online Crime, Malicious Software use and detection, Cyber Terrorism • Network Security Threats	• Digital Signature, Digital Watermarking and Steganography • E-Commerce Security • Biometric Security

MODULE 4	MODULE 5	MODULE 6
Identity & Access Management	**Cyber Security & Risk Management**	**Creating Cyber Security Culture in Enterprises**
• Authentication & Authorization • AAA Triads • Access Control Model • Active Directory • Identity Theft and Intellectual property theft	• Introduction to Security Risk Management & Risk Assessment • Security Assurance Approaches: OCTAVE and COBIT Approaches. • Cyber Security Management in Enterprises & Businesses: Network Security Management, Firewalls, IDS, IPS, and IDPS Management. • Web and Wireless Security Management. • Cyber Security Models: Access control models, Role-Based and Lattice Models.	• Computer Security Log Management • Malware Handling and Vulnerability Management programs. • Specifying and enforcing security policies, • Information security audit and principles of audit. • Information Security Standards and Compliance: Overview of Security Standards, ISO 17799 Standard, Legal and Ethical issues, PCI DSS • Cyber Insurance: Risk Transfer • NIST Cybersecurity Framework

PARTICIPANT PROFILE

- Aspiring professionals who want to unleash the potential in them.
- Government officials, professionals, executives Managers at all levels in all lines of business and enterprises.

DURATION - 2 Weeks