Cyber Security: an overview of the global landscape, the defence strategies and the GDPR

Course Outline

Day 1:

- **Background of information security and Cybercrime**

  - Definitions (World Wide Web, The Deep Web, The Dark Web, Cloud computing, Software as a Service (SaaS), Platform as a Service (HaaS), Infrastructure as a Service (IaaS), database structure, Internet protocol (IP) addressing, domain Name servers, routers and gateways, data packets, etc).
  - Distinctions (how cyber security is distinct from information security, Cybercrime and cyber-enabled crime)
  - Fundamental issues (Policies & Standards, Identity & Access Management, Threat & Vulnerability Management, Service Providers, IT Risk Management)
  - Technical Cybercrime attacks (denial of Service (DoS), man-in-the-middle attacks (MitM), Botnets, Spam, device intrusions / hacking, password cracks, data breaches, bring your own device (BYOD) risks, Viruses, ransomware, crypto-extortion attacks, online frauds and other financially motivated eCrimes)
  - The human element (errors and accidental disclosures, rogue insiders, Insider frauds, identity theft, Phishing, Pharming, physical intrusions, password sharing and weak passwords, self-provisioning)
  - Social engineering (identity theft, blackmail, harassment, stalking, grooming, data breaches, reputational harm and brand damage, Facebook/Twitter/LinkedIn issues)

- **The Regulatory environment & The Role Of Authorities**

  - Fundamental Concepts (internet law, net neutrality, free speech, Internet censorship, privacy expectations, Intelligence services surveillance, responsibilities of ISPs)
  - An overview of the General Data Protection Regulation,
  - EU Legislation (EU Legislation Landscape, Convention on CyberCrime, Data Privacy, Electronic Identity, Regulation of Investigatory Powers, Computer Misuse)
  - Vertical Market Regulation (PCI DSS, Basel III, Solvency II, FCA/PRA)
  - Soft Law and Standards (ISO 27001)
  - International Landscape (US, UK, EU)
  - The Role of Authorities (ENISA, EU-CERT, Europol, Local Authorities)

Day 2:

- **Preventing, Detecting and Responding To Cybercrime**
    - An overview of technology (Firewalls & IDS, anti-malware applications, logging and reporting, penetration testing, methodologies)
    - Recognising the threat (exposure, “Hacktivists” or single-issue extremists, nation states, organised crime networks, etc.)
    - Known vulnerabilities (networks, connected devices, common applications and browsers, database systems, online services)
    - Cybercrime response strategies

- **Strategies & Technology Options for Cyber Security**
    - Emerging threats (emerging vulnerabilities, “Internet of Things” (IOT), big data analytics, cryptocurrencies, unregulated payment models, Cloud computing, Cybercrime insurance policies)
    - Ethical issues (ethical search engine optimisation, fair usage policy, good online practice, employee monitoring and privacy)
    - Governance (organisational and third-party relationships, key cyber security risk metrics, information security framework, cyber security control frameworks, due diligence techniques, impact of culture on cyber security for international business)
    - Risk management (manage the risk of Cybercrime, technological procurement, employee lifecycle)
    - Testing (penetration testing, SDLC, cyber risk modelling)
    - Incident response (the role of a computer emergency response team (CERT), recovery time objectives (RTO), incident management procedure, incident management response plan)
    - Business continuity (business/disaster recovery planning (DRP))
    - Best Practices for better Personal, Team and Corporate Cyber Security [2 hrs]
    - Physical Security (equipment security, mobile phone security)
    - Identity and Access Security (encryption, strong passwords, use of USB)
    - Online and Social Security (Social Networks, social presence, social engineering)
    - Software Security (protection against viruses, spams, phishing emails)
    - Sharing Confidential Information (data leakage, cloud-sharing, online services).