Postgraduate Award in Cyber Security Management

Developed, fully taught and awarded by WMG, University of Warwick, UK

MODULE OUTLINES

Managing Cyber Risk, Audit and Compliance (15 credits)

The module introduces participants to various approaches of information risk assessment and management as well as how to establish and maintain a risk management framework for business continuity and resilience. Participants will be involved in the detailed understanding of relevant cyber law, ethics, principles and rules of cyber security, data protection, consent and privacy, with emphasis on domestic legislation and cross-boundary issues and international efforts as well as an examination of legal issues relating to the authorised conduct of cyber operations such as ethical (as opposed to unethical) hacking. The contents include:

- Risk assessment and management approaches and frameworks. International Standards - ISO27001 & ISO3100; certification; the risk assessment and accreditation process; organisational life-cycle methodologies and processes; interpreting and implementing a security policy as an organisational Information Security Management System (ISMS) Programme.
- Information governance. Strategic planning and best practices; policy development; business consideration and legal functions; E-discovery; standardisation and accepted practices; auditing and enforcement; monitoring; records management and inventorying; information governance in the Cloud; social media and mobile devices; maintaining an Information governance programme; capability maturity models.
- Business continuity planning. Relating risks to mitigating safeguards and procedures; developing, reviewing and enacting business continuity plans.
- Compliance and auditing. Regulation and compliance including: GDPR, The Data Protection Act, PCI DSS; Understanding auditing standards such as: the International Standards on Auditing (UK) (ISAs (UK)) and International Standard on Quality Control (UK) (ISQC (UK)); security certifications; understanding auditability; the internal audit process.
- Culture and Communication. Techniques and controls; culture and awareness; communicating risk and developing uptake.

Proactive Cyber Defence (15 credits)

The module will introduce the state-of-the-art in effective and proactive cyberattack deterrents, including tools and techniques that can have long-term benefits in organisational policies while maintaining the resilience of agile and delicate cyberinfrastructures. Participants will be expected to critically synthesise tools and approaches to adequately model threat landscapes against efficient and autonomous information systems while transferring these skills in different areas where potential threats to business operations might be present. The contents include:

- Confidentiality, integrity, availability. Applied cryptography with applications to confidentiality, integrity; privacy vs confidentiality, trustworthiness and accuracy of data; business continuity and disaster recovery principles.
- Authentication, authorisation and accounting (the AAA of cyber security). Public key infrastructure and Identity management; Protocols for authentication and key establishment;. Access control, Network Access Controls, (NAC); Network Access Protection (NAP); Kerberos; Firewall

Technologies, IDPS; HoneyPots; VoIP security

- Vulnerabilities. Constituent elements of a vulnerability: pre-conditions, pre-condition logic, exploits, post-conditions. Vulnerability inventories, disclosure and mitigation; Standard Security Description references; Cyber mission system development frameworks; Cyber defence measurables & evaluation criteria. Virtualisation and the challenges it brings; Threat modelling and vulnerability analysis.
- Standard security descriptors, DDoS, EDoS and its variations; Intelligence gathering for adaptive network defence; Kill-chain model and the APTs paradigm; STIX and CybOX; Threat actors. Cyber criminals, hacktivists, state-sponsored attackers (advanced persistent threats) and insider threats (malicious, incompetence, negligence); Cyber threat analytics.
- Semantic network and threat modelling techniques. Attack graphs, attack trees and fault trees. The application of attack modelling techniques in aiding attack analysis, event prediction, outlining of mitigation strategies. investigation of incidents and system hardening; STRIDE; DREAD; Experimental approaches; Threat Model Validation & DFDs; Diagram types & Trust Boundaries.
- Cyber security in industrial contexts. Supply-chain, autonomous vehicles, cyber physical systems, IoT.