Master of Science in Cyber Security Management

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

CORE MODULE OUTLINES

Cyber Security Consultancy (15 credits)

The module seeks to develop participants' thorough understanding of the cyber security consultancy lifecycle which typically involves presales, execution and closure. The content includes:

- The role of a consultant. The strategic context setting of Cyber Security; the culture of cyber security; roles in an enterprise; human factors in cyber security; roles and responsibilities within a cyber team; security professionalism; security culture and raising cyber awareness.
- Managing consultancy projects. The consultancy life-cycle; elucidating requirements; planning, developing, controlling and delivering consultancy projects; developing consultancy proposals; consultancy tools, skills and techniques; dealing with uncertainty such as vague specifications and rapidly changing environments.
- Cyber security in an organisation. Understanding the role and function of security policy in an organisation; types of security policy; acceptable use policies; security standards (e.g. ISO/IEC 27000); the role and function of security policy; governance and compliance requirements in law.
- Managing cyber security projects from a system, application and physical security viewpoint. Identity management: authentication, access control and privilege management; securing mobile devices; managing BYOD; securing applications; Email, web and database security; social networks; DRM; database security; big data security; physical and environmental controls; physical protection of IT assets.

Digital Forensic Investigation (15 credits)

Cyber security teams are routinely called on to investigate incidents ranging from the downtime of critical resources such as servers and networks to complex cyber-attacks, which lead to the loss of resources, reputational damage and potential fines. This module outlines the steps an investigator should adopt in a wide range of incidents and equips participants with the skills required to apply scientific techniques and industry standard tools to a digital investigation and present convincing results. The content includes:

- Digital Evidence. The nature of evidence, chain of custody, contamination; specific features of digital evidence, fragility and integrity, hashing; capturing, preserving, replicating.
- Interpreting. Structure of digital material in a variety of forms; structure of stored material; volumes, partitions, file systems, deleted material, persistence of earlier material; other sources of stored digital material (phones, cameras etc).
- Tools and techniques. Validation and verification, scientific process; selected standard tools (imaging, carving, triage), capabilities and limitations; open source, commercial.
- Investigation. Briefing document. Record keeping, contemporaneous notes, negative / absence and positive / presence findings. Valid inferences, testing of nonstandard techniques in novel situations. Analysing memory forensics, analysing network forensics. Anti-forensics.

- Presentation. Eyewitness, expert witness testimony, responsibility.
- Incident response and management. Preparation, trusted toolset; issues, maintaining power vs cutting power, transmitting devices, live systems, encrypted storage.
- Intrusion detection methods. Intrusion response, management and handling; intrusion analysis, monitoring and logging.
- Judicial systems. Jurisdiction (national vs international context), agencies; cyber specific issues, geolocale of actor, agent, data, communications, agency cooperation; the scope of criminal, civil and enterprise investigations; ACPO guidelines.

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.

Penetration Testing (15 credits)

This module begins with an extensive understanding of computer networks, followed by the knowledge and practical experience of performing penetration/vulnerability testing and producing professional penetration testing reports for client organisations. The contents include:

<u>Computer Networks</u>

- Background. IP4/6 networks, addressing, routing, network architecture, trust domains; TCP/UDP, packet capture and analysis using tools such as Wireshark; Ingress and egress filtering via

(stateful) packet firewalls.

- Network design. Enacting basic network design using tools such as packet tracer.
- Network security. Network security monitoring, passive, proactive, technical, non-technical, consequences; Operating system security, web security, embedded security, cloud and virtualisation security, security as a service.

Penetration Testing

- Information gathering methods, techniques and tools. Footprinting, reconnaissance, network port scanning.
- Vulnerability exploitation. Gaining and maintaining access, covering tracks, enumeration techniques and vulnerability assessment, static and dynamic analysis of malware, social engineering, SQL injection, and zero-day exploits, session hijacking, denial-of-Service, password cracking, firewalking techniques, evading intrusion detection systems and firewalls, hacking web applications and SQL injection attacks.
- Penetration testing. Professionalism, ethics and responsible reporting; penetrations testing methodologies, standards and plans.

Management of Cryptosystems (15 credits)

Participants will gain critical insight into the application of cryptography in a range of practical scenarios. This is with emphasis on how cyber security consultants position cryptosystems in system designs and understand the resulting properties of sophisticated cryptographic protocols, algorithms and configurations. There will be analysis of standard cryptographic patterns that may be applied to achieve particular patterns of protection in typical scenarios, as well as exploration of the role and application of cryptography in various blockchain technologies including cryptocurrencies. The contents include:

- Cryptographic hashes. Understand terminology: hash, digest, message authentication code, function. Hash properties: irreversible, deterministic, collision resistance, length. Application: authentication, known good / bad files, file integrity. Cryptographic attacks: brute force, rainbow tables, password salting / stretching, collisions. Hash algorithms: MD5, SHA, and others.
- Encryption theory. Terminology: plaintext, ciphertext, key, algorithm, protocol. Concepts: entropy, one-time pad, complexity, initialisation vectors.
- Symmetric encryption. Encryption over distance or time – the key exchange problem. Example algorithms – DES, Triple DES, AES.
- Asymmetric encryption. Properties: encrypting for known recipient, signing by authentic sender. Establishing trust: certificate authenticity, hierarchy (X509) and web (OpenPGP), certificates. Consequences of loss of key control – revocation certificates.
- Hybrid encryption. Using asymmetric encryption to share symmetric key. SSL/TLS.
- Other specific protocols. Kerberos, IPSEC.
- Data protection. At rest, in transit.
- Blockchain and virtual currencies. Distributed consensus, peer-to-peer network, the ‘51% attack’, immutability, apparent anonymity. Virtual currencies: bitcoin Ethereum, wallets, transactions, smart contracts, anonymity and privacy in the Bitcoin ecosystem.

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.

Study, Professional and Analytical Skills (15 credits)
This module is divided into three interlinked yet distinctive learning strands, Study Skills, Professional Skills and Competencies and Analytical Skills, purposefully designed to meet the complex learning and professional needs of postgraduate students. The contents include:

- Study skills: academic and technical report writing; referencing; critical thinking; presentation/communications to express yourself broadly and academically
- Professional skills: a range of implicit and explicit transferable employability skills applicable synergetically across all aspects of learning
- Research methods: knowledge and skills to enable participants to complete an independent and original price of research

In addition to above, global competencies such as ethical behaviours and professionalism, multi-cross

cultural working etc, will run across all aspects of the module and equip participants with high-level employability skills fit for the global workplace.

MSc Project (60 credits)
The individual MSc Project accounts for 33% of MSc degree's overall grade, submitted in the form of a written dissertation between 10,000 and 13,000 words. Participants will specialise in a particular area of cyber security approved by the University, and conduct appropriate research in the cyber domain in compliance with the course regulations.

Participants are required to successfully complete the MSc Project to be awarded the Master of Science in Cyber Security Management by the University of Warwick.

ELECTIVE MODULE OUTLINES

Cloud Native Computing (15 credits)
Cloud native principles, particularly containerisation and microservices, are becoming widely used across a whole host of organisations and industries from media (for example Netflix) through to finance (for example Goldman Sachs). Participants on this module will gain experience in these new technologies and approaches to manage portfolios of complex applications. The contents include:

- What is Cloud Native Computing?: cloud computing; 12-factor app; service orientated architecture and microservices
- Cloud Native Computing in Practice: five R's methodology for cloud migration; cloud migration assessment; Agile, DevOps and DataOps; infrastructure as code and configuration management; microsoft azure labs
- Containerisation and container orchestration: virtual machines and containers; docker labs; container orchestration; kubernetes labs
- CI/CD and IT operations: continuous integration / continuous deployment; jenkins labs; platforms-as-a-service; cloud foundry
- Capstone project: application assessment; modernisation; containerisation; building a CI/CD pipeline; scaling the application

Enterprise eCommerce Solutions (15 credits)
Participants will study the specific technologies and processes that characterise the transactional aspect of digital commerce to meet the industry demand for graduates who are able to design, develop and optimise eCommerce solutions. The contents include:

- Theoretical models of eCommerce
- eCommerce Technology: hosting solutions; web frameworks; programming languages for the web; content management solutions
- Delivery and payment methods for eCommerce: supply chain; delivery methods; payment methods and transactions; multichnnel sales
- Building an eCommerce business case: search engine optimisation; digital marketing; writing a business case
- Design for eCommerce: best practice; analysing website quality; wireframing and protyping;

conversion rate optimisation

- Capstone project: eCommerce website build; client presentations

Programming and Fundamental Algorithms (15 credits)
This module focuses on algorithms and programming/development to empower participants with the ability and confidence to solve problems efficiently using computers for complex system designs in business, engineering, science and IT. Participants will develop an understanding of which solutions/algorithmic paradigms work best for certain types of problems; learn programming methods and how to design a good code for a proposed algorithm. The contents include:

- Introduction to algorithms
- Data structures
- Complexity and decision making
- Brute force and divide and conquer methods for solving problems
- Dynamic programmig and greedy methods
- Exhaustive search and recursion
- Limitations of algorithms and coping with limitations
- Tutorials: programming; types and commands; dealing with pointers; generics and abstract data types; concepts of object oriented programming inheritance polymorphism; file I/O; introduction to multithreading
- Advantages, pitfalls and practicalities of programming as part of a team

Machine Intelligence and Data Science (15 credits)
Participants will build a solid knowledge of key AI techniques and the underlying theory that are widely used in the development of autonomous vehicles. The contents include:

- An overview of autonomous vehicles technology: system architecture; localisation; sensing and perception; motion planning in complex environments
- A general overview of AI systems
- Data science basis for machine intelligence: understanding experimental data and fitting; clustering and classification
- Deep learning systems: introduction to neural networks; deep learning neural networks; reinforced learning; supervised and unsupervised learning; convolutional neural networks; recurrent neural networks
- Industry expert seminars
- Tutorials on tools and examples