Title	Emerging Cyber Trends
Long Title	Emerging Cyber Trends
Credits	**5**
NFQ Level	**8**
Module Author	**Sean McSweeney**

Module Description:

The cornerstone security concepts which underpin current cyber trends are essential knowledge to understanding emerging cyber trends. These concepts also have a significant role in directing effective and efficient personal cyber defences, something that is essential for a professional in the field. In this module students will learn the main cornerstone concepts, the current and emerging trends in the industry and how to successfully harden themselves against cyber attacks.

Learning Outcomes

On successful completion of this module the learner will be able to:

LO1 Evaluate the impact of poor user behaviour on the cyber risk profile of an organisation.
LO2 Develop a security training and awareness programme for an organisation with the aim of establishing a security conscious culture.
LO3 Critique emerging and current enterprise cybersecurity trends with the aim of building a cybersecurity program.
LO4 Analyse the impact of increased digitalisation and connectivity from emerging technologies such as the Internet of Things (IoT).

Indicative Content

Malware & Ransomware
Viruses, worms, spyware, ransomware, rootkits & backdoors, botnets, social engineering. Ransomware – locker and Crypto. Impact of malware and ransomware on home and business users. Target systems i.e. OS, Windows, iOS, Android. Infection methods – traffic distribution systems, spam email, downloaders, social engineering etc. Malware and ransomware mind tricks. Famous malware and ransomware attacks.

User Behaviour & security
User passwords for home and business accounts. Passwords setting, length, complexity and recall. Alternative modes of authentication i.e. biometric, geo location, dual factor etc. Best practices and policy when setting passwords at a corporate level. Remote working and user behaviour. Risks when working from home and best practices and policy for an organisation. Wifi – remote workers accessing public wifi services. USB devices, risks, policy and behaviour. Cost of the bad user behaviour to company.

User Awareness & Education
User awareness and educational programmes, protecting personal privacy, elements of the digital footprint, security technologies and tools, host firewalls, VPN, proxies, access points, SSL/TLS, anti-spam, anti-virus, considerations for different device categories, computer backups (on and offline), patch application and management. Incident Reporting culture. Security Operating Procedures. Insider threats. External Attacks. Staff induction process. Maintaining user awareness.

Enterprise/IT Cybersecurity/Cloud
Cloud and virtualization security issues, cloud deployment models security issues, resiliency and automation strategies, secure application development and deployment concepts, security technologies. Societal challenges, next generation IT systems i.e. SDN, 5G, virtual and augmented reality, autonomous systems, AI and robotics, Blockchain, Quantum Computing. Cyber crisis management co-operation – challenges, opportunities.

Internet of Things (IoT) & Cyber Physical Systems (CPS)
What are the IoT, CPS and Industrial IoT. Challenges – increased connectivity, alignment between IT/OT security awareness and expertise, organisational policies, process lifecycle management, standards fragmentation, technology heterogeneity, bad password practice etc. Good practices for IoT security. IIoT asset taxonomy. Threats Taxonomy i.e. nefarious activity, eavesdropping, outages, disaster, physical attack, failures. Attack Scenarios. Security Measures and good practice.

Course Work

Assessment Type	*Assessment Description*	*Outcome Addressed*	*% of Total*	*Assessment Date*
Written Report	This report will assess the student's understanding of the cornerstone security concepts and current security landscape. The student may be expected to write a report a specific current trend in the industry, it's origin and the expected implications for the future.	1, 2	50.0	Week 7
Project	The focus of this project will be for the student to develop a cyber defense programme for an organisation in which a number of the current emerging technologies have been realized (e.g. cognitive EDR) which incorporates the impact this technology will have on current operations and security. The core focus of this project is quantifying the practical implication of these technologies and the financial and competitive advantage they may yield.	3, 4	50.0	Sem End
No End of Module Formal Examination				

Assessment Breakdown

	%
Coursework	100

Re-Assessment Requirement

Coursework Only
This module is reassessed solely on the basis of re-submitted coursework. There is no repeat written examination.

Workload – Full Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support learning outcomes.	1.0	Every Week	1.00
Independent & Directed Learning (Non-contact)	Independent study.	4.0	Every Week	4.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		3.00

Workload – Part Time

Workload Type	*Workload Description*	*Hours*	*Frequency*	*Average Weekly Leaner Workload*
Lecture	Lecture delivering theory underpinning learning outcomes.	2.0	Every Week	2.00
Lab	Lab to support learning outcomes.	1.0	Every Week	1.00
Independent & Directed Learning (Non-contact)	Independent study.	4.0	Every Week	4.00
		Total Hours		7.00
		Total Weekly Learner Workload		7.00
		Total Weekly Contact Hours		3.00

Recommended Book Resources

- **Charles J. Brooks 2018, *Cybersecurity Essentials*, Sybex [ISBN: 1119362393]**
- **Christopher Hadnagy 2018, *Social Engineering: The Science of Human Hacking*, 2nd Ed., Wiley [ISBN: 111943338X]**

Supplementary Book Resources

- **Kevin D. Mitnick 2003, *The Art of Deception: Controlling the Human Element of Security*, Wiley [ISBN: 076454280X]**

Recommended Article/Paper Resources

- **Lu, Yang, and Li Da Xu 2018, *Internet of things (iot) cybersecurity research: A review of current research topics*, IEEE Internet of Things Journal, Vol 6, Issue 2**
- **Olmstead, Kenneth, and Aaron Smith 2017, *Americans and cybersecurity.*, Pew Research Center, Volume 26**

Other Resources

- **Website: USA Cybersecurity and Infrastructure Security Agency*ICS-CERT Virtual Learning Portal***
  https://ics-cert-training.inl.gov/learn
- **Website: SANS*Cyber ACEs***
  https://www.cyberaces.org/