MAKERERE UNIVERSITY BUSINESS SCHOOL
FACULTY OF COMPUTING AND INFORMATICS
DEPARTMENT OF INFORMATION SYSTEMS

COURSE OUTLINE

Programme:	**Master of Business Administration – Business Analytics**
Course Name:	**Cyber Security**
Course Code:	**MBA8138**
Contact Hours:	**45 hours**
Credit Units:	**3**
AY:	**2025/2026**
Semester:	**I**

Facilitator: Dr. Samali V. Mlay, (PhD, Cert in E-Learning, CISA, MIT, BBC) smlay@mubs.ac.ug

a) Course Introduction

The evolution of Information Communication Technology and growing security concerns demand flexible and generally comprehensive approach to the issue of cyber security. The rapid growth of ICT has raised various complex questions which need to be addressed. This course has been prepared with an aim to create more aware, responsive and responsible digital citizens, thereby contributing effectively to an overall healthy cyber security posture and ecosystem. It aims at equipping a learner with knowledge and skills in ensuring security against cyberattacks in data usage, e-commerce, social media as well as highlighting the laws, regulations, compliance, management and governance of cybersecurity.

b) Course Objectives:

The course is intended to achieve the following objectives:

1. Highlight the foundations of Cyber security and cyber threat landscape.
2. To equip students with the technical knowledge and skills needed to protect and defend against cyber threats.
3. To develop skills that can help learners plan, implement, and monitor cyber security mechanisms to ensure the protection of information technology assets.
4. To expose students to governance, regulatory, legal, economic, environmental, social and ethical contexts of cyber security.

5. To expose students to responsible use of online social media networks.
6. To systematically educate the necessity to understand the impact of cybercrimes and threats with solutions in a global and societal context.
7. To select suitable ethical principles and commit to professional responsibilities and human values and contribute value and wealth for the benefit of the society.

c) Learning Outcome

By the end of this course, the student should be able to:

1. Define the cyber security threat landscape and risks.
2. Develop a deeper recognition and familiarity of the various types of cyberattacks, cybercrimes, vulnerabilities and remedies thereto.
3. Analyse and evaluate existing legal framework and laws on cyber security.
4. Analyse and evaluate the digital payment system security and remedial measures against digital payment frauds.
5. Analyse and evaluate the importance of data, its privacy and security.
6. Analyse and evaluate the security aspects of social media platforms and ethical aspects associated with use of social media.
7. Evaluate and communicate the human role in security systems with an emphasis on ethics, social engineering vulnerabilities and training.
8. Develop cyber security plans and policies for management and governance of organisations.

d) Course content

	Topic	**Description**	**Hours**
1.	**Overview of cyber security**	1. Cyber security terminologies 2. Types of cyber attackers 3. Cyber security increasing threat landscape 4. Critical IT and National Critical Infrastructure 5. Cyberwarfare 6. Case studies	6
2.	**Cybercrimes**	1. Cybercrimes targeting Computer systems and Mobiles 2. Online scams and frauds 3. Social Media Scams & Frauds 4. Social Engineering attacks 5. Case studies	6
3.	**Digital Security, Technologies and**	1. End Point device and Mobile phone security 2. Password policy 3. Security patch management	6

	Tools for Cyber Security	4. Data backup 5. Downloading and management of third party software 6. Device security policy 7. Host firewall and Anti-virus management 8. Network security 9. Cyber Security best practices	
4.	**Data Privacy, Data Security and Data Protection**	1. Defining data, meta-data, big data, non-personal data. 2. Data privacy and data security 3. Big data security issues and challenges 4. Data protection 5. Data protection principles 6. Data protection regulations and compliance 7. Social media data privacy and security issues.	5
5.	**E-Commerce and Digital Payments**	1. Elements of E-Commerce security 2. E-Commerce threats 3. E-Commerce security best practices 4. Digital payments related common frauds and preventive measures. 5. Case studies	6
6.	**Forensic Investigation**	1. Computer Forensics Today 2. Computer Forensics Investigation Process 3. Hard Disks and File Systems 4. Data Acquisition 5. Anti-Forensics Techniques	4
7.	**Cyber Law**	1. Cybercrime and legal landscape around the world 2. IT Laws and Regulations in Uganda 3. Cybercrime and punishments, Cyber Laws and Legal and ethical aspects related to new technologies 4. Case Studies.	4
8.	**Cyber security Management, Compliance and Governance**	1. Cybersecurity Plan 2. Risk assessment 3. Business continuity 4. Cybersecurity audit and compliance 5. Cybersecurity governance	8
	Total		**45**

e) Mode of Delivery

- Face-to-face lectures
- Online lectures
- Case studies
- Group and class discussions

f) Score Distribution

Assignment	40%
End of semester examination	60%
	100%

Learners are required to attempt at least two assignments and the final examination in order to complete the course. The pass mark for the course is 60%.

g) Learning Management System

Learners are required to enrol themselves on the Makerere University Business School Education Portal - MUBSEP (mubsep.mubs.ac.ug); an online Moodle Online Learning Management System. All communication, teaching materials, assignments, results and discussion forum will be done on that forum.

h) Participation

Every learner is required to attend at least 70% of the classes to fulfil the minimum requirements to sit for the final examination. Learners must use their official names when logging on for the online classes.

i) Statement of Academic Dishonesty

Academic dishonesty (e.g. cheating on assignments and examinations, plagiarism) is a serious offense. All work that you submit in this class must be your own. Each student is responsible for being familiar with the MUBS policies on academic dishonesty. Any student engaging in academic dishonesty in this course will receive a fail grade (0) and appropriate disciplinary action will be taken.

Your submissions will be subjected to a similarity test using Turnitin antiplagiarism software. Therefore, you are advised to desist from plagiarism. Any plagiarized submission will be returned and you will be required to resubmit the assignment within 12 hours after the return time.

j) Indicative Reference List

1. The Data Protection and Privacy Act, 2019. Government of Uganda
2. The Electronics Transaction Act, 2011. Government of Uganda

3. The Computer Misuse Act, 2011. Government of Uganda
4. The Computer Misuse Act (Amendment), 2022. Government of Uganda
5. The Electronic Signatures Act, 2011. Government of Uganda
6. The General Data Protection Regulation (GDPR), 2018. European Public Service Union
7. PCI DSS Quick Reference Guide. Understanding the Payment Card Industry Data Security Standard version 3.2.1, 2018. PCI Security Standards Council
8. Personal Information Protection and Electronic Documents Act (PIPEDA), 2000. Government of Canada

k) Reference Textbooks

1. Dorothy E. Denning (1998). *Information Warfare and Security*, 1st Edition, Addison Wesley.
2. Henry A. Oliver (2015). *Security in the Digital Age: Social Media Security Threats and Vulnerabilities*. Create Space Independent Publishing Platform.
3. Krag W. Brotby (2009). *Information Security Governance: A Practical Development and Implementation Approach*. 1st Edition, Wiley Publication.
4. Krishna Kumar (2011). *Cyber Laws: Intellectual Property and E-Commerce Security*, Dominant Publishers and Distributors.
5. Martin Weiss, Michael G. Solomon (2015). *Auditing IT Infrastructures for Compliance*, 2nd Edition, Jones and Bartlett Learning.
6. Natraj Venkataramanan and Ashwin Shriram (2016). *Data Privacy Principles and Practice*, 1st Edition, CRC Press.
7. Nina Godbole, Sunit Belapure and Kampesh Bajaj (2011). *Understanding Cyber Crimes, Computer Forensics and Legal Perspectives*, Wiley India Pvt. Ltd.