Global Network for Advanced Management
MBA and AMBA
School Year 2023-2024
Course Outline

School	W. SyCip Graduate School of Business
Course Code	ICS
Course Title	Introduction to Cybersecurity
Units	1
Term	3

Faculty Name	Kwa, Philip
Email Address	pkwa@aim.edu
Consultation Hours	

Program Staff	0
Email Address	None
Extension No.	

A. Course Description

The Introduction to Infosecurity module is for managers who wants to learn more about information security and to apply what you have learned to respond and manage information security issues.
You will be learn about the various attack surfaces and attack vectors and how they impact businesses and organization as well as the various risk management techniques to use in order to reduce threats, how to manage incidents and respond to incidents. You will be introduced to the framework to assist you to jumpstart cybersecurity practices in your business .
Additionally, you will also exposed to real-world case studies and practical experiences to put what you have learned into practice and acquire the skills necessary for leadership roles.

Note: Content of the course outline is subject to change.

B. Pre-requisites

C. Course Learning Outcomes

At the end of the course, students will be able to:

1. Evaluate the current status of cybersecurity and its effects on businesses and organizations
2. Critically examine, evaluate, identify, and comprehend how cybersecurity threats may affect a business;
3. Utilize industry best practices and cybersecurity framework to manage information assurance and risk;

4. Understand risk by specifying risk tolerance and prioritize vulnerabilities as part of an ongoing risk management process in organizations;
5. Utilize industry best practices and cybersecurity framework to manage information assurance and risk;
6. Apply knowledge and skills to circumstances that arise in the real world by working on real-world projects and case studies.
7. Manage and respond to incidents
8. Present cybersecurity principles, threats, and solutions in a clear and concise manner to both technical and non-technical audiences
9. Participate in self-directed learning and professional development activities to stay current on the latest developments in cybersecurity.

D. Course Contribution to Program Learning Goals and Objectives

Course Learning Outcomes	Program Learning Goals/Objectives
	1. AIM MBAs will be analytical, critical, and logical thinkers.
	1.1 Identify critical factors in management setting.
	1.2 Identify reasonable alternatives.
	1.3 Apply appropriate qualitative and/or quantitative analytical methods
	1.4 Reach conclusions using well-structured and logical reasoning
	1.5 Students incorporates creativity and innovative thinking in problem solving
	2. AIM MBAs will be effective communicators.
8	2.1 Deliver oral presentations that are well organized, engaging and informative.
6	2.2 Produce written projects that are well-structured, concise, and analytical.
9	2.3 Engage in substantive dialogue, actively listen and contribute to an exchange of ideas.
	3. AIM MBAs will be effective and ethical leaders and team players.
	3.1 Recognize the consequences and impact of business decision on contemporary social issues
	3.2 Evaluate ethical dilemmas in profit and non-profit organizations.
	3.3 Achieve team objectives by collectively expending their efforts for the group task
	3.4 Demonstrate professional interpersonal relations with other team members
	4. AIM MBAs will effectively manage the interaction of various functional areas.
	4.1 Set organizational goals
	4.2 Understand the importance of functional interdependence and linkages in achieving organizational goals
	4.3 Understand the functional integration in managing the stakeholder objectives of an organization

	5. AIM MBAs will have adequate understanding of Asian and global business.
	5.1 Understand the purpose, function and goals of world and regional trade organizations and agreements
1, 2, 3, 4, 5	5.2 Analyze the opportunities and threats in the environments associated with managing organizations, regionally and globally
	5.3 Understand the qualities that enhance cross-cultural effectiveness and develop strategies to improve their own competencies
	6. AIM MBAs are numerate.
	6.1 Understand quantitative techniques in assessing markets and forecasting sales potential
	6.2 Manage risks effectively and efficiently.
	6.3 Understanding of scenario analysis to assess environments
EMBA Program Learning Goals and Objectives	

E. Learning Methodology

• All course material relevant to the course will be in ALICE
• Leverage Harvard Business School Publishing cases and simulation exercise
• Hybrid Methodology Instructions - students may attend in person or online via zoom
Because of the course's rapid pace and heavy workload, you must study the readings before attending each lecture and exercise. Active student participation is required in both lectures and learning team activities. Any student who is unwilling to devote the required amount of study time for the course could anticipate challenges and may perform poorly on the exam.

F. Grading Criteria

			Weight
Class participation (Hybrid Class)	Class participation and discussion board	(Individual)	10%
Class participation (Hybrid Class)	Simulation Exercise	(Individual)	20%
Group Reports/Submissions	Case Analysis	(Group)	40%
Exam(s)		(Individual)	30%
Total			**100%**

**Final Grades automatically calculated in the ALICE Grade Center are not conclusive and are subject to Program Deliberations of the Faculty at the end of the Program Term*

G. Student Responsibilities and Conduct

Students are expected to conduct themselves with the utmost professionalism in all classes. Information and policies on student responsibilities and conduct, including dysfunctional

behavior (such as attendance, plagiarism, cheating, etc) and grievance procedures are in the Student Handbook.

H. Course Schedule

Session Number	Session Topic (in-session)	Pre-session Activity	*Faculty/Resource Speaker*	Learning or Case Materials	Supplementary Readings	Assessment activities	Requirements or Submissions	Post-session Activity
Session 1 Feb 20, 2024 6:00PM - 7:30PM	Introduction and Overview - Course/Expectations/Class Rules		Philip Kwa			Class Participation		
Session 2 Feb 22, 2024 6:00PM - 7:30PM	State of Cyber Security - Cyber Landscape and Practices - - CIA - Cybersecurity Cube		Philip Kwa		World Economic Forum - Global Cybersecurity	Class Participation		
Session 3 Feb 27, 2024 6:00PM - 7:30PM	Threat and Vulnerabilities - Threat Actors, Threat Surface, Threat Vectors - Current and Emerging), Cyber Kill Chain		Philip Kwa			Class Participation		
Session 4 Feb 29, 2024 6:00PM - 7:30PM	Defence Strategies for IT and OT - Hardening, Configuration and Patch Management, Perimeter Security, Edge Security, Security by Design, Defence In Depth, Principles of Least Privileges, Principles of Obscurity		Philip Kwa	"Case Assignment : (LT 1) Kaseya (LT 2) Norsk Hydro (LT 3) Panama Papers (LT 4) Equifax Data Breach (LT 5) Florida Water Supply (LT 6) Colonial Pipeline Attack Each LT group will be given a case assignment.		"Written Case Analysis Each LT Group will be assigned a cyber attack case. Each group is to analyse the assigned case . The deliverable will be a presentation (in power point format) which they will need to (a) Background Information: - Provide a brief overview of the organization or system targeted in the cyber attack case. - Explain the significance of the attack in terms of its impact on the organization, customers, or stakeholders.	"Ppt presentation - not more than 12 slides - to be submitted by each group. All students to complete a Peer Review exercise including the Peer Review All work (presentation and peer review) due on 15th March 2024 at 11:59 PM	

						(b) describe the nature of the attack - using the Cyber Kill Chain Approach - including the timeline (c) Provides information on the impact and consquences (d) The mitigation strategies that the company has put in place as well as in your own views highlight the mitigation strategies that the company should have adopted (e) Lesson Learned "		
Session 5 Mar 05, 2024 6:00PM - 7:30PM	Discussion on CII	Students to read about Philippines National Cybersecurity Plan to understand the various initiatives in the plan	Philip Kwa		(1) National Cybersecurity Plan - 2022			
Session 6 Mar 07, 2024 6:00PM - 7:30PM	Governance , Risk and Compliance (GRC) Security Standards, Guidelines and Framework (ISO 27000, NIST, etc)							
Session 7 Mar 12, 2024 6:00PM - 7:30PM	Incident Management - Events vs Incidents , NIST Framework, Red Teams , Blue Team, Assumed Breach , Incident Response Plan							
Session 8 Mar 14, 2024 6:00PM - 7:30PM	Incident Management - Events vs Incidents , NIST Framework, Red Teams , Blue Team, Assumed Breach , Incident Response Plan	Login to IT Management Simulation - Go through the tutorial		IT Management Simulation - Cyber Attack (HBSP)		Simulation Exercise	Individual assignment to be submitted during the session. Online completion and submission -. Students will have to complete the Simulation Exercise in class. 40 mins given for the simulation exercise	

Session 9 Mar 19, 2024 6:00PM - 7:30PM	Cybersecurity Career Pathway				https://www.pauljerimy.com/OC/Security%20Certification%20Progression%20Chart%20v7.0.png https://www.imda.gov.sg/cwp/assets/imtalent/skills-framework-for-ict/index.html			
Session 10 Mar 21, 2024 6:00PM - 7:30PM	Final Exam					Final Exam		

Required References

Refer to Course schedule for required materials and supplementary readings

Additional References