Yea& Sem: IV-I Course Code:	**CYBER SECURITY**	L	T	P	C
Prerequisites: Computer Networks & Cryptography & Network Security		3	0	0	3

Course objectives:

1. To understand various types of cyber-attacks and cyber-crimes
2. To learn threats and risks within context of the cyber security
3. To have an overview of the cyber laws & concepts of cyber forensics
4. To study the defensive techniques against these attacks.
5. To Analyze the Cyber Security needs of the Organizations.

Course Outcomes:

CO 1. Analyze and evaluate the cyber security needs of an organization.
CO 2. Understand Cyber Security Regulations and Roles of International Law.
CO 3. Design and develop a security architecture for an organization.
CO 4. Understand fundamental concepts of data privacy attacks
CO 5. Analyze the cyber security needs of an organization.

[12 hrs]

UNIT-I: Introduction of Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes: Email Spoofing, Spamming, Internet Time Theft, Salami Attack/Salami Technique, Data Diddling, Forgery, Web Jacking, Newgroup Spam, Industrial Espionage, Hacking, Online Frauds, Pornographic offenses, Software Piracy, Computer Sabotage, E-Mail bombing, computer network intrusions, password sniffing, credit card frauds, identity theft, Cybercrime Era: Survival mantra for the Netizens.

[10 hrs]

UNIT-II: Cyber offenses: Criminals Plan: Categories of Cybercrime, Cyber Attacks: Reconnaissance, Passive Attack, Active Attacks, Scanning/Scrutinizing gathered Information, Attack, Social Engineering: Classification of Social Engineering, Cyberstalking: Types of Stalkers, Working of Stalking, Real-Life Incident of Cyber stalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Botnet, Attack Vector: Theft, viruses, mishing, vishing, smishing, hacking Bluetooth, Cybercrime and cloud computing.

[12 hrs]

UNIT-III: Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit Card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication Service Security, Attacks on Mobile/Cell Phones, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.

[10 hrs]

UNIT-IV: Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks.

[10 hrs]

UNIT-V: Cybercrimes and Cyber security: Organizational Implications–Introduction–Insider threats, Privacy, Key challenges to organizations, Cost of Cybercrimes and IPR issues, Incident Handling: Definitions, Why Organizations need Incident Response systems, Examples of incidents, what organizations can do to protect, best practices for organizations.

TEXT BOOKS:

1. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Nina Godbole, SunitBelapure, Wiley India Publications

REFERENCES:

[1] James Graham, R Howard, R Olson, "Cyber Security Essentials" CRC Press, 2018

[2] Michael E Whitman, Herbert J Mattord, "Principles of Information Security", 4th Edition, Cengage Learning, 2012

[3] William Stallings, “Cryptography and Network Security- Principles and Practice”, 7th Edition, Pearson Education, 2017

E-RESOURCES AND OTHER DIGITAL MATERIAL

[1] MITOPENCOURSEWARE Computer Systems Security
https://ocw.mit.edu/courses/6-858-computer-systems-security-fall- 2014/video_galleries/video-lectures/

[2] Oxford Home Study Center, Cyber Security short course available@
https://www.oxfordhomestudy.com/courses/cyber-security-courses/free-cyber-security-online

Correlation between Outcomes (COs) and Program Outcomes (POs):

Course Name	Course Outcomes	Program Outcomes (PO)													
		PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CYBER SECURITY	**CO1**	2	2	1	1	3	3	1	3	-	1	-	3	-	2
	CO2	2	2	1	1	-	3	2	3	-	1	-	3	-	3
	CO3	2	2	1	1	-	3	1	3	-	1	-	3	-	3
	CO4	2	2	1	1	3	3	1	3	-	1	-	3	-	2
	CO 5	2	2	1	1	-	3	1	3	-	1	-	3	-	3
	Target	**2**	**2**	**1**	**1**	**1**	**3**	**1**	**3**	**-**	**1**	**-**	**3**	**-**	**3**