Listen

Syllabus

POL-385: Foundations of Cybersecurity Systems

Written by:
Larry Snyder, Ph.D.
Joed Carbonell-López, Ph.D.

Course Description

Students in this course will identify and evaluate network fundamentals, cyber system components, and cybersecurity best practices within an international context. Students will identify and evaluate various cybersecurity threats and common vulnerabilities in organizations' information networks and systems. Students will produce network diagrams, provide cybersecurity recommendations for given networks and world regions, and study current trends in this field. This course will integrate legal, ethical, and biblical frameworks with the analysis of cybersecurity systems.

Credit Hours: 3
Prerequisite Courses: None

Course Outcomes

Upon completion of this course, you should be able to:

1. Identify the foundations of a well-engineered network.
2. Evaluate vulnerabilities within networks.
3. Integrate legal, ethical, and biblical frameworks with the analysis of cybersecurity systems.
4. Design a network with contemporary cybersecurity components.
5. Evaluate the primary international governing bodies relating to the Internet and cybersecurity practices.
6. Analyze the role of each major cybersecurity system component.
7. Describe industry and government best practices to ensure confidentiality, integrity, and availability of data via information systems.

Course Textbook

Easttom, C. (2016). *Computer security fundamentals* (3rd ed.). Boston, MA: Pearson. (**students need this text for the next course: POL-380**)

Grading Scale

NOTE: In graduate-level courses, a grade of C- or below will require the course to be repeated.

Grade	Quality Points Per Credit	Percentage	Score
A	4.0	95%–100%	950–1000
A-	3.7	92%–94.9%	920–949
B+	3.3	89%–91.9%	890–919
B	3.0	85%–88.9%	850–889
B-	2.7	82%–84.9%	820–849
C+	2.3	79%–81.9%	790–819
C	2.0	75%–78.9%	750–789
C-	1.7	72%–74.9%	720–749
D+	1.3	69%–71.9%	690–719
D	1.0	65%–68.9%	650–689
F	0.0	0%–64.9%	0–649

Grading Policies

Your grading policy for your course is dependent on your school and program. Your grading policies can be found in the IWU Catalog.

Letter Grade Equivalencies

NOTE: In graduate-level courses, a grade of C- or below will require the course to be repeated.

Grade	Description of Work
A	Clearly stands out as excellent performance. Has unusually sharp insights into material and initiates thoughtful questions. Sees many sides of an issue. Articulates well and writes logically and clearly. Integrates ideas previously learned from this and other disciplines. Anticipates next steps in progression of ideas. Example “A” work should be of such nature that it could be put on reserve for all cohort members to review and emulate. The “A” cohort member is, in fact, an example for others to follow.
B	Demonstrates a solid comprehension of the subject matter and always accomplishes all course requirements. Serves as an active participant and listener. Communicates orally and in writing at an acceptable level for the degree program. Work shows intuition and creativity. Example “B” work indicates good quality of performance and is given in recognition for solid work; a “B” should be considered a good grade and

	awarded to those who submit assignments of quality less than the exemplary work described above.
C	Quality and quantity of work in and out of class are average. Has marginal comprehension, communication skills, or initiative. Requirements of the assignments are addressed at least minimally.
D	Quality and quantity of work are below average. Has minimal comprehension, communication skills, or initiative. Requirements of the assignments are addressed at below-acceptable levels.
F	Quality and quantity of work are unacceptable and do not qualify the student to progress to a more advanced level of work.

Course Summary

Workshop	Discussion*	Assignment*	Devotional*	End-of-Course Survey	Total Points
Workshop One	1/30	3/135	1/5		170
Workshop Two	2/60	2/100	1/5		165
Workshop Three	2/60	2/100	1/5		165
Workshop Four	1/30	3/135	1/5		170
Workshop Five	1/30	3/130	1/5		165
Workshop Six	2/60	2/100	1/5	10 (Extra Credit)	165
Course Totals	**9/270**	**15/700**	**5/30**	**10 (Extra Credit)**	**1000**

*Number of Activities/Sum Point Totals

Course Assignments

Workshop One Outline

Title	Due Dates	Time	Points

Title	Due Dates	Time	Points
1.1 Discussion: Building a Solid Foundation	Due by the end of the workshop	30 minutes	5
1.2 Assignment: Identifying Types of Threats	Due by the end of the workshop	3 hours	35
1.3 Discussion: Introduction to Networks	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop	3 hours	30
1.4 Assignment: Responding to Threats	Due by the end of the workshop	4 hours	50
1.5 Assignment: Securing a Network, Team Project Part 1	Due by the end of the workshop	4 hours	50
	Totals	**14:30 hours***	**170**

*These times are only estimates. Actual assignment completion times will vary.

Workshop Two Outline

Title	Due Dates	Time	Points
2.1 Discussion: Understanding Weaknesses	Due by the end of the workshop	30 minutes	5
2.2 Assignment: Understanding Denial of Service Attacks	Due by the end of the workshop	3 hours	50
2.3 Discussion: Understanding Malware: Viruses	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop	3 hours	30
2.4 Discussion: Understanding Malware: Trojan Horses, Spyware, and Others	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop	4 hours	30
2.5 Assignment: In-Depth Case Study: Cyberattack on a Government Organization, Part 1	Due by the end of the workshop	4 hours	50
	Totals	**14:30 hours***	**165**

*These times are only estimates. Actual assignment completion times will vary.

Workshop Three Outline

Title	Due Dates	Time	Points
3.1 Discussion: Understanding the Adversary	Due by the end of the workshop	30 minutes	5
3.2 Discussion: Why Do They Do It?	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop	3 hours	30
3.3 Assignment: Hacking Techniques	Due by the end of the workshop	3 hours	30
3.4 Discussion: Industrial Espionage	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop	4 hours	30
3.5 Assignment: Securing a Network, Team Project Part 2	Due by the end of the workshop	4 hours	70
	Totals	**14:30 hours***	**165**

*These times are only estimates. Actual assignment completion times will vary.

Workshop Four Outline

Title	Due Dates	Time	Points
4.1 Discussion: Understanding Your Tools	Due by the end of the workshop	30 minutes	5
4.2 Assignment: Understanding Encryption	Due by the end of the workshop	4 hours	50
4.3 Discussion: Understanding Computer Security Technology	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop	3 hours	30
4.4 Assignment: Ubiquitous Technology and the CIA Triad	Due by the end of the workshop	4 hours	35
	Totals	**15:30 hours***	**170**

Title	Due Dates	Time	Points
4.5 Assignment: In-Depth Case Study: Cyberattack on a Government Organization, Part 2	Due by the end of the workshop	4 hours	50
	Totals	**15:30 hours***	**170**

*These times are only estimates. Actual assignment completion times will vary.

Workshop Five Outline

Title	Due Dates	Time	Points
5.1 Discussion: Do Not Be Anxious	Due by the end of the workshop	30 minutes	5
5.2 Discussion: Organizational Cybersecurity Policies	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop	3 hours	30
5.3 Assignment: Simulation: Scanning	Due by the end of the workshop	4 hours	30
5.4 Assignment: No Excuse	Due by the end of the workshop	4 hours	30
5.5 Assignment: Securing a Network, Team Project Part 3	Due by the end of the workshop	4:30 hours	70
	Totals	**16 hours***	**165**

*These times are only estimates. Actual assignment completion times will vary.

Workshop Six Outline

Title	Due Dates	Time	Points
6.1 Discussion: "Hate evil; love good"	Due by the end of the workshop	30 minutes	5
	Totals	**15:30 hours***	**165**

Title	Due Dates	Time	Points
6.2 Discussion: International Crime through Cyberspace	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop	3 hours	30
6.3 Discussion: International Terrorism through Cyberspace	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop	4 hours	30
6.4 Assignment: Cyber Warfare	Due by the end of the workshop	4 hours	50
6.5 Assignment: In-Depth Case Study: Cyberattack on a Government Organization, Part 3	Due by the end of the workshop	4 hours	50
End of Course Survey	Due by the end of the workshop	30 minutes	10 Extra Credit Points
	Totals	**15:30 hours***	**165**

*These times are only estimates. Actual assignment completion times will vary.

Course Development Resources

Ali, A. (2017). Ransomware: A research and a personal case study of dealing with this nasty malware. *Issues in Informing Science & Information Technology, 14,* 87-99.

Balboni, P., & Pelino, E. (2013). Law enforcement agencies' activities in the cloud environment: A European legal perspective. *Information & Communications Technology Law*, *22*(2), 165–190. doi:10.1080/13600834.2013.821812

Beaver, M. (2016). The United Nations and cyberwarfare. Retrieved from https://globalriskadvisors.com/blog/united-nations-cyber-warfare/

Brenner, J. (2015). The new industrial espionage. *American Interest*, *10*(3), 28-36.

Computer virus. (2017). In *Funk & Wagnalls New World Encyclopedia*.

Daly, J. (n.d.). *The evolution of malware*. Retrieved from https://www.wired.com/brandlab/2016/12/cylance-evolution-malware/

Dion, J. (2016). *Security (CIA) triad* [Video file]. Retrieved from https://youtu.be/szcmb-lcYV4

Dods EU Monitoring. (2014, Sept. 1). Dods EU alert: International cybercrime taskforce launched to tackle online crime. Retrieved from https://www.theparliamentmagazine.eu/articles/eu-monitoring/dods-eu-alert-international-cybercrime-taskforce-launched-tackle-online-crime

Enigma simulation. (n.d.). Retrieved from http://enigmaco.de/enigma/enigma.html

Fanning, K. (2015). Minimizing the cost of malware. *Journal of Corporate Accounting & Finance, 26*(3), 7-14. doi:10.1002/jcaf.22029

Federal Bureau of Investigation. (2015). *Economic espionage: FBI launches nationwide awareness campaign*. Retrieved from https://www.fbi.gov/news/stories/economic-espionage

Feit, J. (2017). Do your IoT devices risk a security breach? The Internet of Things can open you up to cyber-attacks; stop them with proper security practices. *Buildings*, *111*(7), 18.

Glenny, M. (2011). *Hire the hackers!* [Video file]. Retrieved from https://www.ted.com/talks/misha_glenny_hire_the_hackers/transcript?language=en

Gompert, D. C., & Libicki, M. (2015). Waging cyber war the American way. *Survival, 57*(4), 7-28. doi:10.1080/00396338.2015.1068551

Gupta, U. (2011, Nov. 21). Security challenges BYOD presents. Retrieved from https://www.bankinfosecurity.com/security-challenges-byod-presents-a-4258

Hallman, R., Bryan, J., Palavicini Jr., G., Divita, J., & Romero-Mariona, J. (2017). IoDDoS – The Internet of distributed denial of service attacks: A case study of the Mirai malware and IoT-based botnets. In M. Ramachandran, V. Méndez Muñoz, V. Kantere, G. Wills, R. Walters & V. Chang (Eds.), *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security* (IoTBDS 2017) (pp. 47-58). doi:10.5220/0006246600470058

Hougland, B. (2014). *What is the Internet of Things? And why should you care?* [Video file]. Retrieved from https://youtu.be/_AlcRoqS65E

Hui, K., Kim, S. H., & Wang, Q. (2017). Cybercrime deterrence and international legislation: Evidence from distributed denial of service attacks. *MIS Quarterly, 41*(2), 497.

INTERPOL. (n.d.). *Cybercrime*. Retrieved from https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Johnson, M. P. (n.d.). *Welcome to Cryptography.org cryptology links*. Retrieved from http://cryptography.org/

Jordan, B. (2016). *U.S. still has no definition for cyber act of war.* Retrieved from https://www.military.com/daily-news/2016/06/22/us-still-has-no-definition-for-cyber-act-of-war.html

Measures for the prevention and management of computer viruses. (2016). *Chinese Law & Government, 48*(1), 88-91. doi:10.1080/00094609.2015.1048141

Madarie, R. (2017). Hackers' motivations: Testing Schwartz's theory of motivational types of values in a sample of hackers. *International Journal of Cyber Criminology, 11*(1), 78. doi:10.5281/zenodo.495773

Mitchell, B. (2018, Jan. 1). *Gallery of home network diagrams.* Retrieved from https://www.lifewire.com/home-network-diagrams-4064053

Nickisch, C. (2016). Industrial espionage is more effective than R&D. *Harvard Business Review, 94*(11), 30-31.

Office of General Counsel, United States Department of Defense. (2015, June). *Law of war manual*. Retrieved from https://www.defense.gov/Portals/1/Documents/law_war_manual15.pdf

Parker, D. B. (2013). Plenty more hacker motivations. *Communications of the ACM, 56*(7), 8. doi:10.1145/2483852.2483856

Raja Plus (2014, Sept. 1). *Attack tree tutorial* [Video file]. Retrieved from https://youtu.be/2ZT3xNOa6iQ

Rollins, A. (2016). Facing the cyber challenge. *Journal of the Australian & New Zealand Institute of Insurance & Finance, 39*(2), 1-4.

Salisch, W. J., & Mayfield, M. (2017). Multi-layered security. *Film Journal International, 120*(4), 88-90.

Schneier, B. (1999). *Attack trees.* Retrieved from https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Solberg Søilen, K. (2016). Economic and industrial espionage at the start of the 21st century – Status questions. *Journal of Intelligence Studies in Business, 6*(3), 51-64.

Stohl, M. (2007). Cyber terrorism: A clear and present danger, the sum of all fears, breaking point or patriot games? *Crime, Law & Social Change, 46*(4/5), 223-238. doi:10.1007/s10611-007-9061-9

Technopedia. (n.d.). Footprinting. Retrieved from https://www.techopedia.com/definition/16098/footprinting

Techquickie. (2015). DDoS attacks as fast as possible [Video file]. Retrieved from https://youtu.be/0I4O4hoKzb8

The risk of cyber war and cyber terrorism. (2016). *Journal of International Affairs, 70*(1), 179-181.

Touchette, F. (2015). *The evolution of malware.* Retrieved from https://www.darkreading.com/risk/the-evolution-of-malware/a/d-id/1322461

Young, A. L., & Yung, M. (2017). Privacy and security cryptovirology: The birth, neglect, and explosion of ransomware: Recent attacks exploiting a known vulnerability continue a downward spiral of ransomware-related incidents. *Communications of the ACM, 60*(7), 24-26. doi:10.1145/3097347

Wolff, J. (2016). Perverse effects in defense of computer systems: When more is less. *Journal of Management Information Systems, 33*(2), 597-620. doi:10.1080/07421222.2016.1205934

Yakuza112v3. (2013). Defcon: *The history and evolution of malware* [Video file]. Retrieved from https://youtu.be/L8lA1pNvcz4

Zhengchuan, X., Qing, H., & Chenghong, Z. (2013). Why computer talents become computer hackers. *Communications of the ACM, 56*(4), 64. doi:10.1145/2436256.2436272

Download and review the **POL-385 Credits Page (PDF)**.

Expectations, Policies, and Important Student Information

School/Division	Link
DeVoe School of Business Division of Liberal Arts School of Services and Leadership	View School/Division Expectations, Policies, and Student Information
School of Educational Leadership	View School/Division Expectations, Policies, and Student Information
Wesley Seminary @ IWU	View School/Division Expectations, Policies, and Student Information
Nursing – Undergraduate	View School/Division Expectations, Policies, and Student Information
Nursing – Graduate	View School/Division Expectations, Policies, and Student Information