Syllabus

CRJ-464: Cyber Crime

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

Collaborator: Tony Manganello

Course Description

This course is designed to provide students with an overview of the legal, social, and technical impact of cybercrime. It will also analyze the tools needed to combat cybercrime through both the private and public sectors and evaluate such efforts.

Credit Hours: 3
Prerequisite Courses: None

Course Outcomes

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

1. Define terms associated with cybercrime.
2. Evaluate specific plans for preventing cybercrimes.
3. Compare the role of the private sector and public sector agencies in investigating and preventing cybercrime.
4. Evaluate law enforcement's response to cybercrime.
5. Integrate biblical principles related to criminal justice.

Course Textbook

Holt, J., Bossler, A. M., Seigfried-Spellar, K. C. (2018). *Cybercrime and digital forensics: An introduction (2nd Ed.).* New York, NY: Routledge.

Grading Scale

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

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*	Dropbox*	Devotional*	Quiz*	End-of-Course Survey	Total Points
Workshop One	1/30	1/75	1/5	1/40		150
Workshop Two	1/30	2/150	1/5	1/40		225
Workshop Three	1/30	1/75	1/5	1/40		150
Workshop Four	1/30	2/150	1/5	1/40		225
Workshop Five	1/30	2/175	1/5	1/40		250
Course Totals	5/150	8/625	5/25	5/200	10 (Extra Credit)	**1000**

* Number of Activities/Sum Point Totals

Course Assignments

Workshop One Outline

Title	Due Dates	Time	Points
1.1 Discussion: It Begins with "Why?"	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop.	1 hour	5

.2 Discussion: Developing Cybercrime Expertise	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
1.3 Assignment: The Feds and Cybercrimes	Due by the end of the workshop.	6 hours	75
1.4 Quiz	Due by the end of the workshop.	1 hour	40
	Totals	**12 hours***	**150**

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

Workshop Two Outline

Title	Due Dates	Time	Points
2.1 Discussion: The Establishment	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop.	1 hour	5
2.2 Discussion: Fighting Cybercrime	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
2.3 Assignment: The Feds and Cybercrime Prevention	Due by the end of the workshop.	6 hours	50
2.4 Assignment: Global Cybercrime and Security	Due by the end of the workshop.	6 hours	100
2.5 Quiz	Due by the end of the workshop.	1 hour	40
	Totals	**18 hours***	**225**

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

Workshop Three Outline

Title	Due Dates	Time	Points
3.1 Discussion: A Standard of Excellence	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop.	1 hour	5
3.2 Discussion: Stages in Digital Forensic Investigations	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
3.3 Assignment: Open Source Code	Due by the end of the workshop.	6 hours	75
3.4 Quiz	Due by the end of the workshop.	1 hour	40
	Totals	**12 hours***	**150**

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

Workshop Four Outline

Title	Due Dates	Time	Points
4.1 Discussion: Do Not Be Anxious	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop.	1 hour	5
4.2 Discussion: Criminological Theories: Do They Work in Cybercrime?	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
4.3 Assignment: Effectiveness of Traditional Theories	Due by the end of the workshop.	6 hours	75
4.4 Assignment: Global Cybercrime and Security	Due by the end of the workshop.	6 hours	75
4.5 Quiz	Due by the end of the workshop.	1 hour	40
	Totals	**18 hours***	**225**

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

Workshop Five Outline

Title	Due Dates	Time	Points
5.1 Discussion: "Hate Evil; Love Good"	Initial post due by the end of the fourth day of the workshop; two responses due by the end of the workshop.	1 hour	5
5.2 Discussion: Combating Online Cybercrime	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
5.3 Assignment: Cyberterrorism	Due by the end of the workshop.	6 hours	75
5.4 Assignment: Global Cybercrime and Security	Due by the end of the workshop.	6 hours	100
5.5 Quiz	Due by the end of the workshop.	1 hour	40
End-of-Course Survey	Due by the end of the workshop.	30 minutes	10 (Extra Credit)
	Totals	**18:30 hours***	**250**

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

Course Development Resources

Associated Press. (2014, November 10). Efforts to protect US government data against hackers undermined by worker mistakes. *The Guardian.* Retrieved from https://www.theguardian.com/technology/2014/nov/10/us-government-hacking-cybercrime-workers-crime

Barlow, C. (2017). *Where is cybercrime really coming from? | Caleb Barlow* [Video file]. Retrieved from https://www.youtube.com/watch?v=FqrLUtIFVjs

Breach Level Index. (2017). *Data breach resource library*. Retrieved from http://breachlevelindex.com/data-breach-library

Denning, D. (2015, September 8). The rise of hacktivism. *Georgetown Journal of International Affairs.* Retrieved from http://journal.georgetown.edu/the-rise-of-hacktivism/

Duggan, M. (2014, October 22). *Online harassment.* Retrieved from http://www.pewinternet.org/2014/10/22/online-harassment/

Ellyatt, H. (2016, September 28). *The 2016 trends in cybercrime that you need to know about.* Retrieved from http://www.cnbc.com/2016/09/28/the-2016-trends-in-cybercrime-that-you-need-to-know-about.html

Federal Bureau of Investigation. (2014, January 31). *A byte out of history: $10 million hack, 1994-style.* Retrieved from https://www.fbi.gov/news/stories/a-byte-out-of-history-10-million-hack

Federal Bureau of Investigation. (2014, January 22). *Scam on the run: Fugitive identity thief led global criminal enterprise.* Retrieved from https://www.fbi.gov/news/stories/fugitive-identity-thief-led-global-criminal-enterprise

Glenny, M. (2011). *Hire the hackers!* [Video file]. Retrieved from https://0-fod-infobase-com.oak.indwes.edu/p_ViewVideo.aspx?xtid=48218

Hypponen, M. (2011). *Fighting viruses, defending the net* [Video file]. Retrieved from https://www.ted.com/talks/mikko_hypponen_fighting_viruses_defending_the_net

Information Technology Laboratory: Computer Forensics Tool Testing Program. (2015).

International Telecommunications Union. (2017). *National strategies repository.* Retrieved from http://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx

INTERPOL. (2017). *Cybercrime*. Retrieved from https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime

Leukfeldt, E., & Yar, M. (2016). Applying routing activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior, 37*(3), 263-280. Retrieved from http://www.tandfonline.com/doi/full/10.1080/01639625.2015.1012409

Lyle, A. (2016). Legal considerations for using open source intelligence in the context of cybercrime and cyberterrorism. In B. Akhgar, P. S. Bayerl, and F. Sampson (Eds.), *Open source intelligence investigation: From strategy to implementation* (pp. 277–294). Available from https://link.springer.com/chapter/10.1007%2F978-3-319-47671-1_17

National Institute of Standards and Technology (2015). Information Technology Laboratory: Computer Forensics Tool Testing Program. Retrieved from https://www.cftt.nist.gov/

Naval Criminal Investigative Services. (n.d.). Cyber. Retrieved from http://www.ncis.navy.mil/CoreMissions/Cyber/Pages/default.aspx

Norton. (2016). *The most dangerous town on the internet: Where cybercrime goes to hide* [Video file]. Retrieved from https://www.youtube.com/watch?v=CashAq5RToM

Ponemon Institute. (2017). *2016 Cost of cyber crime study & the risk of business innovation.* Retrieved from http://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf

PricewaterhouseCoopers. (2017). *Global economic crime survey 2016: Adjusting the lens on economic crime.* Retrieved from https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf

Quimbee.com. (2017). *Daubert v. Merrell Dow Pharmaceuticals* [Video file]. Retrieved from https://youtu.be/JnjmNCstCjw

Sparrow, A., & Hern, A. (2017, March 24). Internet firms must do more to tackle online extremism, says No 10. *The Guardian*. Retrieved from https://www.theguardian.com/media/2017/mar/24/internet-firms-must-do-more-to-tackle-online-extremism-no-10

Symantec Corporation. (2016). *An ISTR special report: Ransomware and business 2016.* Retrieved from https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ISTR2016_Ransomware_and_Businesses.pdf

Teo, D. (2015). *Digital forensics | Davin Teo* [Video file]. Retrieved from https://www.youtube.com/watch?v=Pf-JnQfAEew.

U.S. Air Force. (2005). *Air Force Office of Special Investigations*. Retrieved from http://www.af.mil/About-Us/Fact-Sheets/Display/Article/104502/air-force-office-of-special-investigations/

U.S. Department of Homeland Security. (2017). *Combating cyber crime.* Retrieved from https://www.dhs.gov/topic/combating-cyber-crime

U.S. Army Criminal Investigations Division. (2017). Retrieved from http://www.cid.army.mil/mission.htm

U.S. Department of Justice. (2010, October 26). Leader of hacking ring sentenced for massive identity thefts from payment processor and U.S. retail networks. Retrieved from https://www.justice.gov/opa/pr/leader-hacking-ring-sentenced-massive-identity-thefts-payment-processor-and-us-retail

U.S. Department of Justice. (n.d.). *CCIPS press releases.* Retrieved from https://www.justice.gov/criminal-ccips/ccips-press-releases

U.S. Immigration and Customs Enforcement. (n.d.). ICE investigators expose Darknet criminals to the light. Retrieved from https://www.ice.gov/features/darknet

Wainwright, R., & Culluffo, F. (2017). Responding to cybercrime at scale: Operation Avalanche—A case study. Retrieved from https://cchs.gwu.edu/sites/cchs.gwu.edu/files/Responding%20to%20Cybercrime%20at%20Scale%20FINAL.pdf

Wilson, C. (2011). Digital evidence discrepancies – Casey Anthony trial. *Digital Detectives.* Retrieved from http://www.digital-detective.net/digital-evidence-discrepancies-casey-anthony-trial/

Wordsworth, M. (2017, February 27). Cybercrime victims on their own as police fail to follow up cases, helpline head says. Retrieved from http://www.abc.net.au/news/2017-02-27/cybercrime-victims-on-their-own-as-police-fail-to-follow-cases/8306814

Download and review the CRJ-464_Credits_Page.

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

School/Division	Link
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