New Jersey City University
EDTC 804 - Global Curriculum Project

Group Members:
Edith Adewumi
Barbara Green-McCarty
Manuel Negron
Emily Vandalovsky (team leader)

1. **Abbreviated Course Title:** SECU 200

2. **Course Title**: Introduction to Cyber Security

3. **Credits**: 3 credits / 4 contact hours

4. **Course Components:** 2 hour lecture, 2 hour lab; blended format

5. **Course Level: 200-level**

6. **Catalog Description**

This course introduces the field of cyber security using a practical approach through an interactive, hybrid collaboration between NJCU and the University of Birmingham. Focusing on analyzing security problems and employing simulated security activities, it will examine policy, risk management, cryptography, authentication and encryption processing from individual to Internet-based systems.

7. **Course Prerequisites or Corequisites:**

none

8. **Rationale:**

As cyber attacks increase in frequency, complexity and severity around the globe, the need for a highly trained cybersecurity workforce is essential. A 2015 report from the US department of Labor predicts that employment of information security analysts is projected to grow 18% from 2014-2024. In a Global Economic Crime Survey 2016, McConKey of PricewaterhouseCoopers of London reported that only four out of ten respondents had trained professionals ready to act should they become victims of cybercrime. Introduction to Cyber Security will provide an important basic education on the subject of cyber security for students from NJCU and the University of Birmingham. Available to students in related majors, such as Computer Science and National Security Studies, this course may serve as an invitation to the field of cyber security for future concentration.

Introduction to Cyber Security will serve as an overview to the international problem of cyber security, increasing awareness to vulnerability and equipping students with a practical toolset for cyber defense. Taught as a hybrid class across both universities, students will interact with professors on their respective campuses as well as participate in video or online discussions and learning activities with their international peers. This exposure to different viewpoints will provide both sets of students with a unique opportunity to view cyber security through an international lens. This course will also help to address the goals of "Strengthening Cyber Security Skills," "Promoting Cyber Security Science and Technology" as well as the International Action Goals of the United Kingdom's National Cyber Security Strategy 2016-2021. It will also act in accordance with "New Collar Jobs Act of 2017" (H.R. 3393) introduced to US Congress on July 25th, 2017 with the intent "[t]o increase cyber security education and job growth".

Sources:

Bureau of Labor and Statistics, U.S. Department of Labor. (2017, October 24). *Occupational Outlook Handbook*, Information security analysts. Retrieved from https://stats.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6

H.R.3393, 115th Congress. (2017) (enacted). Retrieved from https://www.congress.gov/bill/115th-congress/house-bill/3393/text

McConkey, K. (2016). Cybercrime. Retrieved from http://www.pwc.com/gx/en/services/advisory/forensics/economic-crime-survey/cybercrime.html

U.K. Cabinet Office, National Security and Intelligence, HM Treasury, and The Rt Hon Philip Hammond MP. (2017, September 11). *U.K. National Cyber Security Strategy 2016 to 2021*. Retrieved from https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

9. Student Learning Outcomes

By the end of this course students will be able to:

A. Define the field of cyber security and its evolvement.
B. Explain basic cyber security terminology, build skills for keeping up to date on cyber security issues, and identify information assets.
C. Describe basic authentication mechanisms and alternative authentication methods.
D. Identify main malware types and build skills for recognizing different malware propagation methods and preventing malware infections.

E. Explain basic networking concepts and recognize network security challenges and build knowledge of key networking standards.
F. Describe cryptography terminology and the application of cryptography in email communication, and employ the applications of cryptography.
G. Demonstrate understanding of firewalls, virtual private networks, network intrusion detection and prevention technologies.
H. Describe legal and regulatory issues relating to cyber security and understand how to recover from security failures.
I. Recognize challenges in cyber security education and communicate possible ways of dealing with them.
J. Apply basic risk analysis and critical thinking skills to propose solutions to security-related problems.
K. Use experiential learning techniques for identifying and building applied cyber security skills.
L. Analyze how cyber security connects with individuals, society, and the overall global workforce.

10. Instructional Procedures

1) Required readings (Student Learning Outcomes A, B, C, D, E, F, H)
2) Class participation and discussion (Student Learning Outcomes G, I, J, L)
3) Research (Student Learning Outcomes H, I, J, L)
4) Instructional online content (Student Learning Outcomes A-H)
5) Hands-on labs (Student Learning Outcomes G, J, K)

11. Course Content

Week #	Topics, Learning Outcomes	Assignments & Assessments
Week 1	Topic: Course Introduction. Discussion 1: Legal, Ethical, and Political Issues Related to US - UK cyber security Policies; state and private partnerships (Student Learning Outcomes A, B, E, H, J, L)	Read (available through NJCU Databases): Stoddart, K. (2016). Live free or die hard: U.S.-UK cyber security policies. *Political Science Quarterly* (Wiley-Blackwell), 131(4), 803-842. Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43-62. doi:10.1111/1468-2346.12504

		Participate in Discussion 1
Week 2	Topic: Security from the ground up Discussion 1 (Cont.): Legal, Ethical, and Political Issues Related to US - UK Cyber Security Policies; state and private partnerships (Student Learning Outcomes A, B, E, H, J, L)	Study Chapter 1 Submit Lab 1 Complete Quiz 1 Read (available through NJCU Databases): Myauo, M. (2016). The U.S. department of defense cyber strategy: A call to action for partnership. *Georgetown Journal of International Affairs*, 17(3), 21-29 Watch: "Governments don't understand cyber warfare. We need hackers" (Bijou) Participate in Discussion 1 (Cont.)
Week 3	Topics: Controlling a Computer Controlling Files Discussion 2: Complexity and international nature of cyber security field (Student Learning Outcomes E, I, J, K, L)	Study Chapters 2 and 3 Submit Ch. 2-3 Lab Complete Ch. 2 and Ch. 3 Quiz Read (available through NJCU Databases): Rai, N., & Chansarkar, S. R. (2017). Cyberspace security : An overview for beginners. *Defence Science Journal*, 67(4), 483-484. Participate in Discussion 2
Week 4	Topics: Sharing Files Sorting Files Discussion 2 (Cont.): Complexity and international nature of cyber security field (Student Learning Outcomes E, I, J, K, L)	Study Chapters 4 and 5 Submit Ch. 4-5 Lab Complete Ch. 4 and Ch. 5 Quiz Complete Exam 1 (Chapters 1-5) Read (available through NJCU Databases): Denning, P. J., & Denning, D. E. (2016). Cybersecurity is harder than building bridges. *American Scientist*, 104(3), 154+. Participate in Discussion 2 (Cont.)
Week 5	Topic:	Study Chapter 6

	Authenticating People Discussion 2 (Cont.): Complexity and international nature of cyber security field (Student Learning Outcomes C, D, J, K)	Submit Lab 6 Complete Quiz 6 Read (available through NJCU Databases): Opara, E. U., & Hussein, M. T. (2017). Cyber security, threat intelligence: Defending the digital platform. *Journal of International Technology and Information Management*, 26(1), 138-160 Participate in Discussion 2 (Cont.)
Week 6	Topic: Encrypting Files Discussion 3: Challenges of cyber security education and cyber related challenges in the field of education (Student Learning Outcomes E, F, I, J, L)	Study Chapter 7 Submit Lab 7 Complete Quiz 7 Read: Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 491-497 Participate in Discussion 3
Week 7	Topic: Secret and Public Keys Discussion 3 (Cont.): Challenges of cyber security education and cyber related challenges in the field of education (Student Learning Outcomes E, F, J, L),	Study Chapter 8 Submit Lab 8 Complete Quiz 8 Read (available through NJCU Databases): Napolitano, J. (2012). DHS proposes cyber security education to begin in kindergarten. *New American* (08856540), 28(22), 8. Watch: "Why Cybersecurity Education Matters" (Palo Alto Networks) Participate in Discussion 3 (Cont.)
Week 8	Topic: Encrypting Volumes Discussion 3 (Cont.):	Study Chapter 9 Submit Lab 9 Complete Quiz 9 Complete Exam 2 (Chapters 6-9)

	Challenges of cyber security education and cyber related challenges in the field of education (Student Learning Outcomes B, F, J, L)	Read (available through NJCU Databases): Pascopella, A. (2017). Report: Students cheat and access banned content. Now what?.*District Administration*, *53*(10), 50 Participate in Discussion 3 (Cont.)
Week 9	Topic: Connecting Computers Discussion 4: Multidisciplinary and multicultural approach to dealing with cyber security issues (Student Learning Outcomes E, G, J, L)	Study Chapter 10 Submit Lab 10 Complete Quiz 10 Read: Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175 Participate in Discussion 4
Week 10	Topic: Network of Networks End-to-End Networking Discussion 4 (Cont.): Multidisciplinary and multicultural approach to dealing with cyber security issues (Student Learning Outcomes D, E, G, L)	Study Chapters 11 and 12 Submit Ch. 11- 12 Complete Ch. 11 and Ch. 12 Quiz Read (available through NJCU Databases): Waldrop, M. M. (2016). How to hack the hackers: The human side of cybercrime. *Nature*, 533(7602), 164-167. Participate in Discussion 4 (Cont.)
Week 11	Topic: Enterprise Computing Discussion 4 (Cont.): Multidisciplinary and multicultural approach to dealing with cyber security issues (Student Learning Outcomes D, E, G, K, L)	Study Chapter 13 Submit Lab 13 Complete Quiz 13 Complete Exam 3 (Chapters 10-13) Watch: "Where is cybercrime really coming from?" (Barlow) Participate in Discussion 4 (Cont.)
Week 12	Topic:	Study Chapter 14

	Network Encryption Discussion 5: Current demand and future trends of cybersecurity skills (Student Learning Outcomes D, E, F, G, L)	Submit Lab 14 Complete Quiz 14 Read (available through NJCU Databases): Herald, B. (2017). Cyber security skills in demand. *Education Week*, 36(25), 1-15 Participate in Discussion 5
Week 13	Topic: Internet Services and Email Discussion 5 (Cont.): Current demand and future trends of cybersecurity skills (Student Learning Outcomes E, F, K, L)	Study Chapter 15 Submit Lab 15 Complete Quiz 15 Read (available through NJCU Databases): Smith, J. (2011). Cyber security experts wanted here. *National Journal*, 13. Participate in Discussion 5 (Cont.)
Week 14	Topic: The World Wide Web Discussion 5 (Cont.): Current demand and future trends of cybersecurity skills (Student Learning Outcomes E, F, K J, L)	Study Chapter 16 Submit Lab 16 Complete Quiz 16 Read (available through NJCU Databases): Dupont, B. (2013). Cybersecurity futures: How can we regulate emergent risks? *Technology Innovation Management Review*, 3(7), 6-11. Kour, J., Hanmandlu, M., & Ansari, A. Q. (2016). Biometrics in cyber security. *Defence Science Journal*, 66(6), 600-604 Participate in Discussion 5 (Cont.)
Week 15		Final Exam (Chapters 1-16)

Course content includes:

- Introduction to Information Security
- The Need for Security

- Legal, Ethical, and Professional Issues in Information Security
- Planning for Security
- Security Technology: Firewalls, VPNs, and Wireless
- Security Technology: Intrusion Detection and Prevention Systems
- Cryptography
- Physical Security
- Implementing Information Security
- Security and Personnel

12. Undergraduate General Education Courses
n/a

13. Graduate Course Status
n/a

14. Degree Requirements

The proposed course may be included as an elective in the following undergraduate programs in NJCU:

- A collateral requirement course in Bachelors of Science degree in Computer Science: http://www.njcu.edu/academics/bs-computer-science
- A restricted elective course in Bachelors of Science degree in Criminal Justice: http://www.njcu.edu/criminal-justice/undergraduate-program
- An elective course in a Bachelor of Science degree in National Security Studies: http://www.njcu.edu/professional-security-studies/bs-national-security-studies

The proposed course may be included as an elective in the following undergraduate programs in The University of Birmingham:

- A collateral requirement course in Bachelors of Science degree in Computer Science: https://www.birmingham.ac.uk/undergraduate/courses/computer-science/computer-science.aspx
- An elective course in a Bachelor of Science degree in Security Studies: https://www.birmingham.ac.uk/schools/government-society/courses/masters/modules/polsis/security-studies.aspx

The proposed course will not change the required number of credits in any of the above listed programs, but will rather offer a new elective option.

Additionally, the proposed course will become available to matriculated and nonmatriculated students, interested in exploring the area of cyber security within the context of computer engineering, computer networks, telecommunications and other related fields.

15. Specialized Accreditation, Certification, and Licensure

The course will not impact any programs recognized by specialized accreditation, certification and/or licensure.

16. Assessment/Evaluation of Student Outcomes and Determining Student Grades

Course grades will consist of:

Discussions / Class Participation	25%
Lab Work / Hands-on Assignments	25%
Exams, Quizzes	30%
Final Exam	20%

Grading Scale:

Percentage	Assigned Grade
89-100	A
79-88	B
69-78	C
59-68	D
0-58	F

The proposed course will follow NJCU Grading Scale.
The standing of each student at the completion of each course is determined by the instructor and recorded at the end of each semester.

A (4.0)	**D. (1.0)**
A- (3.7)	**P (Pass)**
B+ (3.3)	**F (0.0)**
B (3.0)	**W (Withdrawal)**
B- (2.7)	**IN (Incomplete)**
C+ (2.3)	**R (Repeat - Academic Foundation Course only)**
C (2.0)	
C- (1.7)	

Grade Point Averages: The numbers in parentheses represent index values used to compute grade point averages. The number of credits/semester hours assigned to the course multiplied by the grade index received gives the grade points earned for that course. The sum total of grade points earned divided by total credits attempted constitutes the student's grade point average.

17. Bibliography (APA)

Required Text:

Smith, R. (2015). *Elementary information security*. (2nd Edition). Burlington, MA: Jones & Bartlett Learning.

Supporting Bibliography:

Arnove, R., Torres, C., & Franz, S. (2012). *Comparative education: the dialectic of the global and the local*. (4th edition). Lanham, Maryland: Rowman & Littlefield Publishers.

*Barnard-Wills, D., & Ashenden, D. (2012). Securing virtual space: Cyber war, cyber terror, and risk. *Space and Culture*, 15(2), 110-123.

*Carr, M. (2016). Public-private partnerships in national cyber-security strategies. *International Affairs*, 92(1), 43-62. doi:10.1111/1468-2346.12504

*Denning, P. J., & Denning, D. E. (2016). Cybersecurity is harder than building bridges. *American Scientist*, 104(3), 154+. Retrieved from http://draweb.njcu.edu:2048/login?url=http://link.galegroup.com/apps/doc/A452585641/OVIC?u=jers45639&xid=b6c04eea

*Dupont, B. (2013). Cybersecurity futures: How can we regulate emergent risks? *Technology Innovation Management Review*, 3(7), 6-11. Retrieved from https://search.proquest.com/docview/1614472239?accountid=12793

Elmaghraby, A. S., & Losavio, M. M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of Advanced Research*, 5(4), 491-497. Retrieved from http://www.sciencedirect.com/science/article/pii/S2090123214000290

*Goyal, N., & Goyal, D. (2017). Cyber crime in the society: Security issues, preventions and challenges. *Research Journal of Engineering and Technology*, 8(2), 73-80. doi:http://dx.doi.org/10.5958/2321-581X.2017.00012.5

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175. Retrieved from https://www.nyu.edu/projects/nissenbaum/papers/digital%20disaster.pdf

*Herald, B. (2017). Cyber security skills in demand. *Education Week*, 36(25), 1-15. Retrieved from http://draweb.njcu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=122029673&site=ehost-live

*Inan, F. A., Namin, A. S., Pogrund, R. L., & Jones, K. S. (2016). Internet use and cyber security concerns of individuals with visual impairments. *Journal of Educational Technology & Society*, 19(1), 28-40. Retrieved from http://draweb.njcu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=112223274&site=ehost-live

*Kour, J., Hanmandlu, M., & Ansari, A. Q. (2016). Biometrics in cyber security. *Defence Science Journal*, 66(6), 600-604. Retrieved from https://search.proquest.com/docview/1838726819?accountid=12793

*Myauo, M. (2016). The U.S. department of defense cyber strategy: A call to action for partnership. *Georgetown Journal of International Affairs*, 17(3), 21-29. Retrieved from https://search.proquest.com/docview/1924872574?accountid=12793

*Napolitano, J. (2012). DHS proposes cyber security education to begin in kindergarten. *New American* (08856540), 28(22), 8. Retrieved from http://draweb.njcu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=86228298&site=ehost-live

*Opara, E. U., & Hussein, M. T. (2017). Cyber security, threat intelligence: Defending the digital platform. *Journal of International Technology and Information Management*, 26(1), 138-160. Retrieved from https://search.proquest.com/docview/1938528758?accountid=12793

*Pascopella, A. (2017). Report: Students cheat and access banned content. Now what?.*District Administration*, *53*(10), 50. Retrieved from http://draweb.njcu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=125421075&site=ehost-live

*Rai, N., & Chansarkar, S. R. (2017). Cyberspace security : An overview for beginners. *Defence Science Journal*, 67(4), 483-484. Retrieved from https://search.proquest.com/docview/1949335525?accountid=12793

*Smith, J. (2011). Cyber security experts wanted here. *National Journal*, 13. Retrieved From http://draweb.njcu.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aph&AN=66839018&site=ehost-live

*Stoddart, K. (2016). Live free or die hard: U.S.-UK cyber security policies. *Political Science Quarterly* (Wiley-Blackwell), 131(4), 803-842. doi:10.1002/polq.1253

*Taddeo, M. (2013). Cyber security and individual rights, striking the right balance.

Philosophy & Technology, 26(4), 353+. Retrieved from http://draweb.njcu.edu:2048/login?url=http://draweb.njcu.edu:2072/ps/i.do?p=AONE&sw=w&u=jers45639&v=2.1&it=r&id=GALE%7CA352849607&sid=summon&asid=5c0cadb8362206aa02f29c1453e89b22

*Waldrop, M. M. (2016). How to hack the hackers: The human side of cybercrime. *Nature*, 533(7602), 164-167. Retrieved from https://search.proquest.com/docview/1789281700?accountid=12793

Relevant Periodical Sources

American Scientist
Defence Science Journal
Georgetown Journal of International Affairs
International Journal of Cyber-Security and Digital Forensics
International Journal of Computer Network and Information Security
Journal of Advanced Research
Journal of Educational Technology & Society
Journal of International Technology and Information Management
Nature
Political Science Quarterly
Security and Communication Networks
Technology Innovation Management Review

Relevant Online Materials

Barlow, C. (2017, February 15). Where is cybercrime really coming from? Retrieved from https://www.youtube.com/watch?v=FqrLUtIFVjs

Bijou, R. (2016, January 21). Governments don't understand cyber warfare. We need hackers. Retrieved from https://www.youtube.com/watch?v=_nSHsb5xKPo

Palo Alto Networks (2017, September 29). Why Cybersecurity Education Matters. Retrieved from https://www.youtube.com/watch?v=Zevtqsu4uSg&feature=youtu.be

18. Budget

Annual academic membership for acquiring necessary software: $500-$700
Faculty professional development: $900 - $1200
Final course revision before deployment: amount equal to 1-2 credit(s) of faculty release time