Executive Summary: Cybersecurity program @ Le Moyne College

This program's strength is in the liberal arts tradition - students receive broad exposure to cybersecurity topics that span the social sciences and security technology. Students will probe the meanings and motivations behind cyber security threats, protective needs, and the role and limitations of technology. The program courses are meant to bring together critical thinking, effective communications, and the ability to meaningfully connect concepts, policies, technologies, and their critiques.

This program's interdisciplinary approach is unique in that it presents broad coverage of policy, societal and technical topics, while allowing a student to specialize by selecting a concentration. This program is a strong example of liberal arts education that is clearly distinguishable from programs at peer institutions, which tend to emphasize only the technical aspect of cybersecurity. A 2014 paper published by the National Council in the Social Studies[1] includes the following quote.

> *... the disciplines of the social sciences promote ways of knowing and deliberating about data and information that are critical to policy development and the implementation of cybersecurity initiatives. Building the capacity of the next generation of social scientists to tackle these emerging issues is imperative.*

In addition, a summary report from a workshop on social science, computer science, and cybersecurity held in 2013[2] included white papers written by the attendees. The following is a quote from one of the computer scientists in attendance at this workshop.

> *The fact that humans from several different walks of life are interacting with these systems on a daily basis has prompted a paradigm shift: rather than designing secure systems with arbitrarily defined use models, we must design secure systems with use models informed by how people interact with each other, computers, and information. This security paradigm necessitates a close collaboration between technical and social scientists so that the design of secure systems incorporates an understanding of the needs and capabilities of the billions of people that will rely on them.*

Le Moyne's cybersecurity program presents a holistic approach to thinking about cybersecurity issues. This program is designed to give students foundational knowledge regarding the varied cybersecurity challenges that individuals and organizations face on a daily basis. It will prepare students for graduate programs and careers that include international relations, legal studies, government (federal, state and local), criminology, military, security compliance, and cybersecurity technology specialist. Another way to think about this program is to reflect on the question - *do you believe that technology can solve all of our cybersecurity problems?* Le Moyne's program is designed based on the belief that technology alone is not sufficient to solve our cybersecurity challenges.

This program requires a student to complete the following requirements:

- Seven courses that introduce social science and technology topics. These common requirements are intended to demonstrate the interdisciplinary nature of cybersecurity.
- Six courses in one of three concentrations:
  - Crime, Society & Culture;
  - Information & System Security; or
  - Policy & Law.
- Eight major support courses.

The table on the next page delineates these program requirements and courses.

[1] Berson, M. J., & Berson, I. R. (2014). Bringing the Cybersecurity Challenge to the Social Studies Classroom. Social Education (National Council for the Social Studies), 78(2), 96-100.

[2] Hofman, L. J. (2013). Social Science, Computer Science, and Cybersecurity, Workshop Summary Report. Cyber Security Policy and Research Institute, The George Washington University, Report GW-CSPRI-2013-02 retrieved on October 21, 2016 from https://www.seas.gwu.edu/~cspri/s/Final-08-22-13-1301-Report-Social-Science-66cn.pdf.

The program requirements are described in the following table.

<table>
<tr><th colspan="3">All cybersecurity majors take seven courses from the following common requirements:</th></tr>
<tr><td>(1) One of the following:
• ANT 101 Intro to Anthropology
• CJS 101 Intro to Criminology
• SOC 101 Intro Sociology
(2) SOC 201 Research Methods</td><td>(3) CYS 167 Intro to Cybersecurity
(4) CYS 263 Intro to Risk Assessment and Security Monitoring
(5) CYS 269 Intro to Protection and Recovery Strategies</td><td>(6) PSC 261 Intro to International Politics
(7) PSC/LGS 377 Security Studies</td></tr>
<tr><th colspan="3">All cybersecurity majors take six courses in a concentration:</th></tr>
<tr><th><i>Crime, Society & Culture</i></th><th><i>Information & System Security</i></th><th><i>Policy &amp; Law</i></th></tr>
<tr><td>(1) SOC 402 Program Evaluation Research Methods and Policy Analysis
(2-6) Any five from the following list:
• CJS 301 Crime & Punishment in Comparative Perspective
• CJS 305 Criminological Theory
• CJS 321 Law, Society & Social Science
• CJS 322 Economics of Crime and Punishment
• CJS 326 Deviance
• CJS 381 Understanding Modern Terrorism
• SOC 303 Social Theory in Anthropology/Sociology
• SOC 341 Human Services Caseload Management - Theory & Service Learning</td><td>(1) CYS 331 Network Fundamentals
(2) CYS 337 Scripting for Cybersecurity
(3) CYS 347 System and Software Security
(4) CYS 349 Digital Forensics: Recovering from and Responding to an Attack
(5) CYS 431 Intro to Network Security
(6) CYS 490 Cybersecurity Internship</td><td>(1) PSC/LGS 253 Cybersecurity Law
(2-6) Any five from the following lists.
Courses from an international relations perspective:
• PSC/PGS 105 Comparative Government
• PSC/PGS 344 (SOC/CJS 343) Immigration
• PSC/PGS 363 Foreign Policy
• PSC 366 Globalization
• PSC/PGS 367 War, Peace, and Violence
Courses from a pre-law perspective:
• PSC/LGS 205 Introduction to Legal Studies
• PSC 340 Science, Technology, Society
• PSC/LGS 451 American Constitutional Law I
• PSC/LGS 452 American Constitutional Law II</td></tr>
<tr><th colspan="3">All cybersecurity majors take eight support courses:</th></tr>
<tr><td colspan="3">(1-2) Two courses in a foreign language.
(3) One of the following logic courses:
• PHL 310 Informal Logic
• PHL 311 Introduction to Formal Logic
(4) One of the following ethics courses:
• PHL xxx (to be determined)
• REL 336 Comparative Religious Ethics and Social Concerns
(5) One programming course:
• CSC 175 Intro to Algorithms & Program Design
(6) One statistics course:
• MTH 111 Introduction to Statistics I
(7-8) Two courses from a different cybersecurity concentration:
• Students in Crime, Society & Culture take any 2 courses within Information & System Security.
• Students in Information & System Security take any 2 courses within the other two concentrations.
• Students in Policy & Law take any 2 courses within Information & System Security.</td></tr>
</table>

In fall 2018, the Center for Information Security & Risk Management (CISRM) will be created. The purpose of the CISRM is to provide research and experiential learning opportunities for faculty, staff, and students. This center will allow individuals and teams to apply their knowledge and skills while providing information security and risk management services to the not-for-profit sector. The center will be created by an individual that has experience creating centers that support not-for-profit organizations. Management of the CISRM will transition to a faculty or staff person once the center is fully operational.