Megan Garedakis, M.A.
Sociology

Assignment #1: Report on Cybersecurity and Sociology

Cybersecurity remains among the top-earning job fields available to recent college graduates and contains multiple avenues of application and specialization.

According to the U.S. Cybersecurity and Infrastructure Security Agency, more than 300,000 cybersecurity jobs are open in the United States. The median average salary for entry-level positions in cybersecurity is $71,876, making it an appealing career field for STEM majors entering the workforce. In 2018, the median yearly salary for an information security analyst with less than five years in the field, says the U.S. Bureau of Labor Statistics, was $98,350.

Despite the realities of the job market, not every student wants to major in a STEM subject, such as computer engineering or mathematics. The realities of the current socio-historical moment, such as the Black Lives Matter movement and the Russian invasion of Ukraine, have resulted in students seeking more comprehensive knowledge of the world around them, and an urge to apply their educations to serve vulnerable communities in more compelling ways.

Sociology offers a unique opportunity for students to learn the theoretical frameworks that help us understand society, while also providing training in qualitative and quantitative methods that prepare students to enter the workforce with strong research skills. Such courses at UCCS include the following:

- SOC 3070 – Social Research Methods
- SOC 3170 – Social Statistics
- SOC 4170 – Advanced Statistics and Methods

Sociology also teaches cybersecurity professionals how to identify the link between social conditions and crime, and the link between cybersecurity and globalization. UCCS offers coursework in this area in the following courses:

- SOC 3150 – Modern Sociological Theory
- SOC 4190 – Deviant Behavior
- SOC 4380 – Globalization and Development
- SOC 4600 – Critical Analysis of Capitalism

The skills gained from these courses related directly to qualifications found in entry-level cybersecurity positions. This includes the following:

- Well versed in communicating technical information effectively to various audiences
- Critical thinking skills; namely, exercise independent judgment
- Making decisions based on data
- Effective writing skills to capture issues and recommendations
- Actively participate in meetings to review and assess compliance of systems and technology

- Report on cybersecurity risk and compliance to team members

Yet, despite the advantages gained with a foundation in sociology, students and parents often express hesitation about the ability of sociology majors to obtain gainful employment upon graduation.

Cybersecurity offers a unique opportunity for sociology majors to apply their passion and training to make a lasting difference in service of communities who are most vulnerable to cyberattacks. In recent years, this has solidified into the development of a new subfield: **social cybersecurity.**

Social cybersecurity is an emerging branch of cybersecurity that deals with understanding human behavior. The subfield cuts across different and seemingly unrelated fields such as communication technology, machine learning, psychology, sociology, and forensics, among others, making it an ideal dimension of cybersecurity for students who want the financial security of a cybersecurity job with the ability to positively contribute to society.

An article published by the Military Review of the United States Army positions social cybersecurity as a vital "emerging subfield of national security that will affect all levels of future warfare, both conventional and unconventional, with strategic consequences." Where traditional cybersecurity involves people who use technology to "hack" technology, such as databases and private servers belonging to large corporations and intelligence communities, social cybersecurity involves people who use technology to "hack" other people, often those who are particularly vulnerable. (Beskow and Carley, 2019) This includes domestic and foreign groups who manipulate algorithms in global online marketplaces and social media platforms to skew election results and influence political opinion. Furthermore, Dr. Sauvik Das at the Georgia Institute of Technology argues that social cybersecurity is a vital facet of cybersecurity's ongoing development, as security systems must become more social to be effective. He asserts in a recent article that "social influences strongly affect cybersecurity behaviors," and that the future of cybersecurity hinges on its ability to understand society.

Cybersecurity jobs are plentiful, existing both in the private and public sectors. Current entry-level positions in cybersecurity, which include plentiful remote options, include the following positions:

- Junior Cybersecurity Compliance Specialist, at VMD Corp (starting salary: ($78k)
- Cybersecurity Analyst, at Summit Technical Solutions, LLC (starting salary: $85-$93k)
- Cybersecurity Analyst, at CyberForce (starting salary: $55k – $80k)

Main technical competencies for these positions include knowledge of:

- hacking and "ethical hacking"
- blockchain security
- network security control, including the ability to configure a network
- coding knowledge in common languages, such as C++ and Python

- experience in supporting cyber scans and logging
- security clearance or ability to obtain a security clearance, which is required for most positions but not all.

You can read more about security clearances using this article.

In addition to technical knowledge, key "soft skills" learned by sociology majors are in demand by employers and will set applicants apart from the competition. These include: (1) problem-solving skills; (2) attention to detail; (3) critical thinking skills; (4) strong research skills, including strong written communication skills; (5) communication skills; and (4) knowledge of human behavior and the societal systems that shape it.

Possible career paths and sectors for those entering the field of cybersecurity from a sociology background tend to center behavioral modeling, which is outlined in this program for a recent symposium of social cybersecurity professionals. Aside from entering the academic sector as a cybersecurity professor, sociology majors with the requisite technical training may enter any entry-level cybersecurity position; this includes

Moreover, sociology majors may enter fields pertaining to behavioral modelling and intelligence analysis to provide possible signals intelligence data (SIGNIT) to members of the intelligence community. This includes multiple positions within the private and public sector, including:

- Security Information Specialist with the National Security Agency
- Computer Network Defense Analyst Computer Network Operator
- Capabilities Development Specialist
- Computer Network Defense/Exploitation Analyst
- Cyber Network Professional – Offensive/Defensive Operations
- Threat Hunter, at CrowdStrike
- Cybersecurity Awareness and Education Lead, at Deloitte
- Information Security Analyst, at General Assembly.

Salaries for these positions average over $61,000 - $168,035 per year at the entry-level with public companies paying a considerably higher salary than the private sector. Most jobs are concentrated in the following areas: Fort Meade, MD; Raleigh, NC; Colorado Springs, CO; Salt Lake City, UT, and along the east and west coasts.