UCCS LAS-Cybersecurity Initiative from The Perspective of Economics.

Aidan G. Westbrook

UCCS Department of Economics

Abstract

The following report highlights the relationship between economics, studying economics at UCCS, and potential applications of economics in the field of Cybersecurity. This report includes the economic issues relevant to cybersecurity, economic competencies, career opportunities, experience, and salary estimate for future occupations in this growing industry.

Keywords: Economics, undergraduate, cybersecurity, career opportunities.

UCCS LAS-Cybersecurity Initiative from The Perspective of Economics.

Cybersecurity related attacks in the United States and globally provide an incentive for criminals to extort, terrorize, and corrupt public/private institutions from a relatively safe & anonymous vantage point. Economics majors can apply their education to the *behaviors, decisions, and thought patterns* of those seeking to prevent & mitigate cyber-attacks to benefit the cyber security industry. By analyzing risks of a digital system, observing payoffs for cyber criminals, and balancing allocations between reactive and proactive actions, economists in cyber security must be mindful of the implications of cybercrimes and cybercrime deterrence while consulting traditional economic models. One must also consider that models do not completely solve problems but provide a foundation for the consultation needed to perform well in cybersecurity positions.

Cybersecurity Issues Pertaining to Economics

Approximately 2,000 cyber-attacks are reported to the FBI every day (FBI, 2020). The cost of cyberattacks will total nearly $10.5 Trillion USD by 2025 (Cybersecurity Ventures, 2020). Financial scams and ransomware are just the beginning of the economic impact of cyberattacks. The essential industries of health, energy, and finance are the most likely to be targeted. Economists can analyze the opportunities for cyber criminals to target specific industries to gain the most ransom money from their efforts. Cybersecurity economists should consider the behavioral aspect of the criminals by creating a product that can penetrate cyber defenses and focus on increasing a company's ability to internalize all risks and costs of a compromised cyber defense. Economists should be mindful of the incurred costs of companies, consumers, domestic and global markets by failing to protect their cyber presence and should find the appropriate costs of measures to protect them.

Cyberattacks are committed for financial gain, or have as a byproduct, financial disruption. Cybercriminals often hold IT services hostage and demand financial payout for the release of the digital property. Other cases are more related to scams and identity theft. Some cases are based upon damaging digital infrastructures, but these attacks seldom occur unless in wartime. The following are examples of recent cyberattacks on national and local scales.

Colonial Pipeline

The Colonial Pipeline gas company that stretches from Texas to New Jersey was attacked in May 2021, causing IT staff to be locked out. The hack prevented millions of Americans in the gas pipeline industry and commuters from daily tasks and daily workflow. The company and the FBI paid the $5 Million ransom demands in Bitcoin to the Russian cybercriminal group named *DarkSide* (Grose, 2021). The fallout of the attack caused petrol shortages, and inspired companies to rely less on internet/cloud-based/digital infrastructure with increased redundancies at significantly increased costs of operation.

UCCS Economics Department

In the Spring of 2021, a cyber scammer contacted the UCCS Economics Department seeking “a tutor for my daughter.” After researching the internet, UCLA and other schools reported the same prompt for a fraud scheme. The scammer was caught and reported to the FBI, and other professors were warned of the prompt to prevent future scam emails.

Ocean Piracy

Modern pirates hack into GPS systems of freight ships and can deter the vessel’s course. The ships are targeted for essential commodities such as foodstuffs and petrol and are held at ransom. In 2016, A.P Moeller Maersk, the world’s biggest ocean shipping line was struck with a

computer virus (Grose, 2021). This blocked all global operations for weeks. Los Angeles harbor was stalled for days. Oil fields were shut down due to the lack of oil transport. The shipping industry learned from this attack but at added costs.

Additional Examples

- Appx 50% of all U.S consumers experienced identify theft in 2019 or 2020 (Stouffer, 2021).
- In 2020, the amount of money paid in cryptocurrency for ransomware attacks reached of $400 Million (Freeze, 2020).
- The healthcare industry is expected to spend at least $125 billion on cybersecurity investments from 2020 to 2025 (Freeze, 2021).

Competencies of A Cybersecurity Economist

Undergraduate economics students at UCCS are taught a comprehensive range of economic theory to develop the necessary mathematical and written skills. These skills include such topics as: microeconomics, macroeconomics, decision theory, statistics, behavior, environmental impacts, and mindsets. UCCS offers plenty of applicable courses that provide relevant and actionable intelligence to economics students seeking a career in cybersecurity. UCCS Economics courses will ensure students interested in cybersecurity are confident and prepared with the following skills:

- High-pressure, high-performance decision making
- Ability to apply behavioral economic theory such as the *Kahneman-Tversky Asymmetric Value Function*

- Draw from various models of economic schools of thought: Adam Smith, Dr. Richard Thaler, Dr. Daniel Kahneman, Dr. Amos Tversky, and Dr. Daniel Ariely.
- Apply perspective from the Austrian School of Economic Thinking: Milton Friedman, Ludwig von Mises, F.A Hayek.
- Showcase risk & utility in the *Von-Neumann-Morgenstern Expected Utility Model*
- Apply game theory
- Create statistical models and forecasts
- Apply law & economics such as *Coase Theorem*
- Demonstrate consumer & Producer Choice Theory models
- Identify incentives and externalities of actions
- Conduct simulations and experiments
- Apply general microeconomic theory to issues related to labor, wages, payoffs, shortages, and surpluses.
- Apply general macroeconomic theory to issues related to GDP, world trade, fiscal & monetary policy

Career Opportunities.

Cybersecurity careers are more than just science, technology, engineering, and mathematics (STEM) graduates. Economists are needed to provide consultation, leadership, differing perspectives, and additional tasks unrelated to engineering. Careers that involve policy and protocol creation such as establishing digital action plans for system recovery or personnel identity protection are suitable for cybersecurity economists as well. A cybersecurity economist is a perfect fit for a team dedicated to cybersecurity in an industry that does not specialize in cyber defense such as healthcare, transportation, and energy, whereas a cybersecurity task force

in law enforcement/national security may have an economist provide historical insight or metrics regarding the probability of attacks and the subsequent costs thereof. The industry is rapidly developing, and an economist can provide proper insight to the allocation of resources and tradeoffs necessary for each task. The following industries have shown need for cybersecurity reinforcement due to their draw for cyberattacks or specialize in cybercrime deterrence.

Industries	Career Path/Title
Financial Sector	Founder, Co-Founder, Owner
Healthcare providers/insurers	Personnel Director
Transportation: Public & Commercial	C-Suite Member
Digital Entertainment & Media	Special/Senior Advisor
Agriculture	Consultant
Lodging	Project Manager
Automotive/Aviation Engineering	Security Analyst
Artificial Intelligence	Policy Analyst
Retail	Researcher
National Defense	Counterintelligence Analyst
Education	Statistician

Entry Level Experience

Newly graduated economists who do not plan on obtaining further education in economics can engage in the following

- Data Gathering & analysis
- Identifying economic trend directions
- Creatin data and trend reports

These graduates likely have completed an internship regarding data gathering/analytics for a firm or as a research assistant. Future cybersecurity economists will find positions or create positions in their organizations and work closely with cybersecurity engineers to develop protocols and plans based upon current cyberattack metrics. Evaluating risks and probabilities of

attack based upon the status of the IT security will be forefront in the future. Spending time as an intern for a cybersecurity firm would also provide necessary work experience needed to become a consultant for various firms with a cybersecurity component.

Not many entry level opportunities for cybersecurity economists currently exist, but the Bureau of Labor Statistics estimates a 13% growth in economist positions (U.S BLS, 2022) and with a projected 464,420 job opening in cybersecurity (Grose, 2021), more positions will be created to increase the demand for cybersecurity economists. *In rare cases*, entrepreneurially inclined economics graduates may find themselves in a position to create a cybersecurity company given the projected growth rates from 2022-2030 (U.S BLS, 2022), and may find a viable option if the networking, startup funding, and a well-connected labor force is within competitive advantage against other cybersecurity firms.

Average Salary Ranges

Salaries for economists vary depending upon the credibility of the economist and their field of study. The following ranges were provided by the Bureau of Labor Statistics (U.S BLS, 2021), Start-Engineering LLC (Grose, 2021), and zippia.com (Zippia, 2022).

Occupation	Average Salary
Entry Level Economist with bachelor's degree	$ 55,000
Entry Level Economist with graduate degree	$ 70,000
Median Economist Salary	$ 108,350
Average Economics Professor Salary	$ 83,427
Entry Level Cybersecurity Analyst	$ 63,168
Risk Manager	$ 118,222
Senior Security Consultant	$ 129,251
Director of Information Security	$ 188,708
Chief Information Officer	$ 129,299
Business Owner/Founder	Unlimited

Cybersecurity's Future with Economists

Economists interested in cybersecurity have a new venue to enter the workforce with this growing industry. Another option for economists would be to enter academia and begin research-based efforts about the metrics of cyberattack incentives/frequency/targets. As economists enter the cybersecurity field with their expertise of critically analyzing data for resource allocation decisions, administrative and analytically based career opportunities will be created within the industry for all levels of cybersecurity needs. Paired with the rise of digital transactions, E-commerce, cryptocurrency, digital real estate, cybersecurity has existing applications that will overlap and extend towards opportunities the world has yet to encounter. While the current industry is primarily in need of STEM positions, the rapid expansion of cybersecurity needs will overlap into roles that encompass more than just computer engineering skills. Economists have the unique opportunity to hold significant responsibilities in regulating, analyzing, and safeguarding cybersecurity alongside STEM workers for present and future encounters in the future of cybersecurity.

References

Average economics professor salary - zippia. (n.d.). Retrieved March 31, 2022, from https://www.zippia.com/economics-professor-jobs/salary/

FBI. (n.d) *2020 internet crime report*. Retrieved March 31, 2022, from

https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Freeze, D. (2020, November 11). *Healthcare industry to spend $125 billion on cybersecurity from 2020 to 2025*. Cybercrime Magazine. Retrieved March 30, 2022, from https://cybersecurityventures.com/healthcare-industry-to-spend-125-billion-on-cybersecurity-from-2020-to-2025/

Freeze, D. (2021, April 27). *Cybercrime to cost the world $10.5 trillion annually by 2025*. Cybercrime Magazine. Retrieved March 30, 2022, from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Grose, T. (2021). *Cybersecurity Career Guide*. Start-Engineering. Robert F. Black Publisher.

Stouffer, W. by C. (n.d.). *115 cybersecurity statistics and trends you need to know in 2021*. Norton. Retrieved March 30, 2022, from https://us.norton.com/internetsecurity-emerging-threats-cyberthreat-trends-cybersecurity-threat-review.html

U.S. Bureau of Labor Statistics. (2022, February 15). *Economists : Occupational outlook handbook*. U.S. Bureau of Labor Statistics. Retrieved March 30, 2022, from https://www.bls.gov/ooh/life-physical-and-social-science/economists.htm