**Career Paper**

**Introduction**

When most people think of cybersecurity, they usually picture hackers, firewalls, or people working with code all day. But cybersecurity is about more than just technology it’s also about people. That’s where social science comes in. One cybersecurity career where social science really plays a big role is that of a cybersecurity policy analyst. These professionals help create and evaluate the rules and guidelines that keep our digital systems safe. But to do that effectively, they need to understand human behavior, society, and how policies affect different groups of people especially those who are often left out or harmed by tech systems. In this paper, I’ll talk about how social science concepts apply to the work of cybersecurity policy analysts and why it’s so important in their day to day jobs.

**Understanding Human Behavior**

One of the main ways policy analysts use social science is by looking at how people behave when it comes to cybersecurity. A lot of policies are only effective if people actually follow them. For example, requiring strong passwords or multi-factor authentication seems like a good idea, but what if it’s too complicated or annoying for people to use? Or what if someone doesn’t have access to a smartphone for two-factor authentication? Analysts use research from psychology and sociology to figure out what people are likely to do, not just what they *should* do. According to Anderson and Agarwal (2010), many users make decisions based on what’s easiest or fastest, not necessarily what’s most secure. If a policy doesn’t take that into account, it probably won’t work well in real life.

**Looking Out for Marginalized Communities**

Another really important part of this job is making sure cybersecurity policies don’t unfairly harm marginalized groups. That includes communities like immigrants, low-income families, and racial minorities. For example, facial recognition software has been shown to misidentify Black and Brown people more often than white people. If policy analysts don’t think about this, they could end up supporting technologies that lead to discrimination. Social science especially fields like sociology and critical race theory helps analysts understand how systems can be biased, even if they weren’t designed to be. Ruha Benjamin (2019) talks about how technology can reinforce racism in subtle but powerful ways. A good policy analyst uses this kind of research to make sure that cybersecurity solutions are fair and don’t make existing problems worse.

**Building Trust Through Communication**

Another big part of the job is communicating with different groups of people governments, companies, and the public. When there’s a cyber threat or a new policy being rolled out, it’s the analyst’s job to help explain what’s happening and why it matters. This is where psychology and communication studies come in. How you explain a risk makes a big difference in how people respond. Paul Slovic (1987) wrote about how people often don’t react to risks logically they react based on emotion or how the information is presented. If a message causes panic or seems dishonest, people might lose trust. This is especially important when working with communities that already feel targeted or left out by government and tech systems.

**Global Awareness and Ethics**

Cybersecurity policy doesn’t just affect one country it’s a global issue. Analysts often have to work with international partners or consider laws from other countries. That means understanding different cultures, political systems, and values. For example, privacy means very different things in the U.S. compared to the European Union. Analysts need to think about how policies will be understood and accepted in different parts of the world. They also have to make ethical decisions, like whether it’s okay to limit certain online speech to stop misinformation, or how much data a government should be allowed to collect on its citizens. These aren’t technical questions they’re social and political, and social science helps guide those choices.

**Conclusion**

In the end, cybersecurity policy analysts aren’t just writing rules about computers they’re making decisions that affect people’s lives. That’s why social science is such a big part of the job. Understanding human behavior, social inequality, communication, and ethics helps them create policies that are both effective and fair. As our world becomes more digital, we need cybersecurity professionals who can think beyond the tech and see the bigger picture. The more we bring in ideas from the social sciences, the better our policies and our digital future will be.

**Reference**

Slovic P. Perception of risk. Science. 1987 Apr 17;236(4799):280-5. doi: 10.1126/science.3563507. PMID: 3563507.

*What does a cyber policy analyst do? insights from a cybersecurity expert*. Cyber Insight. (2023, June 17). <https://cyberinsight.co/what-does-a-cyber-policy-analyst-do/>

 Anderson, Catherine L., and Ritu Agarwal. “Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions.” *MIS Quarterly*, vol. 34, no. 3, 2010, pp. 613–43. *JSTOR*, <https://doi.org/10.2307/25750694>. Accessed 14 Apr. 2025.

Longworth, Jackson. (2021). Benjamin Ruha (2019) Race After Technology: Abolitionist Tools for the New Jim Code. Medford: Polity Press. 172 pages. eISBN: 9781509526437. Science & Technology Studies. 34. 92-94. 10.23987/sts.102639.