

Isaiah Browne
CYSE 201S
November 22, 2024

Cybersecurity Career Focus: Cybersecurity Policy Analyst

BLUFF: In this paper, we'll look at how social science research and concepts inform the day-to-day work of cybersecurity policy analysts, with a focus on how these analysts interact with underrepresented groups and society at large.

An Analysis of Cybersecurity Policy Expertise

An organization's approach to cybersecurity is guided by policies that are analyzed, developed, and evaluated by a cybersecurity policy analyst. Risk assessments, security framework creation, and vulnerability management advice are all part of their job description. To develop fair, effective, and enforceable policies, Policy Analysts need to combine technical expertise with a knowledge of human behavior. This is in contrast to technical cybersecurity experts, who mostly concentrate on system security.

Understanding the social dynamics of security behaviors, the ethical implications of security decisions, and how people engage with technology are all crucial components of a policy analyst's job, which is largely impacted by social science research. An understanding of user behavior inside a system, the accessibility of security measures, and the impact of policies on vulnerable populations are all areas where social science principles play a crucial role in developing cybersecurity policies that prioritize both security and social welfare.

Social science research in making policy

The fact that humans are responsible for both the design and the use of technological systems is an essential part of cybersecurity policy. Hence, cybersecurity policy can't ignore human behavior in favor of a more technical approach. Psychological concepts pertaining to trust, decision-making, and risk perception are essential for a cybersecurity policy analyst. Psychology studies provide light on the mental processes that lead people to take unnecessary risks while interacting with sensitive information online, such as creating weak passwords or neglecting to install software updates. Why some groups of people might disobey security protocols despite knowing the hazards can be better understood by looking at social science research on cognitive biases like overconfidence and the bystander effect.

In order to create policies that are easy for users to comply with, cybersecurity experts rely on social psychology. Policies are less likely to be effective if they are overly complex or ignore the psychological obstacles faced by users. In order to safeguard systems while also conforming to people's real-world behaviors, policy analysts must employ behavioral science.

Social Structures and Sociology

The larger societal ramifications of cybersecurity regulations can be better understood by policy analysts with the aid of social science research. The field of sociology offers unique insights into the potential effects of cybersecurity measures on various social groups and societies. For example, analysts should think about the effects on low-income people, those with impairments, and minority ethnic groups when they draft cybersecurity regulations.

More fair and inclusive cybersecurity policy can be informed by research on social inequality. Take the fact that not everyone can afford or has the knowledge to follow security protocols as an example. It is important for a policy analyst to be cognizant of the "digital divide"—the difference between people with and without easy access to technology. By advocating for universal digital literacy, fair resource access, and cybersecurity protections, social science research can shed light on how policymakers can reduce these inequalities.

Social Responsibility and Ethics

When crafting cybersecurity policies, ethical issues must be front and center. In particular, in the domains of data privacy and surveillance, policy analysts have a responsibility to make sure that cybersecurity regulations do not violate civil liberties. When deciding how to strike a balance between security and individual rights, social science principles, particularly those from politics and ethics, can be helpful. For instance, there is a possibility that privacy rights will be violated by surveillance measures that aim to detect cybercriminal actions. Ethics in cybersecurity policymaking can be better understood by consulting social scientific literature on topics such as human rights, justice, and fairness.

It is the analyst's responsibility to think about how policies will affect society as a whole, making sure that disadvantaged or marginalized people aren't unintentionally hurt. Excessive data collecting from marginalized populations, for instance, may pave the way for discrimination or exploitation. Effective and socially responsible cybersecurity policies are guaranteed by social science research on systemic inequities.

Effects on Society and Marginalized Groups

Take cybersecurity education as an example. There may be a lack of resources for low-income families and rural regions when it comes to cybersecurity education and equipment. A policy analyst who is cognizant of these inequalities can push for legislation that guarantees underprivileged groups access to free cybersecurity education and tools. To make sure that security measures don't exclude certain populations, social science studies can reveal the specific obstacles these communities encounter.

In addition, in crafting cybersecurity rules, it is important to consider the potential effects of systemic discrimination on technological systems. Studies in sociology and politics, for example, can shed light on how algorithmic biases, for example, might have an outsized impact on

minority groups. In order to promote equality and justice in cybersecurity practices, policy analysts depend on this study to formulate regulations that reduce these biases.

Conclusion

The work of cybersecurity policy analysts is essential in determining how governments and businesses handle cybersecurity. This position requires technical knowledge, but it also relies significantly on social science ideas to develop inclusive, successful, and ethical policies. The formulation of policies that take into account the demands and vulnerabilities of marginalized groups is informed by social scientific research in psychology, sociology, ethics, and human behavior. This ensures that cybersecurity protections are accessible and equitable for everyone. In an increasingly digital environment, cybersecurity experts may use these ideas to build rules that protect networks while also promoting social responsibility and equity.

Sources:

Nicholas Patterson
STEM, & Nov 15, 2024
Oct 16, 2024, Nov 20, 2024
STEM. (n.d.). *Types of cybersecurity roles: Job growth and career paths*. Southern New Hampshire University.
<https://www.snhu.edu/about-us/newsroom/stem/cyber-security-roles>

Nicholas Patterson
STEM, & Nov 15, 2024
Oct 16, 2024, Nov 20, 2024
STEM. (n.d.). *Types of cybersecurity roles: Job growth and career paths*. Southern New Hampshire University.
<https://www.snhu.edu/about-us/newsroom/stem/cyber-security-roles>

Allen, B. (2024, August 13). *Council post: Minorities and the Cybersecurity Skills Gap*. Forbes.
<https://www.forbes.com/councils/forbestechcouncil/2022/09/30/minorities-and-the-cybersecurity-skills-gap/>