Cybersecurity Professional Career Paper: Information Security Analyst

Nicolas R. Stephens

School of Cybersecurity, Old Dominion University

CYSE 201S: Cybersecurity and the Social Sciences

Diwakar Yalpi

April 4th, 2026

Introduction

An Information Security Analyst is a cybersecurity professional who is dedicated to protecting data within an organization's computer systems, networks, and databases. Specifically, Information Security Analysts monitor networks, implement security safeguards and controls, investigate security incidents, and test and harden network devices. Information Security Analysts and general cybersecurity are vital in today's digitized society for a plethora of reasons, from businesses transitioning to cloud-based infrastructure to the increasing frequency of cyber-attacks. For these and many more reasons, cybersecurity is becoming the fastest-growing and most in-demand career path in the United States, with the Federal Bureau of Labor Statistics' 2025 report projecting a 29% increase in job growth for the Information Security Analyst position from 2024 to 2034, while the national average for job growth sits at 3%. However, as cybersecurity rises in popularity, so do misconceptions about the field, specifically, the idea that cybersecurity is a purely technical field. This notion is false, as it's estimated that 90% of all security incidents are attributable to human factors, rather than purely technical factors. As such, cybersecurity professionals often refer to humans as the weakest link in the defense of business-critical systems.

The purpose of this paper is to examine the position of an Information Security Analyst through a social science lens. This paper will discuss how Information Security Analysts rely on a foundational understanding of human behavior to better understand and mitigate risks and to develop operational standards for the businesses in which they are employed. This paper will specifically cover in-class concepts, such as relativism, neutralization theory, and human factors, and apply them to an Information Security Analyst's daily routines of ensuring adherence to the C.I.A. Triad. Furthermore, this paper will explore professional interactions with marginalized

groups to contribute to the stability of critical infrastructure. Ultimately, this paper aims to demonstrate that cybersecurity is a complex social science process that requires a blend of technical and social knowledge to protect real-world assets.

Social science principles

Information Security Analysts rely on a mixture of criminology, psychology, and sociology to better understand the behaviors behind human-related cybersecurity incidents. By applying principles from these social science fields, analysts can better understand the human element involved in cyber incidents to predict and mitigate future incidents.

Social science principles are integrated into the daily routines of Information Security Analysts as they study how humans interact with technology and the human factors that lead to security incidents. Specifically, Analysts can apply the theory of relativism, recognizing that the technology they deploy is part of a larger social system in which technological changes can influence organizational behavior and business policy. By focusing on human-centered design, Information Security Analysts can ensure that technological deployments and protocols are compatible with human use while considering human limitations. This prevents common scenarios in which employees circumvent security safeguards and controls for convenience.

Additionally, cybersecurity professionals use social science principles to develop effective cybersecurity awareness and education training for employees. By using social science principles in training material, cybersecurity professionals are able to design training that considers the cognitive behaviors and biases of employees, such as optimism bias, or the tendency to believe that one will not be affected by cybercrime. Through an in-depth understanding of these

psychological patterns, analysts can configure a human firewall, grounded in the principle that human behavior is the primary deterrent to cybercrime.

Application of Key Concepts

Beyond the general principles and applications of social science principles, Information Security Analysts utilize specific frameworks to optimize security practices. Analysts can apply neutralization theory to assess risks from external to internal threats, specifically by examining how offending individuals rationalize their misconduct through methods such as denial of responsibility or denial of injury. On the other hand, analysts must ensure compliance with standardized frameworks, such as the NIST Risk Management Framework (RMF). The NIST Risk Management Framework enables professionals to categorize their systems and select appropriate security controls to secure them. Another foundational framework is the C.I.A. Triad, also known as Confidentiality, Integrity, and Availability. This framework provides a methodology to maintain data security, trustworthiness, and authorized access. These frameworks provide user-friendly, secure, human-centered designs that allow for easy implementation and are less likely to be circumvented by inconvenienced employees. These frameworks help cybersecurity professionals, especially Information Security Analysts, manage mandatory compliance procedures and ensure that implemented controls are human-focused and secure.

Marginalization

Information Security Analysts and cybersecurity professionals in general should recognize that the field has significant diversity gaps, with the workforce being 72.6% white. Marginalized groups, particularly people of color and women, face four primary barriers to

entering the cybersecurity field. Lack of formal cybersecurity education in school curriculum, less diverse interview panels, scarcity of diversity training, and cultural biases. For example, approximately 77% of individuals report never having received cybersecurity training in their formal education, and colored startups receive less than 1% of venture capital investments, creating systemic hurdles on their path to success (All Together, 2021).

Information Security Analysts are making efforts to address these barriers. For example, the Making Space Pledge aims to get businesses to diversify hiring. Women in Cybersecurity (WiCys) and Blacks in Cybersecurity (BIC) aim to create inclusive environments for marginalized groups as they navigate the cybersecurity industry.

Career Connection to Society

Information Security Analysts contribute significantly to the safety and stability of societal infrastructure, particularly in the healthcare and financial sectors. Information Security Analysts protect sensitive personal and financial information, which is essential in modern society. Consumers need to maintain trust in the organizations that hold their personal information, or those organizations could lose business, especially in the case of a data breach where millions of consumers could be affected. Information Security Analysts are a vital part of the defense against the growing cybercrime industry, which is already costing the global economy trillions of U.S. dollars and is only rising. Analysts aid and ensure compliance with public policies, such as the EU General Data Protection Regulation (GDPR) and the Computer Fraud and Abuse Act (CFAA), which protect the human right to privacy by requiring companies to take certain steps to prevent personal information from becoming public.

Scholarly Journal Articles

Source 1. Nobles, C. (2018). Botching human factors in cybersecurity in business organizations.

This scholarly article highlights that approximately 90% of cybersecurity incidents are caused by human error and argues that traditional employee training is ineffective because it fails to modify actual employee behavior. This article is relevant to this paper because it supports a human-centered approach to cybersecurity, which is highly applicable to Information Security Analysts.

Source 2. Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors.

This cybersecurity study analyzes how gender affects cybersecurity behaviors and beliefs. The study is clear in demonstrating how disparities between demographics manifest in the self-efficacy of professionals, which reinforces the aforementioned initiatives like WiCys, BIC, and the Making Space Pledge in bridging the gender and race gap in cybersecurity.

Source 3. Moore, T. (2010). The Economics of Cybersecurity: Principles and Policy Options.

This study examined how public policy and economic principles manage risks in the digital world. This study also contributes to understanding the career connections to society by depicting the work of Information Security Analysts as a social and economic process that maintains the stability of critical infrastructure.

References

All Together. (2021, October 21). 4 barriers to diversity in cybersecurity and how to address them. All Together. https://alltogether.swe.org/2021/10/4-barriers-to-diversity-in-cybersecurity-and-how-to-address-them/

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. https://doi.org/10.1016/j.chb.2016.12.040

Moore, T. (2010). The Economics of Cybersecurity: Principles and policy options. *International Journal of Critical Infrastructure Protection*, *3*(3–4), 103–117. https://doi.org/10.1016/j.ijcip.2010.10.002

Nobles, C. (2018). Botching human factors in cybersecurity in business organizations. *HOLISTICA – Journal of Business and Public Administration*, *9*(3). https://doi.org/10.2478/hjbpa-2018-0024

U.S. Bureau of Labor Statistics. (2025, August 28). *Information security analysts*. U.S. Bureau of Labor Statistics. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm