

Policy Analysis Paper 4: The Social Implications of ZTA

Jacob Rivera

School of Cybersecurity, Old Dominion University

CYSE425W: Cybersecurity Strategy and Policy

Dr. Hamza Demirel

April 12, 2026

Introduction

In the previous two policy analysis papers, it is revealed that Zero Trust Architecture (ZTA) is a modern developing cybersecurity strategy that replaces the previous perimeter security model by requiring all users to be verified every time they access a system. The political and ethical implications of ZTA were also explored. Now, we will be looking at the social side of ZTA. It is safe to say that all Cybersecurity policies affect people, and it is important to understand how society has influenced ZTA and how ZTA has affected society in return. This paper will go through the social factors that led to the creation of zero trust, the social consequences that come with the use of it, and the cultural/subcultural influences that shaped the strategy.

Social Factors That Led to the Development of ZTA

ZTA was not developed just because of technical problems relating to perimeter based security. There were social factors that played a part in it as well. For example, the way people live and work in their daily lives heavily contributed to the upbringing of zero trust. One of the biggest factors was the growth of remote work. According to Michael Blanding, companies that needed more talent from different regions of the country offered remote work as a means to tap into additional markets and talent pools (2024). Combined with the COVID-19 pandemic, almost every office-based organization was forced to shift to remote work. This meant that employees were accessing company systems from their own personal devices and WiFi instead of from their usual secure office network. Gambo and Almulhem point out that the traditional perimeter-based security model stopped working well once employees were no longer operating inside of the network (2025). Another social factor that led to the development of ZTA was the rise of bring-your-own-device (BYOD) policies. Similar to remote work, this would allow employees to use their own personal laptops and phones. Around the same time remote work and BYOD

became popular, cloud computing was on the rise as well. This meant all company data could be stored and accessed online rather than on a single server. All of these social factors combined made the perimeter based model less reliable and cybersecurity agencies ultimately pushed for the development of a new cybersecurity model.

Social Consequences of ZTA

As social changes caused the establishment of ZTA, the adoption of it also created social changes of its own, especially in the workplace. One of the most noticeable consequences is the decrease of trust between the employees and their employers. It is recorded that employees generally have mixed feelings about zero trust. According to a journal article published by ISACA, the author states that “in a zero trust environment, management explicitly and implicitly takes the stance that the trustee (the employee) is neither dependable nor trustworthy” (Johnson, 2020). While they do support the security benefits ZTA offers, employees feel uncomfortable having to be constantly monitored and verified. Also, on top of being uncomfortable, the whole verification process can be tedious with how repetitive it is. It can cause workplace friction. Overall, this negatively impacts work culture.

Cultural and Subcultural Influences on ZTA

In the field of cybersecurity, there is a common mindset revolving around caution and skepticism. After all, people need to be wary of their actions in order to keep the best safety practices. This mindset would directly be involved in the influence of ZTA’s core idea of “never trust, always verify” (Kang et al. 2023). ZTA has been heavily pushed by the United States governments according to mandates discussed in Executive Order 14028 in 2021 and the Office of Management and Budget’s Memorandum M-22-09. It is clear that the focus has been more on national security and protecting critical infrastructure over the value of individual privacy. Although this can create some tension on the topic of ZTA, most people would agree that protecting national security is a

necessary priority. In the United States, people would generally value personal privacy and freedom, but with major cybersecurity incidents like the SolarWinds attack, the consequences show that weak security affects everyone. Catastrophic events like this shape public opinion toward accepting strict security measures like ZTA.

Forensic Lab Floor Plan

References

- Blanding, M. (2024, September 19). *Global Talent, Local Obstacles: Why Time Zones Matter in Remote Work*. Harvard Business School.
<https://www.library.hbs.edu/working-knowledge/global-talent-local-obstacles-why-time-zones-matter-in-remote-work>
- Gambo, M., & Almulhem, A. (2025). *Zero Trust Architecture: A Systematic Literature Review*.
<https://arxiv.org/pdf/2503.11659>
- Johnson, G. (2020, October 30). *The Unintended Consequences of Zero Trust on Enterprise Culture*. ISACA.
<https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/the-unintended-consequences-of-zero-trust-on-enterprise-culture>
- Kang, H., Liu, G., Wang, Q., Meng, L., & Liu, J. (2023). Theory and Application of Zero Trust Security: A Brief Survey. *Entropy*, 25(12). <https://doi.org/10.3390/e25121595>