Ethical Implications of Zero Trust Cybersecurity Policy

Jaden Walker

CYSE-425W

Dr. Shideh Yavary Mehr

7/1/2025

Implementing Zero Trust strategies into your cybersecurity framework while making sure you mandate ethical practices is no small feat. The organization will undergo extensive change because ethics are related to privacy, security, and individual rights. The fundamentals challenges the status quo because it has the universal principle of "never trust, always verify," which means all users and devices are required to be continuously authenticated and validated before gaining access to network resources (NIST, 2020). While this changes the security landscape substantially, it also introduces arguments and concerns about the ethicality of such changes.

A primary ethical consideration is the balance between enhanced security and individual privacy. By continuously verifying identities and actions, Zero Trust models necessitate detailed monitoring and data collection about user behaviors, potentially infringing on individual privacy rights (Health Information Technology Solutions, 2023). Continuous surveillance, even if it was meant to protect assets and information, may foster an environment of distrust and anxiety among users who may feel constantly scrutinized. Extensive monitoring can also lead to the abuse of collected data, which is why there needs to be safeguards and strict policies around the protection of personal data. A great counter argument for these concerns would be that users should not be conducting personal business on workstations, because that adds an additional risk to the enterprise due to human error and general negligence.

Another Ethical consideration would be the incurred cost of implementing Zero Trust. On the one hand, the primary benefit of Zero Trust would be the reduction of breaches, ransomware attacks, and unauthorized access by shrinking the attack surface of threat actors. (CISA, 2023). The Cons would be the investment into Infrastructure changes and the training of personnel. But I would argue the cost of training and infrastructure changes will happen whether you implement changes or not. Companies have clients that they support, and a silent responsibility is to always

stay up to date in order to provide the best service and continue the client relationship. So ethically, this raises concerns about equity and access to security resources. Organizations unable to afford sophisticated Zero Trust frameworks will become vulnerable and likely will lose their market share to organizations with more funding and superior cybersecurity policies.

Additionally, Zero Trust policies can impact individual autonomy and rights. Employees or users might see a decrease in productivity due to frequent authentication requirements or restricted access to essential resources, which potentially could challenge their ability to perform job functions efficiently (Health Information Technology Solutions, 2023). The operational constraints this might cause are a great reason to make sure that Zero Trust policies are curated to each sector and organization. If there are concerns about the time it takes to manually put in a username and password each time you want to access a resource, organizations could look into having access tokens for each employee. The Department of Defense does this with CAC cards, but organizations could create their own tokens with 6-8 digit passwords, this way you can satisfy the security requirements while keeping a streamlined workflow.

In conclusion, while Zero Trust cybersecurity significantly enhances security posture, it introduces complex ethical implications surrounding privacy, equity, autonomy, and rights protection. The implementation of Zero Trust requires a deliberate, transparent, standardized, and accountable approach to balance security with individual rights effectively.

References:

- LLC, P. F. S. (2025, March 25). Balancing Ethical & Privacy concerns with Zero trust. Health Information Technology Solutions. https://healthinformationtechnologysolutions.com/balancing-ethical-privacy-concerns-with-zero-trust/
- Zero trust maturity model: CISA. Cybersecurity and Infrastructure Security Agency CISA. (n.d.). https://www.cisa.gov/zero-trust-maturity-model
- Kerman, A. (2025, March 6). Zero trust cybersecurity: “never trust, always verify.” NIST. https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify