Dylan Shaver

Professor Duvall

CYSE 200T

April 22, 2025

Cybersecurity Resilience: Balancing the CIA Triad and Human Behavior

BLUF: This paper argues that long-term cybersecurity resilience requires integrating ethical, inclusive policies with both human and technical safeguards. Using the Responsible Cyber-Infrastructure Development lens, I contend that we must reshape future cybersecurity strategies to emphasize both the CIA triad and the human factor. This dual approach strengthens digital systems and empowers users as vital partners in cybersecurity.

Cyber Policy Foundations

As digital systems grow in complexity, it becomes ethically urgent to craft cybersecurity policies that serve not only organizational goals but also societal well-being. The Responsible Cyber-Infrastructure Development perspective insists that digital infrastructures are inclusive, transparent, and supportive of all users. This lens asks us to consider not just whether a system is secure, but whether it was built with the user in mind, avoiding punitive models that blame human error while ignoring structural design flaws. [7] Cybersecurity policies informed by this philosophy should prioritize ethical foresight, user education, and equitable access to security resources. It also urges us to ask: Who is left behind when policies prioritize automation over inclusion? Small businesses, marginalized communities, and underfunded public institutions often lack access to elite security infrastructure. Ethical foresight means designing policies that close this gap. For instance, future cybersecurity laws could mandate open-source training platforms, or subsidize security audits for at-risk non-profits and public schools. These efforts reflect an understanding that cybersecurity is a public good, not just a private luxury. In the following section, we examine the CIA Triad as a technical model that, when guided by ethical policy, lays the groundwork for resilient cybersecurity infrastructure.

CIA Triad

[2c] The CIA Triad, which stands for confidentiality, integrity, and availability, is foundational to any cybersecurity strategy. Confidentiality ensures that only authorized individuals access data, while integrity safeguards the accuracy and reliability of information. Availability ensures systems are accessible to users when needed (Chai, 2022). Together, these three principles form the backbone of secure information systems. For instance, encrypting medical records protects confidentiality, while implementing version controls and regular backups maintains integrity. Redundant servers and uptime protocols protect availability during emergencies or attacks.

Authentication and authorization are equally essential. Authentication verifies a user's identity, and authorization governs their access privileges. In real-world terms, a

hospital's IT system might authenticate a nurse via password and biometrics, then authorize access to only the patient files relevant to their unit (Okta, 2024). Without clear role-based access controls, breaches become more likely. Confidentiality is not just a matter of encryption; it's about setting clear policies and communicating those policies to users. For example, healthcare organizations using role-based access must ensure frontline workers know exactly what data they're authorized to see. Integrity extends beyond cryptographic hashing; it also involves structured management processes and audit logging to track who alters data. As for availability, organizations must consider disaster recovery, denial-of-service protections, and redundancy. These aren't just IT issues; they are business continuity mandates. Moreover, the triad can be seen not just as a checklist, but as a set of design values that guide how systems should be built and maintained. A system that is highly confidential but not accessible fails its users just as much as one that is open but lacks integrity. Thus, policies and technical teams must continuously reassess trade-offs across the triad in real time, particularly as new technologies like cloud computing, remote work tools, and AI introduce new risks.

Human Factor

[4] Now let's look at how human behavior intersects with cybersecurity in ways that technology alone cannot address. Despite the strength of technical frameworks, like the CIA triad, human error remains the leading cause of data breaches. [5] According to Verizon's 2023 Data Breach Investigations Report found that social engineering attacks and mistakes, such as falling for phishing emails or mishandling sensitive credentials, continue to be among the most common threats (Verizon, 2023). These errors are not always due to negligence but often stem from unclear policies, lack of training, or system design that fail to support users. To mitigate this, organizations must evolve from blaming users to focusing on cybersecurity strategies that support them. A 60/40 investment model—60% of financial resources toward employee education and 40% toward technical tools could provide a balanced, effective approach. Training efforts might include phishing simulations, interactive modules, and policy walkthroughs tailored to each role within an organization. From a social science perspective, this reveals a critical insight: users are not merely endpoints but active participants in the security environment. Psychology shows us that behavioral change requires reinforcement and consistency. Security training must go beyond one-time sessions, and it should be continuous, relevant, and updated regularly to reflect emerging threats. Cultural reinforcement, such as recognizing good security habits or including cybersecurity awareness in performance evaluations, strengthens this approach.

Integration of Systems and People

Which leads me to my next topic, the synergy between human behavior and technical defense. Even with best-in-class tools like EDR systems, multi-factor authentication, or firewalls, security can still fail due to human oversight. That's why it's crucial that training and tools operate in tandem. Cybersecurity investments must prioritize tools that not only detect threats but also guide users with intuitive interfaces and just-in-time security prompts.

According to Smith and Lee (2022), layering human-centered design with technical defense reduces both accidental and malicious insider threats. Policies must reflect this by integrating security into everyday workflows, not as a burden, but as a shared responsibility. Encouraging a security-positive culture, backed by leadership support, makes this integration effective. For example, a bank might deploy MFA to protect client

accounts, but if clients are unaware of phishing scams that bypass MFA via social engineering, the tool is undercut. Thus, user engagement must be embedded in the policy design process. Involving users in the creation of cybersecurity policies fosters buy-in, reduces resistance, and surfaces blind spots that technologists might miss.

Conclusion

The viability of cybersecurity depends not just on technical innovation but on ethical and inclusive policy development. Through the Responsible Cyber-Infrastructure Development lens, this paper has argued that we must recognize the social implications of technical systems like the CIA triad while simultaneously elevating the role of human factors in our defense strategies. While some may argue for full automation or zero-trust models that remove discretion from users, such approaches risk alienating the very people who must interact with these systems every day.

Ambivalence remains over how much responsibility should rest with users versus systems. Still, by acknowledging that both people and protocols matter, we can create cybersecurity environments that are resilient and sustainable. [6] Cybersecurity isn't about keeping systems safe; it's about keeping people safe within those systems. Another potential objection is the scalability of human-focused approaches. Can large corporations realistically train tens of thousands of workers without incurring excessive costs? While this is a valid concern, the answer lies in hybrid delivery methods such as blending automated modules with live training and tailoring content. Also, investing in people often pays off in lower incident rates and stronger internal accountability.

References

Chai, W. (2022). What is the CIA triad? Definition, explanation, examples. TechTarget. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Okta. (2024). Authentication vs. authorization. https://www.okta.com/identity-101/authentication-vs-authorization/

Smith, R., & Lee, J. (2022). Cybersecurity strategy in resource-constrained environments. Cyber Defense Press.

Verizon. (2023). Data breach investigations report. https://www.verizon.com/business/resources/reports/dbir/