Managed Trust and Operational Resilience While Implementing Zero-Trust Architecture in a Multi-Stakeholder Telecommunications Organization

Guy E. Toibin *, Yotam Lurie, Shlomo Mark

Posted Date: 17 March 2026

doi: 10.20944/preprints202603.1371.v1

Keywords: zero-trust architecture; telecommunications infrastructure; organizational trust; technology acceptance model; operational resilience; cybersecurity governance; multi-stakeholder systems; explainable artificial intelligence

 doi:10.20944/preprints202603.1371.v1

Article

Managed Trust and Operational Resilience While implementing Zero-Trust Architecture in a Multi-Stakeholder Telecommunications Organization

Guy E. Toibin [1,*], Yotam Lurie [1] and Shlomo Mark [2]

[1] Guilford Glazer Faculty of Business and Management, Ben-Gurion University of the Negev, P.O. Box 653, Beer-Sheva, 84105, Israel

[2] Software engineering department, SCE - Shamoun College of Engineering, 84 Jabotinsky St. Ashdod, 77245 Israel

* Correspondence: toibing@post.bgu.ac.il; Tel.: +972.545.600.200

Abstract

Telecommunication networks operate as highly distributed, multi-vendor, and mission-critical infrastructures, making them prime targets for sophisticated cyber threats. As networks evolve toward cloud-native, virtualized, and software-defined architectures, traditional perimeter-based security models have become insufficient. Zero-Trust Architecture (ZTA) has therefore emerged as a key security paradigm in telecommunications, enabling continuous verification, fine-grained access control, and improved protection of network and information assets. While ZTA strengthens technical security and operational resilience, its large-scale deployment introduces significant socio-technical and governance challenges that extend beyond network engineering. This study examines the implementation of ZTA in a multinational telecommunications infrastructure organization using a four-wave longitudinal design (2020 - 2023). Drawing on an extended Technology Acceptance Model incorporating Perceived Trust, we analyze employee perceptions of productivity, ease of use, usefulness, and trust before and after ZTA deployment, and following a structured governance intervention. Results reveal a substantial decline in the composite TAM index following ZTA enforcement (−25%, Cohen's d = 1.12), with no meaningful spontaneous recovery over time (d = 0.08). A Communication Campaign emphasizing transparency and stakeholder engagement produced a partial but incomplete recovery (d ~ 0.52), indicating that trust erosion under Zero-Trust conditions is measurable and contingent upon governance design rather than technological determinism. The findings demonstrate that ZTA functions not merely as a technical safeguard but as a socio-technical governance mechanism that restructures organizational trust. The study advances a Proactive Trust Management framework tailored to telecommunications environments, integrating security enforcement with transparency, participatory oversight, and ethical calibration to sustain operational resilience in cloud-native infrastructures.

Keywords: zero-trust architecture; telecommunications infrastructure; organizational trust; technology acceptance model; operational resilience; cybersecurity governance; multi-stakeholder systems; explainable artificial intelligence

1. Introduction

1.1. Technological Transformation and Trust

Technological changes have profound and significant effects on individuals and society. One such change examined in this research is the impact these technologies have had on the way trust is embedded in organizational life. While trust plays a central role in all intra- and inter-organizational life, recent disruptive technological trends are changing how trust is embedded in organizational life. Trust is no longer just an interpersonal relationship between individuals but is increasingly

 doi:10.20944/preprints202603.1371.v1

embedded in technological systems. Within this context, the Fourth Industrial Revolution [1] leverages these technological trends to drive changes in the economic, social and interpersonal relations between stakeholders who are now expected to work together through the use of a trustworthy, reliable IT environment. Moreover, recent disruptive technologies have enhanced the use of industry clouds; these industry clouds are accelerating cloud deployment and provide significant benefits to a variety of businesses by altering the economics of corporate agility, stakeholders' collaboration, speed, and process differentiation. While advanced digital technologies are changing the nature of trust, shaping the possibilities for human interactions, enabling more open, flexible, and scalable organizations, this is also a breeding ground for cybersecurity threats that force organizations to adopt and move to practices and approaches that ultimately challenge trust and transform it. In telecommunications infrastructure environments, characterized by cloud-native architectures, distributed network functions and multi-vendor operational dependencies, cybersecurity failures can propagate systemic risk far beyond organizational boundaries.

1.2. Conceptual and Terminological Framework

To delineate the conceptual boundaries of this research, it is essential to explicate several foundational constructs, specifically, disruptive technology, cloud computing, industry clouds and Trustworthy AI. Within contemporary organizational ecosystems, these constructs are not discrete; rather, they are thematically and operationally interwoven, collectively reshaping the structural, cultural, and ethical dimensions of organizational life, and thereby reconfiguring the nature and meaning of work [2–5]. Technology as a transformative driver of socio-economic and organizational change is not a novel phenomenon; however, the advent of disruptive technologies has become a defining feature of today's economic systems, significantly shaping competition and the way organizations operate. Disruptive Technology refers to a product or a service that fundamentally changes how a market or industry functions [3,6]. Christensen, Raynor and McDonald [7] identified key conditions for recognizing when an invention disrupts the market: serving previously underserved consumers, expanding beyond existing boundaries, and reaching a level of maturity that enables widespread adoption. An essential disruptive milestone in the co-evolution of technological infrastructure and organizational forms was the emergence of cloud technology. Cloud technology refers to the paradigm wherein all information technology (IT) capabilities; including computing power, infrastructure, applications, business processes, and collaborations are provisioned as on-demand service via the internet [8]. The primary business drivers motivating organizations adopting cloud technology include elastic scalability in resource allocation, accelerated solution deployment within compressed timeframes, cross-platform compatibility, and enhanced predictability of project deliverables [9]. Cloud technology has facilitated the transition of organizational IT from hardware-centric architectures of the '70s, through the software-dominated system of the 80's and 90's, to the present era characterized by socio-technical integration, wherein computing is intentionally designed to meet both individual psychological needs and collective, community-oriented objectives [5]. To fully realize the strategic potential of cloud technology, organizations require a robust and well-governed cloud ecosystem underpinned by established best practices [9]. Such an environment enables and promotes organizational agility, flexibility, availability, accessibility, and innovation [10]. Today's organization increasingly expects IT infrastructures to facilitate seamless access to diverse digital ecosystems, ranging from professional communities and social networks to large-scale data repositories, artificial intelligence capabilities, robotic process automation, and emergent computational applications. Simultaneously, **the imperatives of** Cybersecurity, regulatory compliance, fairness, and transparency render these expectations more challenging – complex and demanding. Cloud computing is thus not solely a technological shift but a transformation in the organizational logics governing IT deployment and governance. Gartner [11] predicted that, as the technology matured, cloud computing would become a critical enabler of cross-sectoral innovation, a forecast borne out during the Covid-19 pandemic, when unprecedented social distancing mandates catalyzed demand for social computing (Zoom,

 doi:10.20944/preprints202603.1371.v1

Teams, etc.), e-commerce, and AI solutions. Cloud-based technological solutions are disruptive in that they supplant both stand-alone personal computing and centralized mainframe architectures, thereby challenging entrenched technological and organizational norms [7]. Beyond altering technical infrastructures, cloud computing reshapes workplace values and organizational culture.

When an organization migrates its operations to the cloud, this transition extends beyond the relocation of data and software systems (CRM, ERP, etc.) to bear upon organizational culture, communicative practices, and value systems. This shift can initially diminish perceived individual autonomy, as work in a cloud environment is contingent upon infrastructural attributes such as transparency, resource-sharing, and remote accessibility [10]. Such conditions can foster a heightened dependence on external technological actors and amplify concerns regarding the potential misuse or overexposure of both personal and professional information. Moreover, cloud technology operates as a double-edged phenomenon [12]: while expanding informational reach and operational capability, it simultaneously amplifies exposure to cybersecurity threats.

A notable emerging trajectory in this domain is the evolution toward industry-specific cloud ecosystems, commonly referred to as "industry clouds". Industry Clouds is a term used to describe cloud systems that are significantly customized to meet the needs of a given industry, accommodating business, operational, legal, regulatory, and security requirements (Techopedia, 2021). Since 2022, industry clouds have gained momentum across multiple sectors, including banking, healthcare, manufacturing, and government services. They combine cloud services, applications, tools, and technologies with industry-specific workflows, APIs, and other tailored solutions. At the platform layer, strategic partners may offer accelerators to extend functional capabilities; at the SaaS layer, user experiences and workflows are calibrated to domain-specific processes. These tailored environments are particularly advantageous for highly regulated industries, where they address systemic challenges in security, compliance, and operational governance while enabling vertical integration and strategic differentiation. Additional benefits include standardized configurations, greater operational efficiency, closer customer engagement, targeted investment, and integrated solutions.

Several studies identify AI systems as key enablers for managing ZTA [13,14]. Related research also highlights their role in enhancing industry clouds environments [15]. Such systems are described as capable of iteratively improving their performance based on the data they acquire [15]. They integrate multiple technologies that enable machines to perceive, act, and learn with capabilities resemble human-like intelligence [16,17]. Machine learning (ML), a subset of AI, defined as the ability of system to improve and adapt from experience without explicit reprogramming [18,19]. As algorithms become more complex and operate across diverse domains, concerns have grown among regulators, the public, and users regarding undetected biases, errors, and unfounded assumptions that may influence automated decision-making. In such contexts, explainability is considered essential for ensuring that AI driven process are fair, accountable, and transparent [20–22]. Two main approaches to making AI explainable are identified: Global explanation techniques, which provide an overview of an algorithm's general behavior, and Local explanation techniques, which clarify the reasoning behind specific predictions or outputs [23,24]. Transparency, as a defining characteristic of Explainable AI (XAI), refers to processes and methods designed to make an AI system's purpose, logics, and decision-making comprehensible to stakeholder [25].

1.3. Zero-Trust Architecture in Cloud-Native and Telecommunications Network Environments

"Zero-Trust" is an innovative strategic security mechanism that was introduced in recent years to provide fully automated security for people, devices, things and networks. The basic idea of ZTA is that all users, devices, applications, and packets, i.e., entities, should never be trusted by default, regardless of whether such entities are inside or outside a secure network [26]. In telecommunications infrastructure environments, Zero-Trust principles are increasingly applied to protect access to network functions, source code repositories, CI/CD pipelines, configuration management systems, and operational platforms spanning multiple vendors and organizational boundaries. In practice,

 doi:10.20944/preprints202603.1371.v1

ZTA is a security model designed to ensure that all entities are authenticated, verified, and granted only the minimal privileges appropriate in the current context. One of the goals of ZTA is to optimize security architectures and technologies for future flexibility [27]. For that, the term ZTA was coined [28] to describe an approach that optimizes cybersecurity architecture in organizations that use multiple integrated technology solutions aligned with zero-trust principles. This research examines the socio-ethical dimensions of the organizational changes resulting from the demands of cybersecurity and the adoption of the ZTA approach, looking at user-related issues, the evolution of intra- and inter-organizational trust, and the implications for individuals and other stakeholders when organizations adopt ZTA, with cybersecurity as the primary driver. High-profile cyber-attacks, such as the NotPetya Attack in 2017, highlighted the limitations of perimeter-based security and underscored the need for advanced mechanisms to protect networks with blurred or absent boundaries [29,30]. The concept of ZTA addresses these challenges. While no single definition exists, ZTA is generally summarized by the principle of "Never Trust, Always Verify" [27,31–33] replacing the traditional "Trust but Verify" approach [34,35]. In this research, ZTA is not examined solely as a technical model but as a socio-ethical phenomenon that reshapes organizational trust, collaboration, and autonomy. Telecommunications security governance increasingly aligns Zero-Trust principles with industry standards such as ETSI and 3GPP security frameworks, reflecting the convergence of network, software, and organizational trust controls.

1.4. Cybersecurity and ZTA at Telecommunication Infrastructure Providers

Telecommunication infrastructure providers operate at the intersection of critical digital services, large-scale distributed systems, and high levels of systemic risk. Unlike consumer-facing service operators, infrastructure and equipment providers form the technological backbone of telecommunications networks deployed across multiple customers, regions, and operational environments. As a result, successful cyber intrusions at this layer may propagate harm far beyond a single organization. For example, the prolonged breach disclosed by Ribbon Communications (Ribbon Communications, 2023) a major telecommunications infrastructure provider demonstrated how attackers were able to persist undetected within core systems for an extended period, highlighting both the attractiveness of telecom infrastructure targets and the potential downstream impact on network reliability and trust. Such incidents underscore why infrastructure-oriented telecommunications firms have become early and intensive adopters of advanced cybersecurity models such as Zero-Trust Architecture (ZTA). At the same time, telecommunications infrastructure providers are typically high-technology organizations with strong research and development (R&D) capabilities that rely on flexibility, rapid experimentation, and seamless collaboration across engineering teams. From this perspective, rigid enforcement of zero-trust controls such as continuous authentication, segmented access, and restrictive permission models may be experienced as disruptive, slowing development cycles and constraining innovation. This creates a fundamental two-edged tension: while cyberattacks on telecommunications infrastructure can generate severe and systemic harm, poorly managed Zero-Trust implementations risk undermining the organizational capabilities required to sustain technological leadership and operational excellence.

Addressing this tension requires treating Zero Trust not as a purely technical security deployment, but as a managed organizational and operational transition. The transition to ZTA reshapes working practices, alters established trust relationships, and reconfigures interactions among security teams, network operations, IT, and R&D units. Consequently, successful implementation depends on active stakeholder involvement, managerial coordination, and continuous governance throughout the transition process. Effective Zero-Trust adoption requires mechanisms for listening to affected stakeholders, receiving structured feedback, and adjusting controls in response to operational realities. Moreover, expectations must be established clearly from the outset through transparent policies and value-based ethical guidelines endorsed at the board level. By articulating principles such as proportionality, transparency, accountability, and respect for professional autonomy, boards and senior management can provide a normative foundation that

 doi:10.20944/preprints202603.1371.v1

guides both technical design choices and managerial actions. In this way, Zero Trust can be implemented "right the first time," mitigating not only external cyber threats but also the internal operational and trust-related risks that may otherwise arise from the security controls themselves.

Socio-Ethical Implications of Disruptive Security Architectures Organizations face a fundamental dilemma in adopting ZTA; they require information systems for operational efficiency and strategic decision-making, yet these same systems introduce new vulnerabilities and ethical challenges. Technology systems automate numerous organizational processes and generate large volumes of data [36]. Much of this data originates from internal units, including marketing, finance, production and engineering, project management, OB and more, though external sources, such as market and social data, increasingly contribute to organizational insights [37]. Cloud computing, in its various forms, has transformed how organizations collect, process, store, maintain and secure information. Consequently, it reshapes organizational decision-making by increasing the accessibility and visibility of information at relatively low cost. Analytics enables actionable insights and supports the integration of big data, artificial intelligence into operational and strategic processes [12]. However, this transformation introduces significant concerns, including cyber-attack risks, loss of trust, threats to employee autonomy, surveillance, and potential impacts on satisfaction, performance and motivations [38,39]. The traditional "hard-shell" information security model assumes organizational control over IT infrastructure and clear perimeters. This model erodes when organizations rely on cloud services, share infrastructure, or when personnel operate across multiple organizations [40]. The shift toward collaborative, cloud-enabled environments necessitates perimeter abstraction, where strict boundaries are replaced by flexible, trust-managed access [41,42]. Two points are critical for understanding ZTA. First, "Zero Trust" is not merely a technology; it is a strategic approach that incorporates security mechanisms, technological tools, architectures and organizational policies to protect users, devices, things, data, applications and networks [43]. Second, ZTA operationalizes the management of trust, ensuring that no access or interaction is assumed to be inherently safe. Trust must be explicit, verified, and continuously evaluated, thereby reducing the risks associated with blind or implicit trust [44]. From an ethical perspective, ZTA introduces trade-offs alongside its cybersecurity benefits. While enabling secure inter- and intra-organizational collaboration in cloud and multi-stakeholder environments, it may constrain autonomy, complicate collaborative processes, and increase oversight of user actions. These considerations highlight the need for organizations to carefully manage trust policies and security controls to balance security with ethical and operational values. In telecommunications infrastructure providers, these socio-ethical tensions are intensified by the need for continuous availability, rapid fault resolution, and close coordination between security, network operations, and R&D teams.

1.5. Application-Layer Security Measures in ZTA

Although ZTA is often discussed in terms of identity verification, network segmentation, and continuous monitoring, its principles also extend to the application layer. One way to reinforce the "never trust, always verify" mindset is to make software components themselves more resistant to interpretation and manipulation. Code obfuscation refers to the deliberate transformation of source or executable code into a form that maintains the program's functionality while making it significantly harder to analyse, reverse-engineer, or misuse. It is widely employed in the software industry, particularly in research and development (R&D) contexts and security-sensitive applications, to protect intellectual property, conceal proprietary algorithms, and deter malicious actors [45,46]. Within telecommunications infrastructure providers, such techniques are commonly applied to network functions, embedded systems, signaling logic, and proprietary control software deployed across customer networks. However, it is significantly more difficult for humans or automated tools to analyse. Common techniques include altering control flow, renaming identifiers to meaningless terms, encrypting embedded data, and inserting redundant code [3,28]. These methods can protect sensitive algorithms, configuration files, and security routines from reverse engineering [46–49]. The effectiveness of these techniques is often evaluated in terms of potency

 doi:10.20944/preprints202603.1371.v1

(complexity added), resilience (resistance to de-obfuscation), stealth (ability to blend with normal code), and cost (performance or maintenance overhead). In multi-stakeholder environments, where applications may be deployed across organizational boundaries and maintained by diverse actors, obfuscation provides a security layer that remains effective even if perimeter defences are bypassed [50,51]. However, this approach has limitations. Increased code complexity [52] can hinder maintainability, reduce transparency, and potentially erode user trust [53,54]. Such opacity may also conflict with principles of openness and explainability, particularly in systems where multiple stakeholders require accountability. For these reasons, within ZTA governance, obfuscation should be strategically scoped, fully documented for authorized maintainers, and aligned with agreed ethical standards. This ensures that security benefits are achieved without undermining trust [45]. In telecom environments, reduced code transparency may also complicate cross-team troubleshooting, incident response, and coordinated fault resolution, making governance and documentation critical complements to obfuscation.

1.6. Trust and Organizational Collaboration

Trust is one of the most extensively studied topics in organizational research and is widely recognized as essential for collaboration and organizational growth [55]. It can mitigate opportunism, reduce inter-partner conflicts, and lower transaction costs [56,57]. Studies on trust [58] distinguish between two types: dispositional trust and subjective trust. Dispositional trust reflects an individual's general tendency to trust others, shaped by their attitude, personality, and prior experience. It varies between individuals and over time but is not context-specific. In contrast, Subjective trust depends on specific circumstances and a particular partner. Structural and situational factors, including the nature of the task, familiarity with the partner, power dynamics, and incentive structures, affect the level of subjective trust [59]. Despite the centrality of trust in the term "Zero Trust" there is no universally agreed-upon definition of trust, and its role in intra- and inter-organizational interactions creates challenges when implementing ZTA for users. ZTA represents a paradigm shift from a perimeter-centric security model to one centered on resources and identity [60]. Under this model, no implicit trust is granted based solely on network location, prior access, or ownership of assets. Trust must be explicitly verified through authentication and authorization before access to any enterprise resource is permitted [61]. The approach incorporates network segmentation, zone-based access controls, and continuous monitoring to manage and protect sensitive resources, whether accessed by users, applications, or other entities [44]. In summary, ZTA is both a technical and strategic response to modern cybersecurity challenges. By minimizing implicit trust and enforcing continuous verification, it strengthens protection against cyber threats in perimeter-less environments. At the same time, it requires deliberate management of ethical and organizational implications, particularly regarding collaboration, empowerment, privacy, and organizational identity. In telecommunications organizations, where service continuity depends on rapid collaboration across network operations, security teams, and R&D units, shifts in trust perceptions can have direct operational consequences.

1.7. Case Study: Managing Trust in a Global High-Tech Company

Cloud computing has since become an infrastructural necessity across corporate, governmental, academic, and non-profit sectors. Yet, while the ethical tensions and organizational risks posed by ZTA are increasingly acknowledged, theory alone does not reveal how these risks materialize in practice or how they can be mitigated. To address this gap, the following case study presents a real-world example of a global high-tech company where the implementation of ZTA initially eroded trust between IT and R&D units. The case study examines a global high-technology company operating in the telecommunications infrastructure domain, providing network technologies and software deployed across multiple customers, regions, and operational environments. The case demonstrates how managerial practices, grounded in ethical principles, stakeholder dialogue, and continuous performance measurement, can prevent trust erosion and, when necessary, rebuild it. In

 doi:10.20944/preprints202603.1371.v1

doing so, it offers a concrete roadmap for managers seeking to embrace security technologies without compromising collaboration, autonomy, or core organizational values. This case also serves as a practical bridge to the research objectives of the present study, linking the theoretical and empirical insights on trust with the operationalization of ZTA in multi-stakeholder systems.

1.8. Theoretical Framework: Technology Acceptance Model (TAM)

Building on the scientific and technological background, this section introduces the theoretical framework that will be used to make sense of the socio-ethical implications of a disruptive technology. The Technology Acceptance Model (TAM) [62]. provides the conceptual foundation for this study. TAM has been widely applied in information systems research to explain technology adoption, centring two core constructs: Perceived Usefulness (PU), defined as the degree to which a person believes that a system enhances their job performance, and Perceived Ease of Use (PEOU), defined as the degree to which using the system is free of effort. Prior studies have validated TAM across diverse domains, including enterprise platforms, cloud computing, and digital collaboration systems, underscoring its applicability to disruptive technologies such as ZTA In this research, TAM is extended with a third construct, Perceived Trust (PT) [63]. While ZTA aims to enhance security through continuous verification, it simultaneously reconfigures interpersonal and interdepartmental trust relationships by shifting reliance from implicit trust to explicit, technology-mediated verification. PT captures the user's perception that the system supports fairness, transparency, collaboration, and legitimacy across multiple stakeholders. While originally, TAM (PEOU, PU) focus on Technical and cognitive aspects the extending farmwork (PT) captures the human dimension. PT alongside PU, PEOU (an extended TAM framework) allow to account for both technical acceptance dynamics and the socio-ethical dimensions of ZTA. This extension is particularly relevant to multi-stakeholder environments, where user acceptance depends not only on efficiency and usability but also on whether the system supports autonomy, fosters collaboration, and is perceived as legitimate. By adopting this extended TAM framework, the study is positioned to investigate how employees experience ZTA as both a cybersecurity mechanism and as an organizational change that transforms trust, collaboration, and decision-making processes.

1.9. Application and Expansion of TAM

The Technology Acceptance Model (TAM) has emerged as one of the most influential theoretical frameworks for analyzing individual-level technology adoption. Originally developed by Davis (1989), TAM models user acceptance through two primary beliefs: Perceived Ease of Use (PEOU) and Perceived Usefulness (PU), which together shape attitudes and behavioral intentions toward a system. Over the past three decades, TAM has been extensively validated and extended across different domains such as healthcare [64], telemedicine [65], e-commerce [66], as well as cross-cultural IT adoption. With the evolution of cloud-based enterprise systems, TAM has become particularly valuable in analyzing organizational transitions to digital platforms [67,68]. It has also informed research in educational technologies [69–71], fintech [72], and blockchain [73], demonstrating its flexibility across both public and private sector applications. TAM's original structure has been enriched through successive models such as TAM2 and UTAUT, which incorporate external variables including social influence, facilitating conditions, and experience [74]. Later work has integrated TAM with trust, privacy, and perceived risk to better explain acceptance under uncertainty, especially in security-sensitive or privacy-aware. Given this extensive and evolving literature, TAM offers a parsimonious yet robust lens through which to analyze how employees experience advanced technology hence a great framework to measure the impact of cloud computing and Zero-Trust Architecture on the individuals in global technology companies, as well as leverage to learn the differences if exists between tech savvy such as R&D verses other internal G&A.

 doi:10.20944/preprints202603.1371.v1

1.10. Why TAM Is the Right Approach to Assess Individual-Level Impact (Empowerment vs. Erosion)

TAM is purpose built to capture how employees cognitively appraise new workplace technologies through PEOU and PU. This mechanism has been validated in organizational settings, including longitudinal field studies and mandatory-use contexts typical of enterprise systems [74]. Critically, PEOU and PU align with the psychological channels through which advanced technologies affect empowerment versus erosion at work. High PEOU supports felt competence and control (self-efficacy); low PEOU signals friction and loss of autonomy [75]. PU captures performance enablement the belief that a system helps accomplish core tasks which are linking acceptance beliefs to satisfaction and performance outcomes [76]. Complementary evidence shows that high security demands and digital complexity raise strain and depress performance [77,78], which lead to declines in PEOU/PU. Because these constructs have validated, sensitive scales, a pre/post (and post-intervention) design can measure whether cloud computing and ZTA empower employees or erode self-esteem.

1.11. Why TAM Is Appropriate for Analyzing Relationships in a Zero-Trust Environment

Zero-Trust Architecture (ZTA) explicitly replaces assumed interpersonal trust with continuous, technology-mediated verification [61]. Acceptance in such settings depends not only on effort and utility but also on whether controls are perceived as competent, fair, and legitimate. Extending TAM with PT is theoretically grounded in research that integrates trust with acceptance under uncertainty: trust acts as an antecedent to PU [79]. In ZTA, perceived security should raise PT and, through PT, increase PU and intention, while stringent verification can lower PEOU via added effort. Moreover, procedural and informational justice, clarity, consistency, voice, and recourses can establish antecedents of trust and compliance [80], making them actionable facilitating conditions that elevate PT and attenuate the PEOU cost of verification. A trust-extended TAM therefore ties technical controls (continuous authentication, policy decision points) to human judgments (effort, usefulness, trust, risk) in a parsimonious, testable structure that is well suited to security-intensive, multi-stakeholder rollouts.

Our three-wave longitudinal design (pre-ZTA, post-ZTA, post-communication) operationalizes this framework by testing the predicted time-course, an initial decline in PEOU/PU after verification hardening, followed by recovery mediated by gains in PT produced through targeted communication and procedural-justice interventions.

2. Research Objectives and Expected Significance

2.1. Research Objectives

Previous research on ZTA has primarily emphasized technical aspects such as architecture design and performance optimization [32]. However, there is limited attention to user-related, socio-ethical dimensions of ZTA, which are central in multi-stakeholder organizational environments. This study addresses this gap by focusing on how ZTA impacts perceptions of trust, collaboration, and autonomy among employees and managers. While ZTA is associated with the slogan "Never Trust, Always Verify," reducing it to a purely technical framework obscures its broader implications. Security is necessary for organizational survival, but modern organizations also require IT systems that support remote work, inter- and intra-organizational collaboration, and individual empowerment. The central objective of this study is to broaden theoretical and practical understanding of how ZTA affects user-related trust dynamics in multi-stakeholder environments. By empirically analysing user experiences with ZTA, the study clarifies trade-offs between strict security enforcement and values like empowerment, privacy, and collaboration. The study pursues the following objectives:

1. Broaden theoretical understanding of ZTA's impact on multi-stakeholder trust, including negative effects and managerial strategies for positive outcomes.
2. Examine strategies for managing trust in ZTA environments, highlighting challenges and collaborative opportunities.

 doi:10.20944/preprints202603.1371.v1

3. Illustrate conceptually, how technical mechanisms such as code obfuscation, commonly employed by R&D organizations, can shape stakeholders' perceptions of fairness, legitimacy, and autonomy, depending on governance and ethical implementation practices.

Based on these objectives, the study is guided by the following research questions:

RQ1: How do users perceive trust under ZTA conditions when access is continuously monitored and verified?

RQ2: How might ZTA mechanisms, particularly technical practices such as code obfuscation, shape stakeholders' perceptions of fairness, legitimacy, and autonomy within R&D organizations, depending on governance and ethical implementation?

RQ3: What governance and design principles can ensure that ZTA actively manages, rather than erodes, user trust in multi-stakeholder environments?

2.2. Research Hypotheses

H1a: The adoption of ZTA reduces default interpersonal and organizational trust but enables new forms of managed trust via structured verification.

H1b: The extent to which ZTA undermines or enables trust depends on how effectively organizations balance strict security enforcement with collaboration, accessibility, and empowerment.

H2a: ZTA mechanisms, especially code obfuscation implemented without transparency or governance, are hypothesized to undermine trust by creating perceptions of disempowerment and opacity, with a stronger negative impact on R&D organizations than on G&A and Sales functions.

H2b: Code obfuscation implemented proportionately, auditable, and transparently may conceptually strengthen managed trust by reinforcing fairness and legitimacy.

H2a and H2b are presented as conceptual considerations and were not directly tested in an empirical study.

2.3. Expected Significance

This research bridges technology, management, and ethics, addressing gaps in cybersecurity literature and practice.

Theoretical significance includes:

1. Extends understanding of ZTA beyond technical functionality to include trust, collaboration and values.
2. Identifies user-related drivers beyond security imperatives and evaluates trade-offs like privacy, autonomy and empowerment.
3. Conceptually considers the role of mechanisms such as code obfuscation in shaping trust.

Practical significance includes:

1. Offers managers insights on designing and implementing ZTA that balance security with stakeholder collaboration.

Expected contributions include:

1. Demonstrating how organizations balance cybersecurity with collaboration.
2. Identifying managerial practices (communication campaigns, stakeholder dialogue, monitoring mechanisms) that mitigate trust erosion.
3. Exploring conditions under which ethical governance preserves trust in ZTA environments.
4. Illustrative Example – Code Obfuscation: Shows conceptually how technical mechanisms within ZTA can erode or strengthen trust depending on ethical governance and transparency, though not empirically tested in this study.

 doi:10.20944/preprints202603.1371.v1

3. Methodology and Research Design

3.1. Research Approach - Longitudinal Design and Repeated Measures

This study is a longitudinal study with four-wave longitudinal design (or time points) of data collection, testing the effects of ZTA on employee perceptions of productivity and trust within a multinational high-tech organization. [1] Baseline surveys conducted in 2020, following the adoption of Cloud-Based Technological Systems (CBTS), indicated high perceived productivity (M = 4.38, SD = 0.78, n = 546). In 2021, a cybersecurity incident, led the organization to adopt ZTA. Several technical mechanisms were implemented in parallel, calibrated to align with the functional roles of different stakeholder groups. [2] Although the implementation was technically effective, it coincided with a notable decline in perceived productivity, measured in December 2021 (M = 3.28, SD = 1.17, n = 126) and September 2022 (M = 3.37, SD = 1.04, n = 120), suggesting potential erosion of trust and employee confidence. [3] To address these challenges, in late 2022, the organization launched a comprehensive Communication Campaign (CC), emphasizing transparency, stakeholder engagement, and collaborative problem-solving. [4] The subsequent survey conducted in January 2023 (M = 3.82, SD = 0.9, n = 176) provides systematic evidence of improvements in productivity and trust following the campaign, particularly among teams most constrained by ZTA controls. These results provide information for Research Question 1, which examines how users perceive trust under continuous monitoring and verification in ZTA environments. In telecommunications environments, decline in employee perceptions of productivity and trust have implications beyond individual experience, as reduced coordination and trust may delay fault resolution, incident response, and cross-team collaboration essential for network reliability. The four survey waves represent repeated cross-sectional measurements rather than a strict panel design. While the surveys were distributed organization-wide at each time point, individual responses were anonymized and not longitudinally matched across waves. Consequently, statistical comparisons reflect aggregate shifts in organizational perceptions rather than within-subject changes. This approach is appropriate for assessing system-level trust dynamics during large-scale technological transitions in multi-stakeholder environments.

3.2. Data Collection and Instrument - Questionnaire and Validation, Population and Sample

The study employed a pulse-check survey instrument explicitly grounded in the Technology Acceptance Model (TAM), extended to capture PT. This design enabled the assessment of employees' perceptions of the Zero-Trust working environment and its implementation in the organization.
Data Collection and Instrument - All survey items were measured on a five-point Likert scale (1 = strongly disagree / very poor, 5 = strongly agree / excellent). The instrument included three core dimensions: (1) PU, assessing productivity in ZTA environments, measured with the questions: "How productive is your working environment in a Zero-Trust setting?" and "How productive is your working relationship with third parties in a Zero-Trust environment?". (2) PEOU, measuring adaptation and comfort with the technological environment, assessed with: "How well did you adjust to the Zero-Trust working environment?" and "The technological working environment is easy and fun / okay / a big challenge". and (3) PT, capturing collaboration, empowerment, and confidence in workplace relationships, evaluated with: "People readily collaborate across departments for the good of the company", "I feel trusted to combine work from home and office work", and "At work, I have the opportunity to do what I do best every day". The survey was distributed via Microsoft 365 Forms to approximately 1,000 employees across six continents. Anonymity was ensured, while collecting demographic data on geography, department, and managerial status to enable subgroup analyses. Data were collected across three waves to examine changes over time: pre-ZTA in 2020 (baseline before adoption), post-ZTA in 2021–2022 (after ZTA implementation), and post-Communication Campaign in 2023 (after the intervention aimed at restoring trust and engagement). This longitudinal design allowed for diachronic comparisons to assess both the immediate and delayed effects of ZTA and organizational interventions.

 doi:10.20944/preprints202603.1371.v1

Population and Sample – geographic distribution, departmental distribution

Data Analysis - To ensure the reliability and validity of the survey, Cronbach's alpha exceeded 0.7 for all constructs, and additional sanity checks were conducted on item means, standard deviations, and response frequencies. The analytical approach included descriptive statistics, one-way ANOVA, paired-samples t-tests, and Cohen's d effect sizes to evaluate the magnitude and statistical significance of observed changes across waves. This operationalization of TAM ensured that theoretical constructs of usefulness, ease of use, and trust were directly linked to empirically measurable outcomes such as productivity, collaboration, and stakeholder perceptions. Overall, the survey design provided a structured and validated method to capture employee perceptions of ZTA, enabling a rigorous examination of how technical implementation, organizational interventions, and stakeholder engagement influence trust and productivity in a multinational context.

Data Analysis The analysis of employee survey responses across three waves shows a clear impact of ZTA on perceived productivity and trust, as well as the mitigating role of the organizational Communication Campaign (CC). Across the organization, perceived productivity fell sharply following ZTA adoption, declining from a pre-ZTA baseline mean of 4.38 (SD = 0.78, n = 546) in 2020 to 3.28 (SD = 1.17, n = 126) in December 2021. This was followed by only a modest stabilization in September 2022 (M = 3.37, SD = 1.04, n = 120). After the Communication Campaign in January 2023, perceived productivity partially recovered to 3.82 (SD = 0.90, n = 176), suggesting a meaningful but incomplete rebound (Table 1).

Table 1. TAM Index (PEOU, PU, PT) Across Waves (Pre-ZTA, Post-ZTA, Post-CC).

Wave	Timing	N	Mean	SD
Pre-ZTA	2020 (baseline)	546	4.38	0.78
Post-ZTA (1)	Dec 2021	126	3.28	1.17
Post-ZTA (2)	Sep 2022	120	3.37	1.04
Post-CC	Jan 2023	176	3.82	0.90

Figure 1 illustrates this trajectory, emphasizing the sharp decline after ZTA implementation and the partial recovery following the Communication Campaign. The figure underscores the importance of organizational interventions, such as transparency, stakeholder engagement, and proactive communication in restoring PEOU, usefulness and trust after disruptive technological changes.

 doi:10.20944/preprints202603.1371.v1

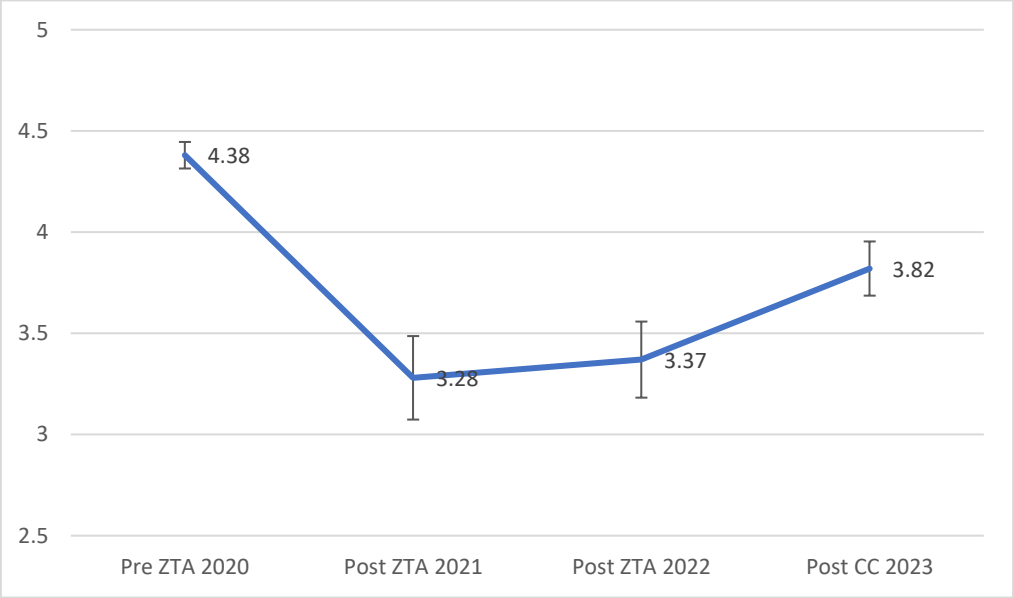

Figure 1. Timeline of TAM Index (PEOE, PU, PT) Across Survey Waves.

A one-way ANOVA across the three post-implementation waves confirmed that changes were statistically significant ($p < .05$), with no meaningful difference between December 2021 and September 2022 ($p = .776$). Effect size analyses further clarified the magnitude: the decline from pre-ZTA to post-ZTA was large ($d = 1.12$), the recovery from post-ZTA to post-CC was medium ($d \sim 0.52$), and the difference between the two post-ZTA waves was trivial ($d = 0.08$). These findings confirm that ZTA implementation initially disrupted workflow and trust, while the Communication Campaign produced a meaningful, though incomplete, restorative effect. Critically, this recovery did not restore productivity to pre-ZTA levels, highlighting the persistent adjustment costs associated with stringent security frameworks.

3.3. Geographic Differences Across Waves

Regional analyses revealed substantial variation across geographies (Table 2). Prior to the Communication Campaign, employees in the EU and Romania reported the steepest productivity declines, while employees in APAC, India, and Israel maintained comparatively higher scores. After the Communication Campaign, EU and Romania showed a recovery of over 20%, which narrowed but did not entirely eliminate the gap with regions such as APAC, India, and Israel. Tukey HSD post hoc tests confirmed statistically significant differences ($p < .05$), particularly between EU and APAC/India/Israel, and between India and EU/LATAM/NA/Romania.

These geographic disparities highlight that ZTA adoption does not affect all contexts equally. Local management practices, cultural orientations toward authority and security, and pre-existing levels of organizational trust likely shaped these outcomes. The EU's sharper decline may reflect stricter interpretations of ZTA enforcement or lower baseline flexibility in work practices. Future analyses should more explicitly examine contextual moderators such as regional leadership styles, team structures, or prior remote work experience.

3.4. Departmental Differences Across Waves

Differences across departments were also pronounced (Table 2). Technical functions, particularly Product and R&D, were disproportionately affected by ZTA, with post-implementation scores falling to 2.76. However, this group also demonstrated the largest relative recovery post-CC, increasing to 3.63 a gain of approximately 26%. By contrast, Delivery and Sales & Marketing showed moderate changes, while General & Admin consistently reported higher productivity throughout the study period.

 doi:10.20944/preprints202603.1371.v1

Table 2. TAM Index by Department and Wave.

Department	Pre-PCS3 Mean (SD, N)	Pre-PCS4 Mean (SD, N)	Post-PCS5 Mean (SD, N)
Delivery	3.51 (1.08, 45)	3.54 (1.19, 37)	3.93 (0.91, 56)
General & Admin	3.75 (1.07, 20)	4.05 (0.62, 19)	4.13 (0.81, 31)
Product & R&D	2.76 (1.20, 41)	3.02 (0.91, 46)	3.63 (0.96, 48)
Sales & Marketing	3.35 (1.09, 20)	3.17 (0.99, 18)	3.68 (0.82, 41)

ANOVA and Cohen's d effect sizes confirmed significant differences between Product and R&D and other departments, with large effects compared to Delivery ($d > 0.8$) and medium effects compared to Sales & Marketing ($d < 0.8$). This suggests that departments highly dependent on technical collaboration and innovation are more sensitive to strict security enforcement, but they also benefit the most from targeted restorative measures.

3.5. Effect Size Summary

Table 3 summarizes the key effect sizes. The largest effect was the decline from pre-ZTA to post-ZTA ($d = 1.12$, large), demonstrating the disruptive impact of implementation. The medium effect size for post-CC recovery ($d \sim 0.52$) underscores the practical value of organizational interventions in restoring trust and productivity. Meanwhile, the trivial effect size between the two consecutive post-ZTA waves ($d = 0.08$) confirms that adaptation without additional intervention was minimal.

Table 3. Key Effect Sizes (Cohen's d).

Comparison	Cohen's d	Interpretation
Pre-ZTA (2020) vs Post-ZTA (Sep 2022)	1.12	Large decline
Post-ZTA (Dec 2021) vs Post-ZTA (Sep 2022)	0.08	Trivial change
Post-ZTA (Dec 2021) vs Post-CC (Jan 2023)	~0.52	Medium improvement

Overall, the empirical evidence demonstrates a trajectory of initially high productivity ($M = 4.38$ in 2020), a sharp decline post-ZTA ($M \sim 3.3$ in 2021–2022), and a meaningful but incomplete rebound after the Communication Campaign ($M = 3.82$ in 2023). These findings strongly support the argument that communication campaigns can mitigate, though not fully eliminate, productivity declines triggered by disruptive technological interventions. They also reinforce the theoretical perspective that technical implementations interact with organizational trust, legitimacy, and autonomy, rather than operating in isolation. Critically, while these results provide robust evidence of ZTA's impact, several limitations must be acknowledged. Productivity was measured through self-reports, which may introduce bias; some regional and departmental samples were small (e.g., APAC $n = 5$–19), limiting statistical power; and while fairness, legitimacy, and autonomy were central to RQ2, they were not directly measured. Additionally, the Communication Campaign itself was not operationalized in terms of intensity or exposure, making it difficult to pinpoint which elements were most effective. These limitations point to future research opportunities, including integrating objective productivity measures, ensuring larger sample sizes across subgroups, and directly measuring fairness and legitimacy perceptions.

 doi:10.20944/preprints202603.1371.v1

4. Discussion

The findings presented in this chapter demonstrate significant impacts of Zero-Trust Architecture implementation on employee perceptions and organizational dynamics. In telecommunications infrastructure environments, trust deterioration has operational implications beyond organizational climate. Network reliability depends on rapid cross-functional coordination between security teams, R&D engineers, and network operations centers. Reduced perceived usability or trust may plausibly delay incident response cycles, increase troubleshooting latency, and weaken collaboration across distributed network functions. In cloud-native and software-defined architectures, where availability and resilience are mission-critical, even moderate coordination friction may translate into measurable systemic risk. The empirical results observed in the longitudinal analysis provides concrete evidence of the socio-technical shock induced by Zero-Trust implementation. The transition from the pre-ZTA baseline (M = 4.38) to the post-ZTA stabilization (M =3.37) represents a large effect (Cohen's d = 1.12), indicating not merely incremental friction but fundamental disruption in perceived usefulness, ease of use, and trust. Notably, the absence of significant change between December 2021 and September 2022 (d = 0.08) demonstrates that passive adaptation alone was insufficient to restore confidence, refuting assumptions that employees naturally accommodate new security frameworks over time. Only after the structured Communication Campaign launched in late 2022 did the data reveal a medium-sized recovery effect (d ~ 0.52), reinforcing the argument that managerial governance acts as an active moderator of Zero-Trust outcomes rather than a peripheral complement to technical deployment. These patterns provide strong empirical support for Hypothesis 1a, which proposed that ZTA reduces default trust but enables managed trust. The 25% decline in the composite TAM index (d = 1.12) confirms that continuous verification initially disrupts default interpersonal and organizational trust. Critically, the trivial effect between the two post-ZTA waves (d = 0.08) demonstrates that trust does not spontaneously recover through passive adaptation. However, the medium recovery effect following the Communication Campaign (d ≈ 0.52) validates that structured managerial governance can facilitate the emergence of "managed trust". This empirical pattern confirms that Zero-Trust does not eliminate trust but transforms it from an implicit cultural assumption into an actively mediated organizational process requiring deliberate governance to sustain. Immediately following ZTA enforcement, the composite TAM index declined by 25%, with Perceived Trust showing particularly sharp deterioration. Future research should examine whether the decline in trust components was sharper than changes in perceived usefulness and ease of use, which would support the theoretical proposition that trust functions as a leading indicator in security-intensive transformations. Following structured managerial interventions including targeted communication and stakeholder engagement, perceived productivity partially recovered (+16.4%), although not to pre-implementation levels. Regional analysis using one-way ANOVA revealed statistically significant variation across geographic regions ($p < .05$), with post-hoc tests identifying significant differences between EU and India ($p = .003$) and between EU and APAC ($p = .009$), underscoring the contextual sensitivity of ZTA outcomes. Collectively, these quantitative findings and regional variations underscore that Zero-Trust Architecture is not merely a security enhancement, but a socio-technical intervention whose success depends on how it is governed and managed during transition. The immediate decline in the TAM index following ZTA adoption provides strong evidence that stringent access controls are interpreted by employees as barriers to autonomy, creativity, and collaboration regardless of their technical necessity or security effectiveness. This disruption aligns with socio-technical systems theory and procedural justice research, which predict that restrictive security measures, when introduced abruptly without stakeholder consultation, will erode employees' sense of fairness and legitimacy [80]. In telecommunications infrastructure environments, such declines are not merely perceptual or cultural phenomena, they carry operational risk implications. Reduced perceived trust and usability can plausibly slow incident response cycles, delay cross-team troubleshooting, and weaken coordination across distributed network functions, though the present study did not measure these operational outcomes directly. Because telecom infrastructures operate

 doi:10.20944/preprints202603.1371.v1

under strict availability and latency requirements, even moderate reductions in collaborative efficiency may translate into measurable resilience risks. The partial recovery observed after the Communication Campaign demonstrates the mediating role of organizational interventions: transparency, structured communication, and stakeholder engagement proved effective in rebuilding confidence and partially restoring workflow continuity. Importantly, however, the recovery was incomplete, with Wave 4 perceptions remaining 13% below pre-ZTA baseline, suggesting that managerial actions can mitigate but not fully erase the frictions caused by disruptive security measures because ZTA inherently introduces permanent workflow changes including authentication steps, access restrictions, and verification protocols that persist regardless of communication quality. This partial recovery directly supports Hypothesis 1b, which proposed that trust outcomes depend on governance balance. The Communication Campaign's measurable impact ($d \approx 0.52$) demonstrates that ZTA's effect on trust is contingent upon how effectively organizations balance security enforcement with accessibility, collaboration, and empowerment. The incomplete restoration to baseline (13% persistent gap) further validates this hypothesis by showing that even optimal governance cannot fully eliminate the inherent constraints of continuous verification architectures. Success in managing trust under ZTA therefore depends not on technical excellence alone but on calibrating governance mechanisms to accommodate legitimate operational requirements while maintaining security integrity. From a theoretical perspective, these results extend socio-technical systems research by showing how technical design choices, such as ZTA enforcement and application-layer security mechanisms including code obfuscation, are deeply entangled with perceptions of legitimacy and trust. Rather than being neutral tools, security mechanisms reshape power relations within organizations. For example, when employees perceive that access restrictions undermine their autonomy or create workflow inefficiencies, trust is eroded even when the technical security rationale is strong, and the controls are technically effective. Conversely, when such mechanisms are embedded within transparent governance structures, stakeholder engagement processes, and ethical oversight through board-endorsed principles, they can be interpreted as legitimate safeguards rather than barriers. This suggests that cybersecurity frameworks must be theorized not only in terms of resilience and protection but also in terms of fairness, autonomy, and proportionality. These theoretical insights translate into concrete implications for managerial governance. The study demonstrates empirically that technical interventions such as ZTA must be accompanied by deliberate communication, training, and organizational support. The trivial effect size ($d = 0.08$) between post-ZTA waves demonstrates that managers cannot assume passive adaptation to heightened security protocols; instead, structured campaigns, participatory decision-making, and ethical framing are empirically validated as required to sustain trust and productivity. The Communication Campaign demonstrated measurable value ($d \approx 0.52$), particularly for groups most negatively affected by ZTA. Yet the evidence also reveals residual productivity gaps compared to the pre-ZTA baseline, pointing to the need for ongoing engagement and iterative adjustment rather than one-off interventions. Geographic and departmental analyses reinforce that ZTA adoption is not experienced uniformly across organizational contexts. Product and R&D teams with high interdependence and reliance on technology and collaborative workflows, were disproportionately affected, with sharp declines in TAM index ($M = 2.76$, the lowest across all departments) yet demonstrated the strongest recovery following the Communication Campaign (31.5% increase, the largest across all departments). This departmental heterogeneity further reinforces Hypothesis 1b: collaboration-intensive environments proved particularly sensitive to enforcement rigidity but also particularly responsive to governance mechanisms incorporating dialogue and participatory adjustment, confirming that ZTA's organizational consequences are not technologically deterministic but depend on governance calibration. By contrast, departments such as G&A, whose work practices do not depend on code transparency or rapid cross-functional collaboration, reported more stable outcomes ($M = 3.75$–4.13 across waves). These differences highlight that ZTA interacts with existing organizational structures and cultural orientations, amplifying vulnerabilities in some contexts while leaving others relatively

 doi:10.20944/preprints202603.1371.v1

unscathed. Tailoring communication strategies, support mechanisms, and governance frameworks to local contexts is therefore empirically validated as a crucial success factor in implementation, as evidenced by the differential recovery patterns across functional groups. While the survey did not directly measure code obfuscation's impacts, the departmental analysis provides indirect evidence. Product and R&D teams, subject to application-layer security measures including code obfuscation, reported the lowest post-ZTA scores (M = 2.76), consistent with H2a that technical opacity undermines trust when conflicting with professional norms emphasizing code transparency and collaborative debugging. However, R&D's strongest recovery following the Communication Campaign (31.5% increase) supports H2b that governance quality moderates these effects, demonstrating that transparent communication, stakeholder engagement, and organizational responsiveness enable the most negatively affected groups to restore trust despite persistent technical constraints. While Hypotheses 2a and 2b were developed as conceptual propositions rather than empirically tested constructs, the R&D departmental patterns provide indirect evidence regarding their validity. H2a proposed that code obfuscation implemented without transparency undermines trust in R&D contexts; the substantially lower R&D scores (2.76 versus 3.28 organizational average) align with this proposition, suggesting that technical opacity mechanisms create perceptions of disempowerment when conflicting with professional norms emphasizing code transparency and collaborative debugging. H2b proposed that proportionate, auditable, and transparently governed obfuscation can strengthen managed trust; R&D's 31.5% recovery, the largest across all departments, provides preliminary support for this proposition by demonstrating that governance quality moderates technical opacity's trust impacts. However, the incomplete recovery even in R&D (3.63 versus presumed higher baseline) indicates that transparent governance can mitigate but not eliminate the constraints that code obfuscation imposes on collaborative technical work. Future research should directly measure fairness, legitimacy, and autonomy perceptions in relation to specific technical opacity mechanisms to more definitively test the governance-moderated relationship proposed in these conceptual hypotheses. ZTA adoption must be understood as a socio-technical challenge rather than a purely technical decision. Success depends not only on the strength of the technical safeguards but also on organizational design, governance mechanisms, and the inclusivity of stakeholder engagement. The evidence demonstrates that without adequate communication and participatory practices, ZTA will undermine trust and collaboration, the very conditions required for resilient and adaptive cybersecurity. Conversely, when accompanied by thoughtful governance, transparency, and responsiveness, disruptive technical interventions are integrated more smoothly, limiting productivity losses and sustaining long-term organizational trust, as demonstrated by the medium effect size recovery following the Communication Campaign.

5. Conclusions

This study addressed three interrelated research questions concerning Zero-Trust Architecture implementation in multi-stakeholder telecommunications environments. Research Question 1 asked how users perceive trust under ZTA conditions when access is continuously monitored and verified. The findings demonstrate that continuous monitoring produces substantial trust erosion (25% decline, d = 1.12), with employees interpreting stringent access controls as organizational signals of distrust that undermine perceived autonomy and professional discretion. However, the Communication Campaign's recovery effect (d ≈ 0.52) reveals that trust erosion is not inevitable but contingent upon governance quality. Research Question 2 asked how ZTA mechanisms, particularly code obfuscation, shape perceptions of fairness, legitimacy, and autonomy in R&D organizations depending on governance. The departmental analysis showed R&D teams experienced disproportionate negative impacts (M = 2.76) yet demonstrated strongest recovery (31.5%), confirming that technical opacity undermines trust when conflicting with professional norms but that transparent governance can substantially mitigate these effects. Research Question 3 asked what governance principles can ensure ZTA actively manages rather than erodes trust. The evidence validated several mechanisms: proactive communication, stakeholder engagement, procedural

 doi:10.20944/preprints202603.1371.v1

transparency, demonstrated responsiveness, and role-sensitive calibration. Collectively, these findings demonstrate that trust under Zero-Trust Architecture is neither eliminated nor automatically sustained by technical excellence; rather, it is actively managed through deliberate governance.

Trust plays a central role in intra- and inter-organizational life, yet contemporary digital transformations are fundamentally reshaping how trust is established, maintained, and institutionalized. In cloud-based and telecommunications-oriented environments, trust is no longer solely an interpersonal phenomenon; rather it is embedded within technological architectures and governance mechanisms. This study examined the organizational consequences of adopting ZTA focusing on employee perceptions of productivity, ease of use, usefulness, and trust through an extended Technology Acceptance Model across four longitudinal waves. The empirical findings reveal a substantial and statistically significant decline following ZTA enforcement, with the composite TAM index falling from a pre-ZTA baseline ($M = 4.38$) to the immediate post-implementation stabilization ($M = 3.37$), representing a large effect (Cohen's $d = 1.12$). Critically, the trivial change between two consecutive post-ZTA waves ($d = 0.08$) refuted assumptions about natural adaptation, demonstrating that passive exposure alone cannot restore trust. While a structured Communication Campaign facilitated partial recovery ($M = 3.82$; $d \approx 0.52$), perceptions remained 13% below baseline, indicating that governance can mitigate but not eliminate the workflow constraints inherent in continuous verification architectures.

The findings validate H1a and H1b. H1a proposed that continuous verification initially disrupts default trust but enables managed trust through governance; the large disruption effect ($d = 1.12$) followed by governance-enabled recovery ($d \approx 0.52$) confirms this transformation. H1b proposed that trust outcomes depend on governance balance; the incomplete recovery (13% persistent gap) validates that even optimal governance cannot fully eliminate verification constraints, confirming that success requires calibrating security enforcement with collaboration, accessibility, and empowerment. H2a and H2b, developed conceptually rather than empirically tested, propose that code obfuscation either undermines or reinforces legitimacy depending on governance transparency; R&D's disproportionate impact and strongest recovery provide preliminary indirect support for these governance-moderated relationships, establishing an agenda for future direct measurement.

Theoretically, this study advances the literature in four key ways. First, it reframes ZTA as a socio-technical governance mechanism rather than merely a technical safeguard, positioning security architectures as trust-reshaping interventions requiring ethical and organizational governance alongside technical implementation. Second, it extends Technology Acceptance Model theory by validating Perceived Trust as a critical third dimension alongside Perceived Usefulness and Perceived Ease of Use in security-intensive contexts, demonstrating that trust deteriorates more rapidly than utilitarian perceptions during disruptive transitions. Third, it contributes to organizational trust theory by showing how technology-mediated verification systems fundamentally alter trust objects from interpersonal relationships to institutional governance processes, requiring reconceptualization of trust as confidence in fairness, procedural justice, and system legitimacy. Fourth, by integrating quantitative longitudinal evidence with ethical and organizational analysis, it bridges cybersecurity research with broader debates on institutional trust, legitimacy, and digital transformation, demonstrating that security effectiveness and operational resilience depend not only on technical controls but on how these controls interact with perceptions of autonomy, fairness, and professional discretion.

Practically, the results yield five actionable contributions for telecommunications organizations and infrastructure providers. First, they validate that ZTA adoption in telecommunications and infrastructure-intensive environments must be governed as an organizational change process rather than purely technical deployment, requiring cross-functional governance structures integrating IT, HR, legal, and business leadership. Second, they demonstrate the necessity of proactive trust measurement through pulse-check surveys and trust-extended TAM frameworks, transforming trust into a measurable governance variable enabling timely interventions. Third, they confirm that

 doi:10.20944/preprints202603.1371.v1

managerial capability development is decisive, as managers function as trust brokers requiring training in security communication, change management, and ethical reasoning. Fourth, differential impacts across departments, particularly R&D's heightened sensitivity, validate the need for tailored governance strategies that align security controls with workflow interdependence and innovation requirements. Fifth, the evidence confirms that participatory governance mechanisms including stakeholder engagement, transparent policy development, and demonstrated responsiveness produce measurable trust restoration, justifying resource allocation for meaningful rather than performative consultation. In distributed and software-defined telecom networks, where operational continuity is mission-critical, the ability to manage trust during security transitions becomes a determinant of resilience.

While these findings provide robust longitudinal evidence, several limitations warrant acknowledgment. The reliance on self-reported perceptions introduces potential response biases that future research should address through objective performance metrics including incident response times and collaboration network analysis. Sample size variation across waves (546 baseline to 120-176 post-ZTA) and small regional subsamples (n = 2-6 in some geographies) limit statistical power and generalizability. The absence of Wave 1 baseline data disaggregated by department and region prevents definitive assessment of differential vulnerability versus pre-existing differences. The Communication Campaign was treated as a binary intervention without measuring individual exposure or component effectiveness, limiting identification of active ingredients. Temporal confounds from the COVID-19 pandemic (2020-2023) complicate causal attribution absent control groups. Most critically, fairness, legitimacy, and autonomy were not directly measured despite being central to Research Question 2, requiring future studies to incorporate validated scales for procedural justice, distributive justice, and perceived autonomy as distinct constructs. These limitations point to clear directions: mixed-method designs combining surveys with qualitative interviews, longer-term longitudinal tracking beyond eighteen months, experimental manipulation of specific governance mechanisms, cross-industry and cross-cultural comparisons, and integration of objective performance metrics alongside perceptual measures.

The forward-looking implications of this study extend to the growing integration of Artificial Intelligence within Zero-Trust environments. As telecommunications infrastructures evolve toward cloud-native, software-defined, and AI-assisted architectures, security enforcement is increasingly delegated to automated systems. The empirical evidence presented here suggests that unmanaged opacity in such systems may amplify trust shocks similar to those observed during initial ZTA deployment. Conversely, explainable and auditable AI mechanisms may function as mediators that reduce the perceived distance between enforcement and fairness, thereby supporting more stable forms of managed trust. In this sense, the transition from assumed trust to managed trust represents not a static end state, but an evolving governance challenge. Future Zero-Trust implementations will depend on the careful alignment of automated decision-making, transparency mechanisms, and participatory oversight structures. For telecommunications organizations operating under high availability and resilience demands, the capacity to integrate AI without undermining legitimacy will become a defining governance competency.

More fundamentally, the ethical question is not whether machines replace human trust, but whether they are designed to preserve the human capacity for judgment, dignity, and proportionality. When automation merely enforces rigid control without explanation or recourse, it risks reducing human actors to compliance nodes within a technical system. However, when automation absorbs mechanical verification, reduces arbitrary bias, and provides transparent reasoning, it can free human actors to focus on collaboration, creativity, and ethical deliberation. In this configuration, machines do not mechanize trust; they protect the conditions under which human trust can meaningfully operate. Zero-Trust Architecture does not eliminate trust but restructures it.

The findings of this study demonstrate that trust erosion is neither technologically inevitable nor permanently destructive. Rather, trust in security-intensive environments is dynamically negotiated through managerial calibration, ethical proportionality, and institutional transparency. As

 doi:10.20944/preprints202603.1371.v1

telecommunications systems become increasingly distributed and intelligent, the ability to actively govern trust across both human and algorithmic actors will become a central determinant of operational resilience and long-term institutional legitimacy. This study has shown that managed trust is achievable, measurable, and consequential. The path forward requires sustained commitment to transparency, stakeholder engagement, and ethical governance, not as supplements to technical security, but as integral components of organizational resilience in an era of continuous verification.

Statement

AI Usage Statement: During the preparation of this work we used ChatGPT by OpenAI and Gemini by Google in order to assist in language, editing, text formatting as well as a searching engine. After using the tools we reviewed and edited the content as needed. we take full responsibility for the content of the publication.

Author Contributions: Conceptualization, methodology, formal analysis, investigation, original draft preparation: Guy Toibin. Review, editing, supervision: Shlomo Mark, Yotam Luria. All authors have read and agreed to the published version of the manuscript**.** Conceptualization, Guy E. Toibin, Shlomo Mark and Yotam Luria.; methodology, Guy E. Toibin, Shlomo Mark and Yotam Luria.; validation, Shlomo Mark and Yotam Luria.; formal analysis, Guy E. Toibin.; investigation, Guy E. Toibin.; resources, Guy E. Toibin.; data curation, Guy E. Toibin.; writing—original draft preparation, Guy E. Toibin.; writing—review and editing, Shlomo Mark and Yotam Luria.; visualization, Guy E. Toibin.; supervision Shlomo Mark.; project administration, Guy E. Toibin.; All authors have read and agreed to the published version of the manuscript.

Institutional Review Board Statement: The study was conducted in accordance with organizational research guidelines. Participation was voluntary and anonymous. No personal identifying information was collected. According to institutional policy, formal IRB approval was not required for anonymous organizational surveys.

Data Availability Statement: The data presented in this study are not publicly available due to organizational confidentiality agreements.

Funding: This research received no external funding.

Conflicts of Interest: The author was employed by the organization during the study period. The research was conducted independently without influence on the analysis or reporting of results.

References

1. K. Schwab, The Fourth Industrial Revolution., Geneva: World Economic Forum, 2016.
2. Berlin, Two Concepts of Liberty, Oxford: Oxford Univercity Press, 1969.
3. C. M. Christensen, The innovator's dilemma when new technologies cause great firms to fail., Harvard Business Review Press., 1997.
4. L. Floridi , J. Cowls, M. Beltrametti, R. Chatila, P. Chazerand, V. Dignum, ... and E. Vayena, "(AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations.," *Minds and machines,* vol. 28, no. 4, pp. 689-707, 2018.
5. B. Whitworth and A. Adnan, "The Social Design of Technical Systems: Building technologies for communities," Institute of Information and Mathematical Sciences, Auckland, 2014.
6. C. M. Christensen, 2021. [Online]. Available: https://claytonchristensen.com/.
7. C. M. Christensen, M. Raynor and R. McDonald, "The big idea: What is disruptive innovation," *Harvard Business Review,* pp. 44-53, 2015.
8. J. Hurwitz, R. Bloor, m. Kaufman and F. Helper, Cloud Computing for Dummies, Hoboken, NJ: Wiley Publishing, Inc., 2010.
9. Q. Zhang, L. Cheng and R. Boutaba, "Cloud computing: state-of-the-art and research challenges," *The Brazilian Computer Society 2010,* 2010.
10. P. Mell and T. Grance, "The NIST Definition of Cloud Special Publication 800-145," National Institute of Standards and Technology, Washington, 2011.

 doi:10.20944/preprints202603.1371.v1

11. K. Panetta, "As cloud computing evolves, it should move away from experimentation and towards enterprise-wide implementation," 30 January 2017. [Online]. Available: https://www.gartner.com/smarterwithgartner/cloud-computing-enters-its-second-decade/.
12. M. Berner, E. Graupner and A. Maedche, "The Information Panopticon in the Big Data Era," *Journal of Organization Design,* p. 7, 2014.
13. S. Ghasemshirazi, G. Shirvani and M. A. Alipour, "Zero trust: Applications, challenges, and opportunities.," *arXiv preprint arXiv:2309.03582.*, 2023.
14. D. Ajish, "The significance of artificial intelligence in zero trust technologies: a comprehensive review.," *Journal of Electrical Systems and Inf Technol* , vol. 30, p. 11.
15. Y. Zhang, S. Balochian, P. Agarwal, V. Bhatnagar and O. J. Housheya, "Artificial intelligence and its applications," *Mathematical Problems in Engineering,* pp. 1-7, 2014.
16. S. Dick, "Artificial intelligence," *Harvard Data Science Review,* p. 1(1), 2019.
17. T. Miller, "Explanation in artificial intelligence: Insights from the social sciences," *Artificial Intelligence, 267,* pp. 1-38, 2019.
18. J. G. Carbonell, R. S. Michalski and T. M. Mitchell, Machine learning: An artificial intelligence approach, Palo Alto, CA: Tioga Publishing Company, 1983.
19. H. Wang, C. Ma and L. Zhou, "A brief review of machine learning and its application," *International Conference on Information Engineering and Computer Science,* pp. 1-4, 2009.
20. N. Balasubramaniam, M. Kauppinen, K. Hiekkanen and S. Kujala, "Transparency and explainability of AI systems: Ethical guidelines in practice.," *Requirements engineering: Foundation for software quality—28th international working conference,* pp. 3-18, 2022.
21. N. Balasubramaniam, M. Kauppinen, S. Kujala and K. Hiekkanen, "Ethical guidelines for solving ethical issues and developing AI systems.," *Product-focused software process improvement,* pp. 331-346, 2020.
22. D. Leslie, "Understanding artificial intelligence ethics and safety: A guide for the responsible design and implementation of AI systems in the public sector.," *SSRN,* p. 97, 2020.
23. C. Molnar, Interpretable machine learning: A guide for making black box models explainable (2nd ed.)., Leanpub, 2020.
24. M. R. Tulio, S. Singh and C. Guestrin, "Why Should I Trust You?: Explaining the Predictions of Any Classifier," in *The 22nd ACM SIGKDD international conference on knowledge discovery and data mining.*, 2016.
25. B. Arrieta, N. Díaz-Rodríguez, J. Del Ser, A. Bennetot, S. Tabik, A. Barbado, S. García, S. Gil-López, D. Molina, R. Benjamins, R. Chatila and F. Herrera, "Explainable artificial intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI.," *Information Fusion,* no. 58, pp. 82-115, 2020.
26. D. Eidle, S. Y. Ni, , C. DeCusatis and A. Sager, "Autonomic security for zero trust networks," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON*, 2017.
27. J. Kindervag, "Build security into your network's dna: The zero trust network architecture.," *Forrester Research Inc* , p. 27, 2010.
28. J. Kindervag and S. Balaouras, "No more chewy centers: Introducing the zero trust model of information security.," *Forrester Research* , 2010.
29. M. Crosignani and et al., "The Propagation of Cyberattacks through Firms' Supply Chains.," New York Fed Staff Reports, NY, 2021.
30. S. Knebel, M. D. Schultz and P. Seele, "Cyberattacks as "state of exception": Reconceptualizing cybersecurity from prevention to surviving and accommodating.," *Journal of Information, Communication and Ethics in Society,* no. 19(3), pp. 372-387, 2021.
31. Wylde, "Zero trust: Never trust, always verify.," In 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, pp. 1-4, 2021.
32. Buck, C. Olenberger, A. Schweizer, F. Völter and T. Eymann, "Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust.," *Computers & Security,* p. 110, 2021.
33. T. L. Nganyewou and F. Khomh, "(2022). Never trust, always verify: a roadmap for Trustworthy AI?," *arXiv e-prints, arXiv-2206.*, 2022.

 doi:10.20944/preprints202603.1371.v1

34. C. Sample, C. Shelton, S. M. Loo, C. Justice and L. H. Poynter, "TA: Never trust, always verify.," *In Proceedings of the 21st European Conference on Cyber Warfare and Security,* pp. 279-288, 2022.
35. R. Yumerefendi and J. S. Chase, "Trust but verify: Accountability for network services," *In Proceedings of the 11th Workshop on ACM SIGOPS European Workshop,* p. 37, 2004.
36. S. Zuboff, Interviewee, Shoshana Zuboff on Surveillance Capitalism's Threat. [Interview]. 20 12 2019.
37. M. Schroeck, R. Shockley, J. Smart, D. R. Morales and P. Tufano, "Analytics: The real-world use of big data: How innovative enterprises extract value from uncertain data," *IBM Institute for Business Value; Saïd Business School at the University of Oxford,* p. 20, 2012.
38. K. Ball, "Workplace surveillance: an overview," *Labor History,* pp. 87-106, 2010.
39. S. Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power, New York: PublicAffairs Kindle Edition, 2019.
40. Van Cleeff, and J. W. Roel, "Rethinking de-perimeterisation: Problem analysis and solutions.," in *The IADIS International Conference Information Systems 2009*, Barcelona, 2009.
41. D. Lacey, "Inventing the future—The vision of the Jericho forum.," *Information Security Technical Report,* vol. 10(4), pp. 186-188, 2005.
42. G. Palmer, "De-perimeterisation: Benefits and limitations.," *Information Security Technical Report,* vol. 10(4), pp. 189-203, 2005.
43. G. Køien, "Zero-Trust Principles for Legacy Components," *Wireless Pers Commun,* pp. 1169-1186, 2021.
44. M. Haber, "Zero Trust. In: Privileged Attack Vectors," in *Privileged Attack Vectors*, Berkeley, Apress, Berkeley, CA, 2020, pp. 295-304.
45. T. Raitsis, Y. Elgazari, G. E. Toibin, Y. Lurie, S. Mark and O. Margalit, "Code obfuscation: A comprehensive approach to detection, classification, and ethical challenges.," *Algorithms,* vol. 18, no. 2, p. 54, 2025.
46. C. Collberg, C. Thomborson and D. Low, "A taxonomy of obfuscating transformations.," 1997.
47. F. Cohen, "Computer viruses: theory and experiments.," *Computers & security,* vol. 6, no. 1, pp. 22-35, 1987.
48. F. B. Cohen, "Operating system protection through program evolution," *Computer Security,* vol. 12, no. 6, pp. 565-584, 1993.
49. S. A. Sebastian, S. Malgaonkar, P. Shah, M. Kapoor and T. Parekhji, "A study & review on code obfuscation.," in *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, 2016.
50. B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan and K. Yang, "On the (im) possibility of obfuscating programs.," *Journal of the ACM (JACM),* vol. 59, no. 2, pp. 1-48., 2012.
51. Balakrishnan and C. Schulze, "Code obfuscation literature survey.," *CS701 Construction of compilers,* vol. 19, p. 31, 2005.
52. D. B. Sohacheski, Y. Lurie and S. Mark, "Software Identifier Naming Conventions & Dictionary.," *WSEAS Transactions on Computer Research,* vol. 9, pp. 21-32, 2021.
53. F. Brunton and H. Nissenbaum, (2015). Obfuscation: A user's guide for privacy and protest., Mit Press., 2015.
54. P. O'Kane, S. Sezer and K. McLaughlin, "Obfuscation: The hidden malware.," *IEEE Security & Privacy,* vol. 9, no. 5, pp. 41-47, 2011.
55. M. D. De Jong and M. Van der Meer, "How does it fit? Exploring the congruence between organizations and their corporate social responsibility (CSR) activities.," *Journal of business ethics,* vol. 143, no. 1, pp. 71-83, 2017.
56. C. Costa, C. A. Fulmer and N. R. Anderson, "Trust in work teams: An integrative review, multilevel model, and future directions.," *Journal of Organizational Behavior,* vol. 39, no. 2, pp. 169-184, 2018.
57. Zaheer, B. McEvily and V. Perrone,, "Does trust matter? Exploring the effects of interorganizational and interpersonal trust on performance.," *Organization science,* vol. 9, no. 2, pp. 141-159, 1998.
58. J. D. Lewis, and A. Weigert, "Trust as a social reality.," *Social forces,* vol. 63, no. 4, pp. 967-985, 1985.
59. P. C. Holland, "The Importance of Trust and Business Relationships in the Formation of Virtual Organisations.," *Organizational Virtualness,* pp. 53-64., 1998.
60. G. Sanders and T. Morrow, "Zero Trust Journey," *Software Engineering Institute,* pp. 1-19, 2021.

 doi:10.20944/preprints202603.1371.v1

61. S. Rose, O. Borchert, S. Mitchell and S. Connelly, "Zero Trust Architecture," NIST Special Publication 800-207, Gaithersburg, 2020.
62. F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology.," *MIS Quarterly,* no. 13 (3), pp. 319-340, 1989.
63. D. B. Uche, O. B. Osuagwu, S. N. Nwosu and U. S. Otika, "Integrating trust into technology acceptance model (TAM): The conceptual framework for e-payment platform acceptance.," *British Journal of Management and Marketing Studies,* vol. 4, no. 4, pp. 34-56, 2021.
64. R. J. &. K. B.-T. Holden, "The technology acceptance model: Its past and its future in health care.," *Journal of Biomedical Informatics,* vol. 43, no. 1, pp. 159-172, 2010.
65. P. J. C. P. Y. K. S. O. R. L. &. T. K. Y. Hu, "Examining the technology acceptance model using physician acceptance of telemedicine technology.," *Journal of Management Information Systems,* vol. 16, no. 2, pp. 91-112, 1999.
66. D. K. E. &. S. D. W. Gefen, "Trust and TAM in online services.," *MIS Quarterly,* vol. 27, no. 1, p. 51–90, 2003.
67. T. O. Fenech, "Using Perceived Ease of Use and Perceived Usefulness to predict acceptance of the World Wide Web.," *Computer Networks and ISDN Systems,* vol. 30, no. 1-7, pp. 59-65, 1998.
68. V. &. R. V. Venkatesh, "Web and wireless site usability: Understanding differences and modeling use.," *MIS Quarterly,* vol. 30, no. 1, pp. 181-206, 2006.
69. M. X. Y. &. Y. Y. Gong, "An enhanced technology acceptance model for web-based learning.," *Journal of Information Systems Education,* vol. 15, no. 4, pp. 365-374, 2004.
70. S. Y. Park, "An analysis of the Technology Acceptance Model in understanding university students' behavioral intention to use e-learning.," *Educational Technology & Society,* vol. 12, no. 3, pp. 150-162, 2009.
71. J. C. C. C.-M. &. M. F. J. Roca, "Understanding E-Learning Continuance Intention: An extension of the technology acceptance model.," *International Journal of Human-Computer Studies,* vol. 64, pp. 683-696, 2006.
72. A. D. Y. K. R. N. P. &. W. M. D. Alalwan, "Factors influencing adoption of mobile banking by Jordanian bank customers: Extending UTAUT2 with trust.," *International Journal of Information Management,* vol. 37, pp. 99-110, 2017.
73. H. K. S. K. &. R. J. J. Albayati, "Accepting financial transactions using blockchain technology and cryptocurrency: A customer perspective approach.," *Technology in Society,* p. 62, 2020.
74. V. M. M. G. D. G. B. &. D. F. D. Venkatesh, "User acceptance of information technology: Toward a unified view.," *MIS Quarterly,* vol. 27, no. 3, pp. 425-478, 2003.
75. Bandura, "Self-Efficacy Mechanism in Human Agency.," *American Psychologist,* vol. 37, no. 2, pp. 122-147, 1982.
76. H. &. T. P. A. Wixom, "A theoretical integration of user satisfaction and technology acceptance.," *Information Systems Research,* vol. 16, no. 1, pp. 85-102, 2005.
77. R. G. V. &. P. R. Ayyagari, "Technostress: Technological antecedents and implications.," *MIS Quarterly,* vol. 35, no. 4, pp. 831-858, 2011.
78. M. C. C. L. &. S. J. F. Tarafdar, "The technostress trifecta—Techno eustress, techno distress and design: Theoretical directions and an agenda for research.," *Information Systems Journal,* vol. 29, no. 1, pp. 6-42, 2019.
79. D. K. E. &. S. D. W. Gefen, "Trust and TAM in online shopping: An integrated model.," *MIS Quarterly,* vol. 27, no. 1, pp. 51-90, 2003.
80. J. A. Colquitt, "On the dimensionality of organizational justice: A construct validation of a measure.," *Journal of Applied Psychology,* vol. 86, no. 3, pp. 386-400, 2001.