Beyond the Buzzword: How do Professionals Understand and Translate Zero Trust?

Ananta Soneji
asoneji@unomaha.edu
University of Nebraska at Omaha

Souradip Nath
snath8@asu.edu
Arizona State University

Moritz Schloegel
moritz.schloegel@cispa.de
CISPA Helmholtz Center for Information Security

Yan Shoshitaishvili
yans@asu.edu
Arizona State University

Gail-Joon Ahn
gahn@asu.edu
Arizona State University

Adam Doupé
doupe@asu.edu
Arizona State University

Carlos Rubio-Medrano
carlos.rubiomedrano@tamucc.edu
Texas A&M University-Corpus Christi

Abstract

Zero Trust has emerged as a prominent paradigm for addressing the limitations of perimeter-based security, gaining momentum through policy mandates, industry adoption, academic interest, and broader public discourse. Yet, little to none is known about how cybersecurity professionals understand and interpret Zero Trust for translation into practice and what roadblocks they perceive.

In this work, we present the first multi-sector study that investigates how cybersecurity professionals across U.S. government, industry, and academia make sense of and translate Zero Trust into practice through 27 semi-structured interviews. Across sectors, participants consistently described Zero Trust as a promising shift in security thinking, while expressing skepticism about the term itself and the impressions it creates. When translating Zero Trust into practice, they reported recurring patterns that span perceiving value, planning, execution, and measuring progress, suggesting that Zero Trust is less a destination than an evolving organizational journey. Our participants highlighted several challenges stemming from ambiguity in guidance, organizational culture, and domain-specific constraints. Our results highlight the socio-technical nature of Zero Trust adoption and identify opportunities for cross-sector collaboration, policy guidance, and future research to better support the translation and realization of abstract security paradigms such as Zero Trust in practice.

CCS Concepts

• **Security and privacy → Human and societal aspects of security and privacy**.

Keywords

Human-centered Security; Zero Trust; Sensemaking

CCS '26, The Hague, Netherlands

ACM ISBN 979-8-4007-2871-6/2026/11
https://doi.org/10.1145/3830454.3832726

ACM Reference Format:
Ananta Soneji, Souradip Nath, Moritz Schloegel, Yan Shoshitaishvili, Gail-Joon Ahn, Adam Doupé, and Carlos Rubio-Medrano. 2026. Beyond the Buzzword: How do Professionals Understand and Translate Zero Trust?. In *Proceedings of the 2026 ACM SIGSAC Conference on Computer and Communications Security (CCS '26), November 15–19, 2026, The Hague, Netherlands.* ACM, New York, NY, USA, 15 pages. https://doi.org/10.1145/3830454.3832726

1 Introduction

Organizations today need to face credential compromises [68], which allow outsiders to bypass traditional perimeter defenses such as firewalls and VPNs. They also contend with large-scale data breaches that not only cause financial losses, but also erode public trust, compromise privacy, and require lengthy recovery efforts [43, 71]. Traditional security models assume that once access to a network is granted, restrictions are minimal. Yet, as cyber threats evolve, this assumption is increasingly challenged [31, 56] through the concept of Zero Trust that advocates for continuous verification, authentication, and authorization of all users, devices, and applications connected to the network [85]. Though its core principles have existed for over two decades [18], Zero Trust has recently gained significant attention through security frameworks [18, 26, 85], academic research [41, 44, 65, 83, 100], commercial tools [105, 113, 116], and industry discourse [15, 23, 56, 66].

Zero Trust is now being operationalized across government, industry, and academia, though the drivers for adoption differ. In U.S. government agencies [16], Zero Trust adoption has been accelerated following Executive Order (EO) 14028 on *Improving the Nation's Cybersecurity* [35] and the accompanying OMB Memorandum M-22-09 [107]. Enterprises are increasingly seeing value in Zero Trust as a response to hybrid work practices and changing threat landscape [115]. The Microsoft Zero Trust Adoption report indicated that the shift to hybrid work has made Zero Trust the top security priority for decision-makers, with 96% reporting that adoption is critical to organizational success [67]. Academic research priorities are also shifting, as seen in the National Science Foundation (NSF) [72] and Department of Energy (DoE) [27] federal grants, directing tens of millions of dollars toward Zero Trust principles in secure cloud and critical infrastructure protection. Notably, the 2023 NSF Secure and Trustworthy Cyberspace (SaTC) solicitation

explicitly called for work on *"models and frameworks for trust in computing, trust metrics, zero-trust architecture, trusted execution environments, and trust through transparency and accountability"* [73].

Zero Trust is, therefore, engaged with across sectors in distinct ways: academia shapes how Zero Trust is conceptualized and researched, industry translates it into organizational strategy and practice, and government agencies apply it through mandates and policy. At the same time, Zero Trust is an intentionally abstract security paradigm [85]. While this abstraction enables broad applicability across sectors, it can also introduce ambiguity, leaving organizations to interpret and translate Zero Trust principles within their specific constraints. To examine these interpretations across sectors, we conducted a qualitative exploratory study using 27 in-depth semi-structured interviews with cybersecurity professionals representing U.S. academic, industry, and government organizations. We focus on professionals responsible for interpreting Zero Trust rather than implementers who execute specific technical controls, because these individuals shape how abstract security paradigms are understood, prioritized, and acted upon [53]. More specifically, these individuals shape organizational responses to change by bridging high-level concepts with practical action [77]. Examining their understandings is therefore critical for uncovering how abstract paradigms such as Zero Trust are interpreted and translated across sectors [3]. This study provides the first empirical, human-centered, multi-sector view of Zero Trust understanding and translation by examining the following research questions:

RQ1: How do cybersecurity professionals responsible for interpretation conceptualize and make sense of Zero Trust?

RQ2: How do cybersecurity professionals translate Zero Trust concepts into practice and what patterns emerge?

RQ3: What challenges and constraints do cybersecurity professionals identify when interpreting and translating Zero Trust?

By answering these questions, our findings show that Zero Trust represents a security paradigm shift characterized by an ongoing journey from initial sense-making and interpretation to translation and finally to navigating challenges that shape how Zero Trust efforts are sustained over time. Across sectors, participants encountered Zero Trust through different professional contexts and entry points; however, nearly all pointed to the NIST special publication on Zero Trust [85] as a foundational reference for making sense of Zero Trust (§ 5.1). While participants largely agreed with the core definition of Zero Trust articulated in the NIST document [85], they interpreted Zero Trust as a concept of "never trust, always verify" and sometimes as a repackaging of existing security practices (§ 5.2), and a response to modern organizational contexts and cybersecurity landscape (§ 5.3). At the same time, participants expressed skepticism toward the term itself, calling it a buzzword and noting that its actual meaning could be misunderstood (§ 5.4).

Rather than following a fixed blueprint, participants identified recurring patterns through which Zero Trust was perceived to be translated into practice, including perceiving value, assessing readiness and planning, selecting and adapting tools, establishing organizational processes, and measuring progress over time (§ 6.1-6.5). Participants envisioned Zero Trust adoption as an ongoing process of evolving maturity rather than a one-time deployment.

Participants also discussed challenges that shape Zero Trust efforts, including ambiguity in existing guidance and its translation beyond enterprise networks (§ 7.1), difficulties coordinating change across organizational units, skill constraints, and budget issues (§ 7.2), and contextual limitations, such as legacy systems and vendor ecosystems (§ 7.3). Our work highlights the critical need to bridge the gap between conceptual ideals and practical implementation for equitable Zero Trust adoption, and we underscore the importance of cross-sector collaboration, clearer guidance, and policy design that remains resilient to hype (§ 8). By surfacing these multi-sector perspectives, our work takes the first step to uncover human-centered insights for Zero Trust understanding.

2 Background and Literature Review

We outline the history of Zero Trust, and draw on human factors research to contextualize this socio-technical problem.

History of Zero Trust. The conceptual foundations of Zero Trust date back to the 1990s, when researchers began to recognize that traditional perimeter-based security models, referred to as "information fortresses," were insufficient for protecting information systems [11]. In 2004, these ideas were further articulated with the emergence of Zero Trust, when Paul Simmonds introduced the concept of "deperimeterization," arguing that security architectures should no longer rely on a well-defined network boundary [92]. Around the same time, the U.S. Defense Information Systems Agency and the Department of Defense (DoD) proposed the *"black core"* architecture, which advocated for securing individual transactions [14]. These early shifts in security thinking culminated in 2010, when John Kindervag of Forrester Research formally introduced the *"Zero Trust"* framework [56], which rejected the idea of a trusted internal network and instead called for security to be enforced consistently across all layers of the infrastructure, irrespective of location or origin. As the idea gained traction, practical implementations of Zero Trust principles also began to emerge, such as Google's BeyondCorp [105].

In 2018, Forrester Research expanded its vision through the Zero Trust eXtended (ZTX) framework [18], identifying seven foundational pillars. That same year, NIST Special Publication 800-207 offered standardized guidance for the architecture and deployment of Zero Trust systems in enterprise environments [85]. Federal guidance intensified with the EO 14028 in May 2021 [35], requiring all U.S. government agencies to develop Zero Trust plans. CISA responded with the Zero Trust Maturity Model (ZTMM) [19], which introduced a phased roadmap across five pillars—identity, devices, networks, data, and workloads—alongside cross-cutting capabilities such as visibility, automation, and governance. The model was updated to version 2.0 in 2023. The DoD's Zero Trust Strategy [26] established its own pillar model, overlapping with civilian guidance but emphasizing operational and mission-critical contexts. Most recently, in November 2025, the DoD released detailed Zero Trust guidance for operational technology (OT) [24], highlighting growing interest in extending Zero Trust to mission-critical systems.

Although the Zero Trust movement originated in the U.S., it rapidly drew global attention. For example, UK's National Cyber Security Centre (NCSC) followed suit and outlined eight core principles for implementing Zero Trust in 2021. Most recently, in June

2025, the National Cybersecurity Center of Excellence (NCCoE), a NIST center, released SP 1800-35: Implementing a Zero Trust Architecture [69]. Developed in collaboration with 24 industry partners, the guide provides 19 detailed example Zero Trust deployments using off-the-shelf technologies to address real-world scenarios, making it the most concrete guidance to date.

Existing Literature on Zero Trust. Academic research predominantly focuses on technical aspects, surveying Zero Trust components, such as identity authentication, access control, trust evaluation algorithms, encryption, and security automation [44, 100, 111]. These surveys map the technical landscape, but they overlook the organizational dimensions of Zero Trust adoption. While one work notes challenges including vendor lock-in, interoperability, and legacy migration [101], these accounts do not reflect practitioner perspectives from real-world implementations.

Recent studies [7, 41, 81] have explored broader strategic and architectural concerns to offer high-level frameworks and recommendations. A few studies [13, 52] have highlighted the disconnect between academic research and practical implementation by reviewing both academic and grey literature [86]. Their findings reveal that while academic research has primarily focused on architectural models and performance improvements, practitioner literature tends to emphasize organizational outcomes and migration strategies. Despite these efforts, neither perspective offers a comprehensive view of Zero Trust adoption, particularly one that integrates human and organizational dimensions.

Human Factors in Cybersecurity. Since its inception by Zurko and Simon [117], *user-centered security* has focused on simplifying security and privacy for end-users [2, 25, 45]. Moreover, research on human factors has also highlighted how social behaviors [21, 110], organizational roles [59], levels of expertise [50], and decision-making processes [33] shape the adoption and effectiveness of security practices. Specifically, researchers have begun to explore the perspectives of security leaders and experts, such as Chief Information Security Officers (CISOs), in shaping organizational security posture [20, 87]. Across several studies, CISOs are portrayed as key interpreters of abstract cyber risks who need to balance technical execution with organizational dynamics, credibility-building, and cultural integration tensions [5, 46, 108]. Recent work also explored how the intra-organizational flow of information influences the decision making about cybersecurity risk at the C-suite level [76]. Building on this work, we extend the literature by examining how professionals across academia, industry, and government understand and translate an emerging security paradigm, Zero Trust, within their respective contexts. In doing so, we fill a gap in existing literature by uncovering the human side of Zero Trust, which can inform collaborations, policy guidance, and future research.

3 Methods

To explore how the concept of Zero Trust is understood and interpreted for translation, we designed a multi-sector qualitative study. We conducted one hour-long semi-structured interviews [1] with 27 U.S.-based cybersecurity professionals from government, industry, and academia between November 2023 and July 2024.

3.1 Recruitment Process

We recruited 27 participants with Zero Trust familiarity and experience through a combination of purposive [32] and snowball [78] sampling from government, academia, and industry. Government participants (n=7, G1–G7) were all federal CISOs. Two participants were recruited through in-person engagement at a Zero Trust workshop, others via LinkedIn [62] outreach (n=2) or referrals from previous participants (n=3). Academic participants (n=11, A1–A11) were principal investigators identified through publicly funded grants that referenced Zero Trust. We sent email invitations to randomly sampled principal investigators. Out of eleven, one participant was recruited via professional network and another through referral. Industry participants (n=9, I1–I9) were CISOs or security leads and the most challenging to recruit due to limited public visibility and time constraints [6]. We recruited them primarily through professional contacts (n=4), participant referrals (n=3), and LinkedIn outreach (n=2). Recruitment required sustained effort over a nine-month period. Overall, we sent 68 email invitations and 86 LinkedIn messages, each accompanied by two follow-ups.

3.2 Interview Design and Data Collection

We designed the interview guide to elicit participants' perspectives across three key areas: (1) understanding of Zero Trust, (2) strategies, patterns, and challenges, and (3) forward-looking perspectives on its evolution.

Interview Guide. We began with rapport-building questions to gather views on trust, trust-related risks, and verification in cybersecurity, followed by questions under each core area. In the first part, we asked participants to reflect on their understandings of Zero Trust, its differences from traditional models, and their experiences engaging with Zero Trust guidance. In the second part, we explored strategies for translation, cost and culture expectations, encountered/perceived challenges, and lessons learned. Lastly, participants articulated their perspectives on the anticipated evolution of Zero Trust and offered any final feedback or reflections.

Piloting. The interview guide was piloted with three cybersecurity professionals: a system administrator involved in implementing Zero Trust at a higher education institution and two academic cybersecurity principal investigators researching Zero Trust-related topics. The system administrator's pilot helped refine question clarity and phrasing, ensure topic coverage, and improve conversational flow. The academia pilots' feedback confirmed the guide's suitability for participants from academic settings to gather conceptual (and practical) nuances related to Zero Trust.

Data Collection. The primary author contacted, received consent, and interviewed all study participants. Recruitment was conducted through email and LinkedIn outreach, using a standardized message and a consent form that explained the study's purpose, procedures, time commitment, and compensation. After providing consent, participants completed a brief demographic survey. Interviews were then conducted via Zoom using a semi-structured interview protocol and lasted 39–109 minutes (mean = ~66 minutes). At the beginning of each interview, the interviewer introduced the study, reviewed participant rights, explained that any sensitive information would be anonymized, and obtained verbal consent to record. After the interviews, participants were thanked, invited to share

Table 1: Coding Progression and Codebook Development

Phase	Transcripts	κ
Initial open coding: Initial themes, codebook created	9	0.76
Round 1: Added themes and open codes	(+4) 13	0.70
Round 2: Refined and structured themes	(+3) 16	0.71
Round 3: Refined theme definitions, minor code additions	(+3) 19	0.76
Final validation: Codebook finalized	(+3) 22	0.75
Independent coding: Remaining transcripts	(+5) 27	–

final thoughts, and asked to recommend potential participants. Participants were then offered a $50 compensation, which 11 declined. Interview recordings were transcribed using Zoom and manually reviewed by the primary author for accuracy. Personally identifiable information (PII) was then removed, and participants were assigned anonymized identifiers prior to analysis. Details of our replication package are provided in the Open Science section.

3.3 Data Analysis

We performed inductive thematic analysis [12] on the interview data using MAXQDA [82]. Two researchers with prior experience in qualitative human-centered security research independently began open-coding [96] on a subset of nine transcripts, equally sampled across all sectors. We coded them in batches of three, followed by collaborative meetings with the team to discuss emerging patterns. These open-coding sessions informed the development of an initial codebook, which was then applied to the same nine transcripts to assess the relevance, clarity, and coverage of the codes. We then iteratively refined the codebook through repeated rounds of double-coding [48], team discussions, and inter-rater reliability (IRR) checks using Cohen's Kappa (κ) [64], summarized in Table 1. This iterative approach is considered best practice in human factors security research to enhance coding rigor and transparency [74]. After double-coding 22 transcripts, we observed thematic saturation (i.e., no new major themes emerged), consistently reached substantial agreement on code application ($\kappa \geq 0.70$), and finalized the codebook. We therefore did not recruit additional participants beyond those already scheduled. The remaining five interviews (1 government, 2 industry, 2 academia) were coded by the primary researcher using the finalized codebook, while keeping the second coder updated. Throughout the analysis, our research questions guided coding decisions and codebook refinement. We organize our results around the major themes and subthemes that emerged from the analysis, together with the five-stage translation process presented in Section 6.

3.4 Limitations

Our study aims to surface nuanced, human-centered insights into how Zero Trust is understood and navigated across sectors. As an exploratory qualitative study, our findings are context-dependent and intended to provide analytical rather than statistical generalization. Despite the double-coding process and iterative codebook refinement, our coding involved interpretation, and other researchers might organize the data differently.

Purposive sampling allowed us to target experienced professionals across sectors, but it inherently limits randomness and may introduce self-selection biases from those already interested in or engaged with Zero Trust. While our participants span diverse roles, responsibilities, and sectors, we did not systematically sample for diversity within each sector (e.g., organization size, region, or research subfield), so some nuances may therefore be underrepresented. Although our participants were based in the United States, organizations worldwide adopting Zero Trust must similarly translate high-level principles into operational practices, coordinate across technical and organizational stakeholders, and balance security goals with existing workflows. As Zero Trust adoption expands globally, future work should examine how regional regulatory, cultural, and organizational contexts shape these translation processes and the extent to which our findings generalize beyond the U.S. context. We may have missed perspectives from individuals with differing levels of opinions on Zero Trust (e.g., from those holding strong negative views of the concept). We sought to mitigate this through semi-structured interviews that encouraged elaboration and follow-up. However, the data is shaped by what participants chose to share and how they framed their experiences.

Finally, our participants primarily occupied leadership, decision-making, or research roles. While this aligns with our goal of exploring Zero Trust sense-making and translation, it may not represent the day-to-day practices and challenges of engineers, operators, and frontline security teams. Future research can build on this work by examining how the interpretations identified here are enacted at the ground level, how they evolve over time as deployments mature, and how Zero Trust is understood and implemented across a broader range of organizational and global contexts.

Table 2: Participant Demographics

Gender	**#A**	**#G**	**#I**	**∑**
Man	10	7	7	**24**
Woman	1	0	2	**3**
Current Job Title	**#A**	**#G**	**#I**	**∑**
CISO (or similar)	N/A	5	5	**10**
Research Professor	6	N/A	N/A	**6**
Research Scientist (or similar)	3	0	0	**3**
Cybersecurity Director (Academic)	2	N/A	N/A	**2**
Security Architect/Engineer	N/A	1	1	**2**
Zero Trust Program Manager	0	1	0	**1**
Others (e.g., Consultant, Self-employed)	0	0	3	**3**
Organization Sector	**#A**	**#G**	**#I**	**∑**
Education and Research	7	0	1	**8**
Information Technology (IT)	1	0	5	**6**
Non-Profit and Others	3	1	2	**6**
Healthcare	0	4	0	**4**
Familiarity with Zero Trust	**#A**	**#G**	**#I**	**∑**
Extremely Familiar	5	7	5	**17**
Moderately Familiar	5	0	4	**9**
Somewhat Familiar	1	0	0	**1**
Areas of Expertise relevant for Zero Trust	**#A**	**#G**	**#I**	**∑**
Network and Endpoint Security	8	7	7	**22**
Identity Governance and Access Control	6	7	8	**21**
Cloud Data Protection and Encryption	2	7	9	**18**
Cybersecurity Policy and Strategy	6	6	5	**17**
Risk Assessment and Management	3	7	4	**14**
Others	1	0	5	**6**

A: Academia, **G:** Government, **I:** Industry, **N/A:** Not Applicable

4 Participants

In total, we interviewed 27 cybersecurity professionals representing academia (n=11), industry (n=9), and government (n=7), categorized

by their primary organizational affiliation. Table 2 outlines participant demographics. Participants reported an average of over 18 years of professional cybersecurity experience and predominantly held senior or leadership roles, positioning them to interpret Zero Trust within their organizational or research contexts. Most were affiliated with large organizations (n=24) and operated in environments handling sensitive data (n=25), such as health records, financial information, proprietary business assets, and research and educational institute data. They reported expertise across technical and governance areas relevant to Zero Trust (Table 2). Twenty participants (government = 7, industry = 8, academia = 5) indicated that their organization was either implementing or considering Zero Trust. All participants reported at least some familiarity with Zero Trust. To contextualize the participants' self-reported Zero Trust familiarity ratings, we analyzed participants' open-ended responses to: *Please provide details regarding your selection of familiarity with Zero Trust,* in which they reported how Zero Trust related to their research and professional activities.

Most academic participants' engagement with Zero Trust was shaped by research agendas and collaborations, rather than by direct responsibility for organizational deployment. They described investigating how Zero Trust could be adapted to environments with domain-specific constraints, how policies could be defined and interpreted across systems (e.g., 5G, energy, and transportation), and how commercial communication infrastructure could be used in government or defense settings not originally designed with hardened security assumptions. They also engaged with Zero Trust through reading relevant literature, incorporating it into coursework, and collaborating with federal or industry partners. Out of eleven, one academic participant was affiliated with a research center, and two worked closely with non-profit organizations where they led and supported Zero Trust research and guidance initiatives.

For all government participants, Zero Trust engagement was driven by policy mandates, with roles focused on oversight and accountability rather than executing individual technical controls. Their work centered on interpreting Executive Order 14028 [35] and OMB M-22-09 [107] and developing agency-level strategies and plans. They also reported working in complex environments involving legacy systems, coordination across organizational units, and interactions with external stakeholders such as vendors.

Our industry participants reported engaging with Zero Trust to improve organizational network security postures, consult on Zero Trust strategies, author Zero Trust guidance, conduct Zero Trust workshops, and research the feasibility of Zero Trust within their respective domains. Five participants were CISOs or security leads, including one who had left within six months of the interview time and reflected on prior Zero Trust-related work. Three participants were independent security consultants providing Zero Trust guidance to industry and government organizations. One was a Zero Trust research lead at a nonprofit organization.

5 Conceptualization and Sensemaking (RQ1)

To understand how cybersecurity professionals make sense of Zero Trust, we asked participants about their initial exposure to the concept, key sources of reference, and interpretive frames used to reason about what Zero Trust is and what it promises.

5.1 Entry Points and Sources of Understanding

Participants across all sectors commonly grounded their understanding of Zero Trust in shared origin narratives and authoritative reference materials. During the interviews, all participants referenced John Kindervag's white paper [56] as a key origin point, with several referring to him as *"the father of Zero Trust"* (G4). Beyond this, they engaged with Zero Trust through a mix of foundational resources, vendor materials, and the EO 14028 [35].

Academia participants (A1, A2, A3, A6) approached Zero Trust through institutional interest and research on identity management, cloud security, and access control. In forming their understanding, they relied on foundational documents such as NIST 800-207 [85], CISA maturity model [19], and MITRE ATT&CK [97]. Several academic participants also consulted industry-authored resources such as BeyondCorp [105] or BastionZero tutorials [10] for their operational clarity. Meanwhile, A8 expressed concern about the proliferation of vague or vendor-driven materials, warning against being *"thrown down a Zero Trust rabbit hole"* and added: *"People throw [Zero Trust] into everything these days."*

Most industry participants often began with *"publicly vetted baselines"* (I2) such as NIST 800-207 [85] (*"excellent foundational document,"* I6) and CISA maturity model [19]. I6 called BeyondCorp [105] *"a huge gift to the industry,"* and I3 emphasized the role of Gartner [40] reports to translate abstract principles into organizational contexts, support tool evaluation and facilitate internal buy-in. According to I4 and I5, Zero Trust evolved from theoretical reports to something that vendors market aggressively without technical grounding (*"Vendors love marketing,"* I5).

All government participants' engagement was triggered by EO 14028 [35] and OMB M-22-09 [107]. They noted relying heavily on NIST [85] and CISA [19] documents to interpret mandate expectations. G2 and G4 blended multiple frameworks to guide agency-specific strategies. Beyond formal guidance, participants, such as G7, emphasized experiential learning, noting that understanding often develops *"from the scar tissue of others."* G2 described the *"crawl, walk, run"* approach to discuss Zero Trust maturity, treating it as a gradual and evolving concept rather than a binary state (§ 6.5).

5.2 Conceptual Understanding

After describing how participants first encountered Zero Trust and the sources they relied on, we next describe how participants conceptualized Zero Trust. Almost all participants agreed with NIST SP 800-207's definition of Zero Trust: *"Zero trust is a cybersecurity paradigm focused on resource protection and the premise that trust is never granted implicitly but must be continually evaluated"* (p. 4, [85]). However, their responses indicated that they understood Zero Trust beyond this formal definition.

Across sectors, almost all participants emphasized that Zero Trust should not be understood as a specific technology, product, or deployable system. Instead, they characterized it as a conceptual approach to security. An academic participant regarded Zero Trust as *"a philosophy... not a method or a framework"* (A3), while a government participant called it *"just a concept"* (G1).

5.2.1 "Never trust, always verify" as a core logic. All participants' conceptual understanding of Zero Trust was closely tied to the principle of "never trust, always verify." The idea of *trust* based

on network location, user role, or past authentication was unanimously rejected. G1, along with eleven other participants, reminded that *"trust implies vulnerability and the word is inherently flawed."* Participants, therefore, used this idea to explain how Zero Trust departs from earlier security models that rely on implicit trust based on network location, role membership, or prior authentication. G3 framed Zero Trust as a shift *"from implicit trust to dynamic, explicit trust"*. Several participants described Zero Trust in functional terms, such as ensuring *"the right people get access to the right resources at the right time"* (A3), but emphasized that access decisions should not be made once and assumed to remain valid. As one government participant, G2, explained that if *"you are a user and want to access something, In Zero Trust, I'm going to keep checking you. In a non-Zero Trust setting, I'd probably let you go and say have a nice day."* Similarly, A10 framed Zero Trust as "the art of not trusting until convinced otherwise." According to some of our participants, with Zero Trust, *trust* was not eliminated, but treated as conditional and was continuously reassessed to contain evolving risks (I7, § 5.3).

5.2.2 A reframing of existing security principles. 22 participants viewed Zero Trust as closely connected to familiar principles of least privilege and defense-in-depth. As A8 noted, "at its root, it's least privilege," while I5 stated: "The principles of Zero Trust are an extension of security principles that have existed for 30 years." At the same time, they also emphasized that Zero Trust reframes how these principles are applied.

Eight participants criticized traditional role-based access control (RBAC) [89] as too coarse for modern Zero Trust environments, noting that access decisions increasingly require accounting for specific identity distinctions and contextual factors. As G6 shared, access decisions increasingly depend on details such as *"whether you're a federal employee or a contractor."* In this context, participants mentioned attribute-based (ABAC) [54] and relationship-based (ReBAC) [38] models as examples of how Zero Trust extends existing access control ideas rather than replacing them as these models shift security decisions from static group memberships to dynamic, context-aware controls.

Several participants also emphasized that Zero Trust shifts the trust boundary, moving away from network-based security toward data-centric security practices. G2 explained: *"In Zero Trust, the network becomes less of the security enforcement and more of the transport. I'm moving the authority away from the network and doing microsegmentation*[1] *around the data"*. A7 similarly said that *"security is about [protecting] data."* Overall, participants considered Zero Trust to prioritize protection of (sensitive) resources rather than reliance on perimeter controls.

5.3 Perceived Benefits of Zero Trust

Participants pointed to several perceived benefits of Zero Trust that shaped how they made sense of the paradigm.

5.3.1 Containing modern attacks and limiting blast radius. Twenty participants viewed Zero Trust as a timely response to modern, high-profile cyberattacks that rely on credential compromise [63, 68] and lateral movement.[2] I7 cited the Scattered Spider hacking group [17], known for identity hijacking, to explain why Zero Trust's emphasis on combining identity, device posture, and contextual signals resonated with them.

Ten participants referred to Zero Trust as embodying an *assume-breach mindset*, reframing security from prevention-only to continuous damage containment. I7 explained that *"Zero Trust always assumes that you are breached... and builds solutions to reduce threat actors' time within your environment."* A3, G3, and G6 praised Zero Trust for its ability to limit the *blast radius* of attacks by tightly controlling lateral movement through continuous authentication, authorization, and verification. This containment logic was seen by participants as a marked departure from earlier perimeter-based models. A7 pointed out that perimeter defenses failed in breaches such as RSA [42], Chase [84], OPM [39], where attackers roamed freely once inside. A11 went further: *"Stuxnet [34] had 87 places where Zero Trust would've blocked it."* A4 acknowledged that *"Zero Trust doesn't solve everything, but it raises the cost for attackers... It deters amateurs and slows professionals."*

5.3.2 Adapting to distributed work environments. Ten participants regarded Zero Trust as better aligned with environments where users, devices, and resources are highly distributed. Pandemic-induced remote workforces were cited as contexts where perimeter-based trust assumptions no longer hold. A1 argued that organizations with *"mobile workforce[s], third-party vendors, and supply chains"* are well-suited. Similarly, I2 shared that fine-grained access needs and growing identity complexity *"should drive Zero Trust architecture."* Industry participants often grounded this reasoning in their own organizational experiences. I7 reflected that in a 98% remote company, *"rather than putting in VLANs... we looked at implementing Zero Trust tied to identity."* I4 noted that early remote-work security changes in 2020 initially seemed effective, but later revealed lingering implicit trust, highlighting the value of Zero Trust in surfacing hidden trust assumptions.

Migrations to the cloud further reinforced these views. G5 questioned the relevance of traditional perimeter defenses in cloud environments, asking, *"Where's that perimeter when it's in the cloud? There is no address for you to protect."* A5 emphasized its relevance across mobile, cloud, and cyber-physical systems. I7 emphasized that organizations transforming their technology stack are more likely to benefit from adopting Zero Trust, *"as their identity and authentication methods begin to improve."*

5.3.3 Supporting scale, asset criticality, and business continuity. Organizational scale and asset sensitivity were considered factors that shaped Zero Trust's perceived value. G4 noted that *"least privilege got lost"* amid scale and speed demands and according to I2, *"the value and sensitivity of assets and the number of different identities to authorize"* should shape Zero Trust decisions. Startups were often seen as better positioned to realize Zero Trust. I7 described them as *"the unicorn version of Zero Trust... the best of the best,"* free from inherited technical debt and legacy infrastructure unlike most companies, where *"it's [Zero Trust is] layered atop what already exists."* We expand on legacy-related barriers in Section 7.3.

[1] Microsegmentation means dividing the network into smaller, isolated zones, each with its own set of security policies and access controls [91].

[2] Lateral movement refers to the process of moving through the network after gaining initial access to search for high-value assets [9].

Moreover, eight participants connected Zero Trust's value to business continuity. G5 said it can mitigate compromise while minimizing disruption to mission-critical operations. A6 and I2 noted that it helps embed authentication and authorization into system design, helping organizations protect assets while scaling securely. Several participants framed Zero Trust as enabling better security. G2 highlighted, it can help organizations move from *check-box compliance to effective security*: *"Compliance says, 'you need authentication'—so people say 'okay, username and password.' That's compliant, but not effective... Zero Trust pushes you toward effectiveness." G7 believes non-federally mandated organizations will* "embrace" *Zero Trust and I6 shared that even less mature enterprises will be drawn by the strong interest and momentum. I7 reinforced this perspective:* "Back in the day, moving to the cloud was a big no-no... But now [all big banks] have a presence in [one of the big three cloud providers]. That shift has already occurred. So, we're going to see more and more companies implement some version of Zero Trust."

5.3.4 Integrating fragmented security. Eight participants also regarded Zero Trust as valuable for addressing fragmentation caused by traditional security approaches. For example, prior research shows that VPN-centric and firewall-based approaches have been difficult to manage at scale and are frequently misconfigured [109]. Reflecting on this challenge, A2 framed Zero Trust as beneficial because it provides a more unified way to reason about security across complex environments. Some participants also linked technical fragmentation to organizational silos. G2 described prior security efforts as *"stovepipes of excellence,"* where identity, networking, and endpoint teams operated independently, often without a shared architectural view. They added: *"The data pillar, the application pillar, the network pillar, the endpoint pillar, and the identity pillar all come together"* in Zero Trust. I5 summarized this shift by framing Zero Trust as moving security away from decentralized enforcement toward a more integrated approach that supports coordinated security decisions across the organization and its processes (§ 6.4).

5.4 Semantic Ambiguity and Skepticism

Across sectors, "Zero Trust" was perceived as simultaneously powerful and problematic. Several noted that the phrase is *"catchy"* (G7) but poorly specified, which complicates shared understanding and communication. As A2 remarked, *"it's a big buzzword, there's not a lot of consensus on what it means."* Others highlighted that *"zero" trust* is misleading or conceptually unrealistic. A8 remarked, *"people say verify everything, but even verification requires trusting something—that's what bothers me. It's not 'zero' trust. You always trust something."* I3 noted that the term often raises concerns among non-technical stakeholders such as business leaders as it sounds *"dangerous... like an undesirable thing to have no trust."* Therefore, I9 said that *"whoever didn't consult a marketing team and called this Zero Trust is killing us."* Hence, G4 suggested that *"we need terminology with staying power"* and eight participants proposed reframing Zero Trust as *"managed or epsilon trust."*

G3 initially dismissed Zero Trust as *"a buzzword... like FISMA [Federal Information Security Management Act of 2002 [37]] all over again."* This skepticism, although not universal, reflected concern that Zero Trust could become another checklist-driven compliance exercise, similar to FISMA [49, 80]. However, G3 called themselves *"a convert"* after seeing how Zero Trust principles could be applied more substantively. G2 noted: *"People are finally coming around; the light bulbs are starting to go off."*

Despite these critiques, several participants did not view the term's ambiguity as purely negative. As per I9, *"[Zero Trust] term has proven useful as a conversation starter and investment driver."* Therefore, G2 advised to *"get over the semantics of what it's called."* A11 added: *"I don't think Zero Trust is a silver bullet solution. But what it does is, it highlights the things we need to be thinking about in a nice, concise, and actionable way."*

> **RQ1 Summary:** Participants consistently described Zero Trust not as a technology but as a conceptual lens for enhancing security and reasoning about modern challenges. At the same time, they viewed it as a hype-driven paradigm that mobilizes attention around important ideas while remaining vulnerable to misunderstanding and oversimplification. This tension can deeply influence whether Zero Trust matures into a coherent security paradigm or remains a loosely understood buzzword.

6 Translation Patterns (RQ2)

While participants shared broad agreement on the core ideas underlying Zero Trust (RQ1, § 5), they viewed translating those ideas into practice as neither straightforward nor uniform. Rather than a fixed checklist or predefined blueprint, 13 participants characterized Zero Trust translation as an ongoing, iterative process of building security maturity [19] through remarks such as *"it's a journey because the landscape is always changing within the infrastructure"* (I5) and *"you'll never arrive at Zero Trust"* (G3). G6 summarized:

> *"Zero trust is not a start-and-finish type thing... we may never get to a fully optimal state of Zero Trust, but we'll keep moving toward that goal."*

Many participants also emphasized that translation extends beyond technical controls. As I8 put it: *"People need to get away from the products and think about what they are protecting."* And G4 noted that effective Zero Trust efforts require deliberately combining *"people, process, and technology,"* highlighting the socio-technical coordination involved.

Building on this, during the interviews, participants described recurring patterns through which Zero Trust was (perceived to be) translated into organizational practice. These patterns reflect how organizations interpreted Zero Trust, coordinated activities, and sustained change under real-world constraints. Industry and government participants reported actively shaping these efforts within their organizations, while academic participants drew on experiences from multi-disciplinary research projects on Zero Trust and collaborations to reflect on similar transitions. We organize these translation patterns into five interrelated stages: perceiving value, assessing readiness and planning, selecting and adapting tools, establishing organizational processes, and measuring progress over time. Participants emphasized that while these stages formed a logical flow, organizations may often revisit them as priorities, resources, and threat conditions evolve, with people—not tools—being seen as moving the needle.

6.1 Perceiving Value

Twelve participants considered it important to *demystify* Zero Trust, noting that greater awareness can improve cybersecurity task management and influence employee behavior [4, 61]. They described this early phase as focused on interpretation and alignment, rather than technical change.

Communicating intent. G1 called *"assume breach"* and *"never trust, always verify"* catchphrases, warning that such jargon risks confusing non-experts if introduced without context. I4 characterized early-stage discussions as sensemaking sessions by asking: *"What is Zero Trust? What are its principles? What are the tenets? What does this mean to us?"*

To overcome translation issues, government participants often relied on analogies for building shared understanding before broader organizational engagement. G1 compared Zero Trust to *"car insurance"*—always present, even when not in active use. Several contrasted Zero Trust with traditional perimeter-based models to illustrate risks of implicit trust and lateral movement. G2 compared legacy security to a multiplex theater where users could *"movie hop"* unchecked once inside, while G3 and G4 referenced *"castle-and-moat"* and *"Tootsie Pop"* architectures to highlight how attackers could move freely after initial access. Such use of metaphors and analogies reflects a broader sensemaking practice, in which leaders reinterpret abstract security paradigms by mapping them onto familiar concepts to facilitate shared understanding [93, 106].

Framing for executive buy-in. Eleven participants emphasized that executive sponsorship played a critical role in adopting Zero Trust [28, 58]. Prior work shows that CISOs often struggle to demystify complex security paradigms to ensure leadership buy-in [20, 87]. Our participants reframed Zero Trust in terms of organizational priorities rather than treating it as a purely technical security initiative. I3 explained: *"I don't ask [leadership] for Zero Trust funds. I ask for the technology that will enable [our mission] to move faster... I very rarely actually invoke the kind of cybersecurity language with most of my executives."* I5 added that *"one of the jobs of a CISO is to bridge that gap between business benefit and technology—and the impact of security on top of that."* G3 cautioned that without leadership support, Zero Trust efforts could stall: *"Zero Trust can't be the CISO saying we need to do it. You need your executive leadership to support it before you ever decide to start... Otherwise you're climbing a very, very long hill by yourself."* A11 echoed:

> *"I don't think boards are going to demand Zero Trust, it needs to be communicated and driven."*

Top-Down meets Bottom-Up. All industry participants, along with G1, G3, and A11, emphasized that perceiving value required both top-down support and bottom-up traction. I1 summarized: *"Bottom-up data to show it's a good idea, top-down leadership to make sure it happens."* I2 viewed this process as iterative and added: *"but once the right people with the right mindset come together, they start building the right structure."* I6 highlighted that Zero Trust required broader organizational involvement: *"Security drives it, IT supports it, but success depends on bringing in the right stakeholders—data owners, application owners, or business leads—especially where they'll be impacted."* Prior work on compliance mandates suggests this dual approach can foster shared ownership of security [94].

6.2 Assessing Readiness and Planning

Following initial value alignment, fourteen participants reported assessing existing infrastructure, identity systems, and organizational capabilities. These *reality checks* were deemed critical to uncover gaps, surface constraints, and establish a realistic scope for Zero Trust efforts. G3 described this stage as a *"critical early win"*—an opportunity to define scope and set expectations.

Twelve participants emphasized the importance of translating Zero Trust principles into concrete roadmaps. G1 shared how the mandate [107] provided structure for their internal plan: *"I laid out all the pillars, recognized all the tools that I needed for optimum maturity, and set it by fiscal year. That's how we had a plan that went from FY23–FY25."* In the absence of a *"ubiquitous solution"* (G5), maturity models such as those from CISA [19] and DoD [26] were commonly used to guide roadmap development. After using CISA's maturity model [19], G6 recalled that *"we already had many of the tools we needed... we just needed to work with the right people to configure them to support Zero Trust."*

All industry participants emphasized that roadmaps had to reflect business realities. I4 noted successful organizations tied Zero Trust phases to internal reporting: *"they deliver some value out of Zero Trust every quarter."* I5 connected Zero Trust planning directly to business risk and said: *"each organization needs to look at their own risk profile and basically do a risk evaluation and look at where are the critical risks from a business perspective. Technology should not exist for technology's sake. Technology exists for supporting the business."* Finally, I6, who provides Zero Trust strategy guidance for multiple enterprises, noted that roadmaps and assessments help organizations shift from ad hoc to structured Zero Trust planning, enabling more deliberate progress rather than reactive change.

6.3 Identifying and Procuring Tools

11 participants emphasized that translating Zero Trust into practice involved decisions about tools and technology, but warned against *"treating Zero Trust like a procurement checklist"* (G4). G2 cautioned organizations not to *"go out and buy 70 things."* Instead, participants described reusing existing capabilities with targeted acquisitions.

Quick wins. A common starting point in academic and government settings was multi-factor authentication (MFA) [75], as A2 explained: *"We have DUO to help with two-factor authentication. If that checks the Zero Trust box, then we were doing it."* A3 framed MFA as an entry point while noting future needs for additional integrations to *"get towards a higher level of Zero Trust."* Government participants referred to MFA as foundational, alongside investments in Secure Access Service Edge (SASE) [51] and endpoint detection tools. G1 called these *"a game changer"* for replacing perimeter-based security at scale.

Vendor engagement. Some participants found vendor interactions as enabling factors rather than administrative hurdles. G5 noted that involving vendors early allowed teams to understand trade-offs. I6 highlighted the importance of clarifying internal requirements beforehand to *"avoid mismatched vendor solutions."* G3 underscored the leverage large institutions, *"the Federal Government is the largest employer in the U.S.,"* can bring during vendor interactions because *"[vendors] want to sell us the products to meet the requirements that we have... a win-win situation."*

At the same time, A3 and A7 noted that outsourcing is an option. A7 cautioned that outsourcing the *"entire Zero Trust transition"* without a full understanding of the enterprise could result in an implementation misaligned with organizational needs.

The role of internal expertise. Nine participants stressed that effective tool selection and integration depended on internal technical expertise. A2 echoed: "If you don't know what the tool is doing, how can you judge if it supports Zero Trust?" and G7 believed: *"You either need to have it [technical competence] or the ability to go get it."* Hence, these teams need sufficient understanding and skills to evaluate, configure, and integrate tools effectively.

While the NIST Zero Trust document [85] defines conceptual components, I6 emphasizes that *"ultimately, they [IT] need to deploy the software"* and I7 stresses that these teams need to *"have the underlying understanding of key stacks within the Zero Trust pillar."*

Some participants described how they addressed these needs through targeted and role-specific training. G6 shared: *"We did multiple trainings—executive level, business user level, developer level. Each one needed a different curriculum."* G4's organization is creating maturity-level-based curricula, because *"not everyone needs to be a Zero Trust architect, but they need to know their role."*

6.4 Establishing Processes

Twenty-six participants discussed establishing organizational processes for Zero Trust translation. Rather than viewing Zero Trust as a set of isolated controls (§ 5.3), participants emphasized the need to embed it into everyday operational workflows, governance structures, and coordination mechanisms [112].

Mapping data flows and assets. Eight participants stressed the importance of understanding how data, applications, and devices interact within organizational environments. They identified activities such as network mapping, asset inventories, and dependency analysis as foundational to making informed trust decisions. As I7 explained: *"First and foremost, review your environment and have an understanding of where your crown jewels are located and how your users interact with data within your environment. Because once you have that understanding, the technology portion will be an easier journey to apply."* A5 described their observation: *"You see universities slowly auditing what connects to what—printers, lab systems, cloud data—and that gives them a picture to make trust decisions."* G6 found understanding data, applications, and their risk levels crucial to implement *"a microsegmentation strategy"* as it can help block communication *"with high risk devices."*

Continuous authentication and authorization. Seven participants regarded Identity and Access Management (IAM) as central to Zero Trust processes. G4 said: *"If we don't know who you are and what you should access, Zero Trust is meaningless. So, identity became our north star—we invested in cleaning up directories, standardizing attributes, and building consistent onboarding and offboarding."* Moving from static authentication to dynamic, context-aware access decisions was heavily mentioned. I4 explained: *"We started by tightening IAM, but the long-term target was adaptive access looking at device posture, location, and even behavior before granting access."* A9 observed a similar shift in academic environments, noting that "universities already rely heavily on federated identity like Shibboleth, but what changed was how strictly access is enforced and how often it is re-evaluated." G7 illustrated this shift:

> *We are experimenting with behavior analytics; if someone usually logs in from D.C. and suddenly shows up in Singapore at 3 a.m., that would be triggered.*

I5 emphasized the need to integrate authorization across systems under Zero Trust: *"it's not just about users—it's also about workloads, endpoints, servers, and network devices. Identity is central, not just the subject but the object too."* G6 added: *"We had to get our authentication and authorization stack understood top to bottom, because Zero Trust breaks fast if you don't know how tokens, attributes, and roles actually work in your environment."* This shift demands a deep understanding of how access decisions are made and enforced through policy.

Grounding policy in practice. While fewer in number, four participants emphasized that translating Zero Trust into clear, enforceable policy required attention to real-world workflows. I5 explained: *"Policy is where the rubber meets the road; if you don't define who can access what under what conditions, the tools don't matter."* They emphasized that writing effective policies requires understanding how users actually accessed systems and resources.

Establishing governance and coordination. Five participants reported forming dedicated teams or governance structures as necessary to coordinate Zero Trust efforts across organizational silos that traditionally operated independently. G2 shared: *"We created a tiger team, full-time folks just for Zero Trust. Their job was to coordinate pillars, make sure IAM, network, and data teams were actually working from one playbook."* A10 described a similar governance structure in an academic setting: *"There's now a Zero Trust steering group—mostly IT security, some faculty—to decide on priorities and funding."* Beyond dedicated teams, participants emphasized broader coordination across the organization. G1 referred to Zero Trust as a *"team sport."* I4 shared that their organization created a steering committee with all the key stakeholders including legal, compliance, IT, and security to realize Zero Trust efforts. G6 echoed this need for cross-functional engagement, noting involvement of "finance, mission ops, and others—not just tech."

6.5 Measuring Progress

Twenty-one participants framed Zero Trust as a way to sustain momentum, demonstrate value, and support accountability over time. Moreover, during the interviews, participants consistently highlighted that measuring Zero Trust progress was necessary but challenging, pointing to the absence of a clear endpoint, standardized metrics, or shared definition of success.

Establishing baselines and tracking change. To assess progress, participants emphasized the importance of establishing baselines and tracking changes over time. For several government participants, CISA's maturity model [19] proved valuable to plan roadmaps (§ 6.2) as well as evaluate progress. G2 shared that their organization established a baseline through a "Zero Trust roadmap development workshop," which was used to track and visualize progress over time and highlight areas of weaknesses. A11 emphasized how maturity models could guide prioritization and track progress over time: *"Going down the different pillars and deciding, either we've made progress here and can build on it, or we have a serious gap here."*

A3 shared that CISA's Maturity Model [19] emphasizes *"tiered Zero Trust maturity"* rather than treating a one-off compliance checklist: *"you start at the base, then level one, two, and three... it breaks the goal into achievable levels of automation."*

Behavioral analytics. Metrics were viewed as critical to tracking Zero Trust progress and offered a variety of practical strategies, though approaches revealed a lack of consistency. A2 suggested measuring real-world usage to assess transition coverage: *"X percent of the network traffic in my business applications is using Zero Trust-based services."* I4 emphasized outcome-driven metrics: *"You're looking for risk reduction—I got to better handle my devices. I've eliminated X number of unpatched applications, those sort of things."* I7 described tracking user acceptance, rollout friction, and complaints, while I8 noted that comparative metrics could influence executive behavior: *"Executives feel responsible when they see how they compare with peers, and competition changes how people behave."* This reflects a broader shift away from compliance toward being intentional on how Zero Trust affects both systems and people.

Continuous Improvement. Participants perceived Zero Trust as a journey of continual improvement rather than a one-time deployment (§ 6). And A5 captured this sentiment in the age of evolving adversaries:

> *You deploy Zero Trust principles, they [adversaries] also deploy Zero Trust principles. It's really like an arms race, like the long competition between the U.S. and Soviet Union.*

Since *"there is no Zero Trust stamp"* (G2), measurement was seen as a mechanism for continuous refinement. G4 echoed this sentiment, noting that ongoing measurement *"keeps you honest, it shows where things are drifting and where you need to push harder."*

RQ2 Summary: Participants viewed the translation of Zero Trust as a multi-step journey spanning perceiving value, planning, execution, and measuring progress, rather than a fixed checklist or end state. Reflections on translation patterns were driven largely by government and industry participants with direct responsibility for Zero Trust adoption. Academic participants contributed complementary, domain-focused perspectives, often from early-stage research contexts. These perspectives reinforce that there is *no one-size-fits-all path to Zero Trust adoption*; instead, organizations follow different trajectories and adapt their approaches based on their priorities, constraints, and operational contexts.

7 Challenges in Translating Zero Trust (RQ3)

Our study participants described a range of hurdles they either experienced or perceived when translating Zero Trust from theory to practice. Across sectors, participants emphasized that the difficulty lies not only in technology but in interpreting, coordinating, and sustaining change under real-world organizational constraints.

7.1 Interpretation Issues

A critical hurdle for translating Zero Trust was the **ambiguity surrounding what Zero Trust entails in practice.** While our participants valued Zero Trust guidance as initial entry points (§ 5.1), 16 found them vague and overly conceptual. I1 compared existing guidance to food recipe blogs:

> *80% is the story of somebody's grandparents eating pancakes, and then 20% is what you actually need—flour, eggs, milk. Sometimes Zero Trust guidance feels the same way—too much fluff and not enough about how to actually rotate certificates or enforce controls.*

A2 critiqued: *"I don't want to call it snake oil, but maybe that's right. When you look at a lot of these documentation, it's very vague about how it actually works, how it actually enforces things."* Others echoed the need for clarity and concise information. For instance, I5 thought of frameworks as not actionable: *"You've got this framework, and it says, 'secure your identity, secure your workloads, secure your network.' Does it say distinctly how to do that? No."* G6 found long documents such as NIST 800-207 [85] *"too much"* and wished that it could be a 10-page framework that said, *"these are the pieces of the puzzle you need."*

On the one hand, G3 emphasized the need for a single, authoritative source of truth: *"there are a lot of options out there, and you can very much get lost because there are so many choices."* And on the other hand, some participants questioned whether Zero Trust could ever be deployed using a single, prescriptive approach—*a standard.* A7 warned: *"If framework means prescriptive approaches, it can be challenging as different organizations have very different working models and needs, so a one-size-fits-all approach can be counterproductive."* G6 similarly noted: *"because we all have different technologies, risk appetites, and missions... you can't just take one playbook and apply it everywhere"* [95]. I9 remarked: *"My crystal ball does not show what is next, but if we get in a position where Zero Trust is incredibly prescribed and checklist-based, we're gonna have problems."* Finally, A3 highlighted both the value and limitations of the reference materials and said:

> *Standardization helps because not everybody has the resources or skills to implement or understand the systems. But... having a standard out for security solutions is not really the end game—it's about refining it to fit your sector or application.*

Nine participants, including all academics, noted how Zero Trust concepts have "mostly been applied to enterprise environments" (A6) and **struggle to translate into sensitive and complex domains**, such as operational technology (OT), IoT, 5G, and large-scale routing infrastructure. A2 illustrated this ambiguity: *"People bring up like, well, can we have Zero Trust for [the software supply chain]? I'm like, what do you mean by that?"* A5 candidly shared: *"wireless communication is already complicated... now we have to distrust everything? It's a huge overhead."* A6 and A8, applying Zero Trust concepts in routing systems and internet architectures, noted challenges with continuous verification using statements such as *"you verify the path, and the next instant they just do whatever they want... there are still many challenges in this type of distributed system problem."* and *'You can't really do Zero Trust today in the routing system because you need to accept routing announcements from people outside your zone, and you don't necessarily have a 100% accurate way to validate them."* While A3 remained critical of its scalability: *"Continuous authentication sounds great in theory, but practically there are limits—scrutiny can't happen everywhere, all the time."*

I9, researching Zero Trust for autonomous vehicles, highlighted the safety risks in incredibly resource constrained environments:

> *If you put more requirements on it for security, now the vehicle is not getting the message that the brakes are sending to the main unit that says 'stop, stop, stop.'*

7.2 Coordination Issues

Beyond interpretation challenges, many participants emphasized that translating Zero Trust placed significant demands on organizations' human and operational capacity.

Cultural resistance was one of the most cited coordination barriers, reported by 19 participants. Resistance commonly emerged around new authentication requirements. G5 captured the tension succinctly: *"When you start doing more frequent re-authentication, employees complain loudly—sometimes it feels like we're taking away their ability to do their job."* A8 echoed similar concers: *"If I had to log into 50 different systems with unique strong passwords, I'd be frustrated—you have to think about how you apply them [Zero Trust principles] so employees don't want to quit."* I2 warned that Zero Trust initiatives can fail when they add friction without clear value: *"If [new technology] just creates training overhead instead of solving a problem, you're adding burden."* I7 explained how this resistance was linked to **change fatigue**: *"It's not that people don't understand security, but every year there's a new thing. MFA, then VPN, then Zero Trust."* In decentralized settings such as academia, enforcing change emerged as especially challenging. A8 noted: *"Universities don't have a top-down command chain like government. If faculty don't like something, they just don't do it."*

Alongside cultural resistance, **skills and staffing gaps** were identified as coordination obstacles. Ten participants emphasized that Zero Trust transitions depended heavily on skilled personnel. I5 emphasized that *"security is delivered and provided by individuals"* and A9 also described that *"automated tools can help, but they are not going to decide everything on their own. Human judgment is still needed."* Therefore, according to A7, the real cost of Zero Trust is *"skilled admins to perform the transition."* A11 remarked: *"If you really wanted to do a fully mature Zero Trust architecture, I don't know of folks that have that level of staffing."* Government participants highlighted several structural issues. G3 shared that federal hiring takes *"4 to 6 months,"* and *"up-skilling, up-training has not kept pace with the rapid adoption."* G4 noted that since *"all of the federal agencies and many commercial entities have embraced Zero Trust,"* they're all going after the same talent pool. Finally, I8 pointed to access and cost barriers: *"The Cloud Security Alliance (CSA) has some Zero Trust training [114], but you have to pay for it... the people that need it don't necessarily have access to that training."*

A long-standing challenge in cybersecurity operations involves both practitioner [29, 79, 98, 99, 103] and leadership frustrations [70, 87]. Our participants considered **CISO pressures and burnout** as a serious concern. G3 reflected candidly: *"Fatigue is real. The average tenure for a [federal] CISO is 18 to 24 months. These are high-pressure, high-stakes jobs."* When G2 took over the CISO role for their organization's Zero Trust efforts, they were frustrated by limited situational awareness [59], as key systems (e.g., patching and identity) *"operated in silos,"* (§ 5.3) obscuring visibility into the overall risk posture. G1 underscored the ultimate accountability for CISOs and added: *"Nobody wants the CISO's job. If my organization gets hacked, the first one they're going to look at is the chief security officer. That's just the reality."*

In parallel, 19 participants cited **budget constraints** as a barrier [57], with government participants (G1, G3, G4, and G6) describing OMB M-22-09 [107] as an *"unfunded mandate."* G4 noted that funding shortfalls stretch schedules, delaying the achievement of an *"optimal maturity level"* well into the future. Budget limitations were seen rooted in leadership perceptions of *cybersecurity as a cost center* rather than a value generator. A11 called Zero Trust a *"hard sell"* because *"it's just making sure you're out of the news, not necessarily something that sells more products."* I7 linked this mindset to the growing reliance on cyber insurance. G1 lamented on the *"incident-driven"* and reactive nature of funding and said: *"We've got to get our leadership to appreciate what we do to keep the place safe—even when nothing bad happens."* Similarly, A3 framed security spending explicitly as a cost–benefit calculation and said: *"Not everybody needs that level of security. Security comes at a cost."* Finally, I2 questioned whether organizations adequately understood the true costs and trade-offs involved in Zero Trust adoption because they observed that *"people just put a thumb in the air and say, this is what our budget would look like."*

7.3 Contextual Issues

Eleven academic and industry participants described **legacy systems and technical debt** as barriers to Zero Trust adoption. A2 noted that some environments simply cannot be migrated: *"desktops, laptops, and some development servers or file servers... can't be moved into the cloud services. I'm not sure that there's good solutions out there for that yet."* A8 highlighted the scale of the issue:

> *If you have 100 million deployed switches, you're not replacing them all. You need to figure out how to silo and handle all these legacy structures under a Zero Trust architecture.*

I3 explained that enterprises are burdened by decades of accumulated complexity: *"We have too much technical debt... enough to make anything that you took off the shelf hard to use."*

Concerns were raised about the **vendor ecosystem** surrounding Zero Trust. Vendors were seen as both enablers and a potential source of friction in Zero Trust adoption. A common concern was the vendor perception of Zero Trust as a *"product"* rather than an architectural approach. As G4 noted: *"Vendors kept coming in and saying, 'this is your Zero Trust in a box.' We had to keep pushing back."* Because vendors use *"Zero Trust"* as label for marketing (§ 5), I6 noted that *"you have to cut through what's real and what's branding."* For A7, such messaging could mislead leadership into believing that *"buying one tool equals transformation."* Vendor lock-in and integration challenges were widely reported. G3 described contractual limitations: *"The contract basically locked us into their ecosystem, and moving away meant breaking a bunch of integrations. It slowed our ability to pivot."* For I2 and G6, such scenarios impacted flexibility and compromised long-term planning. Several participants questioned vendor tool functionality readiness. G1 reflected: *"Vendors, they're often selling future capability, not something that's fully ready. We ended up having to build custom integrations because their promised API wasn't there yet."*

RQ3 Summary: Challenges in Zero Trust adoption extended well beyond technical aspects. Participants described how vague guidance, human factors, organizational capacity limits, legacy infrastructure, and vendor dynamics collectively constrain what Zero Trust can become in practice. As a result, Zero Trust consistently emerged as a socio-technical security shift shaped by organizational and contextual constraints.

8 Discussion

Across the interviews, our participants highlighted sense-making under ambiguity, coordination across roles and organizational units, and trade-offs between security objectives and context-specific goals as central to Zero Trust understanding and translation. Such insights are often obscured in technically focused research and discourse. At the same time, many of the challenges participants described (§ 7) are familiar from prior work on organizational security implementation and decision-making. Staffing, cross-organizational coordination, and resource constraints [55, 102, 108], cultural resistance [46], communication and awareness gaps [47], and contextual factors and implementation under changing conditions [55] have all been documented. The broad scope of the Zero Trust paradigm and its journey-like framing, rather than a bounded deployment, make these familiar challenges more pronounced by amplifying coordination demands, diffusing accountability, and complicating how organizations define and measure progress.

We now discuss sectoral perspectives, opportunities for cross-sector collaboration, the risks of adopting security paradigms faster than implementation guidance matures, and implications for improving policy and organizational guidance.

8.1 Sectoral Perspectives on Zero Trust

Across sectors, participants shared a common and basic conceptual understanding of Zero Trust. They framed it as moving away from implicit trust and focusing on protecting resources through continuous verification (§ 5.2). Yet they interpreted and operationalized it differently depending on their organizational types, priorities, and constraints. Sectoral differences matter because Zero Trust is not only a technical model but also a translation problem, where its principles must be adapted to diverse organizational contexts.

Government participants framed Zero Trust as mandate-driven. Government CISOs were responsible for demystifying the concept, coordinating efforts across units, and aligning work with policy requirements. Industry participants described Zero Trust through business and risk goals, emphasizing executive buy-in and adoption tied to operational priorities. In both sectors, participants focused primarily on deploying Zero Trust within existing organizations, which surfaced issues related to organizational coordination, contextual adaptation, and resource constraints (§ 7.2, 7.3).

Academic participants, by contrast, shifted the discussion from implementation to applicability. They questioned whether Zero Trust concepts translate effectively to domains such as operational technology, IoT, and networking, highlighting limitations in existing guidance (§ 7.1). This perspective suggests that while deployment experience reveals how Zero Trust operates within organizations, research-driven application exposes where its concepts may not adequately apply and require rethinking. These differences reinforce that there is no one-size-fits-all path, underscoring the importance of continued cross-sector collaboration to refine both implementation guidance and future research.

8.2 Cross-sector Collaboration Opportunities

The sectoral perspectives discussed above suggest that government, industry, and academia play complementary roles in advancing Zero Trust and that no single stakeholder can fully address the translation challenges associated with Zero Trust.

Participants viewed academic involvement not as a substitute for practice, but as a way to question assumptions, validate emerging approaches, and develop stronger methods for evaluating Zero Trust. They noted that confusion around Zero Trust persists in part because the paradigm emerged from industry rather than academia, where new concepts are often accompanied by formal definitions, evaluation frameworks, and sustained scholarly scrutiny. As I2 explained, *"If there was a very well-known model that came from an academic background... I could foresee some level of folks referencing it. But... the term [Zero Trust] is already there. Everyone has their own interpretation of the model."* Participants compared this trajectory to other industry-led trends such as Web 2.0, blockchain, and AI.

Despite this, academia can still make meaningful contributions. Building on these observations, we recommend more structured collaboration across academia, industry, and government as each sector contributes a distinct but incomplete perspective (Section 4). Academic involvement can help question assumptions in Zero Trust guidance, examine applicability beyond enterprise environments, support independent evaluation of tools, and develop metrics that capture both technical progress and organizational realities to measure Zero Trust progress. In parallel, researchers can play a critical role in independently evaluating Zero Trust tools through open testbeds and reproducible benchmarks, helping to verify vendor claims and support more transparent procurement decisions (§ 7.3).

I7 highlighted the example of FIDO, where post-hoc academic research [36, 60, 104] helped validate and improve the standard [30]. A historical parallel can be seen in the development of the RBAC security model, which, although informally practiced in industry first (e.g., mainframe access control, business roles), gained broader momentum only after formalization through academic research [90] and standardization through academia-government collaboration [88]. Programs such as the NCCoE have taken the first step to support enterprises on their Zero Trust journey by developing practical guidance in collaboration with industry and government [69]. Integrating academic research more systematically into such efforts can further strengthen evidence-based evaluation, implementation guidance, and future Zero Trust research.

8.3 Hype-driven Security Paradigm

Participants widely described Zero Trust as gaining momentum across sectors (§ 5.3). However, our findings also suggest that widespread adoption has outpaced shared guidance for implementation. Its abstract framing (§ 5) and the lack of domain-specific guidance often leave its translation into practice unclear (§ 7.1).

In the absence of mature guidance, organizations are left to define implementation scope, priorities, success criteria, and deployment strategies on their own. Organizations may rely more heavily on vendor narratives, organization-specific interpretations of success, and locally developed implementation strategies. Moreover, organizations with more resources can afford trial-and-error approaches, whereas those with fewer resources may face greater barriers to implementation. These findings highlight the importance of developing clearer policy and organizational guidance that supports organizations in operationalizing Zero Trust effectively and reducing variability in implementation.

8.4 Improving Policy and Guidance

Several government CISOs shared that while the Zero Trust mandate [107] was aimed at accelerating security improvements, they were unfunded (§ 7.2) and lacked feasibility analysis. The problem was the absence of an understanding of what the mandate would require in time, staffing, and organizational change. Our participants' concerns about tooling procurement (§ 7.3), workforce up-skilling, and organizational coordination (§ 7.2) suggest that making costs and resource requirements more explicit could improve planning and reduce resistance.

In that sense, the practical implication is not simply to issue more guidance, but to make guidance more realistic about the organizational work required to implement Zero Trust. For policymakers (OMB) and standards bodies (NIST, CISA), we recommend that they include structured feasibility assessments and economic models [22]. For organizations, this means defining Zero Trust scope before procuring technologies, assigning ownership across domains, and translating the "journey" framing into measurable implementation phases.

In addition, appointing a *Business Information Security Officer (BISO)* could help bridge the communication gap between security and mission leaders. Armed with feasibility data and clearer implementation goals, BISOs can better translate security needs into business priorities to build leadership support. These strategies can make mandates more actionable, reduce any adoption frictions, and help organizations plan, budget, and execute Zero Trust in a sustainable and effective manner.

9 Conclusion

Although a widely promoted security paradigm, understanding and translating Zero Trust concepts remains complex and context-dependent. Through interviews with security professionals across industry, academia, and government, this study reveals Zero Trust is perceived not as a single technical shift, but as an ongoing journey. Our findings highlight several challenges in Zero Trust adoption involving interpretation, coordination, and contextual constraints that are socio-technical in nature and beyond purely technical. Overall, this work advances our understanding of how cybersecurity professionals understand and translate Zero Trust into practice.

Acknowledgments

This research is supported in part by the National Science Foundation (NSF) under Grant NSF-CICI-2232911, the Institute of Information & Communications Technology Planning & Evaluation (IITP) under Grants: RS-2024-004398199 and RS-2024-00442085, and the Defense Advanced Research Projects Agency (DARPA) and Naval Information Warfare Center Pacific (NIWC Pacific) under Contract No. N66001-22-C-4026. Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of DARPA or NIWC Pacific.

Finally, we would like to thank our study participants for taking the time to share their experiences and valuable insights on understanding and translating Zero Trust in practice.

Ethical Considerations

In this study, we conduct semi-structured interviews with cybersecurity professionals from U.S. government, industry, and academic organizations. While we do not anticipate any risks arising from our research on the topic of Zero Trust sensemaking, participants may face negative consequences if deanonymized. We structured our interview study to follow the ethical principles outlined in the Menlo report [8]. Prior to conducting interviews, we obtained approval from the Institutional Review Boards (IRBs) at the authors' institutions. Participants received detailed information about the study's goals, methods, and data handling strategies and provided informed consent before participation. The consent form clearly outlined the study's purpose, procedures, time commitment, compensation, and participants' rights, such as the freedom to skip any question or withdraw from the interview at any time without consequence. All data were collected and stored according to our institutions' IRB guidelines for human-subjects research. Participant data and interview recordings from Zoom were stored locally on the primary author's institutionally secured device. They manually reviewed the Zoom-generated transcripts to ensure accuracy and remove PII. They also assigned anonymized identifiers (i.e., G1–G7, I1–I9, A1–A11) to the interview transcripts before sharing the data with other author for analysis. All raw interview recordings were deleted after transcription.

Participants were offered an optional $50 Amazon gift card for an approximately 60-minute interview, which several chose to decline. They were also offered to receive a draft of the paper after submission, with many accepting this. Participants voluntarily contributed to this study to advance the understanding of Zero Trust and its translation into practice. Many described this as their primary motivation for participating.

Open Science

To promote transparency and support future research, we provide our study's replication package containing the recruitment message, demographic survey, interview protocol, interview questionnaire, and the complete codebook (themes, categories/subcategories, definitions, and example open codes), available at: https://github.com/sonejiananta/zero-trust-study.

We cannot share recordings as these were destroyed after transcription. To protect participant privacy and confidentiality, we do not release raw transcripts. Given the depth and specificity of the interview discussions, even anonymized transcripts pose a substantial risk of participant re-identification. Thus, we do not publish anonymized transcripts.

References

[1] William C Adams. Conducting Semi-structured Interviews. *Handbook of Practical Program Evaluation*, pages 492–505, 2015.

[2] Devdatta Akhawe and Adrienne Porter Felt. Alice in Warningland: A Large-Scale Field Study of Browser Security Warning Effectiveness. In *USENIX Security Symposium*, 2013.

[3] Florence Allard-Poesi. The Paradox of Sensemaking in Organizational Analysis. *Organization*, 12(2):169–196, 2005.

[4] Moneer Alshaikh. Developing Cybersecurity Culture to Influence Employee Behavior: A Practice Perspective. *Computers & Security*, 98, 2020.

[5] Debi Ashenden and Angela Sasse. CISOs and Organisational Culture: Their Own Worst Enemy? *Computers & Security*, 39:396–405, 2013.

[6] Rowland Atkinson and John Flint. Accessing Hidden and Hard-to-reach Populations: Snowball Research Strategies. *Social Research Update*, 33(1):1–4, 2001.

[7] Muhammad Ajmal Azad, Sidrah Abdullah, Junaid Arshad, Harjinder Lallie, and Yussuf Hassan Ahmed. Verify and Trust: A Multidimensional Survey of Zero-Trust Security in the Age of IoT. *Internet of Things*, 27, 2024.

[8] Michael Bailey, David Dittrich, Erin Kenneally, and Doug Maughan. The Menlo Report. *IEEE Security & Privacy*, 10(2):71–75, 2012.

[9] Kurt Baker. Lateral Movement Explained. https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/lateral-movement/, 2025.

[10] BastionZero. https://www.bastionzero.com/.

[11] Bob Blakley. The emperor's old armor. In *Proceedings of the 1996 workshop on New security paradigms*, pages 2–16, 1996.

[12] Virginia Braun and Victoria Clarke. *Thematic analysis*. American Psychological Association, 2023.

[13] Christoph Buck, Christian Olenberger, André Schweizer, Fabiane Völter, and Torsten Eymann. Never Trust, Always Verify: A Multivocal Literature Review on Current Knowledge and Research Gaps of Zero-Trust. *Computers & Security*, 110, 2021.

[14] Matthew Bush and Atefeh Mashatan. From Zero to One Hundred: Demystifying Zero Trust and its Implications on Enterprise People, Process, and Technology. *Queue*, 20(4):80–106, 2022.

[15] Mark Campbell. Beyond Zero Trust: Trust is a Vulnerability. *Computer*, 53(10):110–113, 2020.

[16] United States Public Law 101-576-NOV. 15 1990, 104 STAT. 2838. Chief Financial Officers Act of 1990. https://www.congress.gov/101/statute/STATUTE-104/STATUTE-104-Pg2838.pdf.

[17] CISA. Scattered Spider Hacking Group. https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a, 2023.

[18] Chase Cunningham, J Blankenship, S Balaouras, R Murphy, and M Cyr. The Zero Trust EXtended (ZTX) Ecosystem. *Forrester, Cambridge, MA*, 2018.

[19] Cybersecurity and Infrastructure Security Agency (CISA). Zero Trust Maturity Model 2.0. https://www.cisa.gov/sites/default/files/2023-04/zero_trust_maturity_model_v2_508.pdf, 2023.

[20] Joseph Da Silva and Rikke Bjerg Jensen. "Cyber Security is a Dark Art": The CISO as Soothsayer. *ACM on Human-Computer Interaction*, 6(CSCW2), 2022.

[21] Sauvik Das, Tiffany Hyun-Jin Kim, Laura A Dabbish, and Jason I Hong. The Effect of Social Influence on Security Sensitivity. In *Symposium On Usable Privacy and Security (SOUPS)*, 2014.

[22] John Ii S Davis, Martin C Libicki, Stuart E Johnson, Jason Kumar, Michael Watson, and Andrew Karode. A Framework for Programming and Budgeting for Cybersecurity. *The RAND Homeland Security and Defense Center*, 2016.

[23] Zero Trust | Revolutionary approach to Cyber or just another buzz word? https://www.microsoft.com/en-us/security/business/zero-trust, 2021.

[24] Department of Defense. DoW Zero Trust Strategy for Operational Technology. https://dodcio.defense.gov/Portals/0/Documents/Library/ZT-OperationalTechnologyActivitiesOutcomes.pdf.

[25] Rachna Dhamija, J Doug Tygar, and Marti Hearst. Why Phishing Works. In *ACM CHI Conference on Human Factors in Computing Systems*, 2006.

[26] DoD Zero Trust Strategy. https://dodcio.defense.gov/Portals/0/Documents/Library/DoD-ZTStrategy.pdf.

[27] DOE Announces Nearly $23 Million to Bolster Energy Security and Resilience. https://www.energy.gov/ceser/articles/doe-announces-nearly-23-million-bolster-energy-security-and-resilience.

[28] Amitava Dutta and Kevin McCrohan. Management's Role in Information Security in a Cyber Economy. *California Management Review*, 45(1):67–87, 2002.

[29] Josiah Dykstra and Celeste Lyn Paul. Cyber Operations Stress Survey (COSS): Studying Fatigue, Frustration, and Cognitive Workload in Cybersecurity Operations. In 11^{th} *USENIX Workshop on Cyber Security Experimentation and Test (CSET)*, 2018.

[30] Jen Easterly. Next Level MFA: FIDO Authentication. https://www.cisa.gov/news-events/news/next-level-mfa-fido-authentication, 2022.

[31] Bryan Embrey. The top three factors driving zero trust adoption. *Computer Fraud & Security*, 2020(9):13–15, 2020.

[32] Ilker Etikan, Sulaiman Abubakar Musa, and Rukayya Sunusi Alkassim. Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, 5(1):1–4, 2016.

[33] Michael Fagan and Mohammad Maifi Hasan Khan. Why Do They Do What They Do?: A Study of What Motivates Users to (Not) Follow Computer Security Advice. In *Symposium On Usable Privacy and Security (SOUPS)*, 2016.

[34] James P Farwell and Rafal Rohozinski. Stuxnet and the Future of Cyber War. *Survival*, 53(1):23–40, 2011.

[35] The Daily Journal of the United States Government Federal Register. Improving the Nation's Cybersecurity. A Presidential Document by the Executive Office of the President. https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity, 2021.

[36] Haonan Feng, Hui Li, Xuesong Pan, Ziming Zhao, and T Cactilab. A Formal Analysis of the FIDO UAF Protocol. In *Symposium on Network and Distributed System Security (NDSS)*, 2021.

[37] United States Public Law 107-347-DEC. 17 2002, 116 STAT. 2899 (2002). Federal Information Security Management Act (FISMA). Title III of the E-Government Act of 2002. https://www.govinfo.gov/content/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf.

[38] Philip WL Fong. Relationship-based Access Control: Protection Model and Policy Language. In *ACM Conference on Data and Application Security and Privacy (CODASPY)*, 2011.

[39] Josh Fruhlinger. The OPM Hack Explained: Bad Security Practices Meet China's Captain America. https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html, 2020.

[40] Gartner. Implementing Zero Trust Security in the Public Sector. https://www.gartner.com/en/industries/government-public-sector/topics/zero-trust.

[41] Saeid Ghasemshirazi, Ghazaleh Shirvani, and Mohammad Ali Alipour. Zero Trust: Applications, Challenges, and Opportunities. *arXiv preprint arXiv:2309.03582*, 2023.

[42] Andy Greenberg. The Full Story of the Stunning RSA Hack Can Finally Be Told. https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/, 2021.

[43] The Baldwin Group. Understanding the Business Impact of Data Breaches. https://baldwin.com/insights/understanding-the-business-impact-of-data-breaches/, 2025.

[44] Yuanhang He, Daochao Huang, Lei Chen, Yi Ni, and Xiangjie Ma. A Survey on Zero Trust Architecture: Challenges and Future Trends. *Wireless Communications and Mobile Computing*, 2022(1), 2022.

[45] Cormac Herley. So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users. In *Workshop on New Security Paradigms*, 2009.

[46] Jonas Hielscher, Uta Menges, Simon Parkin, Annette Kluge, and M Angela Sasse. "Employees Who Don't Accept the Time Security Takes Are Not Aware Enough": The CISO View of Human-Centred Security. In *USENIX Security Symposium*, 2023.

[47] Jonas Hielscher and Simon Parkin. " what keeps people secure is that they met the security team": Deconstructing drivers and goals of organizational security awareness. In *33rd USENIX Security Symposium (USENIX Security 24)*, pages 3295–3312, 2024.

[48] Randy Hodson. *Analyzing Documentary Accounts*. SAGE, 1999.

[49] Elaine Hulitt and Rayford B Vaughn. Information System Security Compliance to FISMA Standard: A Quantitative Measure. *Telecommunication Systems*, 45(2):139–152, 2010.

[50] Iulia Ion, Rob Reeder, and Sunny Consolvo. "... No one Can Hack My Mind": Comparing Expert and Non-Expert Security Practices. In *Symposium On Usable Privacy and Security (SOUPS)*, 2015.

[51] Mohammed Nurul Islam, Ricardo Colomo-Palacios, and Sabarathinam Chockalingam. Secure Access Service Edge: A Multivocal Literature Review. In *International Conference on Computational Science and Its Applications (ICCSA)*. IEEE, 2021.

[52] Cornelius Itodo and Murat Ozer. Multivocal Literature Review on Zero-Trust Security Implementation. *Computers & Security*, 2024.

[53] Einar Iveroth and Jacob Hallencreutz. *Effective organizational change: Leading through sensemaking*. Routledge, 2015.

[54] Xin Jin, Ram Krishnan, and Ravi Sandhu. A Unified Attribute-based Access Control Model Covering DAC, MAC and RBAC. In *Conference on Data and Applications Security and Privacy (DBSec)*. Springer, 2012.

[55] Kailani R Jones, Dalton A Brucker-Hahn, Bradley Fidler, and Alexandru G Bardas. {Work-From-Home} and {COVID-19}: trajectories of endpoint security management in a security operations center. In *32nd USENIX Security Symposium (USENIX Security 23)*, pages 2293–2310, 2023.

[56] John Kindervag, Stephanie Balaouras, Kelley Mak, and Josh Blackborow. No More Chewy Centers: Introducing the Zero Trust Model of Information Security. *Forrester Research*, 3(1):1–16, 2010.

[57] Tara Kissoon. Optimum Spending on Cybersecurity Measures. *Transforming Government: People, Process and Policy*, 14(3):417–431, 2020.

[58] Kenneth J Knapp, Thomas E Marshall, R Kelly Rainer, and F Nelson Ford. Information Security: Management's Effect on Culture and Policy. *Information Management & Computer Security*, 14(1):24–36, 2006.

[59] Faris Bugra Kokulu, Ananta Soneji, Tiffany Bao, Yan Shoshitaishvili, Ziming Zhao, Adam Doupé, and Gail-Joon Ahn. Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In *ACM Conference on Computer and Communications Security (CCS)*, 2019.

[60] Dhruv Kuchhal, Muhammad Saad, Adam Oest, and Frank Li. Evaluating the Security Posture of Real-World FIDO2 Deployments. In *ACM Conference on Computer and Communications Security (CCS)*, 2023.

[61] Ling Li, Wu He, Li Xu, Ivan Ash, Mohd Anwar, and Xiaohong Yuan. Investigating the Impact of Cybersecurity Policy Awareness on Employees' Cybersecurity Behavior. *International Journal of Information Management*, 45:13–24, 2019.

[62] LinkedIn. https://about.linkedin.com/.

[63] Tina Marjanov and Alice Hutchings. SoK: Digging into the Digital Underworld of Stolen Data Markets. In *IEEE Symposium on Security and Privacy (S&P)*, 2025.

[64] Mary L McHugh. Interrater Reliability: The kappa Statistic. *Biochemia medica*, 22(3):276–282, 2012.

[65] Saima Mehraj and M Tariq Banday. Establishing a Zero Trust Strategy in Cloud Computing Environment. In *International Conference on Computer Communication and Informatics (ICCCI)*. IEEE, 2020.

[66] Protect and modernize your organization with a Zero Trust strategy. https://www.microsoft.com/en-us/security/business/zero-trust.

[67] Zero Trust Adoption Report. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft-Zero-Trust-Adoption-Report.pdf.

[68] Palo Alto Networks. What Is a Credential-Based Attack? https://www.paloaltonetworks.com/cyberpedia/what-is-a-credential-based-attack, 2025.

[69] NIST SPECIAL PUBLICATION 1800-35: Implementing a Zero Trust Architecture: Full Document. https://pages.nist.gov/zero-trust-architecture/.

[70] Calvin Nobles. Stress, Burnout, and Security Fatigue in Cybersecurity: A Human Factors Problem. *Holistica Journal of Business and Public Administration*, 13(1):49–72, 2022.

[71] Luke Noonan. 5 Damaging Consequences of Data Breach: Protect Your Assets. https://www.metacompliance.com/blog/data-breaches/5-damaging-consequences-of-a-data-breach, 2025.

[72] NSF invests $25M to advance technologies and communications to operate securely through 5G networks. https://www.nsf.gov/news/nsf-invests-25m-advance-technologies.

[73] NSF 24-504: Secure and Trustworthy Cyberspace (SaTC). https://www.nsf.gov/funding/opportunities/satc-20-security-privacy-trust-cyberspace/nsf24-504/solicitation.

[74] Cliodhna O'Connor and Helene Joffe. Intercoder Reliability in Qualitative Research: Debates and Practical Guidelines. *International Journal of Qualitative Methods*, 19, 2020.

[75] Aleksandr Ometov, Sergey Bezzateev, Niko Mäkitalo, Sergey Andreev, Tommi Mikkonen, and Yevgeni Koucheryavy. Multi-Factor Authentication: A Survey. *Cryptography*, 2(1):1, 2018.

[76] Jens Opdenbusch, Jonas Hielscher, and M Angela Sasse. "Where Are We On Cyber?" – A Qualitative Study On Boards' Cybersecurity Risk Decision Making. In *Symposium on Network and Distributed System Security (NDSS)*, 2025.

[77] Shaul Oreg and Yair Berson. Leaders' impact on organizational change: Bridging theoretical and methodological chasms. *Academy of Management Annals*, 13(1):272–307, 2019.

[78] Charlie Parker, Sam Scott, and Alistair Geddes. Snowball sampling. *SAGE research methods foundations*, 2019.

[79] Celeste Lyn Paul and Josiah Dykstra. Understanding Operator Fatigue, Frustration, and Cognitive Workload in Tactical Cybersecurity Operations. *Journal of Information Warfare*, 16(2):1–11, 2017.

[80] Daniel R Philpott and Stephen D Gantz. *FISMA and the Risk Management Framework: The New Practice of Federal Cyber Security*. Newnes, 2012.

[81] Alexandre Poirrier, Laurent Cailleux, and Thomas Heide Clausen. Is Trust Misplaced? A Zero-Trust Survey. *Proceedings of the IEEE*, 2025.

[82] Stefan Rädiker and Udo Kuckartz. Focused Analysis of Qualitative Interviews with MAXQDA. *MAXQDA Press*, 2020.

[83] Keyvan Ramezanpour and Jithin Jagannath. Intelligent Zero Trust Architecture for 5G/6G Networks: Principles, Challenges, and the Role of Machine Learning in the Context of O-RAN. *Computer Networks*, 217:109358, 2022.

[84] Sam Ro. JPMorgan Reveals Gigantic Data Breach Possibly Affecting 76 Million Households. https://www.businessinsider.com/jp-morgan-data-breach-2014-10, 2014.

[85] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly. Zero Trust Architecture. *NIST Special Publication 800-207*, 2020.

[86] Hannah R Rothstein and Sally Hopewell. Grey Literature. *The Handbook of Research Synthesis and Meta-Analysis*, 2:103–125, 2009.

[87] Kimberly Ruth, Veronica A Rivera, Gautam Akiwate, Aurore Fass, Patrick Gage Kelley, Kurt Thomas, and Zakir Durumeric. "Perfect is the Enemy of Good"': The CISO's Role in Enterprise Security as a Business Enabler. In *ACM CHI Conference on Human Factors in Computing Systems*, 2025.

[88] Ravi Sandhu, David Ferraiolo, and Richard Kuhn. The NIST Model for Role-based Access Control: Towards a Unified Standard. In *ACM Workshop on Role-based Access Control*, 2000.

[89] Ravi S Sandhu. Role-based Access Control. In *Advances in Computers*, volume 46, pages 237–286. Elsevier, 1998.

[90] Ravi S Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. Role-Based Access Control Models. In *IEEE Computer*, volume 29(2), pages 38–47. IEEE, 1996.

[91] Nabeel Sheikh, Mayur Pawar, and Victor Lawrence. Zero Trust using Network Micro Segmentation. In *IEEE Conference on Computer Communications Workshops (INFOCOM Workshops)*, 2021.

[92] Paul Simmonds. De-perimeterisation. *Black Hat USA*, 2004.

[93] Peter Warren Singer and Allan Friedman. *Cybersecurity and cyberwar: What everyone needs to know®*. Oxford University Press, 2013.

[94] Rock Stevens, Faris Bugra Kokulu, Adam Doupé, and Michelle L Mazurek. Above and Beyond: Organizational Efforts to Complement US Digital Security Compliance Mandates. In *Symposium on Network and Distributed System Security (NDSS)*, 2022.

[95] Rock Stevens, Daniel Votipka, Josiah Dykstra, Fernando Tomlinson, Erin Quartararo, Colin Ahern, and Michelle L Mazurek. How Ready is Your Ready? Assessing the Usability of Incident Response Playbook Frameworks. In *ACM CHI Conference on Human Factors in Computing Systems*, 2022.

[96] Anselm Strauss and Juliet Corbin. *Basics of Qualitative Research Techniques*. SAGE, 1998.

[97] Blake E Strom, Andy Applebaum, Doug P Miller, Kathryn C Nickels, Adam G Pennington, and Cody B Thomas. MITRE ATT&CK: Design and Philosophy. Technical report, MITRE, 2018.

[98] Sathya Chandran Sundaramurthy, Alexandru G Bardas, Jacob Case, Xinming Ou, Michael Wesch, John McHugh, and S Raj Rajagopalan. A Human Capital Model for Mitigating Security Analyst Burnout. In *Symposium On Usable Privacy and Security (SOUPS)*, 2015.

[99] Sathya Chandran Sundaramurthy, Jacob Case, Tony Truong, Loai Zomlot, and Marcel Hoffmann. A Tale of Three Security Operation Centers. In *ACM Workshop on Security Information Workers*, 2014.

[100] Naeem Firdous Syed, Syed W Shah, Arash Shaghaghi, Adnan Anwar, Zubair Baig, and Robin Doss. Zero Trust Architecture (ZTA): A Comprehensive Survey. *IEEE Access*, 10:57143–57179, 2022.

[101] Songpon Teerakanok, Tetsutaro Uehara, and Atsuo Inomata. Migrating to Zero Trust Architecture: Reviews and Challenges. *Security and Communication Networks*, 2021(1), 2021.

[102] Stefan Thalmann, Daniel Bachlechner, Lukas Demetz, and Ronald Maier. Challenges in cross-organizational security management. In *2012 45th Hawaii International Conference on System Sciences*, pages 5480–5489. IEEE, 2012.

[103] Kashyap Thimmaraju, Sybe Izaak Rispens, and Gail-Joon Ahn. Human Performance in Security Operations: A Survey on Burnout, Well-Being and Flow State Among Practitioners. *Workshop on SOC Operations and Construction (WOSOC)*, 2025.

[104] Enis Ulqinaku, Hala Assal, AbdelRahman Abdou, Sonia Chiasson, and Srdjan Capkun. Is real-time phishing eliminated with FIDO? social engineering downgrade attacks against FIDO protocols. In *USENIX Security Symposium*, 2021.

[105] Rory Ward and Betsy Beyer. BeyondCorp: A New Approach to Enterprise Security. *Usenix Login*, 39, 2014.

[106] Karl E Weick and Karl E Weick. *Sensemaking in organizations*, volume 3. Sage publications Thousand Oaks, CA, 1995.

[107] Moving the U.S. Government Toward Zero Trust Cybersecurity Principles. https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

[108] Flynn Wolf, Adam J Aviv, and Ravi Kuber. Security Obstacles and Motivations for Small Businesses from a CISO's Perspective. In *USENIX Security Symposium*, 2021.

[109] Avishai Wool. A quantitative study of firewall configuration errors. *Computer*, 37(6):62–67, 2004.

[110] Yuxi Wu, W Keith Edwards, and Sauvik Das. SoK: Social Cybersecurity. In *IEEE Symposium on Security and Privacy (S&P)*, 2022.

[111] Xiangshuai Yan and Huijuan Wang. Survey on Zero-Trust Network Security. In *International Conference on Artificial Intelligence and Security*. Springer, 2020.

[112] Salifu Yusif and Abdul Hafeez-Baig. A Conceptual Model for Cybersecurity Governance. *Journal of Applied Security Research*, 16(4):490–513, 2021.

[113] The Zscaler Zero Trust Exchange Platform. https://www.zscaler.com/products-and-solutions/zero-trust-exchange-zte.

[114] Cloud Security Alliance Zero Trust Training. https://exams.cloudsecurityalliance.org/en.

[115] Zero Trust Adoption Statistics and Trends in 2025. https://expertinsights.com/zero-trust/zero-trust-adoption-statistics-and-trends.

[116] Fortinet Universal Zero Trust Network Access (ZTNA). https://www.fortinet.com/solutions/enterprise-midsize-business/network-access/application-access.

[117] Mary Ellen Zurko and Richard T Simon. User-Centered Security. In *Workshop on New Security Paradigms*, 1996.