THE IMPACT OF NATIONAL, ORGANIZATIONAL AND INFORMATION SECURITY CULTURES TOWARDS ZERO TRUST MODEL ADOPTION IN UAE

BADER HUSNI ABDEL RAZZAQ ZYOUD

UNIVERSITI SAINS MALAYSIA

2024

THE IMPACT OF NATIONAL, ORGANIZATIONAL AND INFORMATION SECURITY CULTURES TOWARDS ZERO TRUST MODEL ADOPTION IN UAE

by

BADER HUSNI ABDEL RAZZAQ ZYOUD

Thesis submitted in fulfilment of the requirements
for the degree of
Master of Science

November 2024

ACKNOWLEDGEMENT

I extend my heartfelt gratitude to Allah and my esteemed supervisor Dr. Syaheerah Lebai Lutfi, for her unwavering guidance, steadfast support, and motivational assistance throughout my academic pursuit. Her invaluable insights, constructive feedback, and perceptive critique have been instrumental in shaping and refining my research.

I am profoundly thankful to my beloved wife Shaimaa and cherished daughter Dima for their enduring love, support, and encouragement throughout my academic journey. Their steadfast belief in me and their understanding have been a constant source of strength and inspiration.I am also deeply grateful to my family, including my lovely mother,father, brothers, and sisters, for their unconditional love and unwavering support, which have been a constant source of comfort and motivation during my studies.

Lastly, but certainly not least, I want to acknowledge and extend my heartfelt thanks to my friends and coworkers for their support, encouragement, and camaraderie throughout my academic journey. Their presence and companionship have significantly enriched my experience, making it more memorable and rewarding.

TABLE OF CONTENTS

ACKNOWLEDGEMENT ..... **ii**

TABLE OF CONTENTS ..... **iii**

LIST OF TABLES ..... **viii**

LIST OF FIGURES ..... **x**

LIST OF SYMBOLS ..... **xi**

LIST OF ABBREVIATIONS ..... **xii**

LIST OF APPENDICES ..... **xiii**

ABSTRAK ..... **xiv**

ABSTRACT ..... **xvi**

CHAPTER 1 INTRODUCTION **1**

1.1 Background 1

1.2 Problem Statement 3

1.3 Research Gap 5

1.4 Research Questions 6

1.5 Research Objectives 6

1.6 Thesis Structure 7

1.7 Theoritical and Practical Contributions....8

1.8 Research scope 11

Research steps and implementation 12

CHAPTER 2 LITERATURE REVIEW.... 15

2.1 Introduction 15

2.2 Zero Trust History....16

2.3 Zero Trust Reviews 17

2.4 Zero Trust Architecture Review....20

2.5 State of the Art Zero Trust Models and Frameworks....22

2.6 Zero Trust Architecture Adoption Concerns and Challenges in the Organizations 24

2.7 Culture Differences 28

2.8 Information Security Culture....29

2.9 Organizational Culture 35

2.10 National Culture 37

2.11 Information Security Standards Related to United Arab Emirates 40

2.12 The Most Important Factors that Influence the Information Security Culture of Organizations 41

2.13 Information Security Culture Assessment Factors. 46

2.14 Summary 52

CHAPTER 3 METHODOLOGY 54

3.1 Introduction 54

3.2 Participant Consent and Confidentiality 56

3.3 Instrument and Survey Development 57

3.4 Sample Selection 69

3.5 Measurement Scales 70

3.6 Demographic Questions 71

3.7 Quantitative Analysis 72

3.8 Data Preprocessing 72

3.9 Data Processing and Analysis 74

3.10 Research Model and Hypothesis 77

3.11 Research Model 82

3.12 The Methodology Process Flow Chart 85

3.13 Summary 86

CHAPTER 4 RESULTS AND ANALYSIS 87

4.1 Introduction 87

4.2 Demographic Information Section 88

4.3 Gender Distribution 88

4.4 Industry Representation 88

4.5 Age, Profession and Location 89

4.6 Research Model Analysis 89

4.7 Quantitative Data Analysis 91

4.8 Data Analysis and Testing of the Structural Model 98

4.9 Results of Hypotheses Testing 101

4.10 Factors of Information Security Culture and Zero Trust Adoption Correlation 102

4.11 Summary 106

CHAPTER 5 DISCUSSION 108

5.1 Introduction 108

5.2 Demographic Insights 111

5.3 The Impact of Information Security Culture on Zero Trust Adoption in the UAE Organizations in Arabic Culture 112

5.4 The Impact of National Culture on Zero Trust adoption in the UAE Organizations in Arabic Culture 114

5.5 The Impact of Organizational Culture on Zero Trust Adoption in the UAE Organizations in Arabic Culture 117

5.6 Key Information Security Culture Factors Influencing the Adoption of Zero Trust in the United Arab Emirates 120

5.7 Research Model and Hypothesis Output 121

5.8 Summary 126

CHAPTER 6 CONCLUSION 129

6.1 Introduction 129

6.2 Key Findings 129

6.3 Research Contributions 137

6.4 Limitation and Future Work 143

6.5 Implications and Novelty 144

6.6 Summary 147

REFERENCES 150

APPENDICES

LIST OF PUBLICATIONS

LIST OF TABLES

Page

Table 1.1 Research Steps 12

Table 2.1 Findings of the Zero-Trust Architecture review (ascending)..... 20

Table 2.2 Summery of Zero trust models and frameworks..... 22

Table 2.3 Findings of the zero trust organizational concerns 25

Table 2.4 ZT Adoption challenges in organizations 27

Table 2.5 Information Security Culture Reviews 31

Table 2.6 Information security culture extracted factors' summary 45

Table 2.7 The common Information security culture assessment factors and there mapping with UAE IA 48

Table 3.1 Survey statements 58

Table 3.2 Data processing and analysis tests 75

Table 4.1 Descriptive Statistics Summary (NSC,ZTA)..... 93

Table 4.2 Descriptive Statistics Summary (OCS,ZTA)..... 94

Table 4.3 Descriptive Statistics Summary (ISC,ZTA)..... 96

Table 4.4 Results of hypotheses testing 102

Table 4.5 Descriptive statistics summary (ISC factors, ZTA)..... 103

Table 4.6 ISC factors and ZTA correlation results 105

Table 5.1 Results of Hypotheses Testing..... 110

Table 5.2 Mapping research questions with hypotheses..... 124

Table 6.1 Key Findings and There Implications..... 131

Table 6.2 Research contribution with existing Zero trust models and frameworks..... 138

Table 6.3 Research Contribution.....140

LIST OF FIGURES

Page

Figure 2.1 Brief History of Zero Trust 17

Figure 2.2 NIST computer security resource center, "SP 800-2017, Zero Trust Architecture." August 2020 20

Figure 2.3 NIST principles of ZT (Bush & Mashatan, 2022b) 28

Figure 2.4 Hofstede's six cultural dimensions(Hofstede, 1980a) 29

Figure 2.5 Dimensions of CLTRe cyber security culture(KnowBe4, 2022) 44

Figure 3.1 Proposed Conceptual Model for Research 84

Figure 3.2 The conceptual relation of ISC factors and ZTA 85

Figure 3.3 Research methodology Summary 86

Figure 4.1 Gender distribution 88

Figure 4.2 Industry distribution 89

Figure 4.3 Conceptual model and hypotheses 99

Figure 4.4 level of ZT principles adoption within UAE organizations 101

Figure 5.1 Research model and hypotheses 110

Figure 5.2 The correlation of ISC factors and ZTA 121

Figure 5.3 Research model and hypothesis output 123

LIST OF SYMBOLS

n	The required sample size
N	The total population size
e	The desired level of precision or margin of error as a decimal
R^2	R-squared as evidence of a well-fitting model
B	Path Coefficient

LIST OF ABBREVIATIONS

ATS	Awareness and Training Statements
PPS	Policy and procedure Statements
TMSS	Top Management Support Statements
CMS	Change Management Statements
ISMS	Information Security Management Statements
SBS	Security Behavioral Statements
COMS	Communication Statements
CPS	Compliance Statements
NCS	National Culture Statements
OCS	Organization Culture Statements
AVISC	Information Security Culture Average Result
ZTA	Zero Trust Adoption
USM	Universiti Sains Malaysia
AVE	Average Variance Extracted.
NIST	National Institute of Standards and Technology
VPN	Virtual Private Network
UAE	United Arab Emirates

LIST OF APPENDICES

APPENDIX A ARTICLES SUMMARY

APPENDIX B SURVEY DETAILS

APPENDIX C MAPPING OF UAE IA REGULATION CONTROLS

APPENDIX D EXPERT VALIDATION LETTER

IMPAK BUDAYA KESELAMATAN NASIONAL, ORGANISASI DAN MAKLUMAT TERHADAP PENGAMBILAN MODEL KEPERCAYAAN SIFAR DI EMIRIAH ARAB BERSATU

ABSTRAK

Model keselamatan Kepercayaan Sifar, berdasarkan prinsip "jangan pernah percaya, selalu verifikasi," mencabar model keselamatan tradisional dan sangat relevan dalam konteks budaya bukan Barat. Penyelidikan sedia ada mengenai penerimaan Kepercayaan Sifar (KS) sering mengabaikan pengaruh faktor budaya keselamatan, nasional, dan organisasi. Tiada satu model pun yang secara komprehensif menggabungkan aspek budaya ini. Selain itu, terdapat kekurangan kajian mengenai budaya keselamatan maklumat dan penerimaan KS di UAE, meninggalkan jurang dalam memahami dimensi budaya ini. Tesis ini menyiasat hubungan antara keselamatan maklumat, budaya nasional, dan organisasi dengan penerimaan model Kepercayaan Sifar, dengan fokus pada UAE. Ia membina model teori berdasarkan faktor budaya keselamatan maklumat yang biasa dan penerimaan Kepercayaan Sifar dalam konteks budaya Arab, menggunakan data dari tinjauan 98 pakar keselamatan siber di UAE. Menggunakan Pemodelan Persamaan Struktur Least Squares Sebahagian (PLS-SEM), kajian ini menguji hipotesis untuk menentukan hubungan antara faktor budaya keselamatan maklumat dan penerimaan KS. Hasil kajian menunjukkan bahawa budaya nasional dan organisasi, serta budaya keselamatan maklumat, berkorelasi secara signifikan dan positif dengan penerimaan Kepercayaan Sifar. Korelasi signifikan ditemui antara faktor budaya keselamatan maklumat dan penerimaan KS, termasuk kesedaran dan latihan (ATS), dasar dan prosedur (PPS), tingkah laku keselamatan (SBS), komunikasi (COMS), sokongan pengurusan atasan

(TMS), pengurusan perubahan (CMS), pengurusan keselamatan maklumat (ISMS), dan pematuhan (CPS). Terutama, ATS, PPS, SBS, dan TMS menunjukkan korelasi positif yang ketara dengan penerimaan KS, manakala CMS tidak menunjukkan korelasi yang signifikan secara statistik. Budaya keselamatan maklumat muncul sebagai pemacu kritikal untuk penerimaan KS. Penemuan ini sangat berharga bagi pembuat dasar dan pemimpin IT yang bertujuan untuk meningkatkan pertahanan keselamatan siber. Penyertaan UAE menambah elemen budaya yang unik, dengan cadangan praktikal untuk meningkatkan penerimaan KS selaras dengan pertimbangan budaya. Penyelidikan masa depan harus merangkumi faktor tambahan, negara, dan peserta untuk meningkatkan ketepatan.

THE IMPACT OF NATIONAL,ORGANIZATIONAL AND INFORMATION SECURITY CULTURES TOWARDS ZERO TRUST MODEL ADOPTION IN UAE

ABSTRACT

The zero-trust security model, based on the principle of “never trust, always verify,” challenges traditional security models and is particularly relevant in non-Western cultural contexts. Existing research on Zero Trust (ZT) adoption often overlooks the influence of security, national, and organizational cultural factors. No single model comprehensively incorporates these cultural aspects. Additionally, there is a lack of studies on information security culture and ZT adoption within the UAE, leaving a gap in understanding these cultural dimensions.This thesis investigates the correlation between information security, national, and organizational culture and the adoption of the zero-trust model, focusing on the UAE. It constructs a theoretical model based on common information security culture factors and zero trust adoption in the Arab cultural context, using data from a survey of 98 cybersecurity experts in the UAE. Using Partial Least Squares Structural Equation Modelling (PLS-SEM), the study tests hypotheses to determine the correlation between information security culture factors and ZT adoption.The results indicate that national and organizational culture, as well as information security culture, are significantly and positively correlated with Zero Trust adoption. Significant correlations were found between information security culture factors and ZT adoption, including awareness and training (ATS), policy and procedure (PPS), security behavior (SBS), communication (COMS), top management support (TMS), change management (CMS), information security management (ISMS), and compliance (CPS). Notably, ATS, PPS, SBS, and

TMS show substantial positive correlations with ZT adoption, while CMS lacks a statistically significant correlation.Information security culture emerges as a critical driver for ZT adoption. These insights are valuable for policymakers and IT leaders aiming to enhance cybersecurity defenses. The inclusion of the UAE adds a unique cultural element, with practical recommendations to improve ZT adoption in line with cultural considerations. Future research should include additional factors, countries, and participants to increase accuracy.

CHAPTER 1

INTRODUCTION

1.1 Background

In today's hyper-connected digital landscape, Organizations face heightened vulnerability to cyberattacks owing to evolving work cultures and increased exposure to untrusted network traffic(Georgiadou et al., 2021a).The traditional perimeter-based security models, which assume that everything inside an organization's network is trustworthy, are increasingly insufficient in addressing modern cyberattacks. These legacy models fail to account for the complexities of today’s distributed networks, remote work environments, and the rise of sophisticated threat actors. In response, Zero Trust Architecture (ZTA) has emerged as a transformative cybersecurity paradigm, fundamentally shifting how organizations secure their data and resources.

ZTA operates on the principle of "never trust, always verify," asserting that threats can originate both inside and outside an organization's network. It requires continuous verification of the identity and integrity of every person and device attempting to access corporate resources. This approach was first articulated by John Kindervag in 2010, revolutionizing how security frameworks are conceived(Greitzer & Purl, 2022). Unlike traditional models, ZTA is not a single product or technology but rather a comprehensive strategy that demands thorough authentication, strict access control, and continuous monitoring (Xiao et al., 2022). It ensures that no trust is placed by default on any entity, enforcing strict security measures across five core pillars: People, Devices, Data, Networks, and Workloads(Cloud, 2024).

As organizations increasingly adopt Zero Trust principles, they must also recognize the importance of aligning this model with their Information Security Culture (ISC), defined as the collective perceptions, values, attitudes, and behaviors regarding information protection, plays a critical role in ensuring the success of ZTA (AlHogail & Mirza, 2014. A strong ISC fosters an environment where employees are more likely to comply with security protocols, reducing risks associated with insider threats and negligent behaviors.

Organizational culture (OCS), which includes shared values, norms, and practices within a company, directly influences employees' engagement with cybersecurity practices (Schneider et al., 2013). Organizations with a culture that prioritizes security will likely see better outcomes in terms of ZTA implementation. Furthermore, National Culture (NCS), which includes societal values, norms, and customs, also plays a significant role, especially in regions with distinct cultural frameworks like the UAE (Connolly et al., 2017). The UAE's cultural environment is shaped by its Islamic values, which emphasize trust, loyalty, and honor—concepts that can either support or challenge the implementation of stringent security models like Zero Trust.The uniqueness of the Arab cultural landscape, as captured by Hofstede's cultural dimensions, underlines the importance of tailoring security frameworks to fit regional norms (Hofstede, 2010).

As organizations in the UAE face increased demand for adaptable cybersecurity solutions due to the rise of hybrid work environments, many are turning to Zero Trust Architecture (Gulf News, 2023). However, the successful adoption of ZTA in the region will depend not only on technological infrastructure but also on the

careful alignment of these security practices with the UAE's unique cultural, organizational, and social context.

1.2 Problem Statement

The increasing connectivity of devices to the internet in modern digital work contexts has led to a rise in cyber risks and attacks (Muhammad et al., 2022). The primary goal of creating a zero-trust architecture is to enable continuous review and approval to protect sensitive data and valuable resources (Dimitrakos & al, 2020a). Despite the potential benefits, the implementation of zero-trust models presents significant challenges.

Current academic research has primarily focused on zero-trust architectures, maturity models, frameworks, technological aspects, knowledge gaps, cloud computing, artificial intelligence, and the shift towards a zero-trust framework. While the Zero Trust approach offers numerous benefits, its implementation is fraught with challenges. Transitioning from traditional cybersecurity methods to a zero-trust model is complex, causes workflow disruption, and encounters issues related to time, cost, and user behavior (Akhyari et al., 2018b; Akhyari Nasir, 2019; Da Veiga & Martins, 2015; F. Karlsson et al., 2015a; Mohammed & Bamasoud, 2022; Mousavi & Kumar, 2019a; Mwim & Mtsweni, 2022a; Nasir et al., 2022).

The aforementioned zero-trust models and migration strategies, such as BeyondCorp by Google, ZTX by Forrester, the Zero Trust Architecture by NIST, the Jericho Forum concept, the Zero Trust Maturity Model by CISA, the CSA Cloud Control Matrix (CCM), and the Zero Trust Maturity Model (ZETUMM), were developed within specific organizational and technological frameworks (Cloud

Security Alliance, 2024; Cunningham et al., 2018; Google Cloud, 2024; Modderkolk, 2018; Rose et al., 2020a; Zero Trust Maturity Model | CISA, 2024). However, these standardized techniques may not be universally applicable to countries with different cultural origins, as they do not account for the diverse cultural circumstances of individual nations.

Existing research on Zero Trust (ZT) adoption often overlooks the critical influence of security, national, and organizational cultural factors. No single model comprehensively incorporates these cultural aspects into its framework. Additionally, there is a notable lack of studies specifically investigating information security culture and ZT adoption within the UAE, leaving a gap in understanding how these cultural dimensions impact ZT adoption in this region. The substantial disparity between zero-trust architecture and traditional network-based security systems implies considerable risks in a complete shift to the former. Such a transition often disrupts established work processes, affecting user experience and resource accessibility due to challenges in establishing the appropriate level of trust (Adahman et al., 2022a; Hansen, 2022; Teerakanok et al., 2021a).

Although recent research has extensively explored the technological aspects and challenges associated with adopting a zero-trust architecture, there is a notable gap in considering the impact of information security culture, national culture, and organizational culture in the adoption of this model. This gap is particularly evident in the Arab world, with a specific focus on the United Arab Emirates. This study aims to fill these gaps by examining the influence of information security culture, national culture, and organizational culture maturity on zero-trust adoption within the UAE. The overarching goal is to tailor the current zero-trust model to accommodate the

unique factors of information security culture within organizations in the UAE, facilitating a seamless adaptation of the zero-trust model.

1.3 Research Gap

The research gap revolves around the lack of comprehensive studies addressing the cultural aspects—specifically information security culture, national culture, and organizational culture—that influence the adoption of Zero Trust adoption, particularly in the context of Arab countries like the UAE. While existing research has focused on the technological and operational challenges of Zero Trust implementation, it has not adequately explored how these cultural factors affect the adoption of Zero Trust models in different cultural environments.

In particular, there is a notable absence of research examining:

- The impact of information security culture on Zero Trust adoption, especially within the UAE's specific cultural context.
- The role of national and organizational culture in shaping the success of Zero Trust implementation in Arab organizations.
- Holistic maturity models that incorporate cultural dimensions to facilitate Zero Trust adoption in culturally unique environments like the UAE.
- Specific information security culture factors, such as employee behavior, training, management support, and communication, that play a critical role in the seamless transition to Zero Trust models.

Thus, the study aims to address this gap by tailoring Zero Trust frameworks to align with the cultural and organizational dynamics of the UAE, contributing to the development of a culturally sensitive Zero Trust adoption model.

1.4 Research Questions

- What impact do National Culture (NCS) and Organizational Culture (OCS) have on the adoption of Zero Trust in the context of the UAE?
- How does Information Security Culture (ISC) within UAE organizations correlate and influence the adoption of Zero Trust Adoption (ZTA)?
- What are the specific factors of information security culture are most significant in influencing the successful adoption of Zero Trust in the United Arab Emirates?

1.5 Research Objectives

The main objective of this study is to examine the impact of national,organizational and information security cultures towards the adoption of Zero Trust model in UAE.The research includes sub-objectives;

- To examine the role of National and Organizational Culture in shaping the adoption of Zero Trust models.
- To assess the correlation and impact of Information Security Culture on the adoption of Zero Trust Architecture in UAE organizations.

- To examine the correlation of critical Information Security Culture factors that contribute to the adoption of Zero Trust.

1.6 Thesis Organization

This thesis has the below structure:

Chapter 1: Introduction

The first chapter provides an overview and definition of the research area. It examines the research area, outlines the components that define the research aims and limitations, establishes the boundaries of the studies and concludes with a brief summary of the research structure.

Chapter 2: Literature Review

Chapter 2 is devoted exclusively to a thorough analysis of the existing literature. This text comprehensively evaluates the conclusions of recent academic research, conducts a thorough analysis, identifies significant shortcomings and constructs a solid theoretical framework tailored to the specific topic.

Chapter 3: Methodology

Chapter 3 addresses the main points of research design and methodology. This includes the development of a conceptual model using the information from the current literature, a detailed explanation of the research methodology discussed and a comprehensive description of the variables. In addition, the hypotheses are developed in this chapter.

Chapter 4: Results and Analysis

Chapter 4 This chapter include a comprehensive examination of the data collected from the participants. Various tests and statistical analysis technique are used to obtain valuable results.

Chapter 5: Discussion

Chapter 5 This chapter include a comprehensive interpretation and discussion of the results obtained from the data analysis. This section outlines the benefits of the study, deriving both theoretical and practical contributions from the results. It also identifies possible opportunities for further research and concludes by summarizing the key findings.

Chapter 6: Conclusion

Chapter 6 this chapter has a summary of the research findings and provides a general overview of the theoretical and practical implications of the study. It identifies possible opportunities for future research that utilize the integrated understanding gained in the previous chapters.

1.7 Theoritical and Practical Contributions

This study fills a significant information gap on cybersecurity practices and policymaking in the United Arab Emarites. It provides important insights for organizations to effectively manage the complexities of modern cybersecurity by examining the intricate components of information security culture and its influence on the Zero Trust (ZT) model.

1.7.1 Theoretical Contributions:

- This research highlights how national culture significantly influences the adoption of Zero Trust in the UAE, providing a theoretical framework for understanding cultural impacts on cybersecurity practices.

- It offers a theoretical basis for the role of organizational culture in shaping the adoption of Zero Trust models, emphasizing the need for culturally aligned security strategies.

- The study identifies critical factors within information security culture that significantly influence the successful adoption of Zero Trust in UAE organizations, contributing to the theoretical understanding of ISC's role in cybersecurity.

1.7.2 Practical Contributions:

- Development of a Zero Trust model that aligns with the cultural values, traditions, and behaviors of the UAE, ensuring both effectiveness and cultural appropriateness.

- Emphasizing the need to adapt cybersecurity models to different cultural contexts, moving away from a one-size-fits-all approach.

- Proposing the integration of cultural elements into Zero Trust models to improve acceptance and compliance among employees.

- Highlighting a strategy that targets unique security issues in different cultures, thereby enhancing overall security effectiveness.

- Providing explicit guidance for cybersecurity practices and policymaking in Arab countries, especially the UAE.
- Suggesting proactive involvement of cultural aspects to increase employee acceptance and adherence to security measures.
- Offering practical advice for UAE organizations to improve information security practices by addressing cultural factors and regional differences.
- Recommending the alignment of user actions with information protection goals, integrating organizational and information security culture with the Zero Trust model.
- Presenting cultural responsiveness as a tactic to improve organizational effectiveness by enhancing security activities and reducing resistance to change.
- Indicating the need for future research to include more information security factors, countries, and participants to enhance result accuracy.

In summary, this research provides valuable insights into the critical role of national, organizational, and information security cultures in driving successful Zero Trust adoption in the UAE. The findings highlight the need for organizations to prioritize cultural factors alongside technological solutions when implementing Zero Trust security frameworks.

1.8 Research scope

This research aims to examine the multifaceted cultural influences on the adoption of Zero Trust Architecture (ZTA) within organizations in the United Arab Emirates (UAE). By focusing on the interplay between National Culture (NCS), Organizational Culture (OCS), and Information Security Culture (ISC), the study seeks to elucidate how these cultural dimensions shape perceptions, attitudes, values, assumptions, and knowledge related to security practices. It will not cover technical aspects of Zero Trust implementation in detail but will instead focus on cultural and behavioral dimensions.

- National Culture (NCS): The study will explore how the unique cultural values prevalent in the UAE impact the adoption of ZTA. Drawing on Hofstede's Cultural Dimensions, it will analyze factors such as Power Distance, Individualism vs. Collectivism, Uncertainty Avoidance, and Long-Term vs. Short-Term Orientation, assessing how these dimensions influence security perceptions and practices at both individual and organizational levels. The research will investigate whether national cultural traits foster or hinder effective security measures and how they affect compliance and engagement with ZTA.

- Organizational Culture (OCS): The research will also focus on the internal culture of organizations within the UAE, examining how shared values, beliefs, and behaviors impact the successful implementation of ZTA. This aspect will cover perceptions of top management support, communication styles, and adherence to policies and procedures. By analyzing how organizational culture aligns with or

diverges from national culture, the study will assess the implications for security practices, including training, compliance, and change management.

- Information Security Culture (ISC): The study will delve into the specific factors that constitute ISC, including awareness and training, policy adherence, communication effectiveness, and the influence of management on security behavior. By identifying the correlations among these factors and their significance in facilitating ZTA adoption, the research will provide insights into best practices for cultivating a robust security culture that resonates with both organizational and national values.

Research steps and implementation

The below table 1.1 highlite the steps of the research process, along with the detailes related to each step

Table 1.1 Research Steps

Step	Description	Outputs
1. Proposal and Research Setup	Define research objectives, including analyzing how National Culture, Organizational Culture, and Information Security Culture influence ZT adoption.	Research Proposal, Initial Literature Review
	Develop a proposal outlining scope, significance, and expected outcomes.	
	Conduct an initial literature review to understand key concepts and establish a theoretical foundation.	

2. Literature Review on Cultural Impact	Perform an in-depth literature review on National Culture (NC), Organizational Culture (OC), Information Security Culture (ISC), and Zero Trust (ZT).	Comprehensive Literature Review, Key Theories
	Identify relevant theories (Like Hofstede's Cultural Dimensions for NC) to understand cultural dynamics in the UAE.	
3. Identify and Categorize Factors	Extract and categorize factors within NC, OC, and ISC that could influence ZT adoption.	Categorized Factors (NC, OC, ISC)
	Organize factors into categories based on internal and external dimensions, as well as cultural relevance to UAE's cybersecurity environment.	
4. Review of Existing ZT Models	Research existing Zero Trust Models and frameworks to understand current approaches and identify potential cultural gaps.	List of ZT Models, Identification of Gaps
	Document ZT models that emphasize cultural aspects or adaptation to different organizational contexts.	
5. Hypothesis Development	Formulate hypotheses on the relationship between NC, OC, ISC, and ZT adoption	Research Hypotheses
	Define the expected impact of each cultural construct on ZT adoption.	
6. Develop Initial Research Model	Create an initial conceptual model showing how NC, OC, and ISC factors are expected to influence ZT adoption in the UAE.	Initial Conceptual Model
	Illustrate interconnections between cultural dimensions and ZT principles (e.g., segmentation, least privilege, continuous verification).	
7. Survey and Instrument Design	Design a survey instrument that measures cultural dimensions (NC, OC, ISC) and ZT adoption level within UAE organizations.	Survey Questionnaire, Measurement Scales
	Develop survey questions aligned with hypotheses and cultural constructs identified in the literature.	

	Identify senior information security profisionals.	
8. Sampling and Data Collection	Define sampling method and size based on the target population within the UAE cybersecurity sector.	Collected Survey Data
	Distribute survey and collect data from respondents.	
	Ensure data quality and completeness through validation checks.	
9. Data Analysis and Model Testing	Conduct data analysis using statistical methods (PLS-SEM) to test the hypotheses and validate the conceptual model.	Analysis Results, Refined Model
	Analyze the relationship between NC, OC, ISC, and ZTM adoption, and assess the strength and significance of each factor.	
10. Finalize Research Model	Refine the initial conceptual model based on analysis results, highlighting cultural factors that significantly impact ZT adoption in the UAE.	Finalized ZT Adoption Model for UAE
	Finalize the model, focusing on how NC, OC, and ISC should be addressed for successful ZT adoption.	
11. Thesis and Paper Writing	Develop a thesis document detailing research background, methodology, findings, and cultural insights.	Thesis Document, Scientific Paper
	Write a scientific paper summarizing the study's impact, findings, and implications for ZT adoption in UAE's context.	
12. Defense and Future Research	Prepare for thesis defense to present findings to an academic or professional audience.	Defense Presentation, Future R
	Identify potential areas for future research on ZT adoption, considering cultural dynamics in different regions or evolving security models.	

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

The main objective of this literature review is to examine the complex relationship between the culture of information security and the implementation of the Zero Trust paradigm in organizations. It also aims to analyze the key factors that are used to evaluate the information security culture of these organizations. To achieve this objective, the relevant literature and background information on information security culture, the zero trust model and information security frameworks in the UAE were explored in detail.

This in-depth research included a detailed examination of recent studies in the field of information security culture and the zero-trust model, covering aspects such as zero-trust architecture, implementation challenges and various facets of information security culture. The focus was on identifying recent studies that highlight important information security factors and use frameworks to assess the maturity of information security culture. The review criteria included studies that focus on information security culture and its influencing factors, as well as an examination of relevant zero trust studies that include reviews, models, architectures and applications, and any information security standards or frameworks applicable in the UAE.

Within these criteria, the overarching objectives were to: (1) to identify common factors that shape the culture of information security in organizations; (2) to explore common zero trust frameworks and maturity models to understand their

principles and capabilities; and (3) to identify gaps in the existing literature to provide insights for potential future research directions. Through this systematic examination, the literature review aims to provide a nuanced understanding of the dynamic interplay between information security culture and the integration of the zero-trust model into organizational frameworks.

2.2 Zero Trust History

The first principles of Zero Trust (ZT) were introduced by the Jericho Forum in 2004 through the principle of de-perimeterization, which recognizes that users and programs leave the corporate network. This was followed by the "black-core" security strategy developed by the Defense Information Systems Agency (DISA) and the Department of Defense (DoD) in 2007, focusing on securing individual transactions rather than relying on perimeter-based security. End-to-end IP encryption is a communications network design in which all data sent or received by a user over a global IP network is encrypted before it leaves the user's device, as shown in Figure 2.1. In 2010, John Kindervag introduced the Zero Trust model, which operates on the principle of "never trust, always verify," requiring strict identity verification for every person and device attempting to access resources. Google adopted the ZT paradigm and called it BeyondCorp, incorporating Google's knowledge and experience gathered over the last decade, as well as suggestions and recommendations from the broader community. BeyondCorp eliminates the need for a VPN by moving access restrictions from the network perimeter to individual users, enabling secure work from anywhere. In 2018, Forrester released the Zero Trust eXtended (ZTX) platform, providing a comprehensive framework for implementing zero trust principles across an organization. The National Institute of Standards and Technology (NIST) published

SP 800-207 in 2020, which describes ZT and the components of the ZT architecture, to help organizations adopt the framework.

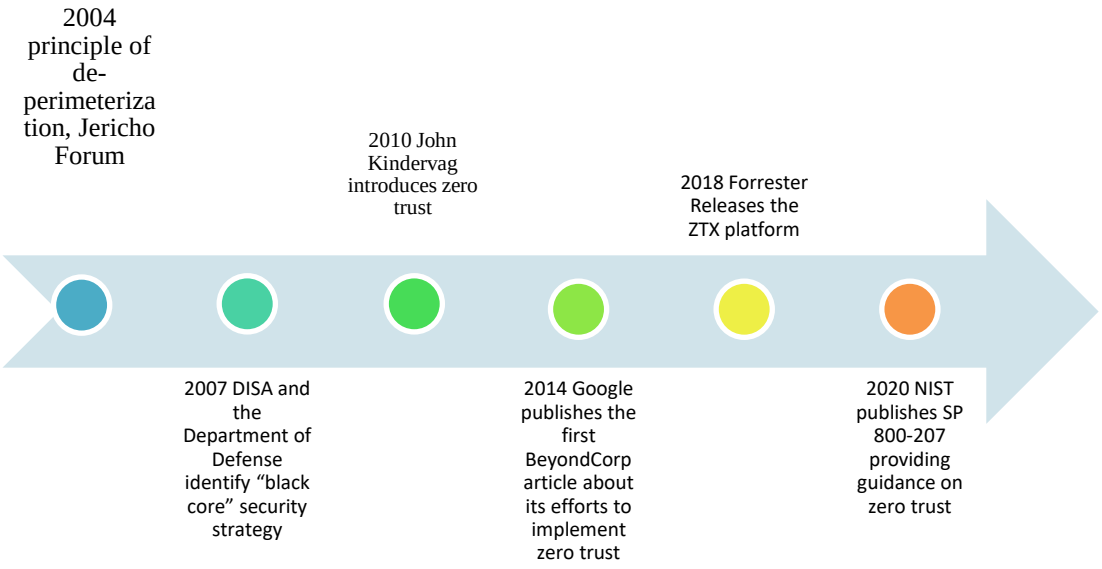

Figure 2.1 Brief History of Zero Trust

2.3 Zero Trust Reviews

This section describes previous reviews conducted in the field of ZT.

The author (Buck et al., 2021b) performed a multi-voiced literature review to identify gaps in the literature and synthesize the present level of knowledge regarding ZT. Idea, architecture, businesses, industries, and user society were the main topics of the review. By completing this review(Buck et al., 2021b), the author identified that researchers have spent most of their time writing about how to improve ZT systems in terms of architecture and performance. On the other hand, practical work has concentrated on the positive effects of ZT in the workplace and different approaches to making the transition(Buck et al., 2021b).

According to (Sarkar et al., 2022) by comparing ZT network security in the cloud computing environment, the researcher reviewed six surveys about the architectural and technical features. The topic-specific issues that affect modern cloud computing networks were also highlighted. The researcher also discusses the requirements for migrating to a ZT architecture, as well as issues with the cloud platform. Although none provide a complete platform solution, it is possible to design a cloud network architecture based on modular, add-drop, trust-based solutions(Sarkar et al., 2022).

However, (Syed et al., 2022) conducted a comprehensive survey about ZT architectures where they emphasized the importance of authentication and access control and provided a detailed analysis of cutting-edge techniques for authentication and access control in various scenarios, as well as traditional methods of encryption, micro-segmentation, and security automation that can be used to create a ZT architecture. Although difficulties associated with existing risk management and trust criteria (micro segmentation, access control, and software-defined) that may impact the adoption of ZT in its actual meaning was investigated, it was determined that these obstacles do not prevent the adoption of ZT.

The importance of authentication and access control approaches that account for the context, behavior, and perceived dangers within an organization must be emphasized because implementing a ZT system requires a combination of technologies and architectural approaches. Realizing a complete ZT environment additionally requires encryption, micro-segmentation, and software-defined perimeters according to(Syed et al., 2022).

(Xiao et al., 2022) performed a systematic investigation of access control as a criterion of risk, ZT, and context awareness to investigate the important components of each and to discover areas of overlap and synergy to optimize the operation and deployment of these systems. The author concluded that many studies on ZT, risk-based access, and awareness had fundamental similarities and that many of these ideas could be applied to ZT models and deployments.

Moreover, (Laplante & Voas, 2022) reviewed artificial intelligence with ZT to determine if "Zero Trust AI" is justified. If not, why do we need AI that can be explained? The researchers identified ability, integrity, and benevolence as elements of AI systems that primarily affect AI-based systems.

(Teerakanok et al., 2021c) used a review of migrating to ZT architecture to introduce the idea and its architecture. Additionally, there are difficulties, procedures, and factors to consider when switching from the old design to ZT architecture. Certain issues with vendor lock-in and a lack of standardization in ZT architecture are mentioned and examined. Brief details on procedures and factors to be considered while switching from perimeter-based architecture to ZT architecture are offered.

These reviews highlight the importance of understanding the challenges and issues associated with ZT adoption and implementation, particularly in the areas of architecture, performance, authentication, access control, and risk management. They also emphasize the need for further research to optimize the operation and deployment of ZT systems in various scenarios.

2.4 Zero Trust Architecture Review

The ZT architecture has different logical components required to deploy the framework in the organization, and they can be cloud or on-premises services. The architecture includes components like a control panel, where the decision of access verification is completed by two main units: the policy engine and the policy administrator. As shown in Figure 2.2, access information can come from various devices such as SIEM, Threat Intelligence, IDM, PAM, and any other device in the infrastructure.

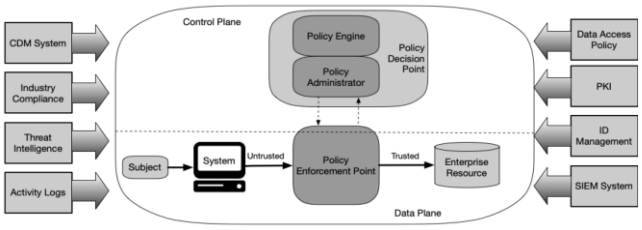

Figure 2.2 NIST computer security resource center, "SP 800-2017, Zero Trust Architecture." August 2020

A collection of published reviews has discussed the concept from different points of view. The following Table 2.1 describes previous studies conducted in the field of ZT architecture and its components:

Table 2.1 Findings of the Zero-Trust Architecture review (ascending)

Author	Year	Findings
(Kindervag, 2010a)	2010	The author introduced a ZT architecture paradigm. Data acquisition: network based ZT architecture proposal to achieve ZT, you must create a data collection network. As network complexity and user communication delay grow, it becomes simpler to extract network data like packets, syslog, and SNMP messages from a single place for near-real-time analysis.
(DeCusatis et al., 2016)	2016	Integrating ZT cloud networks with the security access transport protocol and authentication-on-first packet Using a transport access control system based on

		overlay steganography that embeds authentication tokens in the TCP packet request and first-packet authentication, we demonstrated several ZT networking properties. Multiple layers of security, such as encryption, make it hard for hackers to leave a digital footprint.
(Rose et al., 2020b)	2020	With a better grasp of what a ZT architecture is, API design, maintenance, and monitoring, as well as general deployment patterns and use cases where ZT may improve an enterprise's overall IT security posture, are simplified.
(Sultana et al., 2020)	2020	To address the risks associated with medical and health data, it has been recommended to establish a secure system for exchanging medical images based on ZT principles and block chain technology and solution. Utilized are the immutability of the block chain, the additional security given by ZT principles, and the scalability of off-chain data storage made possible by Inter Planetary File Systems (IPFS). With the wide use of this technology, the safety of medical or health data transfers should increase.
(de Weever & Andreou, 2020)	2020	Despite the widespread use of Kubernetes, a cloud-hosted open-source container, and Istio, an additional open-source service that offers conventional security and advanced features with little service necessary to adapt, deep traffic visibility in containers was not highlighted, which is one of the main tenets of the ZT architecture.
(Ramezanpour & Jagannath, 2021)	2021	The urgent necessity to include ZT concepts into the fifth and sixth generation (5G and 6G) global systems for mobile communications. Using various 5G network technologies, the envisioned intelligent ZT architecture enforces ZT principles for tactical and commercial use.
(Tian & Song, 2021)	2021	A state machine model known as the "Zero Trust approach" based on the V. Bell-Lampedusa model, is used to enforce access control, and the Biba Integrity Model collection of access control rules is meant to protect data integrity. where this approach performs in-depth trust assessments on system characteristics such as determining what persons are authorized to accomplish, the resources to which they have access, and the activities they are permitted to do on a system. Managers may define varying weights for confidentiality and integrity requirements using access controls, which also help limit and monitor system

		usage at the user or group membership level.
(Ghate et al., 2021)	2021	He discussed an innovative architecture for advanced ZT that uses automated policy formulation to provide accurate access control on a limited budget. This architecture is cutting-edge. In order to accommodate a diverse set of regulations, the structure that has been proposed is made to be adaptable, and it requires just a little amount of space to store data and process power.

In summary, ZT architecture is a security paradigm that emphasizes the importance of data collection, multiple layers of security, and the use of ZT concepts in various network environments, including cloud networks. The implementation of ZT architecture requires explicit authentication and authorization decisions, continuous monitoring and verification, and the assumption that every system is surrounded by adversaries and a threat actor is active at all times.

2.5 State of the Art Zero Trust Models and Frameworks

Table 2.2 lists the topics addressed by the seven ZT frameworks and maturity models. These ZT models and frameworks share common principles, such as continuous verification, limiting the blast radius, and automating context collection and response and focusing on the technology. Implementing a ZT approach can be challenging, especially when dealing with legacy technology and piecemeal adoption(Muhammad et al., 2022). However, embracing a ZT strategy can help organizations improve their overall security posture and better protect their digital resources(Rose et al., 2020c).

Table 2.2 Summery of Zero trust models and frameworks

Zero Trust model	Key principles	Key capabilities	Focused area

Google's BeyondCorp (Google Cloud, 2024)	User and Device Trust	Continuous verification of user and device trust. Access decisions based on contextual factors.	User and Device Trust Context-Aware Access
Forrester's ZTX (Cunningham et al., 2018)	Assume breach. Implement strict access controls. Focus on protecting data, not just the network perimeter	Extending ZT to protect workloads and data. Emphasizing the security of user identities.	Workload-Centric Security People-Centric Security
NIST's Zero Trust Architecture (Rose et al., 2020a)	Technology-focused User Focused Continuous verification Limit the "blast radius." Automate context collection and response	Ongoing monitoring of systems, networks, and users. Adjusting access controls based on the evolving risk environment and user behavior.	Continuous Monitoring Adaptive Access Controls
Jericho Forum's IdEA (Spencer & Pizio, 2023)	Technology-focused Secure the network perimeter. Use defense-in-depth Use least privilege access	Focus on establishing and verifying digital identities. Granular control over access permissions.	Identity-Centric Security Fine-Grained Access Control
CISA Zero Trust Maturity Model (CISA, 2022)	Technology-focused	Visibility and analytics Automation and orchestration Governance	Identity Device Network/Environment Application Workload Data
CSA Cloud Control Matrix (CCM) (Cloud Security Alliance, 2024)	Technology-focused	A set of controls covering various security aspects. Emphasis on protecting data regardless of its location.	Comprehensive Controls Data-Centric Security
Zero Trust Maturity Model (ZTMM) (Modderkolk, 2018)	Technology-focused	53 capabilities across the 15 focus areas. Identity and Access Management Endpoint Protection Network Security Data Protection Application Security Incident Response Threat Intelligence Security Awareness Security Monitoring Security Operations Security Automation Security Policy Security Governance Vendor Management Risk Management	Identity and Access Management Endpoint Protection Network Security Data Protection Application Security Incident Response Threat Intelligence Security Awareness Security Monitoring Security Operations Security Automation Security Policy Security Governance Vendor Management Risk Management

2.6 Zero Trust Architecture Adoption Concerns and Challenges in the Organizations

Organizations are always looking to protect their data and assets from potential attacks. One of the key purposes is to protect data confidentiality, integrity, and availability. Since resources are now being used both on-premises and in different clouds, and the perimeter of the security defense area increases, it is getting harder and harder to protect enterprise resources, especially data.

Data is an important asset for any organization that processes critical information(Russinovich et al., 2021). To protect confidential data, it is critical to implement access control measures that meet business requirements for data protection. Organizational information security culture, individual behavior, and technology controls must all be considered to manage human risk effectively(Sattarova Feruza & Kim, 2007). No one can be trusted in a ZT network, and every attempt to obtain access to secured data should be considered a security risk. That is why there is a need to double-check each entry. Access will be granted only when a request has been validated. User permissions can be established to provide users with full access to a resource or only the features or data they need. When checking someone's ID, passwords are not the only thing to look at. There are other parts and sources of information to look at as well (Shore et al., 2021).

Adopting a ZT architecture is challenging both technically and organizationally (Bush & Mashatan, 2022b). However, ZT is not constrained by perimeters, which will expand its scope beyond the company and include all the stakeholders(Chimakurthi, 2020). The ZT concept should be fully infused into an organization's culture and not merely used in IT systems design. Many attackers use