Advance Journal of Business Management and Social Science
ISSN: 2998-7946
Volume 1, **Issue** 2, 2025, **pp.** 1-11, **Article ID:** CM2512101009
DOI: 10.65080/dp4w1990

Research Article

Evaluating the Effectiveness of Zero Trust Architecture in Modern Enterprises: Moderating Role of Organisational Maturity

Talha Sarfaraz[1, *]

[1]*Department of Marketing, College of Business Administration, Imam Abdulrahman Bin Faisal University, Dammam, Kingdom of Saudi Arabia*

Article History

Received: 22 February, 2025 Revised: 27 May, 2025 Accepted: 02 June, 2025 Published: 30 June, 2025

Abstract:

Aim: The study evaluated the performance of Zero Trust Architecture (ZTA) in modern enterprises, particularly focusing on organisational maturity as a moderator. As cyber threats evolve and perimeter security proves insufficient, organisations increasingly implement ZTA to protect their digital assets.

Methods: The study employed a quantitative method based on survey research and collected data from 380 experts involved in cybersecurity decision-making among UK companies. The data was analysed and tested for the relationships between organisational maturity, ZTA, and enterprise performance using Partial Least Squares Structural Equation Modelling (PLS-SEM).

Results: The findings revealed that ZTA ($\beta = 0.388$, $p = 0.000$) significantly and positively influenced enterprise performance, particularly in improving cybersecurity. Furthermore, organisational maturity ($\beta = 0.123$, $p = 0.022$) is a significant moderating factor, enhancing the positive relationship between ZTA adoption and improved performance.

Conclusion: It provides practical business implications by concluding that organisational maturity is necessary for maximum utilisation of ZTA's benefits. The findings also present valuable insights to decision-makers and cybersecurity experts who wish to maximise the use of ZTA and strengthen their cybersecurity position.

Keywords: Zero trust architecture (ZTA), cybersecurity, organisational maturity, digital transformation, enterprise performance.

1. INTRODUCTION

The United Kingdom is now at increased risk regarding cybersecurity, as businesses operating in all sectors are becoming the targets of advanced and more consistent cyberattacks (Government of the UK, 2023). According to 2024 data published by the National Cyber Security Centre (NCSC), over 50% of companies in the United Kingdom had experienced a cyber incident, and ransomware, phishing, and insider threats were most common (Government of the UK, 2024). These risks have strengthened with the fast adoption of clouds, the pace at which hybrid and remote working models are evolving, and the dependence on the sophisticated digital supply chains (Zammani *et al.,* 2021). The earlier perimeter-based methods adequate to secure networks are no longer practical for countering opponents utilising flaws within and outside the corporate perimeters. (Syed *et al.,* 2022) reflect that this change has compelled UK organisations to rethink their security approaches and search for models that focus on constant verification and access according to the least permissions, Zero Trust Architecture (ZTA) being one of the most prominent.

Meanwhile, UK businesses are subject to increasing regulatory and compliance pressures. With the introduction of the UK General Data Protection Regulation (UK GDPR) and other sector-specific requirements, *e.g.,* the cybersecurity rules issued by the Financial Conduct Authority (FCA) and the data protection standards of the NHS in the health industry, organisations feel the pressure to provide continuous and

*Address correspondence to this author at Department of Marketing, College of Business Administration, Imam Abdulrahman Bin Faisal University, Dammam, Kingdom of Saudi Arabia; Tel: +966546591080; E-mail: tsarfaraz@iau.edu.sa

evidence-based data protection (Stamford, 2024). According to (Stafford, 2020), failure to comply also carries financial sanctions, reputation, and loss of stakeholder confidence. Although policymakers and regulators have put forward ZTA as a possible compliance enabler, its success in assisting organisations to fulfil such obligations is debatable, and its adoption is disparate, as (Sholademi, 2024) also reflects.

The main problem impacting businesses in the UK is the overlap of the increase in cyber risks and regulatory requirements, as well as the operation-related challenges of implementing Zero Trust. Despite the potential of frameworks such as ZTA, most organisations, especially those with small and medium-sized enterprises (SMEs), which form 99% of the businesses in the UK, find it difficult because of their limited budgets, lack of in-house expertise and the high costs of connecting these systems with legacy systems (Paya & Gómez, 2024). Larger companies have adequate budgets, but tend to be faced with issues of governance and interoperability that cause the adoption to be ineffective (Onwuegbuzie & Alabi, 2025). As a result, implementation is fragmented and causes discrepancies between strategic objectives and the reality of operations. As specified by (Mijwil *et al.,* 2023; and Omar *et al.,* 2025), this skewed implementation creates both SMEs and large enterprises to be under substantial vulnerability at a moment when cyber threats are beginning to be more serious and when regulatory oversight is starting to become more stringent. Unless there is a clear explanation of how organisations can effectively operationalise ZTA at various maturity levels, the UK will end up with greater inequalities between well-resourced firms and the most vulnerable firms to cyberattacks.

The importance of this research is that it attempts to answer the question of whether ZTA is effective in the UK enterprise environment. Although the idea of Zero Trust has significant support, there is little information regarding its actual implementation and how this implementation has resulted in better security outcomes within UK companies. In addition, organisational maturity, evident in governance systems, IT skills, and digital culture, is likely a moderator of ZTA success. However, this has not been rigorously studied, as supported by (Khan, 2023; and Khan *et al.,* 2024). Existing literature, such as (Igboko & Temitope, 2025; and Jimmy, 2021), is still predominantly conceptual or international generalisations, and little has been done to focus on the UK. The gap areas in this study aim to be filled by offering context-specific evidence that is vital to both practitioners and scholars.

The current study makes three significant contributions: theoretical and empirical contributions, and contributions for policymakers and regulators. Theoretically, the study contributes to the development of the cyberspace security literature by introducing organisational maturity to the research of Zero Trust effectiveness, which provides the possibility of a new perspective on the study of security adoption in non-technical aspects. In terms of empirical contributions, the study provides evidence-based information on UK enterprises regarding whether and how ZTA enhances security outcomes at different maturity levels. Eventually, the study will also make significant contributions to policy and practice by equipping policymakers and regulators, such as the NCSC and the Department for Science, Innovation and Technology, with detailed guidance for endorsing the adoption of Zero Trust. By depicting that maturity conditions tend to impact ZTA outcomes substantially, the study provides policymakers with the evidence required to design and form differentiated strategies that provide both SMEs and large firms, consequently, guaranteeing that regulatory encouragement adheres to the realities of enterprise capabilities.

2. LITERATURE REVIEW

2.1. Theoretical Framework

A framework known as the Technology-Organisation-Environment (TOE) framework is an adequate theoretical framework as it posits that the adoption of technological innovations such as ZTA is influenced by technological, organisational, and environmental factors (Amini & Javid, 2023; Malik *et al.,* 2021). The technological context entails the attributes and the functions of ZTA, including continuous authentication and micro-segmentation, which are essential to improve cyberspace (Igboko & Temitope, 2025). The organisational scenario focuses on the importance of organisational maturity, which involves the dimensions of resources, infrastructure, cybersecurity culture, and governance practices that contribute towards implementing (effective implementation) and scaling ZTA (Fernandez & Brazhuk, 2024). The environmental context considers the external aspects, such as regulatory pressure and market norms, that affect the cybersecurity initiatives of an organisation (Awa *et al.,* 2017; Hoang, 2024). When applying the TOE framework, it is possible to affirm the moderating value of organisational maturity to the adoption and successful use of ZTA, and that highly mature organisations are in a better position to take up and enjoy the application of this technology (Mick *et al.,* 2024; Yeoh *et al.,* 2023).

2.2. Effectiveness of Zero Trust Architecture in Modern Enterprises

ZTA has been identified in existing literature as a practical approach to protect contemporary businesses within the framework of cloud and remote working scenarios. (Sunkara, 2025) provides a detailed explanation of how ZTA could resolve the insufficiency of the traditional organisation of perimeter protection, which is focused on continuous authentication and micro-networking that leads to improving access controls and threat mitigation. On the same note, the Google Beyond Corp and Microsoft ZTA case studies have also proved the system's efficiency in securing sensitive information without compromising the quality of user experiences. However, case studies fail to explore the challenges in scaling ZTA with legacy systems with low cybersecurity maturity. (Bashir, 2024; and Mensah, 2024) also promote the utility of ZTA, especially in hybrid and cloud platforms, to combat insider threats and alleviate security breaches. The study shed

light on cybersecurity as its key advantage; however, it fails to shed light on how it struggles with legacy system integration and the performance overheads it imposes.

(Batan, 2024; and Hasan, 2024) comment on operating problems such as inventories of assets and active monitoring, although they tend to be general statements, without a specific plan for addressing these adversaries of operations in cyber-deficient and ill-informed organisations. However, it fails to discuss the influence of organisational maturity on the success of an organisation when using ZTA. A study by (Ghaffari & Arabsorkhi, 2018) and another by (Yeoh *et al.,* 2023) highlighted that maturity in computer use is crucial even in terms of cybersecurity. However, there is no research on the relationship between maturity and the successful use of ZTA implementation. With the lack of incorporation of this essential element, one gets a knowledge vacuum regarding how organisational infrastructure, culture, and preparedness directly impact the success of ZTA (Igboko & Temitope, 2025). On the other hand, the TOE framework provides a robust theoretical ground for adopting technological innovations such as ZTA. The framework highlights that the technological readiness of an organisation, its internal structure, and the external environment are significant factors that support success in adopting technological innovations such as ZTA, especially in the hybrid and cloud environment (Yeoh *et al.,* 2023).

Moreover, (Aljohani, 2023) uses quantum cryptography in his research on ZTA to increase data security; however, the study fails to critically highlight an in-depth discussion of the existing infrastructures compared to the current ones, potentially leaving a lack of practical applicability. Similarly, (Sunkara, 2025) compares the theoretical and practical implementation of ZTA with case studies on Google and Microsoft, but fails to consider key aspects like the integration of ZTA with the legacy systems and the performance overheads that are of high significance to the organisations when taking up ZTA implementation. The study also fails to adequately discuss when organisational maturity can be used to overcome these challenges; hence, it may not be applicable in less mature organisations. (Mensah, 2024) concentrates on identity management and micro-segmentation in ZTA without paying attention to operational challenges of the ZTA adoption, including its system integration and budgetary issues, which make it less feasible. (Bashir, 2024; and Hasan, 2024) cite the importance of ZTA in a hybrid and cloud setting, but do not include organisational maturity as a central element modulating ZTA success, which can be considered a critical weakness in assessing long-term ZTA implementation. Further, it is not observed in the studies that low maturity levels may restrict ZTA adoption, given the circumstances where organisations experience financial issues, lack, and resistance to change. Hence, it can be hypothesised that;

H1: The adoption of ZTA has a significant positive impact on enterprise performance.

2.3. Role of Organisational Maturity

Organisational maturity as a moderator is an essential aspect of a successful adoption of ZTA, but in the existing research, there is an absence of fully exploring this factor (Bhaskaran, 2025). According to (Brezavšček & Baggia, 2025; and Yeoh *et al.,* 2023), cybersecurity consequences and organisational maturity, where organisations have well-developed knowledge, resources, and security policies, enable a more effective ZTA implementation. These studies, however, fail to acknowledge problems associated with organisations with lower maturity, such as difficulties in integrating ZTA with legacy systems and dealing with the overheads involved in running such a complex security paradigm. (Ghaffari & Arabsorkhi, 2018) found that cybersecurity maturity mediates the association between ZTA adoption and its outcome by allowing organisations to integrate and scale ZTA better. However, they did not provide any particular insights on how maturity directly contributes to the success of ZTA implementation. On a similar note, although the research done by (Hasan, 2024; and Mensah, 2024) about the advantages of ZTA, especially when introduced into hybrid and cloud setups, does not mention the role that different maturity levels play in influencing the flexibility and performance of ZTA. The study by (Ghaffari & Arabsorkhi, 2018) suggests a cybersecurity maturity model but emphasises theoretical rather than real implementation, which reduces its applicability. In a similar light, the topic of machine identity security in ZTA is discussed in the work by (Kotilingala, 2025), with no measures to specify it for enterprises.

On the other hand, the TOE framework implies that organisational maturity is critical to successfully adopting ZTA. As (Ahmadi, 2024) reflects, more mature organisations with more sophisticated security policies and technological infrastructure can better integrate and scale ZTA. On the other hand, organisations with lower maturity face challenges, including legacy systems integration and complex operations, which hinder the adoption process (Brezavšček & Baggia, 2025).

Moreover, literature research experts like (Mick *et al.,* 2024; and Yeoh *et al.,* 2023) focus on the role of organisational maturity. However, they fail to provide evidence directly linking maturity stages to the successful adoption of ZTA. Although studies such as (Ahmad *et al.,* 2021; Zammani *et al.,* 2021) help provide theoretical knowledge about the topic, what is usually not assessed in these studies is the most important practical aspects of the topic that are essential in enhancing the real-life consequences of ZTA, which include integration of the system, problems in operations, and the organisation's readiness. These gaps impose constraints on the practical implications of their results, which do not concern how organisations with a lower level of maturity find it challenging to implement ZTA. Therefore, organisational maturity is key in ZTA adoption and enterprise performance.

H2: Organisational maturity significantly moderates the relationship between ZTA adoption and enterprise performance.

Fig. (**1**) shows the conceptual framework derived from the hypothesis developed above. ZTA is indicated as the

independent variable, Modern Enterprises Performance is the dependent variable, and Organisational Maturity acts as the moderating variable.

2.4. Literature Gap

Although research on ZTA is relatively abundant, there is still a gap regarding the issue of organisational maturity, which is one of the factors impacting the adoption and success of ZTA. (Aljohani, 2023; Sunkara, 2025; and Mensah, 2024) dedicated their studies towards technical individualities of ZTA (data security and system integration), but failed to examine the moderating role of organisational maturity in the relationship between ZTA adoption and enterprise performance. Additionally, (Ghaffari & Arabsorkhi, 2018; and Yeoh *et al.,* 2023) recognise the role of organisational maturity in cybersecurity, but fail to associate it with ZTA implementation adequately. This leaves a gap that was not fully captured in the literature, which is important when examining how organised preparedness and maturity affect the effectiveness and scalability of ZTA.

3. MATERIALS AND METHODS

The study adopts a quantitative method to investigate the effectiveness of ZTA in modern enterprises, focusing on the moderating role of organisational maturity. The survey-based method was selected to obtain the information of IT managers directly involved in the decision-making process on cybersecurity issues and to ensure that the information corresponds to the applied difficulties and approaches to ZTA adoption. This approach enables gaining a wide range of opinions from the respondents who are professionals in the actual implementation of Zero Trust in UK institutions. The research instrument used in the study is a structured survey questionnaire, which was formulated in line with available literature. The target audience included IT professionals, managers and cybersecurity decision makers who were directly engaged in implementing ZTA in UK-based institutions. The questionnaire was based on four parts, including demographics, ZTA implementation, modern enterprise performance and organisational maturity. In order to identify the perceptions of the respondents regarding these critical variables, a five-point Likert scale ranging between Strongly Agree (1) and Strongly Disagree (5) was used. This measure was pilot tested in a relevant, straightforward way, and he feedback corrected the questions. This questionnaire was the primary data collection instrument, as it allowed the investigation of the associations among ZTA adoption, organisational maturity, and enterprise performance. The survey items were designed to capture both the direct and indirect roles of organisational maturity on the successful adoption of ZTA, as shown in Appendix **A**.

The surveys were shared with 600 potential respondents, reaching their sample size, whereas LinkedIn and personal contacts were used to invite the individuals. Three hundred eighty-seven responses were achieved, translating to a response rate of 66.5%. The 380 responses were obtained after seven missing values were removed from the standard sample to be analysed. Participants were reached through the networking functions on LinkedIn, purpose-specific groups on the site, and direct messaging to selected individuals. Additionally, the survey was shared with the IT professionals, managers, and middle-level managers, ensuring the removal of selection bias. The non-response bias is important as there is a comparatively low response rate. An independent sample t-test was used to check the level of non-response bias, where early respondents ($n1 = 25$) and late respondents ($n2 = 25$) were compared. There were no statistically significant differences for ZTA (P-value >0.1), Enterprise performance (P-value >0.1) and organisation maturity (P-value >0.1), indicating that the data collection process was not affected by the non-response bias. The study also considered a common method bias in which the questions used in the survey were highly distinct and measured different constructs. Boxplots were used to check whether there were outliers in the data, and skewness and kurtosis values were used to determine whether the data followed a normal distribution. It was found that the data were not approximately normally distributed, and therefore, PLS-SEM was found to be an appropriate technique. There were no significant outliers that would affect the analysis. Further, the straight-line response technique was questioned, and no indication was identified that there had been excessive usage of the technique; the reliability of the responses was high.

Fig. (1). Conceptual framework

The PLS-SEM was selected due to the normality of the data, which the study of (Hair *et al.,* 2019) also supports. The analysis started with a measurement model test to ensure construct validity and reliability in the form of a Confirmatory Factor Analysis (CFA), where the aspects of loading, composite reliability, and Average Variance Extracted (AVE) were considered. Once the construct validity was confirmed, the structural model was subjected to test variables to investigate the relations between organisational maturity and the effectiveness of ZTA. The relationships were considered significant by looking at path coefficients and *p*-values.

4. RESULTS

4.1. Demographics

The demographics of the study sample, as depicted in Table **1**, which consists of 380 respondents, show that gender and age groups are represented. Of 380 respondents, 60.2% were males, with 39.8% female, as shown in the table. This means that a higher number of males participate in the study than females; hence, the trend in the cybersecurity industry is that the number of male professionals is usually higher than that of female professionals. Gender distribution, however, is also reflective with great female representation, so there is a level of gender diversity in the sample.

Regarding age distribution, most respondents are 30-39, which makes 38.2% of the overall sample. This group of people forms a significant percentage of the human resource base in the cybersecurity industry, which people with extensive experience usually dominate. Additionally, 20 to 29 years old, this group had 28.1% of the respondents, comprising younger professionals, who were maybe at the beginning of their careers. The age groups of 40 to 49 years had 22.1%, and the age group of 50 and above had 11.6%. The results of the education level data indicate that most respondents are at an undergraduate level, with a population of 42%. The percentage of postgraduate respondents was 31%, whereas the percentage of respondents with other educational qualifications was 26%.

4.2. Measurement Model Using Confirmatory Factor Analysis

As per Table **2**, the reliability and convergent validity of the constructs utilised in this study were tested thoroughly, with the existing metrics that rigorously tested the robustness of the measurement model. As per (Hair *et al.,* 2019), both Cronbach's alpha and composite reliability are key indicators of internal consistency, with values above 0.7 confirming results, Table **2**. The Cronbach alpha value of Zero Trust Architecture (0.852), Modern Enterprises (0.815) and Organisation Maturity (0.885) in this study are above the threshold; thus, showing a high internal consistency on the different constructs, Table **2**. The composite reliability scores of these constructs vary between 0.839 and 0.885, confirming the reliability and stability of the measurement instrument. The findings indicate that the constructs are highly consistent, ensuring that items used to measure the constructs are highly reliable.

The convergent validity estimated by the Degree of correlation of the items that are part of the same construct was measured employing the AVE. According to (Hair *et al.,* 2017), good convergent validity is represented by a value exceeding 0.5, Table **2**. The AVE values of Zero Trust Architecture (0.772), Modern Enterprises (0.729), and Organisational Maturity (0.813) exceed 0.5, implying that the measurement items fit their respective constructs. The measurement model is further validated since the factor loadings were greater than 0.6, Table **2**. In particular, the item loadings are all within the acceptable range, ensuring they effectively represent their latent construct. The strong reliability and convergent validity scores provide a solid foundation for the structural analysis, confirming that the constructs are accurately measured and that the path relationships can be interpreted confidently (Cheung *et al.,* 2024).

As per Table **3**, the discriminant validity of the constructs is determined by the ratio of Heterotrait-Monotrait (HTMT), which is widely used to determine whether the constructs are distinct from one another (Henseler *et al.,* 2015). As stated by (Rönkkö & Cho, 2022), the HTMT ratio must be less than 0.85 so that constructs are not highly correlated, thus confirming their discriminant validity Table **3**. The relationship between Modern Enterprise Performance and Organisational Maturity is 0.547, indicating a moderate relationship between these constructs. Additionally, they are related but represent different dimensions of organisational performance. Similarly, Modern Enterprise Performance and Zero Trust Architecture have an association value 0.617. Organisational Maturity and Zero Trust Architecture is 0.718, also within the acceptable range of discriminant validity, as depicted in Table **3**.

The construct between Organisational Maturity and Zero Trust Architecture, which characterises the moderator of the organisational maturity in the effectiveness of ZTA, is found to be 0.107 with Modern Enterprise Performance and 0.436 with Organisational Maturity, which implies a weak relationship. The strongest relationship is indicated between Organisational Maturity and Zero Trust Architecture, with a value of 0.354, implying that constructs are related but not so strongly as to be indistinguishable.

4.3. Path Analysis

The results of the structural model indicated in Table **4** reveal the connections between the organisation maturity, Zero Trust Architecture, and performance in modern enterprises. A direct influence between Organisational Maturity and Modern Enterprise Performance is also statistically significant (β = 0.293, p = 0.000), implying that the effect of organisational maturity on enterprise performance is positive. This is to imply that mature organisations can easily adopt and enjoy the benefits of cybersecurity interventions like ZTA. Additionally, results in Table **4** also show that the use of Organisational

Maturity as a moderator and Zero Trust Architecture influences the performance of the Modern Enterprise (β = 0.123, p = 0.022), demonstrating that organisational maturity strengthens the relationship between ZTA and enterprise performance. It implies that organisations with a high level of maturity will respond better to Zero Trust Architecture. Moreover, the zero-trust architecture has a powerful direct impact on Modern Enterprise Performance (β = 0.388, p = 0.000), which indicates that ZTA itself significantly influences improving the Performance of Modern Enterprises, as depicted in Table **4**. Therefore, the findings imply that an organisation that is well developed in cybersecurity can make better use of ZTA to enhance individual performance. The implications of the whole findings are outlined by the significance of both organisational maturity and ZTA in enhancing modern enterprise success amid the emerging changes relating to cybersecurity threats.

Table 1. Demographics.

Demographic Variable	Category	Frequency	Percentage (%)
Gender	Male	229	60.2
	Female	151	39.8
Age	20 - 29 years	107	28.1
	30 - 39 years	145	38.2
	40 - 49 years	84	22.1
	50 years and above	44	11.6
Education Level	Undergraduate	160	42%
	Postgraduate	120	31%
	Other	100	26%
Total Participants		380	100

Table 2. Reliability and convergent validity testing.

Constructs	Indicators	Factor Loadings	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
Zero Trust Architecture	MEP1	0.872	0.852	0.852	0.772
	MEP2	0.901			
	MEP3	0.862			
Modern Enterprises	MEP1	0.779	0.815	0.839	0.729
	MEP2	0.902			
	MEP3	0.876			
Organisational Maturity	ZTA1	0.887	0.885	0.885	0.813
	ZTA2	0.925			
	ZTA3	0.891			

Table 3. Discriminant validity.

Constructs	Modern Enterprise Performance	Organisational Maturity	Zero Trust Architecture
Modern Enterprise Performance			
Organisation maturity	0.547		
Zero Trust Architecture	0.617	0.718	
Organisation maturity x Zero Trust Architecture	0.107	0.436	0.354

Table 4. Structural model.

Variables	Coefficients	T-Statistics	*P* Values
Organisation maturity -> Modern Enterprise Performance	0.293***	4.381	0.000
Organisation maturity x Zero Trust Architecture -> Modern Enterprise Performance	0.123**	2.297	0.022
Zero Trust Architecture -> Modern Enterprise Performance	0.388***	6.745	0.000

Note: ***p < 0.05 (significant at the 5% level)*
****p < 0.01 (significant at the 1% level)*

Table 5. Model quality assessment.

Variable	R-Square	R-Square Adjusted
Modern Enterprise Performance	0.325	0.319

4.4. Model Explanatory Power

Table **5** shows that the R-square and Adjusted R-square values of Modern Enterprise Performance evaluate the model; in this case, the model has Hypothetical and Expected explanatory power. The value of R-square (0.325) indicates that the independent variables in the model would explain about 32.5% of the variance of performance in modern enterprises. This shows moderate explanatory power, suggesting that though the model explains a considerably higher percentage of the variance, other things may also determine enterprise performance that are not reflected in the model.

H1: The adoption of ZTA has a significant positive impact on enterprise performance.

H2: Organisational maturity significantly moderates the relationship between ZTA adoption and enterprise performance.

5. DISCUSSION

The results of the current study have validated that adopting ZTA has a significant positive impact on enterprise performance, leading to the acceptance of H1 of the study. The effectiveness of ZTA in modern enterprises has been widely embraced as a viable approach to combating evolving cyber threats. As advocated by (Bashir, 2024; and Sunkara, 2025), ZTA's "never trust, always verify" philosophy ensures that all network traffic, regardless of its origin, is continuously authenticated and authorised. (Hasan, 2024) further validated that this approach has been helpful in cloud and hybrid workforce organisation contexts. ZTA enhances security by reducing attack surfaces through micro-segmentation, least-privilege access, and constant monitoring, making it a great approach in combating advanced persistent threats and data breaches (Mensah, 2024). Nonetheless, although prior studies have been keen to note such technical advantages, the present study further broadens that knowledge by noting how ZTA enhances the operational performance of businesses. The research gives fresh information on how ZTA can get much more important results in contemporary organisations, and the paper by (Brezavšček & Baggia, 2025) agrees with this view and emphasises the necessity of ZTA in enhancing the security of enterprises.

The study's findings confirm that organisational maturity plays a significant moderating role in the effectiveness of ZTA, which leads to acceptance of the second hypothesis, H2, of the study. The study results are consistent with those of (Ghaffari & Arabsorkhi, 2018; and Yeoh *et al.,* 2023), who state that the maturity of cybersecurity plays a significant role in implementing such intricate cybersecurity solutions. The results show that older organisations stand a better chance of addressing the legacy system integration obstacles, which, as stated by (Nasiruzzaman *et al.,* 2025), is one of the obstacles to integrating legacy systems. Drawing a contrast, previous studies, including (Bashir, 2024; and Sunkara, 2025), concentrated more on the technical side of ZTA, overlooking the matters of organisational maturity that undoubtedly impact the scalability of ZTA and its success. This paper fills that gap to provide a thorough picture of how the readiness and maturity of the organisational environment predetermines the success of ZTA implementation in the real world. Moreover, the moderating effect of organisational maturity reveals that mature organisations are better positioned to benefit from ZTA, including a lack of security breaches and operational efficiency. This aligns with (Kotilingala, 2025), who explained that more mature organisations can embrace the new cybersecurity models, *i.e.,* machine identities and IoT security.

The present research contributes to the knowledge of the ZTA implementation by indicating that the moderating effect of organisational maturity impacts its effectiveness. Existing studies by (Brezavšček & Baggia, 2025; and Yeoh *et al.,* 2023) supported the relevance of organisational maturity in cybersecurity frameworks and, to some extent, were focused on its effects on the successful adoption of ZTA. These studies aimed to examine the relationship between maturity and cybersecurity outcomes without discussing how maturity affects ZTA deployment and enterprise performance (Ghaffari & Arabsorkhi, 2018). The given research closes that gap by demonstrating that more mature organisations tend to be able to realise and maximise ZTA more successfully, which translates into better results (Nasiruzzaman *et al.,* 2025).

Earlier research by (Bashir, 2024; and Sunkara, 2025) was primarily based on the technical implications of ZTA, including access control, identity verification, and threat prevention. Although they indicated the ability of ZTA to enhance security, they did not refer to organisational aspects that affect the scalability of the framework and its success in the long run. To illustrate, (Mensah, 2024) reported difficulties associated with incorporating ZTA into legacy systems and operational overheads, yet they were also not examined exhaustively regarding organisational maturity. At the same time, this study is concerned that increased cybersecurity infrastructure development and maturity allow organisations to tackle these issues better and scale ZTA easily (Hasan, 2024). Moreover, the results presented in this research can be interpreted within the framework of the Technology-Organisation-Environment model, as these aspects affect the process of innovations adoption, including Zero Trust Architecture (Awa *et al.,* 2017; Malik *et al.,* 2021). According to the TOE framework, the current research reveals that organisational maturity is a key moderating variable for the successful implementation of ZTA. Organisations that have developed security infrastructure can more easily adopt, implement, and scale complex technologies such as ZTA (Brezavšček & Baggia, 2025; Yeoh *et al.,* 2023). This is especially true in the UK, where most organisations upgrade their cybersecurity systems to mitigate the increasing cyber threats. The results are consistent with those of (Ghaffari & Arabsorkhi, 2018), who emphasise that higher cybersecurity maturity can facilitate improved integration of ZTA. Moreover, it is also more directly implied by (Nasiruzzaman *et al.,* 2025; and Liyanage *et al.,* 2024) that the more difficult way of implementing ZTA is as a non-yet-fully-developed organisation, despite the incompatibility problems with the old systems. The results confirm the importance of organisational maturity in optimising the effectiveness of ZTA, which subsequently improves the performance of the enterprise as a whole.

CONCLUSION AND RECOMMENDATIONS

This study adequately establishes the significant moderating role of organisational maturity in the implementation and success of Zero Trust Architecture by UK modern-day enterprises. The study demonstrates that UK organisations with high maturity levels are most likely to adopt ZTA successfully, thus enhancing their cybersecurity position. This study contributes to existing knowledge by bridging the gap between successful adoption of ZTA and organisational maturity, offering valuable insights to both practitioners and scholars. UK SMEs must regularly assess their cybersecurity maturity to detect governance, resources, and infrastructure gaps. This will assist them in knowing they are prepared to adopt more advanced security architectures, such as ZTA, and ensure that their strategy is easy to scale and efficient. The UK NCSC should develop specific support programmes for SMEs to enhance their cybersecurity maturity level. This may involve grants, training, and resources to enable smaller businesses to create the required basis for ZTA implementation so that they are not exposed to increasing cyber threats.

LIMITATIONS

However, there are limitations as the study utilised a convenience sampling method, whose use across all organisational structures and sectors may be limited. The research also addresses the moderating role of organisational maturity without scrutinising the deep-rooted individual factors of maturity, organisational culture, and cybersecurity governance, which may also influence ZTA success. This is also limited to the geographical bounds of the UK; hence, it has limited generalisability.

POLICY RECOMMENDATIONS

Policymakers must focus on creating a conducive environment that contributes to organisational maturity in cybersecurity to increase the success of implementing ZTA. This also involves facilitating the investment in human capital, improving cybersecurity, and developing strategic frameworks for adopting an innovative technology such as ZTA. ZTA must also be part of the mandatory aspect of UK business-related cybersecurity regulations to improve the defences against up-and-coming cyber threats to the industry, particularly those functioning within critical sectors. In addition, policymakers need to encourage UK organisations to review their cybersecurity maturity regularly and provide recommendations to scale up ZTA to deliver continuous growth and reaction to emerging risks.

FUTURE IMPLICATIONS

The future relevance of this study suggests that the companies in the UK that are about to roll out ZTA must focus not only on technical deployment but also on organisational maturity. Since the cyber threats are evolving continuously, more mature organisations will be successful in implementing ZTA and tuning it to their own needs so that they remain resilient in the long run. This research identifies the role of cybersecurity leadership, budgeting, and talent in facilitating ZTA adoption. Moreover, the UK firms can invest in developing their cybersecurity skills and staff competency to extract optimal value from ZTA. Policy makers and organisational leaders also benefit from integrating these results in strategy alignment, sharpening decision-making, and fostering a proactive security climate that facilitates effective handling of threats in the increasingly complex digital landscape.

AUTHOR'S CONTRIBUTION

T.S. has contributed to conceptualization, idea generation, problem statement, methodology, results analysis, results interpretation.

ETHICAL APPROVAL & INFORMED CONSENT

Ethical approval was obtained from the institutional review board. The study was conducted in accordance with the declaration of Helsinki. Participation was voluntary, informed consent was obtained from all participants, and data were anonymized.

AVAILABILITY OF DATA AND MATERIALS

The data will be made available on reasonable request by contacting the corresponding author [T.S.].

FUNDING

None.

CONFLICT OF INTEREST

The author declares no conflicts of interest, financial or otherwise.

ACKNOWLEDGEMENTS

Declared none.

DECLARATION OF AI

During the preparation of this work the author used ChatGPT for editing purposes. After using this tool, the author reviewed and edited the content as needed and take full responsibility for the content of the published article.

APPENDIX A

Survey Questionnaire

Section A: Demographic Information

1) Gender
   a) Male
   b) Female
2) Age
   a) 20 - 29 years
   b) 30 - 39 years
   c) 40 - 49 years
   d) 50 years and above
3) Education Level
   a) Undergraduate
   b) Postgraduate
   c) Other

Section B: Zero Trust Architecture

Rate the following based on the 5-point scale.

1 = Strongly Agree, 2 = Agree, 3 = Neutral, 4 = Disagree, 5 = Strongly Disagree

	1	2	3	4	5
I believe that the implementation of Zero Trust Architecture enhances the security of my organisation's network.					
I feel confident that Zero Trust Architecture can effectively prevent unauthorised access to our sensitive digital assets.					
I think that Zero Trust Architecture has improved the overall cybersecurity posture of my organisation.					

Section C: Modern Enterprise Performance

Rate the following based on the 5-point scale.

1 = Strongly Agree, 2 = Agree, 3 = Neutral, 4 = Disagree, 5 = Strongly Disagree

	1	2	3	4	5
I believe that the adoption of modern cybersecurity measures, like Zero Trust Architecture, has positively impacted the overall performance of my organisation.					
I feel that our organisation's performance has improved in terms of productivity and security since implementing Zero Trust Architecture.					
I think that the overall enterprise performance is significantly enhanced by adopting advanced cybersecurity technologies such as ZTA.					

Section D: Organisational Maturity

Rate the following based on the scale described below.

1 = Strongly Agree, 2 = Agree, 3 = Neutral, 4 = Disagree, 5 = Strongly Disagree

	1	2	3	4	5
I believe my organisation has the necessary resources and infrastructure to effectively implement and scale cybersecurity solutions like ZTA.					
I feel that my organisation’s level of cybersecurity maturity positively impacts its ability to adopt and maintain Zero Trust Architecture					
I think that the maturity of our organisation’s cybersecurity practices makes us more capable of addressing evolving cybersecurity challenges.					

REFERENCES

Ahmad, W., Rasool, A., Javed, A. R., Baker, T., & Jalil, Z. (2021). Cyber security in iot-based cloud computing: A comprehensive survey. *Electronics*, *11*(1), 16. https://doi.org/10.3390/electronics11010016

Ahmadi, S. (2024). Zero trust architecture in cloud networks: Application, challenges and future opportunities. *Journal of Engineering Research and Reports*, *26*(2), 215-228. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4725283v

Aljohani, A. (2023). Zero-trust architecture: Implementing and evaluating security measures in modern enterprise networks. *Shifra*, *2023*, 60-72. https://doi.org/10.70470/SHIFRA/2023/008

Amini, M., & Jahanbakhsh Javid, N. (2023). A multi-perspective framework established on diffusion of innovation (DOI) theory and technology, organization and environment (TOE) framework toward supply chain management system based on cloud computing technology for small and medium enterprises. Organization and Environment (TOE) Framework Toward Supply Chain Management System Based on Cloud Computing Technology for Small and Medium Enterprises (January 2023). *International Journal of Information Technology and Innovation Adoption*, *11*, 1217-1234. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4340207

Awa, H. O., Ojiabo, O. U., & Orokor, L. E. (2017). Integrated technology-organization-environment (TOE) taxonomies for technology adoption. *Journal of Enterprise Information Management*, *30*(6), 893-921. https://doi.org/10.1108/JEIM-03-2016-0079

Bashir, T. (2024). Zero Trust Architecture: Enhancing cybersecurity in enterprise networks. *Journal of Computer Science and Technology Studies*, *6*(4), 54-59. https://doi.org/10.32996/jcsts

Batan, A. (2024). Investigating the Efficacy of Zero-Trust Security Models in Mitigating Insider Threats in Enterprise Environments. *International Journal of Advanced Cybersecurity Systems, Technologies, and Applications*, *8*(12), 10-19. Available from: https://theaffine.com/index.php/IJACSTA/article/view/2

Bhaskaran, D. (2025). Zero Trust Architecture: Securing America's Critical Infrastructure. Available at SSRN 5145800. http://dx.doi.org/10.2139/ssrn.5145800

Brezavšček, A., & Baggia, A. (2025). recent trends in information and cyber security maturity assessment: A systematic literature review. *Systems*, *13*(1), 52. https://doi.org/10.3390/systems13010052

Cheung, G. W., Cooper-Thomas, H. D., Lau, R. S., & Wang, L. C. (2024). Reporting reliability, convergent and discriminant validity with structural equation modeling: A review and best-practice recommendations. *Asia pacific Journal of Management*, *41*(2), 745-783. https://doi.org/10.1007/s10490-023-09871-y

Fernandez, E. B., & Brazhuk, A. (2024). A critical analysis of Zero Trust Architecture (ZTA). *Computer Standards & Interfaces*, *89*, 103832. https://doi.org/10.1016/j.csi.2024.103832

Ghaffari, F., & Arabsorkhi, A. (2018). A new adaptive cyber-security capability maturity model. In *2018 9th International Symposium on Telecommunications (IST)* (pp. 298-304). IEEE. https://doi.org/10.1109/ISTEL.2018.8661018

Government of UK. (2024) Cyber security breaches survey 2024. Official Statistics Cyber security breaches survey 2024 (2024). *GOV.UK*. Available from: https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024

Government of UK. (2023). Cyber security breaches survey 2023. *GOV. UK*, Mar, 30. Available from: https://ciso2ciso.com/wp-content/uploads/2023/11/Cyber-Security-Breaches-Survey-2023.pdf

Hair Jr, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: updated guidelines on which method to use. International *Journal of Multivariate Data Analysis*, *1*(2), 107-123. https://doi.org/10.1504/IJMDA.2017.087624

Hair, J. F., Risher, J. J., Sarstedt, M., & Ringle, C. M. (2019). When to use and how to report the results of PLS-SEM. *European Business Review*, *31*(1), 2-24. https://doi.org/10.1108/EBR-11-2018-0203

Hasan, M. (2024). Enhancing Enterprise Security with Zero Trust Architecture. *arXiv preprint arXiv:2410.18291*. https://doi.org/10.48550/arXiv.2410.18291

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115-135. https://doi.org/10.1007/s11747-014-0403-8

Hoang, H. (2024). Navigating the digital landscape: an exploration of the relationship between technology-organization-environment factors and digital transformation adoption in SMEs. *Sage Open*, *14*(4), 21582440241276198. https://doi.org/10.1177/21582440241276198

Igboko, U. A., & Temitope, O. A. (2025). Securing Public Health in The Digital Age: A Cybersecurity Case Study of Uk Local Council Health Services. http://doi.org/10.37502/IJSMR.2025.8503

Jimmy, F. (2021). Emerging threats: The latest cybersecurity risks and the role of artificial intelligence in enhancing cybersecurity defenses. *Valley International Journal Digital Library*, *1*, 564-74. https://doi.org/10.18535/ijsrm/v9i2.ec01

Khan, K., Khurshid, A., & Cifuentes-Faura, J. (2024). Is artificial intelligence a new battleground for cybersecurity? Science Direct, *Internet of Things*, *28*, 101428. https://doi.org/10.1016/j.iot.2024.101428

Khan, M. J. (2023). Zero trust architecture: Redefining network security paradigms in the digital age. *World Journal of Advanced Research and Reviews*, *19*(3), 105-116. https://doi.org/10.30574/wjarr.2023.19.3.1785

Kotilingala, S. (2025). The non-human identity crisis: Managing machine identities in the modern enterprise. *World Journal of Advanced Research and Reviews*, *26*(1), 944-954. https://doi.org/10.30574/wjarr.2025.26.1.1118

Liyanage, L., Arachchilage, N. A. G., & Russello, G. (2024). SoK: Identifying Limitations and Bridging Gaps of Cybersecurity Capability Maturity Models (CCMMs). *arXiv preprint arXiv:2408.16140*. https://arxiv.org/abs/2408.16140

Malik, S., Chadhar, M., Vatanasakdakul, S., & Chetty, M. (2021). Factors affecting the organizational adoption of blockchain technology: Extending the technology–organization–environment (TOE) framework in the Australian context. *Sustainability*, *13*(16), 9404. https://doi.org/10.3390/su13169404

Mensah, F. (2024). Zero trust architecture: A comprehensive review of principles, implementation strategies, and future directions in enterprise cybersecurity. *International Journal of Academic and Industrial Research Innovations (IJAIRI)*, *10*, 339-346. ISSN: 2454-132X.

Mick, M. M. A. P., Kovaleski, J. L., Mick, R. L., & Chiroli, D. M. D. G. (2024). Developing a sustainable digital transformation roadmap for SMEs: Integrating digital maturity and strategic alignment. *Sustainability*, *16*(20), 8745. https://doi.org/10.3390/su16208745

Mijwil, M., Unogwu, O. J., Filali, Y., Bala, I., & Al-Shahwani, H. (2023). Exploring the top five evolving threats in cybersecurity: An in-depth overview. *Mesopotamian Journal of Cybersecurity*, 57-63. https://doi.org/10.58496/MJCS/2023/010

Nasiruzzaman, M., Ali, M., Salam, I., & Miraz, M. H. (2025). The Evolution of Zero Trust Architecture (ZTA) from Concept to Implementation. In *2025 29th International Conference on Information Technology (IT)* (pp. 1-8). IEEE. https://doi.org/10.1109/IT64745.2025.10930254

Omar, K. O., Zraqou, J., & Gómez, J. M. (2025). From Synthetic Text to Real Threats: Unraveling the Security Risks of Generative AI. In *Examining Cybersecurity Risks Produced by Generative AI* (pp. 1-20). IGI Global Scientific Publishing. https://doi.org/10.4018/979-8-3373-0832-6.ch001

Onwuegbuzie, I. U., & Alabi, O. A. (2025). A Review of Authentication and Authorization Mechanisms in Zero Trust Architecture: Evolution and Efficiency. *Tech-Sphere Journal for Pure and Applied Sciences*, *2*(1). https://doi.org/10.5281/zenodo.15149866

Paya, A., & Gómez, A. (2024). Securesdp: a novel software-defined perimeter implementation for enhanced network security and scalability. *International Journal of Information Security*, *23*(4), 2793-2808. https://doi.org/10.1007/s10207-024-00863-7

Rönkkö, M., & Cho, E. (2022). An updated guideline for assessing discriminant validity. *Organizational Research Methods*, *25*(1), 6-14. https://doi.org/10.1177/1094428120968614

Sholademi, D. B. (2024). Leveraging AI for detecting deep fakes and combating financial fraudulent identity schemes. *International Journal of Research Publication and Reviews*, *5*(12), 4096-4111 December 2024. https://doi.org/10.55248/gengpi.5.1224.250131

Stafford, V. (2020). Zero trust architecture. NIST special publication, 800(207), 800-207. https://doi.org/10.3390/su141811213

Stamford, (2024). Gartner Survey Reveals 63% of Organizations Worldwide Have Implemented a Zero-Trust Strategy. *Gartner*. Available from: https://www.gartner.com/en/newsroom/press-releases/2024-04-22-gartner-survey-reveals-63-percent-of-organizations-worldwide-have-implemented-a-zero-trust-strategy

Sunkara, G. (2025). Implementing zero trust architecture in modern enterprise networks. *SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology*, *17*(03), 1-11. https://doi.org/10.18090/samriddhi.v17i03.01

Syed, N. F., Shah, S. W., Shaghaghi, A., Anwar, A., Baig, Z., & Doss, R. (2022). Zero trust architecture (zta): A comprehensive survey. IEEE Access, 10, 57143-57179. https://doi.org/10.1109/ACCESS.2022.3174679

Yeoh, W., Liu, M., Shore, M., & Jiang, F. (2023). Zero trust cybersecurity: Critical success factors and A maturity assessment framework. *Computers & Security*, *133*, 103412. https://doi.org/10.1016/j.cose.2023.103412

Zammani, M., Razali, R., & Singh, D. (2021). Organisational information security management maturity model. *International Journal of Advanced Computer Science and Applications*, *12*(9). https://doi.org/10.14569/IJACSA.2021.0120974

Cite as: Sarfaraz, T. (2025). Evaluating the effectiveness of zero trust architecture in modern enterprises: Moderating role of organisational maturity. *Advance Journal of Business Management and Social Science*, *1*(2), 1–11, Article ID: CM2512101009. https://doi.org/10.65080/dp4w1990