The Role of Enterprise Architecture in Organisational Adoption of Zero Trust Principles

Matthew Harper-Schmid
University of Melbourne
mharperschmid@gmail.com

Arnab Debashish Nanda
University of Melbourne
mail@arnabnanda.com

Atishay Jain
University of Melbourne
atishay@atishay.co

Aarushi Anand Raichur
University of Melbourne
aarushi2004@gmail.com

Rahil Tushar Shah
University of Melbourne
rahilshah345@gmail.com

Rod Dilnutt
University of Melbourne
rpd@unimelb.edu.au

Abstract

Zero Trust (ZT) is a rapidly evolving and disruptive information security phenomenon allowing companies to develop a sturdy cybersecurity infrastructure addressing the challenges of today's digital age. This paper seeks to explain and understand which factors affect adoption of ZT Principles in organisations, including the role of enterprise applications and architecture. This paper proposes a model which helps to understand how enterprise application environment complexity and different types of enterprise architecture alignment may influence adoption of ZT, both directly and indirectly leveraging the existing Model for the Adoption of Information System Security Innovation in Organisation proposed by Hameed and Arachchilage (2017). This paper provides opportunities for future research to better understand and validate the importance of enterprise applications and architecture as determinants of ZT adoption. This could be done by empirically validating and considering how these characteristics may vary across industries and other organisational contexts.

Keywords: Enterprise Application, Cybersecurity, Enterprise Architecture, Zero Trust, Information Systems Security Innovation, Application Layers, Business-IT Alignment, Information Security, Zero Trust Artefacts, Organisational Adoption

1. Introduction

Zero Trust (ZT) is being rapidly adopted globally as an important IT component within organisations. As of 2023, 61% of organisations have implemented a ZT work program compared to 24% in 2021 (Sarraf, 2023). Most research to date has focused on the advantages ZT provides for companies as well as its technological features. However, there has been limited work done on how organisations implement ZT given that few organisations have successfully implemented it (Buck et al., 2021).

This paper seeks to better understand the role enterprise applications and architecture have in ZT adoption by addressing the following question: *How do Enterprise Applications and Architecture affect adoption of Zero Trust in organisations?*

The paper commences with a literature review which blends both industry-based and academic literature to understand what ZT is and high-level characteristics of enterprise applications and enterprise architecture. Following the literature review, we leverage an existing model first proposed by Hameed & Arachchilage (2017), their Adoption of Information System Security Innovations model. We propose modifications that make it ZT specific and extend the model to recognise the wider role of enterprise applications and architecture in ZT adoption. Finally, the paper will briefly discuss future directions of testing the proposed model and opportunities for further refinement.

2. Literature Review

2.1. Zero Trust

ZT is an information security design philosophy implying nothing can be trusted regardless of its location inside or outside an organisation's network perimeter (Teerakanok et al., 2021). This is an asset-centric security approach that promotes greater organisational flexibility and agility compared to typical, perimeter-based security environments including static rule sets, firewalls, subnetworks, and Virtual Private Networks. These environments, due to their rigid design, usually struggle to efficiently respond to change requirements (Chen et al., 2019; DeCusatis et al., 2016). Changes in contemporary ways of working (such as hybrid working arrangements) where company resources can be legitimately accessed beyond work-issued devices and perimeters have also accelerated the need for alternative security philosophies such as ZT (Tsai et al., 2024).

ZT aims to provide comprehensive resource protection where implicit or inherited trust does not exist and authorisations against resources are continuously validated (National Institute of Standards and Technology, 2020). In its purest form, ZT is a zero-risk tolerance model for resource security and is implemented through strategy, frameworks, policy-driven controls, and micro-segmented security domains (The Open Group, 2023). As ZT is a principles-based philosophy, organisations have the flexibility to implement it through a suite of different controls and governance mechanisms as they see fit, if these mechanisms still adequately meet core principles (The Open Group, 2023). Identity and access management are essential components in ZT but are also supported by broader elements including security zoning of IT resources and assets and security culture awareness (The Open Group, 2023).

ZT's principles are operationalised through the following characteristics:

- ***Least Privilege*** – ZT always assumes compromise and focuses on ensuring users and devices only have minimal required access to perform necessary tasks (The Open Group, 2023). This means if a breach occurs, ZT limits resources accessible by an attacker while allowing systems and people resources to respond and mitigate the breach (Raina, 2023).
- ***Continuous Monitoring*** – trust must be constantly verified to reduce the likelihood of an attack on an asset (also called the threat or attack surface) (The Open Group, 2023). ZT re-evaluates access in real time based on factors including location, device type, and user activity. Every session, device, user, and application must consistently pass security checks and authentication procedures to prove they are authorised to access relevant resources (Durbin, 2022).
- ***Dynamic Access Control*** – ZT allows for access credential adjustments based on evolving needs. Access can be granted or revoked as needed, providing a more granular and adaptable security posture (Teerakanok et al., 2021).

- ***Asset-Centric Security*** – Data, applications and services are recognised as critical resources for protection. Security controls are designed to prioritise protection by sensitivity, regardless of storage location or access method (Buck et al., 2021).

According to Teerakanok et al. (2021), challenges associated with ZT adoption include:

- Vendor lock-in issues that discourage service switching due to factors including proprietary technologies, legal restrictions, or fees to discourage switching,
- Interoperability between applications and hardware to support ZT adoption, Interoperability between applications and hardware to support ZT adoption,
- Handling disparate data formats as there is no common standard,
- User disruptions while implementing ZT changes over IT assets, unmanaged devices, and
- Regulatory laws.

Despite these challenges, there are benefits relating to ZT. Adahman et al. (2022) found that organisations with ZT compared to traditional perimeter-based cybersecurity saved an average of $684,000 in losses caused by a cybersecurity breach. Finally, Chen et al. (2019) identified that ZT can reduce network eavesdropping and scans. As a result, while complex, ZT can offer significant benefits to organisations.

2.2. Enterprise Application Characteristics

Enterprise applications are software solutions designed to streamline organisational operations to increase productivity, efficiency, and collaboration across functions. (Finio & Downie, 2024) Applications serve a range of functions for organisations and are expected to be versatile, agile, and customisable to meet evolving needs (Finio & Downie, 2024). However, while fundamental principles and typical practices exist to tailor applications and optimise performance, they are not generalisable across all applications (Khosla & Saini, 2023). A primary reason is interoperability challenges between hardware and applications due to the volume of configuration options available that may affect systems (Khosla & Saini, 2023).

Applications themselves can also be diverse in what they achieve for an organisation along with their volume and complexity. This creates both direct and indirect costs for an organisation in terms of the underlying cost of application maintenance, integration, and change. (Toomey, 2018). This diversity can be conceptualised through the PACE layers application classification proposed by Gartner (Gartner Research, 2012). These include:

- ***Systems of Record*** - core transactional stable systems handling essential data and processes (e.g., payroll systems) (Toomey, 2018).
- ***Systems of Differentiation*** – systems providing a competitive advantage by supporting unique business processes and functionalities (e.g., Customer Relationship Management (CRM) systems), typically experiencing a moderate rate of change as business needs evolve (Orbus Software, 2024).
- ***Systems of Innovation*** – systems at the forefront of change, supporting experimentation and exploration of new technologies and solutions to address emerging needs (e.g., chatbot integration for customer service). Usually, these are characterised by rapid development cycles and a high-risk tolerance (Orbus Software, 2021).

The volume of applications in an organisation creates additional complexity due to extra applications (and segmentations) needing to be customised to incorporate ZT principles (Zhou et al., 2014). Additionally, as enterprise applications adapt to changing organisational needs, system designers and developers can tend towards more lenient security configurations to enable flexibility and adaptability which enhances security threats if a breach occurs (Goerlich et al., n.d.). This creates an interesting tension with ZT adoption which needs to be robust to meet design principles while still enabling effective response to organisational change requirements.

Given the diversity of size, scale and purposes of enterprise applications, current literature recommends a dynamic approach to governance to ensure applications are not over or under-burdened by governance requirements (Winkler & Brown, 2013). Akbari et al. (2024) found that the fit of governance arrangements to the specific type of application is essential to longevity and successful adoption. This is another factor to be considered in ZT adoption given its design principles cannot be varied but need to fit within a flexible governance structure to ensure an optimised balance of organisational performance and security.

2.3. Enterprise Architecture Characteristics

Enterprise Architecture is the practice of standardising and arranging IT infrastructure to ensure it aligns with and supports organisational strategies and objectives (White, 2022; Shanks et al., 2014). It is a widely accepted practice, particularly in large organisations and used to support strategic transformation, innovation and technology interoperability and can deliver cost savings with effective adoption (Burns et al., 2009). As such, it helps ensure effective business and IT alignment and is being considered more holistically within Enterprise Architecture frameworks and methodologies. In the National Institute of Standards and Technology ZT Architecture publication, it explains what ZT is and possible approaches to adoption but is not explicit about how to incorporate the principles into Enterprise Architecture (National Institute of Standards and Technology, 2020). Additionally, Phiayura & Teerakanok (2023) recommends that ZT is adopted incrementally by identifying candidates for a pilot phase before moving into a wider transition by identifying relevant IT assets and processes. This approach assists Enterprise Architects with the speed and agility of adopting ZT and realising its benefits.

Another example is within The Open Group Architecture Framework (TOGAF®[1]) which contains a Zero Trust Reference Model that presents a framework of models for organisations to address ZT capability requirements (The Open Group, 2023). However, currently, TOGAF does not have its own ZT Reference Architecture with adoption principles. Rather, it broadly recognises the relationship of ZT capabilities and models against the wider organisation and Enterprise Architecture (The Open Group, 2023).

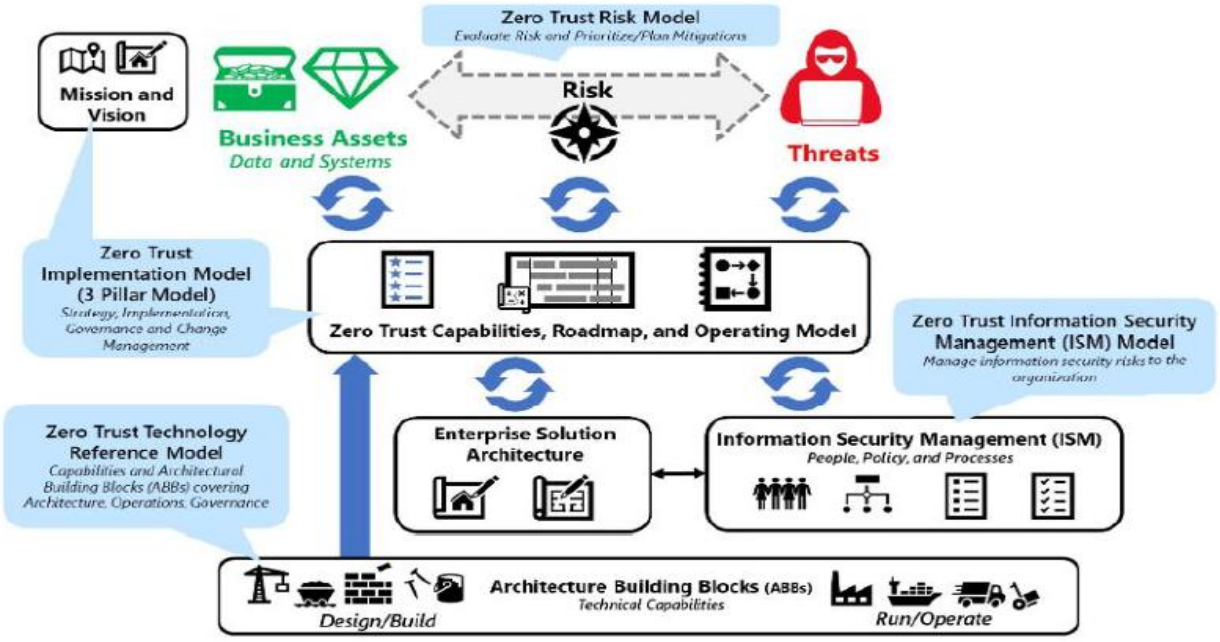

Figure 1 – Zero Trust Model and Relationships for adoption TOGAF (The Open Group, 2023)

Some industry practitioners have started considering how to implement ZT within Enterprise Architecture. The most common method appears to be by incorporating principles into existing artefacts and documents to ensure alignment and minimise friction. (Hiebl, 2023). These include adapting identity and access management principles within Enterprise Architecture to align with ZT principles and incorporating segmentation of applications, data sources and other services to support the principle of minimum access (R, 2023).

[1] TOGAF is a registered trademark of The Open Group.

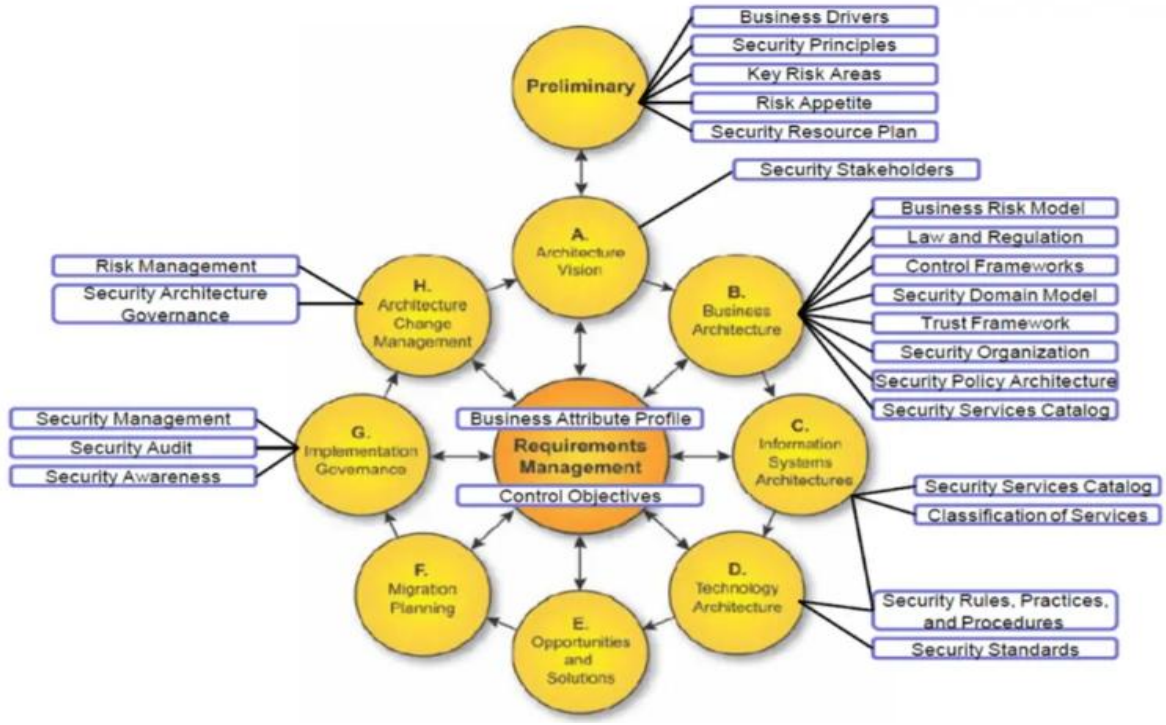

Figure 2 – Sample artefacts of enterprise architecture to incorporate ZT principles within the existing TOGAF Architecture Development Method cycle (Kuiper, 2022)

In exploring the alignment between business and IT, existing literature considers this from multiple perspectives. Chan and Reich (2007) summarised alignment into four key dimensions; strategic and intellectual, structural, social, and cultural dimensions. Baker and Jones (2008) took a further view that to sustain alignment, there are five core types: business, IT, contextual, structural, and strategic alignment. Finally, Magoulas et al. (2012) synthesised these findings and posited four main types of alignment within an organisation:

- ***Structural*** – roles and responsibilities between IT resources and business decision rights.
- ***Functional*** – organisational activities and processes align with IT resources.
- ***Socio-cultural*** – organisational goals, objectives and values align with IT resources; and
- ***Infological*** – expertise and knowledge of organisational stakeholders align with IT resources.

Overall, the literature appears relatively consistent on the importance of alignment and the types of alignment that drive the value of Enterprise Architecture.

3. Proposed Model

3.1. Model Options

Bringing all these elements together requires a model that accounts holistically for connections between ZT, Enterprise Applications and Enterprise Architecture. Existing literature has multiple models that help to conceptualise the impacts of technology on organisations and how they are adopted, including the Diffusion of Innovations, the Technology Acceptance Model, the Theory of Planned Behaviour, and the Technology-Organisation-Environment framework (Rogers, 1983; Davis, 1989; Ajzen, 1991). The Technology Acceptance Model predominantly focuses on user acceptance, focusing on the perceived ease of use and usefulness of a technology (Davis, 1989). The Theory of Planned Behaviour is a psychological theory that posits that human behaviour is based on three conditions; behavioural beliefs on consequences of behaviour, normative beliefs on expectations of others (social pressure) and

control beliefs on the presence of factors that may influence performance (Ajzen, 1991). These combined can also infer insights into user acceptance of innovations (Armitage & Connor, 2001).

Rogers (1983) specifically deals with the characteristics of the technology itself and the factors that influence its adoption by an organisation. Finally, The Technology-Organisation-Environment framework consists of a wider focus on the elements of technology, the organisation, and its operating environment to consider the impact of an innovation more holistically (Tornatzky & Fleischer, 1990).

These theories in isolation may be limited in sufficiently explaining the main reasons for how ZT is adopted in an organisation. Our approach is to adopt a more holistic model which blends these approaches. The model proposed by Hameed and Arachchilage (2017) on characteristics that influence the adoption of Information System (IS) Security Innovation in Organisations (legacy model) provides a strong basis to consider relevant factors to ZT and further refine if necessary.

This model is also designed not only with information technology in mind but also incorporates relevant elements of innovation models to create a holistic model specific to Information System security innovations. It is modular and clear in offering four main characteristic domains that influence innovation adoption: technology, organisation, environment, and user acceptance. The legacy model can be used for ZT as an IS security innovation while also being sufficiently flexible in its design to allow us to include separate criteria for Enterprise Architecture and enterprise applications.

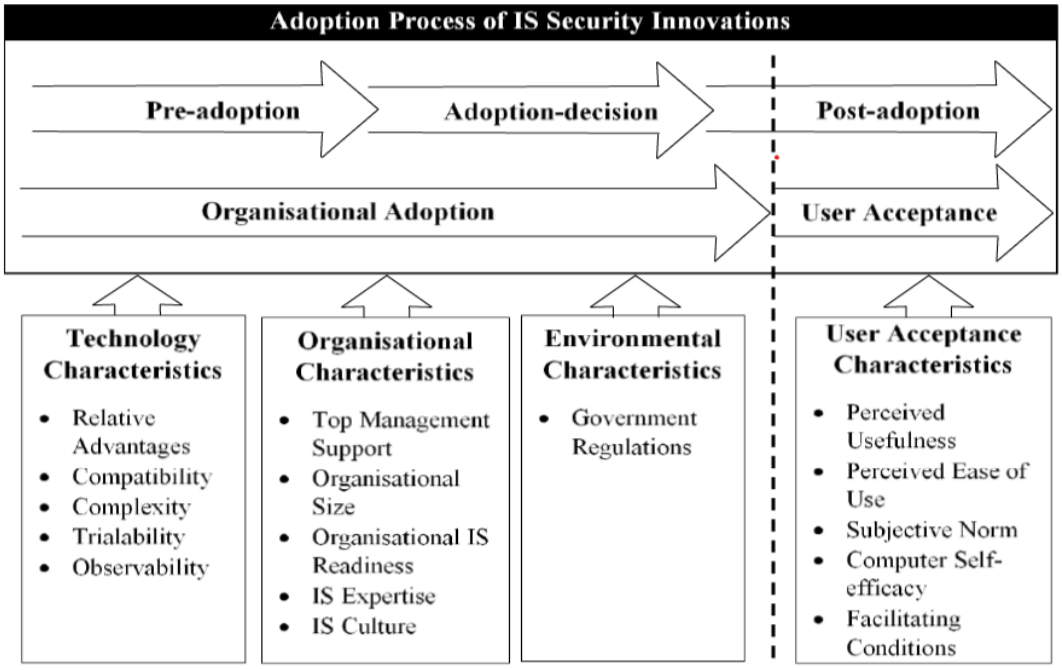

Figure 3 – Model for the Adoption of Information System Security Innovation in Organisations (Hameed and Arachchilage, 2017)

3.2. ZT Technology Characteristics

One of the cornerstones of the model are the five characteristics of an innovation first posited by Rogers (1983); its relative advantage to existing technology, compatibility with existing values and needs of users, perceived complexity of use, how much you can experiment and remove the innovation (trialability) and how visible and observable its results are to others.

All five characteristics are considered relevant to how ZT is adopted within an organisation but are likely to vary between different organisations. For example, the compatibility and relative advantage of ZT in organisations are

expected to differ between organisations depending on factors such as their security culture and relative starting point on the ZT journey. Additionally, its trialability may differ depending on how an organisation decides to adopt ZT by using an incremental model versus a "big bang" approach. As a result, we expect these factors to be relevant to influence adoption, both in terms of the benefits realised and the length of time taken to adopt ZT.

3.3. Environmental, Organisational and User Acceptance Characteristics

The legacy model also introduces a set of organisational and environmental characteristics that influence adoption of IS security innovations.

Environmental characteristics include government regulations which have been previously connected to influencing organisational security adoption (Li, 2015; Hameed & Arachchilage, 2017). We accept this as relevant to ZT, especially given regulations such as the European Union's General Data Protection Regulation which can impose penalties of up to four percent of an organisation's global turnover or 20 million Euros (Intersoft Consulting. (n.d.)). Additionally, the United States Government has mandated Federal Government Agencies to adopt ZT in their operations (The White House, 2021). We expect regulations such as these to incentivise organisations to implement ZT as they seek to minimise the financial loss and reputation damage incurred by these penalties.

Organisational characteristics are also expected to influence ZT adoption. The legacy model proposes that top management support, organisation size, Information System readiness, IS expertise and IS culture are characteristics that influence adoption (Hameed & Arachchilage, 2017). Based on our analysis of ZT, we accept and include these factors as relevant. This is because top management support has been found in previous literature as a critical factor that influences IS adoption (Thong et al., 1996; Hameed & Arachchilage, 2017). Additionally, size enables an organisation to have the finances and resources required to implement innovations such as ZT and fund scope changes/or implementation challenges. (Hameed & Arachchilage, 2017). IS readiness and culture have also been found in previous literature as being positively correlated with IS innovation adoption as it implies knowledge, resources, and governance to implement innovations, which we expect would also apply to ZT (Hameed et al., 2012).

User Acceptance characteristics are also an important element of the model. For simplicity, we propose only perceived ease of use and perceived usefulness are adopted for our model. Perceived ease of use refers to the expected lack of effort needed to utilise a particular IT asset (Hameed & Arachchilage, 2017 2017). This is expected to influence ZT adoption if users perceive ZT as being a significant friction to completing their work, which will make them more likely to complain, explore workarounds and/or reduce their overall productivity. Perceived usefulness is an individual's belief that a particular innovation will enhance work performance (Hameed & Arachchilage, 2017). This is also expected to influence adoption as users will embrace innovations they believe make their work easier or better.

However, subjective norm, computer self-efficacy and facilitating condition present in the legacy model have been removed from our proposed model. Subjective norm refers to the social pressure experienced by an employee to accept an IS innovation (Hameed and Arachchilage, 2017). Computer self-efficacy refers to the self-confidence of an individual to proficiently implement IS behaviours and use tools. Finally, facilitating condition refers to the belief the more services available to the user, the better the probability of the user accepting and trusting the innovation (Hameed and Arachchilage, 2017). We propose these characteristics are largely rendered inert by ZT adoption. This is due to ZT not being a technology which individuals need to engage with by altering their standard use of technology, but only in how they use existing technology. For example, frequency of entering existing passwords. Additionally, factors such as subjective norm and facilitating condition are largely already handled by IS culture. which covers issues such as cybersecurity awareness and policies.

3.4. Enterprise Applications and Architecture Characteristics

Based on our literature review, enterprise applications have complexities that, when considered against how an organisation adopts ZT, can influence its adoption. Specifically, given that ZT is expected to be across all applications, factors including the volume, and characteristics of applications such as vendor lock-in, diversity of applications and volume affect the benefits to be generated, and time taken for adoption. As such, we have amended the legacy model to provide enterprise applications with a separate category given the expected significant impact these factors could have on how complex ZT adoption may be for an organisation.

Similarly for Enterprise Architecture, alignment between IT and business objectives is expected to significantly affect ZT adoption. If architecture is not aligned to business requirements, we expect that creates friction in

implementing any technology, ZT or otherwise. We have selected the alignment model proposed by Magoulas et al. (2012) that specifies the role of EA through structural, functional, socio-cultural and infological alignment. By separating alignment into four separate factors, it provides a better opportunity to diagnose and treat the specific root causes of business and IT alignment issues which increases the probability of a successful ZT adoption and minimises the length of time taken to adopt.

Additionally, the nature of enterprise applications and architecture within an organisation would also influence the five elements of ZT as an innovation. For example, if an organisation has complex applications, it may adversely influence the compatibility of ZT to the organisation but improve its trialability as you have more applications to test it against. As a result, we propose that enterprise applications and architecture can influence organisational adoption directly and indirectly through the ZT characteristics.

3.5. Theoretical ZT Adoption Model

We now combine the aforementioned factors to produce our theoretical ZT adoption model. The key elements changed from the legacy model are the replacement of the adoption process with a simple two-layered approach to defining a successful ZT adoption; the benefits generated, and the length of time taken to adopt. This refines the legacy model to make it more ZT specific while maintaining a set of criteria for assessing the impact of each characteristic proposed.

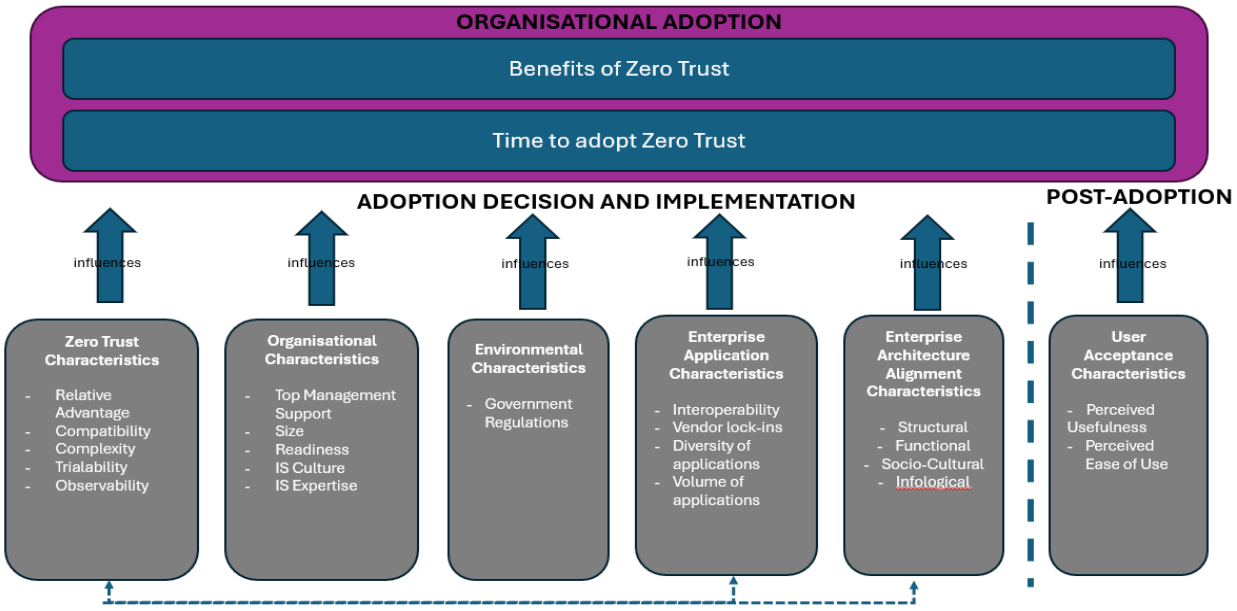

Figure 4 – Proposed model for organisational adoption of ZT based on legacy model.

We expect that the addition of enterprise applications and Enterprise Architecture to the model will both directly and indirectly influence organisational adoption of ZT alongside the other factors proposed in the legacy model.

4. Discussion

We now reflect on the original premise of this paper; ***How do Enterprise Applications and Architecture affect adoption of Zero Trust in organisations?***

In summary, the impact of enterprise applications and architecture is twofold, directly influencing the level of benefit and time taken to adopt ZT while also influencing the complexity of ZT characteristics within a specific organization. Enterprise application characteristics and environment can add complexity to ZT adoption through issues including interoperability challenges, vendor lock-ins, diversity in application purposes and the number of applications

requiring customisation. Similarly, if an Enterprise Architecture does not align strongly with business objectives, it can create friction in implementing ZT. Future research could test the proposed model through either surveys or interviews to confirm whether the proposed characteristics and relationships affect ZT adoption. This includes if all characteristics have similar levels of influence (or weighting) over or across ZT adoption. While we have proposed a singular model, results may vary across different contexts, including organization size, industry, geography, and technology environments.

As previously mentioned, ZT is still an emerging phenomenon in industry and there are no set standards on how to integrate its principles into Enterprise Architecture. The Open Group has stated its intention to develop a ZT Reference Architecture along with the methodology to implement ZT solutions, providing clear frameworks and metrics to assist organisations (The Open Group, 2023). At the time of publication, ZT adoption is still in its infancy, and it would be worth revisiting this theoretical model once global business has a more mature understanding of ZT to re-validate its applicability. Finally, we acknowledge the proposed model has not been empirically tested and validated, meaning it is still only a theoretical model. The proposed model may still be incomplete and is not considered an exhaustive list of factors influencing ZT adoption. This should be carefully considered in any future empirical research design that seeks to validate this theoretical model.

5. Conclusion

As ZT adoption increases globally, it is important to consider how organisations can implement this change effectively and efficiently. This paper provides a possible approach to better understanding the challenges and critical factors that may influence the success of a ZT implementation, particularly the role of Enterprise Architecture and applications. Ideally, the theoretical model in this paper provides an opportunity for organisations to adopt ZT principles more strategically and increase their chance of success while minimising time to adopt. As time progresses, we expect to see greater opportunities for further research and refinement of approaches to ZT adoption, including consistent standards and frameworks to embedded ZT within Enterprise Architecture.

6. References

Adahman, Z., Malik, A. W., & Anwar, Z. (2022) An analysis of zero-trust architecture and its cost-effectiveness for organizational security. *Computers & Security, 122* (November 2022).

Ajzen, I. (1991). The Theory of Planned Behavior. *Organisational Behavior and Human Decision Processes, 50,* 179-211.

Akbari, K., Fürstenau, D., & Winkler, T. J. (2024). Governance and Longevity of Architecturally Embedded Applications. *Journal of Management Information Systems, 41*(1), 266-296. https://doi.org/10.1080/07421222.2023.2301169

Armitage, C. J., & Conner, M. (2001). Efficacy of the Theory of Planned Behaviour a Meta-analysis Review. *British Journal of Social Psychology, 40,* 471-499.

Baker, J., & Jones, D. (2008). A Theoretical Framework for Sustained Strategic Alignment and an Agenda for Research. *Proceedings of JAIS Theory Development Workshop. Working Papers on IS 8*(16).

Buck, C., Olenberger, C., Schweizer, A., Völter, F., & Eymann, T. (2021) Never trust, always verify: A multivocal literature review on current knowledge. and research gaps of zero-trust. *Computers and Security*, 110.

Burns, P., Neutens, M., Newman, D., & Power, T. (2009). *Building value through enterprise architecture – A global study.* PwC. https://www.strategyand.pwc.com/gx/en/insights/archive/building-value-through-enterprise-architecture/strategyand-building-value-through-enterprise-architecture.pdf

Chan, Y.E., & Reich, B. H. (2007). IT alignment: what have we learned? *Journal of Information Technology, 22,* 297-315.

Chen, Y., Hu, H., & Cheng, G. (2019). Design and implementation of a novel enterprise network defense system by maneuvering multi-dimensional network properties. *Frontiers of Information Technology & Electronic Engineering*, *20*(2), 238–252. https://doi.org/10.1631/FITEE.1800516

Davis, F. D. (1989). Perceived Usefulness Perceived Ease of Use Acceptance of Information Technology. *MIS Quarterly, 13*, 319-340.

DeCusatis, C., Liengtiraphan, P., Sager, A., & Pinelli, M. (2016). *Implementing Zero Trust Cloud Networks with Transport Access Control and First Packet Authentication. 2016 IEEE International Conference on Smart Cloud*, 5–10. IEEE. https://doi.org/10.1109/SmartCloud.2016.22

Durbin, S. (2022, June 1). *Council Post: What's Zero Trust, And What's Driving Its Adoption?* Forbes. https://www.forbes.com/sites/forbesbusinesscouncil/2022/06/01/whats-zero-trust-and-whats-driving-its-adoption/?sh=13bdbe781d55

Finio, M., & Downie, A. (2024, January 24). *What are enterprise applications | IBM*. Www.ibm.com. https://www.ibm.com/topics/enterprise-applications

Gartner Research (2012, January 9). *Accelerating Innovation by Adopting a Pace-Layered Application Strategy*. https://www.gartner.com/en/documents/1890915

Goerlich, J. W., Nather, W., & Pham, T. (n.d.) *Zero Trust – Going Beyond the Perimeter.* Cisco Systems. https://www.cisco.com/c/dam/global/en_uk/products/pdfs/zero-trust-going-beyond-the-perimeter.pdf

Hameed, M. A., & Arachchilage, N. A. (2017). A Conceptual Model for the Organisational Adoption of Information System Security Innovations. *Journal of Computer Engineering & Information Technology*, *6*(2).

Hameed, M. A., Counsell, S., & Swift, S. A. (2012). Meta-analysis of Relationships between Organisational Characteristics and IT Innovation Adoption in Organisations. *Information and Management, 49*, 218-232.

Hiebl, S. (2023, August 16). *Zero Trust meets Enterprise Security Architecture: A perfect match.* LinkedIn. https://www.linkedin.com/pulse/zero-trust-meets-enterprise-security-architecture-perfect-hiebl

Intersoft Consulting. (n.d.). *Fines / Penalties*. General Data Protection Regulation (GDPR). https://gdpr-info.eu/issues/fines-penalties/#:~:text=For%20especially%20severe%20violations%2C%20listed

Khosla, C., & Saini, B. S. (2023). Proposed Framework for Performance Tuning in Enterprise Applications using Machine Learning. *Proceedings of the Seventh International Conference on Electronics, Communication an Aerospace Technology*.

Kuiper, R. (2022, September 27). *Security architecture development over 20 years.* Isaca.nl. https://isaca.nl/nieuws/security-architecture-development-over-20-years/

Li, D.C. (2015). Online Security Performances and Information Security Disclosures. *Journal of Computer Information Systems, 55*, 20-28.

Magoulas, T., Hadzic, A., Saarikko, T., & Pessi, K. (2012). Alignment in Enterprise Architecture: A Comparative Analysis of Four Architectural Approaches. *The Electronic Journal of Information Systems Evaluation, 15*(1), 88-101.

National Institute of Standards and Technology. (2020). *NIST Special Publication 800-207 Zero Trust Architecture*. National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf

Orbus Software (2021). *Pace Layering Framework*. (2024, February). LeanIX Enterprise Architecture Management. https://docs-eam.leanix.net/docs/pace-layering

Orbus Software (2024, May 8). *Starting Enterprise Architecture: A Quick-Start Guide*. https://www.orbussoftware.com/docs/default-source/blogs/starting-enterprise-architecture-a-quick-start-guide.pdf?sfvrsn=eb9940fc_0

Phiayura, P., & Teerakanok, S., (2023). A Comprehensive Framework for Migrating to Zero Trust Architecture. *IEEE Access.* 10.1109/ACCESS.2023.3248622.

R., K. (2023, April 4). *Enterprise Architecture and SPD-based Zero Trust*. LinkedIn. https://www.linkedin.com/pulse/enterprise-architecture-spd-based-zero-trust-kris

Raina, K. (2023, April 17). *Zero trust security explained | principles of the zero-trust model*. Crowdstrike.com; CrowdStrike. https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

Rogers, E. M. (1983). *Diffusion of Innovations* (3rd ed.). The Free Press.

Sarraf, S. (2023, October 18). *Most organizations globally have implemented zero trust*. CSO Online. https://www.csoonline.com/article/656108/most-organizations-globally-have-implemented-zero-trust.html

Shanks, G., Gloet, M., Someh, I. A., Frampton, K., & Tamm, T. (2018). Achieving benefits with enterprise architecture. *Journal of Strategic Information Systems, 27*, 139-156.

Teerakanok, S., Uehara, T., & Inomata, A. (2021). *Migrating to Zero Trust Architecture: Reviews and Challenges*. *2021* 1-10. https://doi.org/10.1155/2021/9947347

The Open Group. (2023). *The Open Group Standard Zero Trust Reference Model (Snapshot)*. The Open Group.

The White House (2021, May 12). *Executive Order on Improving the Nation's Cybersecurity.* The White House. https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Thong, J. Y. L., Yap, C., & Raman, K. S. (1996). Top Management Support External Expertise and Information Systems Implementation in Small Businesses. *Information Systems Research*, *7*, 248-267.

Toomey, D. (2018, July 5). *A Pace-Layered Integration Architecture*. Engineering.deloitte.com.au. https://engineering.deloitte.com.au/articles/a-pace-layered-integration-architecture

Tornatzky, L. G., & Fleischer, M. (1990). *The Process of Technological Innovation.* Lexington Books.

Tsai, M., Lee, S., & Shieh, S. W. (2024) *Strategy for Implementing of Zero Trust Architecture*. *IEEE Transactions on Reliability*, *73*(1), 93-100.

White, S. K. (2022, November 23). *What is enterprise architecture? A framework for transformation*. CIO. https://www.cio.com/article/222421/what-is-enterprise-architecture-a-framework-for-transformation.html

Winkler, T. J., & Brown, C. V. (2013). Horizontal allocation of decision rights for on-premises applications and software-as-a-service. *Journal of Management Information Systems*, *30*(3), 13-48.

Zhou, X., Li, F., Dang, Y., Chen, H., Li, S., & Liang, G. (2014). *Collaborative Change Impact Analysis for Enterprise Application Evolution.* https://ieeexplore.ieee.org/document/6960684?arnumber=6960684.