Asia-Pacific Journal of Information Technology and Multimedia 13(02) 2024: 287 – 297
https://doi.org/10.17576/apjitm-2024-1302-09

Adapting Zero Trust: Information Security Cultural Factors Considerations in the UAE Context

Menyesuaikan Zero Trust: Pertimbangan Faktor Budaya Keselamatan Maklumat dalam Konteks UAE

*Bader Zyoud, Syaheerah Lebai Lutfi**

School of Computer Science, Universiti Sains Malaysia, Minden, Penang 11800, Malaysia

**Corresponding author: syaheerah@usm.my*

Received 8 July 2024
Accepted 6 October 2024, Available online 15 October 2024

ABSTRACT

This study explores how cultural factors impact the adoption of Zero Trust Architecture (ZTA) within Middle Eastern culture, focusing on United Arab Emirates (UAE). The zero-trust security model, based on "never trust, always verify," challenges traditional models and is particularly relevant in cultural contexts divergent from Western practices. The study constructs a theoretical model based on common information security culture factors and zero trust adoption in the Arab cultural setting, utilizing data from a survey of 98 cybersecurity experts in the UAE. Using Partial Least Squares Structural Equation Modelling (PLS-SEM), this study tests hypotheses to determine the correlation between information security culture factors and the adoption of Zero Trust Architecture (ZTA). The findings reveal significant correlations between information security culture factors and ZTA adoption, including awareness and training (ATS), policy and procedure (PPS), security behaviour (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 ZTA adoption. However, change management (CMS) lacks a statistically significant correlation with ZTA adoption, indicating that introducing new technology itself is not a hindrance. This study establishes the positive and consistent influence of information security cultural factors on ZTA adoption, highlighting their critical role in achieving a more secure and zero trust network architecture. emphasizing the need for further research to refine conclusions by considering additional factors such as the original nationalities of participants, given the diverse population in the UAE.

Keywords: Zero Trust Models; Information Security Culture; Cybersecurity; Arabic Culture; Security Culture Factors

ABSTRAK

Kajian ini meneroka bagaimana faktor budaya mempengaruhi penerimaan Zero Trust Architecture (ZTA) dalam budaya Timur Tengah, dengan fokus pada Emiriah Arab Bersatu (UAE). Model keselamatan zero-trust, berdasarkan “jangan pernah percaya, selalu verifikasi,” mencabar model tradisional dan sangat relevan dalam konteks budaya yang berbeza dari amalan Barat. Kajian ini membina model teori berdasarkan faktor budaya keselamatan maklumat yang biasa dan penerimaan zero trust dalam setting budaya Arab, menggunakan data dari tinjauan 98 pakar keselamatan siber di UAE. Menggunakan Partial Least Squares Structural Equation Modelling (PLS-SEM), kajian ini menguji hipotesis untuk menentukan korelasi antara faktor budaya keselamatan maklumat dan penerimaan Zero Trust Architecture (ZTA). Penemuan menunjukkan korelasi yang signifikan antara faktor budaya keselamatan maklumat dan penerimaan ZTA, 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 ZTA. Walau bagaimanapun, pengurusan perubahan (CMS) tidak menunjukkan korelasi yang signifikan secara statistik dengan penerimaan ZTA, menunjukkan bahawa pengenalan teknologi baru itu sendiri bukanlah halangan. Kajian ini menegaskan pengaruh positif dan konsisten faktor budaya keselamatan maklumat terhadap penerimaan ZTA, menekankan peranan kritikal mereka dalam mencapai rangkaian keselamatan yang lebih selamat dan zero trust. Kajian ini juga menekankan keperluan untuk penyelidikan lanjut untuk memperhalusi kesimpulan dengan mempertimbangkan faktor tambahan seperti kewarganegaraan asal peserta, memandangkan populasi yang pelbagai di UAE.

Kata kunci**:** Model Zero Trust; Budaya Keselamatan Maklumat; Keselamatan Siber; Budaya Arab; Faktor Budaya Keselamatan

INTRODUCTION

Organizations face heightened vulnerability to cyberattacks owing to evolving work cultures and increased exposure to untrusted network traffic (Georgiadou et al. 2021). This study indicates that recent academic focus is mainly on zero trust architecture, technology, knowledge gaps, and the integration of cloud computing and artificial intelligence. Moreover, it explores the challenges and approaches aligned with the transformation toward a zero-trust model, in organizations. Recognizing the benefits of zero trust in safeguarding security, the conversation also covers migration strategies (Zyoud & Lutfi 2024).

The main purpose of a zero-trust architecture is to protect sensitive information and valuable assets through continuous authorization and authentication (Dimitrakos et al. 2020). In addition, the zero-trust idea allows users and a hybrid workforce to access corporate resources at any time and from any location while maintaining the highest security and compliance standards (Yiliyaer & Kim 2022). To mitigate the impact of risk, insider threats and networks should be considered. The zero-trust principle states, "Never trust; always check"(Greitzer and Purl 2022). As our work environments and world become more digitized, more and more devices will be connected to the Internet, leading to an increase in the number of cyber threats and attacks. To gain access, your request must first be validated [Kindervag, 2010]. The term "zero trust" was originally proposed by (Xiao et al. 2022). The Zero Trust model is a holistic approach to protecting data and resources and does not represent a single product or technology (AlHogail & Mirza 2014). The main obstacle to effective information security today is a lack of trust (Xiao et al. 2022).

Information security culture (ISC) is a critical component of corporate governance, especially in the context of technology adoption. It is defined as the collection of perceptions, attitudes, values, assumptions, and knowledge that determine an organization's approach to protecting information assets and influencing employees' security behaviours (Schneider et al. 2013). Organizational culture (OCS) is a fundamental element of organizational behaviour and management and includes shared values, beliefs, norms, and practices that shape the social and psychological environment of an organization (Conolly et al. 2017). It has a significant impact on how employees think, behave and interact within the organization, which ultimately affects the organization's performance (Connolly et al. 2017). National culture (NCS) is composed of various elements, including symbols, language, norms, values and artefacts [Rita et al. 2022], and reflects an organization's shared values, beliefs and assumptions about how employees should act and make decisions (Akhyari et al. 2018).

RELATED WORK

In a recent study (Zyoud & Lutfi 2024), we explored the relationship between national culture, organizational culture, information security culture and zero trust adoption in the United Arab Emirates. Our findings indicated that national and organizational culture as well as information security culture are significantly and positively correlated with the adoption of the Zero Trust Adoption (ZTA) and highlighted the importance of cultural differences in understanding the zero trust adoption. Building on these insights, the primary objective of this study is to identify which information security cultural factors most significantly influence ZTA adoption in the UAE and analyse the results to provide a more comprehensive understanding of zero trust adoption. By expanding on previous research, we hope to contribute to the ongoing discussion on and provide valuable insights for the UAE organizations.

METHODOLOGY

The methodology employed in this research is elucidated in Figure 1, illustrating the research approach to examine a security model integrating both zero-trust principles and information security cultural factors. Figure 1 illustrates the conceptual relation between Information Security Culture (ISC) factors and Zero Trust adoption (ZTA) , which represents the relation and correlation model visually represents these hypotheses as paths leading from each construct of Awareness and Training (ATS), Policies and Procedures (PPS), Top

Management Support (TMS), Change Management (CMS), Information Security Management System (ISMS), Security Behaviour (SBS), Communication (COMS), and Compliance (CPS) with the Zero Trust adoption (ZT) to understand the significant factors that influence and correlate with this model adoption within UAE organizations culture.

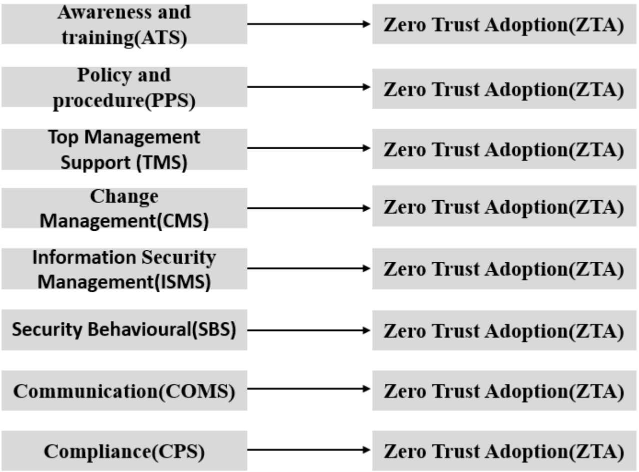
Awareness and training(ATS)
Policy and procedure(PPS)
Top Management Support (TMS)
Change Management(CMS)
Information Security Management(ISMS)
Security Behavioural(SBS)
Communication(COMS)
Compliance(CPS)
Zero Trust Adoption(ZTA)

FIGURE 1. The conceptual relation of ISC factors and ZTA

To gather the required data for this research, a survey was designed by adapting the common information security culture factors which were used by much research to evaluate the information security culture maturity level (Mwim and Mtsweni 2022; Da Veiga 2018; Hassan et al. 2015; Acharya et al. 2013). The sampling technique used in this research was a non-probability sampling method, specifically a convenience sampling approach (Taherdoost et al. 2022). This method allowed to reach out to the target population and collect data based on the availability and willingness of the respondents to participate (Taherdoost et al. 2022). The designed survey was distributed to 130 information security and IT professionals across three sectors in the UAE.

This study utilized a positivist approach and formulated hypotheses based on existing knowledge The survey questionnaire consisted of four primary sections. The first section included three filter questions to identify suitable respondents, such as those working in the UAE education or government sectors, with technical professional experience in IT or cybersecurity, and being affiliated with an IT or cybersecurity vendor. The remaining sections focused on the respondents' demographic information, the dependent variable, and the independent variables. Most of the constructs and indicators were adapted from prior studies. A five-point Likert scale, ranging from "strongly disagree (1)" to "strongly agree (5)," was used for all items except for sections 1 and 5. The carefully crafted survey instrument served as an important data collection tool, which allowed to gather key insights and perceptions in the areas of information security culture and its multiple factors towards zero-trust (ZT) adoption in UAE organizations (Zyoud & Lutfi 2024).

Furthermore, Smart PLS is adept at facilitating both exploratory and confirmatory research. It excels in normal multivariate analysis and proves particularly advantageous in situations involving small sample sizes. The below Table 1 illustrate and outlines various statistical techniques commonly used in this quantitative research, along with their specific purposes and the relevant references. This information was valuable as this study involve the analysis of quantitative data.

TABLE 1. Data processing and analysis tests

Test	Purpose	Threshold	Reference
Mean	Measure of central tendency, provides the average value of a variable	Between 1-5	(Tabachnick et al. 2001)
Median	Measure of central tendency, provides the middle value of a variable	Between 1-5	(Tabachnick et al. 2001)
Standard Deviation	Measure of dispersion, indicates the spread of values around the mean	Between 1-5	(Tabachnick et al. 2001)
Loading	Assesses the strength of the relationship between a latent variable and its indicators in a measurement model	Above 0.5	(Hair et al., 2019)
Cronbach's Alpha	Measure of internal consistency reliability, assesses the reliability of a scale	Above 0.70 to 0.80	(Cronbach, 1951)
Composite Reliability (rho_a)	Measure of internal consistency reliability, assesses the reliability of a scale	Above 0.70	(Dijkstra & Henseler, 2015)
Composite Reliability (rho_c)	Measure of internal consistency reliability, assesses the reliability of a scale	Above 0.70	(Dijkstra & Henseler, 2015)
Average Variance Extracted (AVE)	Measure of convergent validity, assesses the amount of variance in the indicators explained by the latent variable	Above 0.50	(Fornell & Larcker, 1981a)
Model Fit	Assesses the overall fit of the structural equation model to the data	Above 0.95	(Hu & Bentler, 1999)
R Square	Measure of the proportion of variance in the dependent variable explained by the independent variables	Above 0.26	(Cohen, 2013)
f Square	Measure of the effect size of an independent variable on the dependent variable	Above 0.35	(Cohen, 2013)
HTMT	Heterotrait-Monotrait ratio, assesses the discriminant validity between two constructs	Less than 0.9	(Henseler et al., 2015)

RESULTS ANALYSIS AND DISCUSSION

The results and analysis in Table 2 contain a detailed summary in the form of a table listing the measured values for each construct studied. These include values, median, standard deviation, indicator loadings, Cronbach's alpha, composite reliability (rho_a), composite reliability (rho_c), average variance extracted (AVE), model fit, R-squared, f-squared and HTMT ZTA< >ISC. These results provide insight into the measurement properties and correlations within the model.

The indicators of all information security culture factors awareness and training (ATS), policies and procedures (PPS), top management support (TMS), change management (CMS), information security management system (ISMS), security behaviour (SBS), communication (COMS), and compliance (CPS). Awareness and Training (ATS) showed loading values above the threshold 0.50 except ATS1with value 0.396, SBS3(-0.486), SBS5(-0.619).

As shown in the Table 2, all the constructs' values exceeded the threshold of the statistics test which includes Cronbach's alpha, composite reliability (rho_a), composite reliability (rho_c), average variance extracted (AVE), model fit, R-squared, f-squared and HTMT ZTA< >ISC which means that all constructs can be included in the PLS-SEM test for the correlation.

TABLE 2. Descriptive statistics summary (Information Security Culture Factors with Zero Trust Adoption)

Name	Mean	Median	Standard deviation	Indicators loading	Cronbach's Alpha	Composite Reliability	Composite Reliability	Average Variance	Model Fit	R Square	f Square	HTMT ZTA<- >ISC
ATS					0.907	0.972	0.937	0.762	0.041	0.608	1.552	0.788
ATS1	4.561	5.000	0.701	0.396								
ATS2	3.980	4.000	1.195	0.949								
ATS3	3.878	4.000	1.248	0.962								
ATS4	3.867	4.000	1.251	0.947								
ATS5	3.939	4.000	1.211	0.964								
ZTA	3.265	4.000	1.488	1.000								
PPS					0.875	0.945	0.917	0.743	0.058	0.616	1.605	0.812
PPS1	3.959	4.500	1.362	0.960								
PPS2	4.480	5.000	0.811	0.551								
PPS3	3.653	4.000	1.326	0.917								
PPS4	3.786	4.000	1.350	0.951								
ZTA	3.265	4.000	1.488	1.000								
TMS					0.952	0.956	0.966	0.876	0.037	0.664	1.979	0.835
TMS1	3.602	4.000	1.412	0.951								
TMS2	3.684	4.000	1.389	0.971								
TMS3	3.184	4.000	1.587	0.853								
TMS4	3.571	4.000	1.385	0.964								
ZTA	3.265	4.000	1.488	1.000								
CMS					0.758	0.811	0.890	0.801	0.078	0.078	0.020	0.158
CMS1	4.500	5.000	0.674	0.929								
CMS2	4.357	5.000	0.906	0.860								
ZTA	3.265	4.000	1.488	1.000								
ISMS					0.981	0.981	0.986	0.946	0.016	0.600	1.498	0.782
ISMS1	3.694	4.000	1.358	0.973								
ISMS2	3.673	4.000	1.315	0.968								
ISMS3	3.643	4.000	1.380	0.977								
ISMS4	3.694	4.000	1.351	0.973								
ZTA	3.265	4.000	1.488	1.000								

SBS					0.476	0.961	0.779	0.678	0.071	0.644	1.805	0.796
SBS1	3.582	4.000	1.362	0.919								
SBS2	3.765	4.000	1.331	0.942								
SBS3	2.827	2.000	1.457	-0.486								
SBS4	3.755	4.000	1.356	0.922								
SBS5	3.020	3.000	1.317	-0.619								
SBS6	3.837	4.000	1.338	0.932								
ZTA	3.265	4.000	1.488	1.000								
COMS					0.946	0.969	0.960	0.805	0.039	0.669	2.025	0.837
COMS1	3.765	4.000	1.376	0.964								
COMS2	3.684	4.000	1.397	0.967								
COMS3	3.684	4.000	1.389	0.948								
COMS4	4.286	4.000	0.915	0.552								
COMS5	3.755	4.000	1.378	0.967								
COMS6	3.561	4.000	1.400	0.907								
ZTA	3.265	4.000	1.488	1.000								
CPS					0.979	0.980	0.985	0.942	0.015	0.657	1.916	0.819
CPS1	3.735	4.000	1.389	0.975								
CPS2	3.561	4.000	1.333	0.960								
CPS3	3.724	4.000	1.398	0.967								
CPS4	3.673	4.000	1.354	0.980								
ZTA	3.265	4.000	1.488	1.000								

Analysis of the below table revealed relationships between the information security culture factors and the Zero Trust Adoption (ZTA), with all proposed ideas supported by coefficients, t-statistics and p-values. These results validate the structure. They emphasize how these elements are intertwined in the design of ZTA in a setting. Based on the data provided, the factors with the highest correlations and beta values, such as TMS! ZTA, COMS! ZTA, and SBS! ZTA is likely to have the greatest impact on the successful adoption of Zero Trust in the UAE. These factors show strong positive relationships with Zero Trust adoption, as evidenced by their high correlation coefficients and beta values. However, Change Management (CMS) lacks a statistically significant correlation with ZTA adoption. Apparently, introducing new technology itself is not an issue.

TABLE 3. ISC factors and ZTA correlation results

Correlation	β	M	SD	t-statistics	p-values
ATS! ZTA	0.780	0.779	0.051	15.149	<0.05
PPS! ZTA	0.785	0.785	0.052	15.202	<0.05
TMS! ZTA	0.815	0.814	0.048	17.042	<0.05
CMS! ZTA	0.140	0.137	0.138	1.016	P = 0.310
ISMS! ZTA	0.774	0.772	0.056	13.725	<0.05
SBS! ZTA	0.802	0.803	0.042	19.088	<0.05
COMS! ZTA	0.818	0.817	0.044	18.402	<0.05
CPS! ZTA	0.811	0.809	0.049	16.492	<0.05

The results and analysis presented in Table 2 and Table 3 indicate that various information security culture factors are significantly correlated with the adoption of Zero Trust (ZTA) in the United Arab Emirates. These factors include awareness and training (ATS), policies and procedures (PPS), top management support (TMS), change management (CMS), information security management system (ISMS), security behaviour (SBS), communication (COMS), and compliance (CPS).

The highest correlations and path coefficient values are observed for TMS and ZTA, COMS and ZTA and SBS and ZTA, indicating that these factors have the greatest influence on the successful adoption of Zero Trust in the UAE. These factors exhibit strong positive relationships with Zero Trust adoption as evidenced by their high correlation coefficients and path coefficient values.

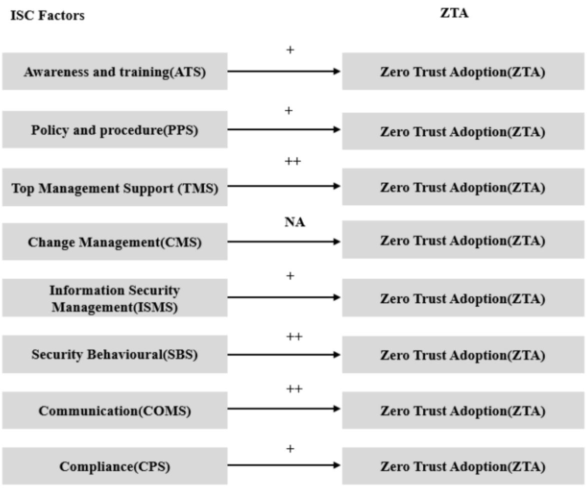

FIGURE 2. The correlation of ISC factors and ZTA

In summary, information security culture factors, particularly top management support, communication and security behaviour, play a critical role in the successful adoption of Zero Trust in the UAE. The adoption of Zero Trust is a necessary response to the evolving threat landscape and changing nature of work and is becoming a standard in cyber security around the world.

CONCLUSION

This study provides a comprehensive overview of the culture of information security and the implementation of the ZT model in the organizations that operate in the United Arab Emirates. In particular, the inclusion of the UAE as a research context adds a special element and underlines the importance of cultural considerations when introducing ZT principles. The implications derived from this study provide crucial insights for UAE organizations, emphasizing the necessity of customized ZT models and comprehensive organizational strategies that consider cultural and contextual variances.

The results, obtained through the Partial Least Squares Structural Equation Modelling (PLS-

SEM), reveal significant findings regarding information security culture and its factors in relation to ZT adoption. The findings highlight significant correlations between information security culture (ISC) factors, with ZTA adoption, particularly top management support, communication and security behaviour, play a critical role in the successful adoption of Zero Trust in the UAE. The research significantly contributes to advancing the development of culturally responsive ZT models, with a particular emphasis on their relevance and applicability in non-English-speaking countries. This innovative approach highlights a detailed understanding of the impact of cultural factors on cybersecurity practices and recognizes the need for a tailored ZT model.

The choice of the United Arab Emirates as the research context brings a unique and distinctive cultural element to the study, rooted in the Arab culture of the Middle East. This choice enriches the study as it provides insights into different behaviours and attitudes toward information security that have not been extensively researched in Western contexts.

The findings of the study go beyond academia and offer practical and valuable recommendations for organizations in the UAE to consider information security culture and its factors (these factors include awareness and training (ATS), policies and procedures (PPS), top management support (TMS), change management (CMS), information security management system (ISMS), security behaviour (SBS), communication (COMS), and compliance (CPS) when adopting ZTA.

ZT model becomes more adaptable and solid when it comes to managing the complexity of the global cybersecurity landscape. By assessing and considering different cultural environments, this study provides recommendations that are not only part of organizations. It’s recommended to be taken also by policy makers as they provide valuable insights to improve information security policies in culturally diverse environments. This study emphasizes the importance of integrating cultural sensitivity into the ZT model to increase its efficiency and flexibility.

In summary, this study concludes with recommendations for future research, which are suggesting the development of a culture-specific ZT security model for UAE organizations and further exploring the intersection of information security culture and ZT. The implications of the research emphasize the global applicability of ZT models, the impact of information security cultural factors, and practical recommendations for organizations to improve their information security policies in the ever-evolving landscape of cybersecurity.

ACKNOWLEDGEMENT

We thank Universiti Sains Malaysia for the partial funding of this research.

REFERENCES

Zyoud, B. & Lutfi, S.L. 2024. “The Role of Information Security Culture in Zero Trust Adoption: Insights from UAE Organizations.” *IEEE Access*: 72420–72444.

Georgiadou, A., Mouzakitis, S. & Askounis, D. 2021. "Designing a Cyber-Security Culture Assessment Survey Targeting Critical Infrastructures During COVID-19 Crisis." *arXiv preprint arXiv*:2102.03000.

Dimitrakos, T., Dilshener, T., Kravtsov, A., La Marra, A., Martinelli, F., Rizos, A., Rosetti, A., & Saracino, A. 2020. "Trust Aware Continuous Authorization for Zero Trust in Consumer Internet of Things." *In 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 1801–1812.

Yiliyaer, S., & Kim, Y. 2022. "Secure Access Service Edge: A Zero Trust Based Framework for Accessing Data Securely." In 2022 *IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, 0586–0591.

Greitzer, F.L., & Purl, J. 2022. "The Dynamic Nature of Insider Threat Indicators." *SN Computer Science* 3(2): 102.

Kindervag, J. 2010. "Build Security into Your Network's DNA: The Zero Trust Network Architecture." *Forrester Research Inc*. 27: 1–16.

Xiao, S., Ye, Y., Kanwal, N., Newe, T. & Lee. B. 2022. "SoK: Context and Risk Aware Access Control for Zero Trust Systems." *Security and Communication Networks* 2022(1): 7026779.

AlHogail, A., & Mirza. A. 2014. "Information Security Culture: A Definition and a Literature Review." *In 2014 World Congress on Computer Applications and Information Systems (WCCAIS)*, 1–7. IEEE.

Schneider, B., Ehrhart, M.G. & Macey, W.H. 2013. "Organizational Climate and Culture." *Annual Review of Psychology* 64(1): 361–388.

Connolly, S. R., Keith, S.A., Colwell, R.K. & Rahbek, C. 2017. "Process, Mechanism, and Modeling in Macroecology." *Trends in Ecology & Evolution* 32(11): 835–844.

Rita, A., Camarero, J.J., Colangelo, M., de Andrés, E.G., & Pompa-García. M. 2022. "Wood Anatomical Traits Respond to Climate but More Individualistically as Compared to Radial Growth: Analyze Trees, Not Means." *Forests* 13(6): 956.

Akhyari, N, Ruzaini, A. A. & Rashid. A. H. 2018. "Information Security Culture Guidelines to Improve Employee's Security Behavior: A Review of Empirical Studies." *Journal of Fundamental and Applied Sciences* 10(2S): 258-283.

Mwim, E.N., & Mtsweni, J. 2022. "Systematic Review of Factors that Influence the Cybersecurity Culture." *In International Symposium on Human Aspects of Information Security and Assurance*, Cham: Springer International Publishing. 147–172.

Da Veiga, A. 2018. "An Approach to Information Security Culture Change Combining ADKAR and the ISCA Questionnaire to Aid Transition to the Desired Culture." *Information & Computer Security* 26(5): 584–612.

Hassan, N.H., Ismail, Z. & Maarop. N. 2015. "Information Security Culture: A Systematic Literature Review." *Proceedings of the 5th International Conference on Computing and Informatics*, Istanbul: ICOCI 2015: 456–463.

Acharya, A.S., Prakash, A., Saxena, P. & Nigam, A. 2013. "Sampling: Why and How of It." *Indian Journal of Medical Specialties* 4(2): 330–333.

Taherdoost, H., Sahibuddin, S. & Jalaliyoon, N. 2022. "Exploratory Factor Analysis: Concepts and Theory." *Advances in Applied and Pure Mathematics* 27: 375–382.

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.

Cronbach, L.J. 1951. “Coefficient Alpha and the Internal Structure of Tests.” *Psychometrika 16(3): 297–334.*

Dijkstra, T.K. & Henseler, J. 2015. “Consistent Partial Least Squares Path Modeling*.” MIS Quarterly* 39(2): 297–316.

Fornell, C., & Larcker, D.F. 1981. “Structural Equation Models with Unobservable Variables and Measurement Error: Algebra and Statistics.” *Journal Storage*: 382–388.

Cohen, J. 2013. Statistical Power Analysis for the Behavioral Sciences. Routledge.

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: 115–135.

Tabachnick, B., & Fidell, L. 2001. Using Multivariate Statistics 4th Edition, Allyn and Bacon, Boston.

Hu, L.-t., & Bentler, P.M. 1999. "Cutoff Criteria for Fit Indexes in Covariance Structure Analysis: Conventional Criteria Versus New Alternatives." *Structural Equation Modeling: A Multidisciplinary Journal* 6(1): 1–55.