Quantitative Analysis of Factors Impacting Organizational Readiness for Cyber security Threats: Relationships and Inter-relationships Assessment

Javad Abed
Johns Hopkins University
Javad.abed@jhu.edu

Saisha Das
Northwest College
saisha.das07@gmail.com

Abstract

This study investigates cyber security readiness in the work-from-home model by examining organizational and individual readiness for change. Novel constructs called "Organizational Security Valence" and "Individual Security Valence" are proposed to assess employees' dedication to security measures. Through empirical examination with 203 security professionals, the study highlights the importance of organizational and individual readiness for change in shaping cyber security readiness in remote work settings.

Introduction

The process of work-from-home, which was driven by the COVID-19 pandemic, has brought great threats to companies' cyber security. Because of the remote workforce, employees now have access to sensitive data from their homes, which has led to an alarming growth in cyber threats. Therefore, as a direct consequence, cyber security readiness in the work-from-home model has turned out to be a very important issue that organizations across the globe have to deal with.

Cyber security readiness is an umbrella term that implies organizational and individual training in the area of detecting, preventing, and responding to cyber threats. But, the remote work environment presents some new challenges to the conventional cyber security practices. Factors like network vulnerabilities, the growing dependency on personal devices, and the likelihood of security protocols being bypassed should be reexamined in the context of organizational cyber security strategies.

In the given context, organization readiness for change is the key factor that can be used to predict the level of cyber security readiness. Organizational readiness that is grounded on change management theories focuses on the state of the members of the organization as to the willingness and capability to embrace and accept the changes being introduced. Through the establishment of a change-ready culture, organizations can efficiently deal with the complexities of remote work environments and also reduce cyber security risks.

Indeed, individual readiness for change is a key determinant of how cyber security readiness is built within organizations. The way employees feel about security procedures, how they perceive them, and how they behave towards them has an effect on the entire security culture of the organization. Therefore, by recognizing and acting upon the personal components of cognitive readiness, resource readiness, and cultural readiness, cyber security readiness in telework environments can be improved.

In consideration of these points, the purpose of this research is to determine the connection between organizational and individual change readiness and cyber security readiness in the work-from-home model. The study develops new constructs-Organizational Security Valence and Individual Security Valence to determine the extent to which employees are in support of security measures and their interest in implementing security protocols. This research will quantitatively investigate these interlinkages using a survey of 203 security professionals, an approach that will provide valuable insights on improving cyber security readiness in the dynamic remote work environment.

Theoretical background

To examine the cyber security Readiness in a work-from-home model, including organizational and individual level variables, we shall benefit from the various theories and studies including the organizational change theory and motivation theory.

Organizational readiness for change

Organizational readiness for change is a crucial factor that determines the outcome of changes implemented in organizations. Weiner, 2009, emphasizes the importance of organizational members' readiness and willingness to embrace change as a key component of organizational readiness for change. This theory implies that high organizational readiness leads to high employees' engagement and support for change (Shea et al., 2014). The idea of organizational readiness for change has already been examined by many researchers in the fields of healthcare, psychology, and business management (Weiner et al., 2008).

Research has clearly shown that factors including leadership behavior, organizational commitment, and perceived organizational support play key roles in organizational readiness for change (Cunningham et al., 2002; Mathur et al., 2023; Deng et al., 2023). Besides, organizational aspects such as climate, leadership practices, and employee relationships are among the factors that determine the organizational readiness for change according to the studies of (Abbasi, 2017; Alolabi et al., 2021; Vaishnavi et al., 2019; Arnéguy et al., 2020). Consequently, the staff's positive mindset, which includes benefits perceived and consistency with the organizational values, is a strong indicator of their commitment to embracing change (Thomas & Dannapfel, 2022).

Moreover, the significance of vision in the organizational readiness for change and growth has also been emphasized which is essential for the organization to change as this vision is the main driving force (Otto et al., 2022; Haque et al., 2016). Research has also been done on transformational leadership, organizational communication, and employee participation which have been shown to be important factors for readiness for change (M et al., 2021; Hannon et al., 2016). Moreover, the research examines organizational readiness in several contexts, e.g. healthcare organizations and libraries, applying theoretical frameworks like the theory of organizational readiness for Change (Qomariyah et al., 2020; Listyawati, 2020). Organizational readiness for change is a multifaceted dynamic that is affected by various individual, organizational and contextual elements. The key elements of the steps for organizational change initiatives are the awareness and the evaluation of the readiness. Considering aspects like leadership, organizational culture, and employees' views can assist in bettering an organization's readiness for change and increasing the chances of successful change implementation.

Organizational vs individual readiness for change

Individual change readiness and organizational change readiness are two concepts that are separate but linked, and their effectiveness in the success of change initiatives in the organizations is crucial. The readiness of the individual to change represents the ability and the openness of individual employees to accept and adjust to change within the organization. While organizational readiness for change refers to the overall spirit and competence of the organization to undergo and manage change, the individual readiness for change refers to the individual employee's acceptance and capability to adapt to the change (Weiner, 2020).

The individual readiness for change is a vital factor for the organizational change as it is one of the components of the organizational readiness. (Haque et al. 2016) Research is conducted on multiple aspects that determine an individual's readiness for change, including the organizational support, the self-efficacy, and mindfulness (Anggraeni & Febrianti, 2022). The determination of these factors is an essential aspect in the formation of individual views and behaviors toward change initiatives. Furthermore, the study has focused on the role of internal context factors in the individual readiness to change and has emphasized that a supportive environment is a key factor in raising the individual readiness to change.

The other side of the coin is the organizational readiness for change which is affected by issues such as leadership culture, organizational commitment, and communication (Shea et al., 2014). Shared commitment and confidence of the organization are the key internal factors that motivate the organization to accept the change. The individual readiness for change is the skill of the employee which consists of his/her attitudes and behaviors, but the organizational readiness for change is the ability of the organization to accept the collective readiness and capability of the organization. Individuals and organizations are intertwined and both are needed to be prepared for the successful implementation of change programs within organizations.

Organizational vs individual valence

Organizational valence relates to the general positive or negative organizational orientation towards change initiatives, while individual valence deals with the personal positive or negative attitudes and perceptions of the individuals in the organization.

The theory of organizational readiness for change proposes that the level of commitment to change is closely correlated with the valence of the change, which means that the overall orientation of the organization towards change that is either positive or negative has a huge influence on the level of commitment of organizational members to embrace and implement change initiatives (Weiner, 2020). This spotlights the organizational valence as the key factor in defining the organizations' readiness and capacity to adopt change.

On the one hand, individual valence is affected by many factors like stress reactivity, emotional ambiguity, and personal needs. Research has demonstrated that stress reactivity can be a factor in the decision-making processes of individuals, which is especially true in ambiguous situations (Brown et al., 2002). Additionally, individual valence can be influenced by factors such as self-disclosure, emotional arousal, and personal biases, which impact how individuals perceive and respond to change initiatives within the organization (Islam et al., 2021).

Organizational valence is crucial in setting the tone and direction for change initiatives within the organization, as it reflects the overall attitude and orientation of the organization towards change. Positive organizational valence can foster a supportive environment for change, while negative valence may lead to resistance and challenges in implementing change initiatives (Oreg et al., 2024). On the other hand, individual valence reflects the personal attitudes and perceptions of employees toward change, which can impact their engagement and commitment to change initiatives (Liu, 2023).

Cyber security readiness in work-from-home model

To analyze the connection between organizational readiness for change and cyber security readiness in terms of work-from-home, we can use the relevant literature on organizational readiness for change, cyber security readiness, and remote work practices. Studies by Kirrane et al. (2016) and Mumtaz et al. (2023) showed that management support, human relations climate, and organizational support played vital role in determining the readiness to change. These components also play a significant role in creating the culture of cyber security readiness in organizations.

The cyber security readiness is the key thing for the organizations, especially in the remote work context, where employees may be more exposed to cyber threats. The research by Berlilana et al. (2021) and other cyber security readiness models underline the fact that the adoption of technological readiness and organizational security plays a key role in strengthening the cyber security readiness. The pandemic of COVID-19 that made us work remotely, as it was emphasized by (Caldeira et al., 2022), highlighted the fact that cyber security readiness is another important tool in the process of providing a secure remote work environment.

Organizational readiness for change and cyber security readiness are now more important than ever considering the context of telecommuting arrangements. Companies should provide for the fact that their employees are ready for organizational changes and also equipped with the cyber security knowledge and tools that will help them to respond to the risks which may come with remote work. The role of leadership, organizational culture, and change management, as emphasized by Engida et al. (2022), is critical in the development of both organizational and cyber security readiness.

Utilizing the Technology-Organization-Environment (TOE) framework, the Hasan et al. (2021) investigate the technological, organizational, and environmental factors affecting cybersecurity readiness and their subsequent impact on organizational performance. The findings underscore the importance of adopting a holistic approach to cybersecurity readiness and provide insights for future research to fortify organizations against cyber threats effectively.

Through combining the knowledge from studies on organizational change readiness, cyber security readiness, and remote working practices, organizations can develop a comprehensive set of strategies to address both organizational change readiness and cyber security readiness in the changing work environment.

Research model and hypothesis

Organizational Security Valence

Wang et al. (2023) addressed the Organizational valence as the perceived benefits of the change, its appropriateness, and its legitimacy in addressing the disparity between the organization's current and desired states. They insist on the need for a clear vision and effective communication tactics which is used to communicate the message to organizational members. This concept is similar to the idea of what is socially acceptable.

As far as Weiner (2020) is concerned, there is a broad gap between the theoretical development of individual readiness for change and organizational readiness for change. Ellis and his team (2023), and Engida and his team (2022) emphasize the importance of leadership style and organizational culture in shaping employees' attitudes toward change. Olafsen et al. (2020) focus on the role of organizational culture and individual readiness in the development of sustainable communities by the implementation of change.

Also, the readiness for change is multidimensional, as Chisare et al (2021) and Masruroh et al (2022) stated, with factors like suitability, management support, self-efficacy, and personal valence being the key aspects of it. Otto et al. (2022) and Treuer et al. (2020) emphasize the role of organizational commitment, resources, and management support in implementing a change readiness program.

Organizational readiness for change is a complicated notion that involves the culture, the leadership, the employees' perceptions, and the various dimensions of the change readiness. The identification and resolution of such factors are of great importance as a basis for the creation of an environment in which the change is positively perceived.

We are building on the idea of organizational valence by introducing a new construct known as "Organizational security valence." This construct is meant to evaluate workers' willingness to follow security measures and their likelihood of actively participating in the implementation of security protocols that are aimed at protecting organizations. Accordingly, we developed the following hypotheses: Accordingly, we developed the following hypotheses:

H1: Enhanced cultural readiness correlates with improved organizational security valence.

H2: Higher partnership readiness leads to higher organizational security valence.

H3: As resource readiness increases, so does their organizational security valence

H4: Higher IT readiness corresponds to greater organizational security valence.

H5: Strategic readiness is positively related to organizational security valence.

Individual Security Valence

It was found by Weiner (2009) that the organizational members' commitment to change is heavily dependent on their perception of the change's value. The people who value the change as important, impactful, beneficial or significant are likely to be dedicated to its implementation. This idea of change valence captures all the elements that were previously explored by authorities on change management and researchers (Holt et al., 2007). Plans of change within an organization may be appreciated by its members because of the sense of urgency to accomplish the goal.

To understand the mechanisms of resource readiness, cultural readiness, and cognitive readiness in the formation of individual security valence, it is necessary to study the interaction of these factors that lead to the shaping of individual perceptions and reactions to security measures.

Resource readiness refers to the presence of the resources that are needed to back up and apply security measures. Studies have shown that resource availability is positively correlated with action efficacy, therefore people are more likely to perceive changes as positive, if they have access to all of the required resources Noor et al. (2022). Yet, the association between resource adequacy and the change commitment could be seen as negligible, which helps in understanding the complex role of resources in the change adoption process (Ghani et al., 2019).

Cultural readiness is about the degree of the fit of organizational culture with security practices and the way culture influences individuals' perception of security measures. Cultural support is emphasized as a major factor in making an organization cyber-ready as organizations with strong cultural support are better capable of answering cyber threats (Berlilana et al., 2021). Moreover, the insights into culturally significant aspects can provide very important clues on how the cultural factors impact individuals' readiness for change, including security-related changes (Dev et al., 2021).

The cognitive readiness that is aimed at building individual mental fitness and readiness for the security measures is a vital factor in shaping people's minds. Emotional readiness is also a factor in cognitive readiness as it draws attention to the close relationship between cognitive and affective factors that affect the way people respond to security changes (Matthysen & Harris, 2018). Also, cognitive evaluations of the benefits and implications of security modifications have a substantial effect on the public's attitude towards security measures, which, in turn, determines their readiness to accept and adapt to security measures.

Organizations can improve individual security valence through the integration of resource readiness, cultural readiness, and cognitive readiness. This involves ensuring that individuals have access to the resources they need, creating an organizational culture that values security, and promoting cognitive readiness and understanding of the measures that enhance security. This all-encompassing approach can help organizations to foster a climate of trust, improve positive communication, and deal with human resource problems arising from the changes in security conditions (Vakola, 2014). Therefore, we developed the following hypotheses:

H6: Enhanced cultural readiness correlates with improved individual security valence.

H7: As resource readiness increases, so does the individual security valence

H8: cognitive readiness is positively related to individual security valence.

Figure 1 shows the conceptual model for this research.

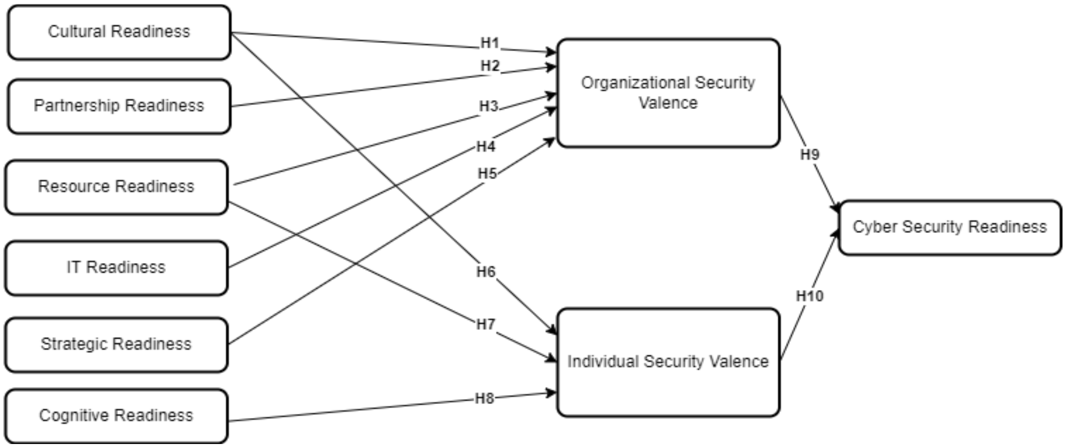


Figure 1. Conceptual Model

Cyber security readiness

Jayaro et al. (2024) talk about the concept of "security valence" and its application in a work-from-home situation where organizational readiness for information security threats is discussed. The paper defines the "security valence" concept as a measure of employees' readiness to carry out organizational readiness and their connection to organizational security policies. It is suggested as an immediate measure for the employee to follow the organization's security policy. The security valence concept is based on change valence and is adjusted to the security context, where employees' commitment to security processes and policies is highlighted as vital to protect the organizations. In this study, we analyze the security valence from both the individual and organizational standpoint. Thus, we proposed the following hypotheses:

H9: Organizational security valence is positively related to cyber security readiness.

H 10: Individual security valence is positively related to cyber security readiness.

Methodology

This paper aims to explore cyber security readiness in a work-from-home environment at the organizational and individual levels as well. The study has employed a quantitative approach to measure the level of the organization's readiness to manage possible security threats. The relationship between the model components was studied, and the model hypotheses were tested empirically. An online questionnaire was created in order to test the proposed hypotheses using a quantitative method.

Measures

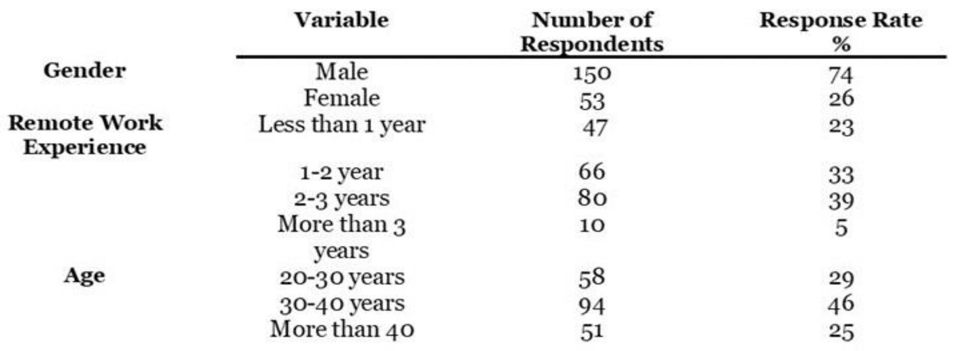
The survey items were designed after a thorough analysis of the information from the literature review. In order to supply a high level of reliability and validity of the items, the study applied existing construct items from previous studies when the situation allowed. Furthermore, new items were created that were based on the definition of the model constructs and also obtained from the consultations with the three information security experts. The details of the constructs are also given, including the number of items and their sources, in Table 2. Participants were asked to rate each construct item on the Likert scale (5-point) which ranged from 'strongly disagree' (1) to 'strongly agree' (5). Demographic information such as respondents and their organizations was also gathered.

The quality of the survey was ensured by conducting a pilot study with 15 cyber security experts who were then used to pre-test the survey items before the actual data collection phase. In the pilot studies the input of different views on the subject is taken into account and the possible problems that might occur in the data collection process are addressed. The pilot study revealed that some of the construct items needed to be adjusted to make them eligible to be part of the final survey.

Sample and data collection

The last survey was sent to a randomly selected number of 360 security experts from different organizations in the US. This sample group was chosen since they were perceived as the most knowledgeable people in their respective organizations regarding information security. The survey was sent as a soft copy. The copies were created using MS Forms and distributed through invitations which consisted of a link to the form within the LinkedIn messages or emails.

Table 1. Sample Information



	Variable	Number of Respondents	Response Rate %
Gender	Male	150	74
	Female	53	26
Remote Work Experience	Less than 1 year	47	23
	1-2 year	66	33
	2-3 years	80	39
	More than 3 years	10	5
Age	20-30 years	58	29
	30-40 years	94	46
	More than 40	51	25

A total of 213 responses were received, which is 59% of the overall response rate. As Gefen et. al (2011) suggest, the sample size of 200 participants is applicable for the moderately complex models in management information systems research. This being the case, a sample size of over 200 was considered adequate, and the final sample size was 203 responses that passed the outlier removal criteria after removing 10 outliers. Out of the 213 participants, 150 were male, and 63 were female. The participants were of varied age groups, among which the age group 30-40 years was the largest. The respondents came from different organizations that had diverse characteristics in terms of age, domain, size (based on the number of employees and annual revenues), and security tools. In Table 1 we see the sample information.

Data analysis and results

Partial least squares (PLS) modeling was implemented in the paper to work on both the measurement and structural models using SmartPLS version 4.1.0 (Ringle et al., 2024). Since the PLS model does not need to make the normal distribution assumptions, the survey data can be used even with a small sample size (Chin et al., 2003). To assess the measurement model and the structural model, Anderson and Gerbing's two-step process was used, as explained in 1981.

Measurement analysis

The study provided the evidence for the convergent and discriminant validity of the measurement items and constructs. The composite reliability was used for determining the reliability of the constructs as the values more than 0.7 are advised to be satisfactory (Hair et al., 2017). Convergent validity was evaluated to measure the extent to which the items reflected the conceptualization of the construct, as indicated by item loadings and AVE. All the constructs had acceptable convergent validity with all item loadings > 0.7 and AVE > 0.5.

The discriminant validity was conducted by the heterotrait-monotrait (HTMT) ratio of the correlations, which is the measure of the extent these constructs differ from and correspond to each other. Values above 0.85 (Kline, 2011) indicate the possibility of violating discriminant validity, while the lower values show that the discriminant validity is acceptable. All values were lower than 0.85 (Kline, 2011). This is an indicator of the validity of the constructs and of the validity and reliability of the measurement items. This also serves as the basis in testing the assumptions as stated in this study.

Structural model analysis

The structural model was evaluated using R2 values, path coefficients, and the corresponding t-values. The study was done to know if the five factors could predict OSV and the three factors could predict ISV. Furthermore, the effect of OSV (Own-Ship Voyage) and ISV (Industry-Ship Voyage) on the cyber security readiness (CSR) was assessed. The OSV, ISV, and CSR R2 values were 0.492 (Q2 = 0.413), 0.405 (Q2 = 0.283), and 0.630 (Q2 = 0.441) respectively. A positive sign of Q2 indicates good predictive relevance, while R2 values from 40.5%(ISP) to 63% (CSR) indicate good in-sample prediction accuracy (Fornell et al., 1994).

The study shows that paths from cultural readiness, partnership readiness, resource readiness, IT readiness, and strategic readiness to OSV are significant, with beta coefficients of 0.344 ($p < 0.01$), 0.298 ($p < 0.01$), 0.671 ($p < 0.05$), 0.641 (p < Moreover, the process from culture readiness, resource readiness, and cognitive readiness to ISV were also significant with beta coefficients of 0.108 ($p < 0.01$), 0.691 ($p < 0.01$), and 0.244 ($p < 0.05$), respectively.

The work showed that OSV was positively correlated with CSR (beta = 0.674, $p < 0.01$), and ISV was also positively correlated with CSR (beta = 0.324, $p < 0.01$). Thus, the study verified all the suggested hypotheses.

Discussion

The results of the study are especially important in cyber security research and organizational change management practice, especially in a remote work setting. The research is aimed at the investigation of the nature of interconnections between organizational and individual readiness for change and cyber security readiness which in turn contributes to the development of a more comprehensive understanding of the multifaceted nature of cyber security readiness in the modern workplace.

The paper is an addition to the existing knowledge base by introducing and testing two new constructs—Organizational Security Valence and Individual Security Valence—which are used to evaluate employees' commitment to security rules in remote work settings. Researchers in cyber security and organizational change management can build on the established theory to find out the interplay between organizational and individual factors that lead to cyber security readiness.

Also, the study stresses the point that the organizational as well as individual level of analysis should be considered while examining cyber security readiness. Future research can be done to identify the exact mechanisms that enable organizational culture, leadership behavior, and individual attitudes to impact cyber security readiness. Furthermore, longitudinal studies could generate information about how cyber security readiness evolves over time in response to organizational developments and external threats.

Furthermore, the researchers can investigate the adaptability of the suggested concepts and the research model among the various industries and organizational settings. Through the exploration of cyber security readiness contrasts between distinct organizations, researchers are able to determine best practices as well as targeted interventions that can help improve cyber security readiness in particular situations.

This study provides valuable practical suggestions for managers, especially cyber security experts and organizational leaders, to enhance cyber security readiness in remote work areas. Through this understanding of the necessity of organizational readiness for change, practitioners will be able to prioritize such initiatives which will be geared towards the creation of a culture of cyber security awareness and resilience within their organizations.

Organizational leaders can use the insights drawn from this study to develop tailored programs that are aimed at the organizational and individual factors that affect cyber security readiness. Initiatives like training programs, awareness campaigns, and communication strategies will increase employees' knowledge about cyber security threats and help them take part in security measures on a voluntary basis.

In addition, security professionals can use the proposed constructs of Organizational Security Valence and Individual Security Valence as diagnostic tools to audit the efficiency of their cyber security initiatives. By continuously checking employees' compliance with the security measures, the organizations can spot and correct the areas where their cyber security strategies need to be improved.

Moreover, experts can benefit from the empirical model and hypotheses that are presented in this study to inform the decision-making process of cyber security interventions. Through coordination of their initiatives in the areas of organizational and individual readiness for change, organizations can increase their cyber security effectiveness and reduce the risks related to remote work.

In particular, the study shows that proactive and integrated measures concerning cyber security readiness in the new context of remote work are essential. Through the integration of knowledge from both organizational change management and cyber security disciplines, practitioners can create a culture of cyber security resilience that gives employees the confidence to take control of the challenges that remote work environments bring while preventing the misuse of organizational resources and data.

Conclusion

Lastly, this research provides the foundation for understanding the cyber security readiness level within remote work environments. This research, through the analysis of organizational and individual readiness for change and cyber security readiness, also explores the multi-dimensional nature of cyber security readiness. The Organizational Security Valence and Individual Security Valence constructs that are proposed in the cyber security assessment model offer a new perspective on the assessing of employees' loyalty to security measures and give organizations useful information on how to enhance their cyber security readiness. Finally, developing an environment of readiness for change at the organization and individual levels is the key to successful cyber security readiness in the new remote work era.

References

Abbasi, B. (2017). Transformational leadership and change readiness and a moderating role of perceived bureaucratic structure: an empirical investigation. Problems and Perspectives in Management, 15(1), 35-44.

Alolabi, Y. A., Ayupp, K., & Dwaikat, M. A. (2021). Issues and implications of readiness to change. Administrative Sciences, 11(4), 140.

Anderson, J. C., & Gerbing, D. W. (1988). Structural Equation Modeling in Practice: A Review and Recommended Two-step Approach. Psychological Bulletin, 103(3), 411–23.

Anggraeni, W., & Febrianti, R. A. M. (2022). Managing individual readiness for change. International Journal of Research in Business and Social Science, 11(2), 127-135.

Arnéguy, E., Ohana, M., & Stinglhamber, F. (2020). Overall justice, perceived organizational support and readiness for change: the moderating role of perceived organizational competence. Journal of Organizational Change Management, 33(5), 765-777.

Berlilana, Noparumpa, T., Ruangkanjanases, A., Hariguna, T., & Sarmini. (2021). Organization Benefit as an Outcome of Organizational Security Adoption: The Role of Cyber Security Readiness and Technology Readiness. Sustainability, 13(24), 13761.

Caldeira, A.M.; Seabra, C.; AlAshry, M.S. Contrasting the COVID-19 Effects on Tourism Safety Perceptions and Coping Behavior among Young People during Two Pandemic Waves: Evidence from Egypt. Sustainability 2022, 14, 7492.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A Partial Least Squares Latent Variable Modeling Approach for Measuring Interaction Effects: Results from a Monte Carlo Simulation Study and an Electronic-mail Emotion Adoption Study. Information Systems Research, 14(2), 189–217.

Cunningham, C. E., Woodward, C. A., Shannon, H. S., MacIntosh, J., Lendrum, B., Rosenbloom, D., ... & Brown, J. (2002). Readiness for organizational change: a longitudinal study of workplace, psychological and behavioural correlates. Journal of Occupational and Organizational Psychology, 75(4), 377-392.

Dev, S., Lincoln, A., & Shidhaye, R. (2021). Evidence to practice for mental health task-sharing: understanding readiness for change among accredited social health activists in sehore district, madhya pradesh, india. Administration and Policy in Mental Health and Mental Health Services Research, 49(3), 463-475.

Deng, J., Cheng, Z., Qi, S., & Deng, R. (2023). Unravelling the relationship between perceived values-congruence with organizational change readiness: a moderated mediation model. Frontiers in Psychology, 14.

Ellis, L. A., Tran, Y., Pomare, C., Long, J. C., Churruca, K., Saba, M., ... & Braithwaite, J. (2023). Hospital organizational change: the importance of teamwork culture, communication, and change readiness. Frontiers in Public Health, 11.

Engida, Z. M., Alemu, A. E., & Mulugeta, M. A. (2022). The effect of change leadership on employees' readiness to change: the mediating role of organizational culture. Futur Bus J, 8, 31.

Fornell, C., & Cha, J. (1994). Partial Least Squares. In: Bagozzi RP, editor. Advanced Methods in Marketing Research. Cambridge: Blackwell.

Gefen, D., Rigdon, E. E., & Straub, D. (2011). Editor's Comments: An Update and Extension to SEM Guidelines for Administrative and Social Science Research. MIS Quarterly, 35(2), iii–xiv.

Ghani, E., Jusoh, W., Hassan, R., & Muhammad, K. (2019). Determinants of auditors' readiness for accrual accounting adoption. International Journal of Recent Technology and Engineering, 8(3), 8664-8673.

Haque, M. N., TitiAmayah, A., & Liu, L. (2016). The role of vision in organizational readiness for change and growth. Leadership & Organization Development Journal, 37(7), 983-999.

Hannon, P. A., Helfrich, C. D., Chan, K. G., Allen, C., Hammerback, K., Kohn, M., ... & Harris, J. R. (2016). Development and pilot test of the workplace readiness questionnaire, a theory-based instrument to measure small workplaces' readiness to implement wellness programs. American Journal of Health Promotion, 31(1), 67-75.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM). 2nd ed. Sage: Thousand Oaks, CA.

Hasan, S., Ali, M., Kurnia, S., & Thurasamy, R. (2021). Evaluating the cyber security readiness of organizations and its influence on performance. Journal of Information Security and Applications, 58.

Holt, D. T., Armenakis, A. A., Feild, H. S., & Harris, S. G. (2007). Readiness for Organizational Change: The Systematic Development of a Scale. The Journal of Applied Behavioral Science, 43(2).

Islam, M. N., Furuoka, F., & Idris, A. (2021). Employee engagement and organizational change initiatives: does transformational leadership, valence, and trust make a difference? Global Business and Organizational Excellence, 40(3), 50-62.

Jayarao, G. B., Ray, S., & Panigrahi, P. K. (2024). Information security threats and organizational readiness in nWFH scenarios. Computers & Security, 140, 103745.

Kirrane, M., Lennon, M., O'Connor, C., & Fu, N. (2016). Linking perceived management support with employees' readiness for change: the mediating role of psychological capital. Journal of Change Management, 17(1), 47-66.

Listyawati, N. S. (2020). Analisis faktor-faktor kesiapan dan dukungan stakeholders terhadap perubahan status menjadi badan layanan umum daerah (studi pada puskesmas-puskesmas di kabupaten klaten). ABIS: Accounting and Business Information Systems Journal, 4(4).

Liu, Y., Zhou, M., Hu, L., & Jaussi, K. S. (2023). Attached to or stuck in? how resource attributes of i-deals influence the variation in continuance or affective commitment. Baltic Journal of Management, 18(5), 579-595.

Mathur, M., Kapoor, T. R., & Swami, S. (2023). Readiness for organizational change: the effects of individual and organizational factors. Journal of Advances in Management Research, 20(4), 730-757.

Matthysen, M., & Harris, C. (2018). The relationship between readiness to change and work engagement: a case study in an accounting firm undergoing change. SA Journal of Human Resource Management, 16.

Mumtaz, S., Selvarajah, C., & Meyer, D. (2023). How does human relations climate and organizational support affect readiness to change? the mediating role of employee participation and leadership excellence. Global Business and Organizational Excellence, 43(2), 79-91.

Noor, W. N. B. W. M., Razak, S. N. A. A., Jusoh, Y. H. M., & Hasan, S. J. (2022). Analysing accounting professionals' readiness for digital economy using the theory of organisational readiness for change. International Journal of Academic Research in Business and Social Sciences, 12(11).

Oreg, S., Sverdlik, N., Paine, J. W., & Seo, M. (2024). Activation and valence in responses to organizational change: development and validation of the change response circumplex scale. Journal of Applied Psychology, 109(1), 135-155.

Otto, J., Ward, N. J., Baldwin, S. T., & Alonzo, W. (2022). Increasing readiness to grow traffic safety culture and adopt the safe system approach: a story of the washington traffic safety commission. Frontiers in Future Transportation, 3.

Qomariyah, A. N., Mursidah, E., Gonti, Y. A., & Wahyuni, D. (2020). Analysis of organizational readiness towards library 4.0: a case study at x library. Record and Library Journal, 6(2), 110.

Ringle, Christian M., Wende, Sven, & Becker, Jan-Michael. (2024). SmartPLS 4. Bönningstedt: SmartPLS. Retrieved from https://www.smartpls.com.

Shea, C. M., Jacobs, S., Esserman, D., Bruce, K., & Weiner, B. J. (2014). Organizational readiness for implementing change: a psychometric assessment of a new measure. Implementation Science, 9(1).

Thomas, K., & Dannapfel, P. (2022). Organizational readiness to implement a care model in primary care for frail older adults living at home in sweden. Frontiers in Health Services, 2.

Ting Wang, Dianne F. Olivier & Peiying Chen (2023) Creating individual and organizational readiness for change: conceptualization of system readiness for change in school education, International Journal of Leadership in Education, 26:6, 1037-1061.

Vaishnavi, V. K., Suresh, M., & Dutta, P. (2019). A study on the influence of factors associated with organizational readiness for change in healthcare organizations using tism. Benchmarking: An International Journal, 26(4), 1290-1313.

Vakola, M. (2014). What's in there for me? individual readiness to change and the perceived impact of organizational change. Leadership & Organization Development Journal, 35(3), 195-209.

Weiner, B. J. (2008). Review: conceptualization and measurement of organizational readiness for change. Medical Care Research and Review, 65(4), 379-436.

Weiner, B. J. (2009). A theory of organizational readiness for change. Implementation Science, 4(1).

Weiner, B. J. (2020). A theory of organizational readiness for change. Handbook on Implementation Science.