INFORMATION SECURITY THREATS AND ORGANIZATIONAL READINESS IN nWFH SCENARIO

सिद्धिमूलं प्रबन्धनम्
भा. प्र. सं. इन्दौर
IIM INDORE

By

Guruprasad B Jayarao

A Doctoral Dissertation Submitted in Partial Fulfilment of the Requirements for the

Executive Doctoral Program in Management
of the

INDIAN INSTITUTE OF MANAGEMENT INDORE

February 2023

INFORMATION SECURITY THREATS AND ORGANIZATIONAL READINESS IN nWFH SCENARIO

सिद्धिमूलं प्रबन्धनम्
भा. प्र. सं. इन्दौर
IIM INDORE

A

Thesis

SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR

THE EXECUTIVE DOCTORAL PROGRAMME IN MANAGEMENT

INDIAN INSTITUTE OF MANAGEMENT INDORE

By

GURUPRASAD B JAYARAO [2018-FPM(I)-02]

February 2023

INFORMATION SYSTEMS

THESIS ADVISORY COMMITTEE

PROF.PRABIN KUMAR PANIGRAHI (Chair)

PROF.SANJOG RAY (Member)

PROF.HASMUKH GAJJAR (Member)

ABSTRACT

The COVID-19 pandemic in 2020 impacted all aspects of life and business, resulting in the adoption of new organizational working models. Organizations mandated their employees to work from home (WFH). As a result, employees adopted it quickly and started work-from-home(as soon as possible and where WFH was feasible). The new age concept of new-work-from-home (nWFH) was elicited by Patricia et. al 2021, to differentiate from earlier routine work-from-home, nWFH is characterised by limited planning, design, or testing (Patricia, 2021). Security Threats to Information systems have also shown an increasing trend (Carlsten, 2021) due to this nWFH. The sudden change in work settings presented several issues for practitioners, forcing them to judge corporate information security. Organizations were not ready to handle this sudden shift in the workplace (Rodbert, 2021). Here the readiness to safeguard against information security threats in the nWFH scenario becomes vital from both the organizational perspective and the overall security posture. Hence we pursued the following objectives in this research. We explored the factors which could lead to organizational readiness (ORE). We developed a framework to be used by organizations when their employees work from home(nWFH). Explored the related influences of nWFH on information security threats of an organization, explored factors for assessing the readiness of organizations to safeguard against the information security threats, and lastly, understood various challenges organizations faced when they intended to implement the readiness guidelines.

We conducted an initial field study to explore the practical issues faced by organizations concerning information security due to nWFH, both in large organizations and small and medium enterprises (SMEs). By SMEs, we refer to the medium sized organizations based on the data collected from this type of organizations, we found that nWFH has

impacted organizations' information security due to changes in the workplace. The organizations required more time to be ready to manage information security when the entire organization worked from home. The state of readiness in medium enterprises differed from large enterprises due to resource constraints (people, process, and technology) (Cates, 2005), the absence of appropriate security policies, expected infrastructure support, and support from top management.

The main concerns reported from our initial study were the impact of nWFH on information security and their non-readiness to manage information security. After the initial discussions with subject matter experts, we found that large enterprises had a better infrastructure to manage the sudden change of workplace from traditional offices to home. However, SMEs faced budget constraints, infrastructure, communication, and security planning. Hence we decided to explore further the factors that lead to the readiness of SMEs.

The organizations' readiness to manage information security in the context of nWFH, the impact of nWFH on information security threat, and challenges in implementing readiness were the main topics of interest that emerged from our initial study. Therefore, our research aims to seek an answer to the following questions. How is the nWFH different from earlier WFH? How does nWFH influence the information security threats of an organization? How ready are organizations, and how do they assess their readiness to address information security risks in nWFH? What challenges do organizations face in implementing their readiness guidelines? Since these topics are not described much in the literature, we approached this research with the exploratory method through primary data collection with in-depth interviews (Showkat, 2017). We followed the purposive sampling method (Recker J. , 2021) , (Etikan, 2015) with snowball sampling to identify the prospective organizations for data collection. We collected data from subject matter experts in 20 organizations in SMEs. The sample size is in line with the recommendation by (Marshall, 2013) for qualitative studies. Transcripts generated from interviews were analyzed using content analysis methodology.

In the first study on nWFH influences on information security threats, we noted mixed responses. Even without essential VPN services, SME organizations did not face threat incidents during the pandemic. Hence this was counter-intuitive to our initial study. As per the researcher's knowledge from the security industry and from the various reports which stated a sizable increment of threats during the pandemic. However, a few respondents indicated they have the required infrastructure but did not choose to elaborate on the tools /products used for nWFH. They also did not face security incidents during the pandemic. Other section of participants from vendors to large organizations said, they used the VPN service and had no incidents. However, during the interviews, we observed the tone of the respondents as they could not reveal the incidents due to confidentiality.

In contrast, some respondents with an experience of 4-5 years informed us of a ransomware attack which they recovered from, as it was an insider threat. When probed more the participants informed that the primary issue they faced was BYOD (Bring Your Own Device) vulnerabilities when people work from home. Also, the suggestion on BYOD was to use the organization's OS(operating system) image and network connection through VPN. Thus ransomware and BYOD vulnerabilities were the top two vulnerabilities when people adopted nWFH during the pandemic.

In the second study, we investigate the degree of readiness in organizations, and the assessment of readiness to address information security risks in nWFH.

First, we figured out the factors leading to the readiness of organizations to safeguard against information security threats when people nWFH. We did multiple levels of analysis and coding from the interview transcripts and identified 11 factors that led to organizational readiness to safeguard against information security threats during nWFH. We identified the following six factors and mapped them to existing literature - resource readiness, cultural readiness, strategic readiness, IT readiness, cognitive readiness, and partnership readiness. We identified five new factors: security valence, cyber security risk management, balanced CIA (confidentiality integrity availability), WFH Policy, organizational best practices, and technical best practices.

Analyzing further, we infer that two factors that drive organizational readiness assessment are – technology assessment and organizational assessment. We have compiled a checklist tool that was verified for its usage in three organizations. We obtained positive feedback, and these organizations were willing to use this checklist tool.

The third study investigates the key challenges the organization's faced to implement the readiness process. We found that the following were the ten key challenges, employee perception towards security and readiness process, employee willingness to change, handling change management process, readiness process of all organizational units, support group challenges, third party compliance process, vendor compliance to readiness process, process burden, training and awareness, employee attitude to adhere to readiness process. The results from this study will help as a reference for practitioners trying to understand the challenges faced in implementing an organization readiness framework to mitigate information security risks.

We have further contributed to this research by documenting the best practices that emerged during our in-depth interviews. During the interviews, participants, mainly

security managers, often spoke about their best practices. Hence, we collated all the best practices as a guide based on the “voice of security managers”, we abbreviate this as VOISM and as an additional contribution to this study. The Best Practices Guide (BPG) comes as a saviour if followed, as every security manager articulated these practices in each interview. Hence we see a high-value contribution to the organizations from this BPG. To nurture this further, the organizations can periodically collate best practices. The motivation should come from the concerned top management team (TMT) to the employees to follow the BPG and enhance the existing BPG.

The key factors contributing to organizational readiness were integrated into a framework(11-factor model) for ease of use and tested in three SME organizations. First, we explained the framework in detail and the associated measurements of each factor. We followed Spencer's requirements for validating the qualitative framework (Spencer, 2003). The feedback received was encouraging, and the organizations planned to implement the framework for their use and embrace it for the betterment of their future readiness programs. The concerned managers in these three organizations prioritized the "security valence" to be measured first to understand the organization's affinity towards security and then go for other factors in a phased manner. We have met the study's objective with the framework's usefulness established from the feedback.

These research findings will help organizations /practitioners get a holistic view of their readiness and conduct self-assessments to safeguard against information security threats in the current nWFH scenario. Should the same situation occur again, they can be future-ready with the implementation of this framework.

Keywords: Information security, cybersecurity, ransomware, BYOD, pandemic, organizational readiness, work from home, CIA, security valence.

Table of contents

List of figures

List of tables

CHAPTER 14 : DISCUSSIONS AND ANALYSIS OF FINDINGS

This chapter describes the findings and discusses the integration of the qualitative results.

This study explores organizational readiness as a construct to safeguard against information security threats in the nWFH scenario. To serve this objective, this research work has adopted a qualitative method for data gathering based on interviews with subject matter experts with relevant experience and who witnessed the nWFH during the pandemic. The findings from this study helped in explaining the phenomenon.

In this section, we attempt to integrate the findings for all the research questions and summarize them to produce theoretical and practical contributions.

This research work, employed an exploratory method to understand and explore each of the research questions categorically. We opted for an exploratory study for the following two reasons. First, we could not find much relevant literature specifically for organizational readiness in the nWFH and security context. Based on initial meetings with subject matter experts we believed that the phenomenon holds the potential to provide a better understanding of nWFH in the pandemic situation and how it impacts the IS threats. Second, the nWFH being a new phenomenon witnessed during the pandemic, the inductive approach was more appropriate since the phenomena were observed at an individual level and generalization came later when the phenomenon was observed later. An observation in this study was there was no direct literature available on ORE for nWFH and IS threats. After exploration from the interviews, we tried to map the factors to the existing ORE model (Lokuge, 2019). This model was explored for digital innovation and had organizational elements. Hence we partially approached the deductive method as well. The final contribution of 5 new factors was purely from the exploration. The new factors have been validated with the subject matter experts and three organizations are positive on one of the five factors “ security valence”, which they felt was a starting point for understanding the affinity of employees and the leadership towards security. This was encouraging to us, as it was the first step towards the ORE model.

The common denominator was the nWFH which triggered all the organizations to get ready and implement various other processes apart from security as well.

We achieved the assessment of readiness through the checklist, again this was validated by subject matter experts with a positive outcome.

The challenges to implementing ORE saw a very vocal discussion as the participants were keen on informing their challenges. We believe some of the challenges may be common per say, but documenting the challenges and a continual follow-up in the organizations can help in mitigating the challenges.

The additional contribution of this research - the best practices guide (BPG) comes in handy and practical to industry colleagues and the practices can be chosen one at a time and implemented to build the secured organization.

CHAPTER 15 : CONCLUSIONS AND IMPLICATIONS

Exploring a multidimensional construct, namely Organizational readiness, the present study contributes to streams of literature in the domain of information systems and information security. The study focuses on the novel concept of organizational readiness as a proactive measure for any such situation which challenges mankind. Should any such situations arise in the future this model is likely to help the industry. The study has both practical and managerial implications. In the following section, we have discussed the implications of the study in detail.

15.1 Contribution to the theory

Our work can be categorized as a methodological contribution as we have employed qualitative methods, in parts used inductive and deductive methods. The inductive part has resulted in capturing the minds of the SME experts and hence contributed to the best practices. The deductive part has helped to map a few factors found from this study to other context models like the ORE for digital innovation (Lokuge, 2019). Our research design, though might not be a first of a kind but sets a rigorous example to approach research problems that broaden the knowledge in IS area. Apart from the rigour in methodology, our findings contribute to important streams in information systems. The new construct " security valence" is yet another contribution to information systems security literature. The other new factors, cybersecurity risk management, balanced CIA, exclusive WFH policy, and cybersecurity insurance will strengthen the model.

15.2 Contribution to the practice

The study has significant implications for practitioners, as managers face serious challenges during the nWFH in managing their teams. In the IT industry, professionals are believed to experience a higher level of stress due to nWFH. The BPG, challenges, and assessment checklist comes in handy as a ready reference for practitioners. Organizations can leverage this model takes care of their security as a whole and security as a habit by the ways of assessing their security posture. The findings have implications for organizations in terms of managing congruence between internal and external (vendors) security expectations. More so with the thinning boundary of traditional offices due to long-term nWFH, the outcome of this study stands firm for SME organizations.

15.3 Implications for human resource management:

Our findings indicate that individuals who perceive "security tasks as a burden" and do not attend to it or perceive it in a negative way are more prone to experience a negative outcome. They are expected to feel lonely as they work from home for the long term without adequate support from IT or security processes and they tend to think about leaving the organization, specific to the IT industry, as it has more people turnover. These results can be employed to create an environment where IT professionals receive the required support and seek security knowledge when they are away working from home. The human resource team can co-create an environment of a secure feeling among their people by proactively engaging with Technology teams and implementing security readiness for the organization as a whole.

Our study also contributes to the other industries where there is a dire need for a framework and knowledge on security. We believe that our findings will be applicable in similar economies of SMEs.

15.4 Limitations and directions for the future research:

The present study has certain limitations that must be acknowledged. First, due to its temporal nature and cross-sectional design, the present study does not provide unequivocal proof of causal direction. While the reciprocal effect may be possible, there might be SME organizations that have limited resources and might be doing well on security and readiness. But our model is consistent with current theories and evidence on security incidents and constraints faced by the SMEs.

Secondly, we used a self-report methodology. Therefore biases may have crept in. We addressed this limitation practically by validating with the experts in the security industry. First, we collected responses directly from the people who witnessed the nWFH during a pandemic and assured them of the confidentiality of data and second validated the findings. Third, we have validated the inter-rater reliability by sending the themes to map to one of the factors, this has resulted in 88% agreement.

Another limitation of this study is that we have only qualitative validation, future research can use our model to quantitatively evaluate, thereby establishing the variance of defining the ORE and building relationships and inter-relationships among the variables. For the convenience of future research, we have provided a draft of a survey instrument to measure the ORE.

On the best practices guide, the present study did not fully utilize the organizational characteristics and just stopped at identifying the best practices. Future researchers can consider the organizational characteristics to find if any of the characteristics influence the following of best practices and if best practices are followed, what are the implications to controlling security incidents in organizations.

This study assumes to an extent most of the participants are technology savvy, but another direction to review is to understand non-technical people from a security perspective. Future researchers can explore this aspect.

REFERENCES

Abukari, A. M. (2020). *Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond*. International Journal of Scientific & Engineering research, 1401-1407.

Acar. (2019). *An Analysis of Malware Trends in Enterprise Networks. International Conference on Information Security* (pp. 360-380). Springer.

Agarwala, B. D. (1996). Supreme Court Cases, 3(9). Retrieved from http://www.ebc-india.com/lawyer/articles/96v3a2.htm. Retrieved from Supreme Court Cases, 3(9). Retrieved from http://www.ebc-india.com/lawyer/articles/96v3a2.htm: Supreme Court Cases, 3(9). Retrieved from http://www.ebc-india.com/lawyer/articles/96v3a2.htm

Ahmad, T. (2020). Corona Virus (COVID-19). SSRN Electronic Journal.

Aithal, P. S. (2015). *AN EMPIRICAL STUDY ON WORKING FROM HOME: A POPULAR E-BUSINESS MODEL*. International Journal of Advance and Innovative Research.

Akello, P. a. (2019). "Information Security in Non-Corporate Cloud Services: The Challenge of Engaging Consumers in Security Behavior Change,. *AMCIS 2019 Proceedings*. (https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/13).

Alavi, R. (2020). *WFH :Think before you click*, ITNOW VOL 62 no 1. IEEE, 40-41.

Aloul, Z. a.-H. (2009). *Two factor authentication using mobile phones*. IEEE/ACS International Conference on Computer Systems and Applications . IEEE.

Aminzade. (2018, May). *Confidentiality, integrity and availability – finding a balanced IT framework*. Network security.

Anderson, J. (1994). *Computer Security techonology planning study*. NJ: Prentice Hall .

Anderson, J. M. (2002). *Why we need a new definition of information security*. Computer & Security, 308-313.

Anderson., J. (1972). *Computer security technology planning study*. Technical Report 73-51, U.S. Air Force Electronic Systems Technical Report. Air Force Electronic Systems Technical Report.

Andress, J. (2014). *The basics of information security*. Waltham Oxford: Syngress.

Anft, M. (2020). An Emerging Threat: Ransomware. *The Chronicle of Higher Education*. Retrieved December 1, 2020, from https://connect.chronicle.com/CHE-CI-WC-2020-EmergingCyber-TrendsSnapshot-PaloAlto_LP-CHE. html. https://connect.chronicle.com/CHE-CI-WC-2020-EmergingCyber-TrendsSnapshot-PaloAlto_LP-CHE. html.

Armenakis, A. A. (2002). *Crafting a change message to create transformational readiness*. Journal of Organizational Change Management.

Armstrong, D. G. (1997). *The Place of Inter-Rater Reliability in Qualitative Research: An Empirical Study*. SAGE Journals Sociology, 31(3), 597–606.

Babar, K. (. (2018). *Over 13 million people estimated to operate out of co-working spaces in India by 2020*. Retrieved from https://realty.economictimes.indiatimes.com/news/ commercial/over-13-million-people-estimated-to-operate-out-of-co-working-spaces-in-india-by- 2020-report/64388830: https://realty.economictimes.indiatimes.com/news/ commercial/over-13-million-people-estimated-to-operate-out-of-co-working-spaces-in-india-by- 2020-report/64388830

Babar, K. (2018). *Over 13 million people estimated to operate out of co-working spaces in India by* .. Read more at: https://realty.economictimes.indiatimes.com/news/commercial/over-13-million-people-estimated-to-operate-out-of-co-working-spaces-in-india-by-2020-report/643. https://realty.economictimes.indiatimes.com/news/commercial/over-13-million-people-estimated-to-operate-out-of-co-working-spaces-in-india-by-2020-report/64388830.

Babbs. (2020). *How to leverage data security in a post-Covid world.* Computer Fraud & Security, vol. 2020, no. 10, pp. 8-11.

Backer, T. E. (1997). *Managing the human side of change in VA's trans- formation*. Hospital & Health Services Administration.

Bandura, A. (1986). *Social foundations of thought and action*. NJ: Prentice Hall.

Bandura, A. F. (1997). *Self-efficacy: the exercise of control*. New York: W H Freeman.

Baruch. (2000). *Teleworking: benefits and pitfalls as perceived by professionals and managers, New Technology, Work and Employment*, vol. 15, no. 1, pp. 34-49,.

Benbasat I., B. C. (2010). *Information Security policy compliance :an amperical study of rationality -based beliefs and information security awareness*. MIS Quarterly, 523-548.

Beznosov, W. R. (2008). *Human,organizational and Technological challenges of implementing information security in organizations*. Proceedings of the second international symposium on Human Aspects of information security & assurance.

Bhattacharjee, R. (2022, April 19). https://www.instamojo.com/blog/smes-targeted-for-cyber-attacks-what-you-need-to-know/. Retrieved from https://www.instamojo.com/blog/smes-targeted-for-cyber-attacks-what-you-need-to-know/: https://www.instamojo.com/blog/smes-targeted-for-cyber-attacks-what-you-need-to-know/

Bick, R. C. (2020). *A blueprint for remote working: Lessons from China*. McKinsey Digital Repor. https://www.mckinsey.com/business-functions/mckinsey-digital/ our-insights/a-blueprint-for-remote-working-lessons-from-china.

Bolle, C. D. (2020, November 11). *How COVID-19-related crime infected Europe during 2020*. Europol.

Bolle., C. D. (2020). europol(2020). *How covid-19 related crime infected europe during 2020*. Europol.

Bond, J. T. (2002). *Highlights of the national study of the changing workforce: executive summary*. Families and Work Institute.

Borkovich, D. J. (2020). *Working from home: Cybersecurity in the age of COVID-19*. Issues in Information Systems, 21(4). informations systems.

Borkovich. (2020). *Working from Home: Cybersecurity in the age of COVID-19*. Issues in Information Systems.

Brodin, M. R. (2015). *Management issues for Bring Your Own Device*. European, Mediterranean & Middle Eastern Conference on Information Systems 2015 (EMCIS2015)1-2 June, Athens, Greece. Greece: European, Mediterranean & Middle Eastern Conference on Information Systems 2015 (EMCIS2015)1-2 June, Athens, Greece.

Burke, S. (2020). *Coronavirus Is Creating A Global 'Work-At-Home' Culture.* CRN.COM.

Camp. (1999). *Web Security and Privacy: An American Perspective*. The Information Society: An International Journal.

Carlsten, F. (2021). *Work from Home – Information Security Threats and Best Practices*. Lund University School of Economics and Management.

Carstedt, P. M. (2001). *Innovating our way to the Next Industrial Revolution*. MIT Sloan Management review.

Cascio, W. F. (2000). *Managing a virtual workplace*. The Academy of Management Executive, 13(3), 81–90.

Cates, J. E. (2005). *The Ladder of Business Intelligence* (LOBI): a framework for enterprise IT planning and architecture. Int. J. Business Information Systems, Vol. 1, Nos. 1/2, 2005, 220.

Chapman, P. (2021, March). *Defending against insider threats with network security's eighth layer.* Computer Fraud & Security .

Chatterjee, R. (2020, March 5). *Analytics India.* Retrieved from https://analyticsindiamag.com/difference-between-cybersecurity-information-security/

Cherdanseva, H. J. (2013). A REFERENCE MODEL OF INFORMATION ASSURANCE & SECURITY . IEEE.

Choo. (2010). *Cloud computing: Challenges and future directions*. Trends & issues in crime and criminal justice no. 400. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi400.

Choudhury, P. (2020). *Our Work-from-Anywhere Future Best practices for all-remote organizations*. Harvard Business Review, (November-December, 1-11. Boston, Massachusetts: Harvard Business Publishing. .

Clarke. (2010). *An Analysis of Information Security Aware- ness within Home and Work Environme. International Conference on Avail- ability, Reliability and Security*.

Colwil, C. (2009). *Human factors in information security: The insider threat e Who can you trust these days?* Elsevier information security tec hnical report 14 (2009) 186 e196.

concur, S. (2020). *SAP Concur India Report*. (2020). 88% of Indian work force prefer to have the flexibility of working from home. SAP .

CSA. (2019). https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/. https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/.

D'Arcy, J. &. (2009). *The multifaceted nature of security culture and its influence on end user behavior*. In International Workshop on Information Systems Security Research , (pp. 145-157).

Daniel, S. (1991). *ON the buzzword 'Security Policy'*. In proceedings of the 1991 IEEE Sumposium on Research in sECURITY AND pRIVACY PP.219-230 , 1991. IEEE.

Dery, K. S. (2017). *The Digital Workplace is Key to Digital Innovation*. MIS Quarterly.

Desai, P. (2018, November 28). Enterpreneur.com. Retrieved from https://www.entrepreneur.com/en-in/technology/is-cybersecurity-required-for-smes/323943: https://www.entrepreneur.com/en-in/technology/is-cybersecurity-required-for-smes/323943

Dey I, .. (1993). Qualitative Data Analysis.A User-Friendly Guide for Social Scientists. London: Routledge London.

Dharmakumar, R. &. (2011). Hackers’ Haven. Forbes India.

Dhillon, G. a. (2001). *Current directions in IS security research: towards socio-organizational perspectives*. Information Systems Journal, 11, 2, 127-153.

Dhillon, G. a. (2011). *Can a cloud be really secure? A socratic dialogue,. Computers, privacy and data protection: an element of choice Springer*, 345-360.

Dholakia, Z. a. (2004). *Whose Identity Is It Anyway? Consumer Representation in the Age of Database Marketing*. Journal of Macro Marketing COMPETITION AND MARKETS.

Doering, M. (2020, Dec 14). *Security Magazine*. Retrieved from https://www.securitymagazine.com/articles/94156-combating-insider-threats-in-the-age-of-remote-work?: https://www.securitymagazine.com/articles/94156-combating-insider-threats-in-the-age-of-remote-work?

Dopson, S. F. (2002). *No magic tar- gets! Changing clinical practice to become more evidence based*. Health Care Manage Rev.

Eilts, D. (2020). *An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses*. Florida.

Ein-Dor, P. &. (1978). *Organizational context and the success of management information systems*. Management Science, 24(10), 1064–1077.

Elo, S. &. (2008). *The qualitative content analysis process*. Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. Journal of Advanced Nursing, 62(1), 107–115. doi:10.1111/j.1365-2648.2007.04569.x , 107-115.

Eloff, J. H. (1988). *Computer security policy: Important issues*. Computers and Security, 7(6), 559–562.

Eslahi, M. N. (2014). *BYOD: Current State and Security Challenges*. IEEE.

Etikan, I. M. (2015). *Comparison of Convenience Sampling and Purposive Sampling. American Journal of Theoretical and Applied Statistics*.

Felstead, A. J. (2005). *The shifting locations of work: new statistical evidence on the spaces and places of employment.* Work, employment and society, 19(2), , 415-431.

Fishbein, M. &. (1975). *Belief, attitude, intention, and behavior: an introduc- tion to theory and research Reading, Mas*. Addison-Wesley Pub. Co.

Flores, W. R. (2016). *Shaping intention to resist social engineering through transformational leadership ,information security culture and awareness*. Computers & security vol 59 , 26-44.

Forbes. (2019). https://www.forbes.com/sites/louiscolumbus/2019/12/15/shadow-it-is-the-cybersecurity-threat-that-keeps- giving-all-year-long/?sh=228f31965561.

Forsdick, S. &. (2020, October). *Security's new normal: How CISOs are coping with pandemic challenges. I–Global Intelligence for Digital Leaders program, Fujitsu*. Retrieved November 25, 2020, from. Retrieved from https://www.i-cio.com/management/best-practice/item/adapting-to-a-new-security-environment-how-cis os-are-coping-with-the-challenges-of-covid-19

Fu, M. K. (2012). *Environmental policy implications of working from home: Modelling the impacts of land-use infrastructure and socio-demographics.* Energy Policy, 47, 416–423.

Furnell. (2020). *Home working and cyber security – an outbreak of unpreparedness? Computer Fraud & Security*, vol. 2020, no. 8, pp. 6-12, 6-12.

Garg, A. K. (2015). *The benefits and pitfalls of employees working from home: Study of a private company in South Africa.* Corporate Board: Role, Duties & Composition / Volume 11, Issue 2, 2015, 36-46.

Garg, A. K. (2015). *The benefits and pitfalls of employees working from home: Study of a private company in South Africa.* Corporate Board: Role Duties & Composition, 11(2), , 36–49.

Gartner. (2016). https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/?cm_mmc=social-_-rm-_-gart-_- swg.

Georgiadou, A. e. (2020). *A Cyber -Security culture framework for assessing organization readiness*. Journal of computer and information Systems, 1-11.

Gibbs, M. e. (2021). *Work from home & productivity: Evidence from person- nel & analytics data on IT professionals.* BFI Working Paper no. 2021–56. Becker Friedman Insti- tute for Economics at UChicago. https://bfi.uchicago.edu/wp-content/uploads/2021/05/BFI_WP_ 2021-56.pdf.

Glen, S. (2013). Inter-rater Reliability IRR: Definition, Calculation" *From StatisticsHowTo.com*. Retrieved from https://www.statisticshowto.com/inter-rater-reliability/: https://www.statisticshowto.com/inter-rater-reliability/

Golden, T. D. (2006). *Avoiding depletion in virtual work: Telework and the intervening impact of work exhaustion on commitment and turnover intentions*. Journal of Vocational Behavior, Volume 69, Issue 1, August 2006, Pages 176-187.

Gollmann, D. (2010). *Computer Security*. Wiley.

Gollmann, D. (2011). *Computer Security Third Edition*. In D. Gollmann. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom .

Graham, R. M. (1968). *Protection in an information processing utility*. Communications of ACM11(5):365-369,1968.

Graneheim U.H., L. (2004). *Qualitative Content Analysis in Nursing Research: Concepts, procedures and measures to achieve trustworthiness*. Nurse Education Today, 105-112.

Grassegger. (2021). *The role of Employees Information Security Awareness on the intention to resist Social Engineering.* Procedia Computer Science, 59-66.

Grimm. (2021). *Securing the remote workforce in the new normal*. Computer Fraud & Security, vol. 2021, no. 2, pp. 8-11.

Guidelines,N.I.(2022).,https://www.surveyofindia.gov.in/documents/NATIONAL%20INFORMATION%20SECURITY%20POLICY%20AND%20GUIDELINES.pdf. Retrieved from

Gupta, P. &. (2020). *Co-working has cradled India's start-up boom – The support it now seeks is well deserved*. Retrieved from https://timesofindia.indiatimes.com/blogs/voices/co-working-has-cradled-indias-start-up-boom-the-support-it-now-seeks-is-well-deserved/: Times of India Blog.

Gusain, A. R. (2020). *Work from home to work from anywhere – The future of co-working spaces*. Arti- cle in ORF Digital Frontiers. Retrieved from https://www.orfonline.org/expert-speak/work-home-anywhere-future- coworking-spaces/: https://www.orfonline.org/expert-speak/work-home-anywhere-future-coworking-spaces/

Haag, S. a. (2014). "Normalizing the Shadows – *The Role of Symbolic Models for Individuals' Shadow IT usage*. ICIS 2014 Proceedings.

Hassan, S. e. (2021). *Evaluating the cyber security readiness of organizations and its influences on performance*. Journal of Information Security and Applications.

Hedström, K. D. (2010). *Using actor network theory to understand information security management*. Springer Berlin Heidelberg, (pp. 43-54).

Hejase, H. J.-K. (2021). *Cyber security amid COVID-19*. Computer and Information Science, 14(2), 1-10.

Herscovitch, L. &. (2002). *Commitment to organizational change Extension of a three-component model.* Journal of Applied Psychology.

Herscovitch, L. &. (2002). *Commitment to organizational change: Extension of a three-component model*. Journal of Applied Psychology, 87:474-487.

Hill, E. J. (2002). *Does it matter where you work? A comparison of how three work venues (traditional office, virtual office, and home office) influence aspects of work and personal/family life*. Journal of Vocational Behavior 63 (2003) 220–241.

Hinsley, F. H. (1993). Codebreakers. Oxford University Press.

Hoffer, J. A. (1994). *The 9 to 5 underground: Are you policing computer crimes? Management of information systems*, pp. 388–401.

Höne, K. &. (2002). *Information security policy—what do international information security standards say?. Computers & security*, 21(5), 402-409.

Hsieh, H.-F. (2005). *Three Approaches to Qualitative Content Analysis*. QUALITATIVE HEALTH RESEARCH, Vol. 15 No. 9, November 2005 1277-1288.

Hsieh, H.-F. a. (2005). *Three Approaches to qualitative Content Analysis.* Qualitative Health Research Vol 15 No 9 , 1277-1288.

Iacovou, C. L. (1995). *Electronic Data Interchange and Small Organizations: Adoption and Impact of Technology*. MIS Quarterly 19, no. 4 (1995):, 465–85. https://doi.org/10.2307/249629.

Imenda, S. (2014). *Is There a Conceptual Difference between Theoretical and Conceptual Frameworks?* Journal of Social Sciences, 38:2.

Indian Express. (2006). The Indian Express. ISO. (1997). *ISO Information Technology Security open Systems interconnection* - The Directory Authentication Framework. International Organization for Standardardization -ISO/IEC 9594-8-ITU-TRec X.509(1997E).

Jacobson, K. (2020). *Scary statistics about the password reuse problem* [Blog]. Security Boulevard. Retrieved December 2, 2020, from. Retrieved from https://securityboulevard.com/2020/04/8-scary-statistics-about-the-password-reuse-problem/

Jain, A. (2022, June 21). https://www.medianama.com/2022/06/223-sme-msme-india-cert-in-directive-deadline-extension/. Retrieved from https://www.medianama.com/2022/06/223-sme-msme-india-cert-in-directive-deadline-extension/: https://www.medianama.com/2022/06/223-sme-msme-india-cert-in-directive-deadline-extension/

Jayadevan, P. (2020). *CORONAVIRUS: HOW TO NAVIGATE THE COVID-19 PANDEMIC TO ENSURE BUSINESS CONTINUITY.* https://www.cio.com/article/193155/coronavirus-lockdown-leads-to-an-enterprise-wide-work-from-home-wfh-in-india.html.

Jeffrey Hill, E. G.-C.-C. (2008). *Defining and conceptualizing workplace flexibility*. Community, Work and Family,, 11(2), 149-163.

Jouini, M. R. (2014). *Classification of security threats in information systems. 5th International Conference on Ambient Systems, Networks and Technologies* (ANT-2014). Elsevier ScienceDirect.

Kankanhalli, A. T. (2003). *An integrative study of information systems security effectiveness*. International journal of information management,, 23(2), 139-154.

Kim, G. S. (2010). *Research note: investigating two contradictory views of formative measurement in information systems research*, MIS Q. 34 (2) (2010) 345–365. MISQ, 345-365.

Klein, K. J. (1994). *Levels Issues in Theory Develop- ment, Data-Collection, and Analysis*. Academy of Management Review.

Klein, K. J. (2000). *From Micro to Meso: Critical Steps in Conceptualizing and Conducting Multilevel Research.* In K. Klein KJ, From Micro to Meso: Critical Steps in Conceptualizing and Conducting Multilevel Research.

Kong H, J. S. (2015 April). *Information security and organizational performance: Empirical study of Korean securities industry*. ETRI Journal, 37(2):428-37.

Kraemer, P. P. (2007). *Fact or Fiction? A Sensemaking Perspective on the Reality Behind Executives' Perceptions of IT Business Value*. Journal of Management Information Systems, 13-54.

Krippendorff, K. (1980). *Validity in Content Analysis*. ScholarlyCommons.

Liaw, G. (2007). *Relationships between critical factors associated with vir- tual work and virtual worker's organizational identification*. Fu Jen Management Review, 15(1), , 105–136.

Lokuge, D. S. (2019). *Organizational readiness for digital innovation: Development and empirical T calibration of a construct*. Information & Management.

Lundgren, B. &. (2019). *Defining Information Security*. Science and Engineering Ethics, 25, 419-441.

Maddux .J E, .. (1995). *Self-efficacy theory: an introduction*. NY: Plenum Press.

Maddux. (1995). *Self-efficacy theory: an introduction*. NY: Plenum Press.

Marr, B. (2020). *The 5 biggest cybersecurity trends in 2020 everyone should know about*. Forbes. Retrieved November 27, 2020, from. https://www.forbes.com/sites/bernardmarr/2020/01/10/the-5-biggest-cybersecurity-trends-in-2020-ever yone-should-know-about/?sh=679eb0647ecc.

Marshall, B. C. (2013). *Does Sample Size Matter in Qualitative Research?* A Review of Qualitative Interviews in is Research, Journal of Computer Information Systems, 54:1, 11-22, 54:1, 11-22.

Martinsons, M. D. (1999). *The balanced scorecard: A foundation for the strategic management of information systems.* Decision Support Systems, 25(1), 71-88.

Mattord, W. a. (2012). 2012. Cengage Learning.

Mayring, P. (2000). *Qualitative Content Analysis*. FQS - Forum Qualitative Social Research.

McDonald, N. S. (2019). McDonald, N., Schoenebeck, S., & Forte, A. (2019). *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW), 1–23. doi:10.1145/3359174. ACM.

Menon, A. R. (1999). *India: Adopting a Pro-Competitive Policy for Telecommunications*.

Meyer JP, H. L. (2001). *Commitment in the workplace: toward a general model*. Human Resource Management Review, 11(3), 299-326.

Microsoft. (2020). Microsoft. (2020). *Microsoft Digital Defense Report*. Microsoft. (2020). Microsoft Digital Defense Report.

Milasi, S. (2021). *Telework before the COVID-19 pandemic: Trends and drivers of differences across the EU,*.

Milkovich, D. (2020). *15 Alarming cyber security facts and stats*. Retrieved November 27, 2020, from https://www.cybintsolutions.com/cyber-security-facts-stats/. Retrieved from https://www.cybintsolutions.com/cyber-security-facts-stats/

Morse, J. M. (1995). *Qualitative research methods for health professionals* (No. 610.73072 M6).

Mukherjee, S. (2022). *Digital Economy and Work-from-Home: The Rise of Home Offices Amidst the COVID-19 Outbreak in India*. Journal of the Knowledge Economy.

Muthaiyah, S. &. (2018). ISO/IEC 27001 *Implementation in SMEs: Investigation on Management of Information Assets*. Indian Journal of Public Health Research and Development.

Nance, W. D. (1988). *An investigation into the use and usefulness of security software in detecting computer abuse*. Proceedings of the ninth annual international conference on information systems, (pp. (pp. 283–294)). Minneapolis, MN.

Newton, J. G. (2003). *Receptivity to Change in a General Medical Practice*. British Journal of Manage- ment.

NICCS. (2017). *National Initiative for Cybersecurity Careers and Studies* (NICCS).

Niekerk, v. S. (2013). *From information security to cyber security*. Computers & Security.

Nippert-Eng, C. (1996). *Calendars and keys: The classification of ‘home’ and ‘work’*. Sociological Forum, 11,563–581.

NIST. (2014). https://www.ftc.gov/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework.pdf. Retrieved from https://www.ftc.gov/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework.pdf: https://www.ftc.gov/system/files/attachments/understanding-nist-cybersecurity-framework/cybersecurity_sb_nist-cyber-framework.pdf

Osborne, C. (2020).*‗Flight risk‘ employees involved in 60% of insider cybersecurity incidents. Zero Day.* Retrieved from https://www.zdnet.com/article/flight-risk-employees-involved-in-60-of-insider-cybersecurity-incidents/

Patricia, A. (2021). *Volitional non-Malicious Insider Threats: At the intersection of COVID-19,WFH,Cloud-Facilitated Shadow -Apps*. AISeL.

Paul, S. (2022). *Cybersecurity for small and medium businesses: The next frontier?* https://www.financialexpress.com/blockchain/cyber-security-for-small-and-medium-businesses-the-next-frontier/2604028/.

Pettigrew, A. F. (1992). *Shaping strategic change: making change in large organizations: the case of the National Health Service London*. SAGE.

PonemanInstitute. (2020). Proofpoint.com. Retrieved from Proofpoint.com: https://www.proofpoint.com/sites/default/files/threat-reports/pfpt-us-tr-the-cost-of-insider-threats-ponemon-report.pdf

Pranggono. (2021). *COVID-19 pandemic cybersecurity issues*. nternet Tech- nology Letters, vol. 4, no. 2, pp. 1-6,.

Prantik, M. S. (2020, August 2020). https://sites.duke.edu/thefinregblog/2020/08/21/smes-in-india-data-privacy-and-security-and-learnings-from-the-world/. Retrieved from https://sites.duke.edu/thefinregblog/2020/08/21/smes-in-india-data-privacy-and-security-and-learnings-from-the-world/: https://sites.duke.edu/thefinregblog/2020/08/21/smes-in-india-data-privacy-and-security-and-learnings-from-the-world/

Promyslov, B. &. (2022). *On Cybersecurity Risk Assessment in Nuclear Power Systems*. ScienceDirect.

Puthal, D. M. (2017). *Building security perimeters to protect network systems against cyber threats.* IEEE Consumer Electronics Magazine.

Radzikowski, S. (2015). *Cybersecurity: Origins of the advanced persistent threat (APT)*. Retrieved from http://drshem.com/2015/10/08/cybersecurity-origins-of-the-advanced-persistent-threat-apt/

Ramakrishnan, S. (2009). Ramakrishnan, S. 2009, August 23. Interview with Kishore Bhargava.

Rao, H. R. (2020). *Retweets of officials' alarming vs reassuring messages during the COVID-19 pandemic: Implications for crisis management. International* . Journal of Information Management, 55, 102187.

Rau, B. L. (2002). *ROLE CONFLICT AND FLEXIBLE WORK ARRANGEMENTS: THE EFFECTS ON ATTRACTION. PERSONNEL PSYCHOLOGY.*

Raymond, L. (1990). *Organizational context and information systems success: A contingency approach*. Management Information Systems, 6(4), 5–20.

Recker, J. (2012). *Scientific research in information systems: a beginner's guide*, Heidelberg, New York, Dordrecht, London: Springer Science & Business Media. Springer Science & Business Media.

Recker, J. (2021). *Scientific Research in Information Systems*. Springer.

Recker. (2012). *Scientific research in information systems: a beginner's guide*. In R. J, Scientific research in information systems: a beginner's guide. Heidelberg, New York, Dordrecht, London: Springer Science & Business Media.

Ritchie, R. (2019). https://www.i-cio.com/management/insight/item/human-factors-in-cyber-security-nine-aspects-of-insider -threat. Retrieved from Human factors in cyber-security: nine facets of insider threat. I–Global Intelligence for Digital Leaders program, Fujitsu.: https://www.i-cio.com/management/insight/item/human-factors-in-cyber-security-nine-aspects-of-insider -threat

Ritchie, R. (2019). *Human factors in cyber-security: nine facets of insider threat. I–Global Intelligence for Digital Leaders program,* Fujitsu.

Rodbert, M. (2021, November 3). *MAG Online Library*. Retrieved from https://www.magonlinelibrary.com/doi/abs/10.1016/S1353-4858%2820%2930092-1

Sachithra Lokuge, D. S. (2018). *Organizational readiness for digital innovation: Development and empirical T calibration of a construct*. Information & Management Elsevier.

Samonas, S. (2014). *THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY*. Journal of Information system security.

SAP. (2020). *88% of Indian work force prefer to have the flexibility of working from home*. https://www.concur.co.in/newsroom/article/88-of-indian-workforce-prefer-to-have-the- flexibility-of-working-from. Retrieved from 88% of Indian work force prefer to have the flexibility of working from home. https://www.concur.co.in/newsroom/article/88-of-indian-workforce-prefer-to-have-the- flexibility-of-working-from: 88% of Indian work force prefer to have the flexibility of working from home. https://www.concur.co.in/newsroom/article/88-of-indian-workforce-prefer-to-have-the- flexibility-of-working-from

Sathe. (1985). *Culture and related corporate realities: text, cases, and readings on organizational entry, establishment, and change Homewood*. R.D. Irwin.

Schneider, B. G. (1995). *The ASA framework: An update*. Personnel Psychology.

Showkat, N. &. (2017, July). https://www.researchgate.net/publication/319162160_In-depth_Interview. Retrieved from https://www.researchgate.net/publication/319162160_In-depth_Interview: https://www.researchgate.net/publication/319162160_In-depth_Interview

SHRM. (2001). *Society for Human Research Management Foundation*. Society for Human Resource Management.

Silverman. (2020). *Qualitative Research V edition*. In Qualitative Research V edition. SAGE Publications.

Silverman. (2020). *Qualitative research*, 5th edn. Los Angeles: Sage Publications.

Skopik, F. S. (2016). *Title: A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing*. Computers & Security (2016).

Solms, B. V. (2000). *Information security-The third wave?* Computers & security, 9(7), 615-615.

Solms, T. M. (1998). *Information security awareness: educating your users effectively*. Information management and computer security .

Spencer, L. R. (2003). *Quality in qualitative evaluation: a framework for assessing research evidence*. UK.

Straub Jr, D. W. (1990). *Effective IS security: An empirical study.* Information Systems Research, 1(3), 255-276.

Straub, D. W. (1990). *Effective IS security: An empirical study*. Information Systems Research, 1(3), 255–276.

Subramanian, R. (2016). *Historical Consciousness of Cybersecurity in India.* AIS Electronic Library (AISeL), 1-16.

Sun, J. A. (2011). *The more secure the better? A study of information security readiness*. ndustrial Management & Data Systems,, 111(4), 570-588.

Sundstrom, E. &. (1986). *Work places: The psychology of the physical environment in offices and factories*. Press Syndicate University of Cambridge.

Susanto, H. A. (2012). *Information security challenge and breaches: Novelty approach on measuring ISO 27001 readiness level.* International Journal of Engineering and Technology. IJET Publications UK, 2(1), 67-75.

Swink, D. R. (2008). *Telecommuter law: A new frontier in legal liability.* American Business Law, 38(4), 857–900., 857-900.

Symantec. (2015). *Internet Security Threat Report*, Volume 20 - 21347931_GA- internet-security-threat-report-volume-20-2015-appendices.pdf. Symantec.

Talib, N. L. (2010). *An Analysis of Information Security Awareness within Home and Work Environments.* 2010 International Conference on Availability, Reliability and Security. IEEE Computer Society.

Thong, J. Y. (1996). *Top management support, external expertise and information systems implementation in small businesses*. Information Systems Research, 7(2), 248–267.

Tietze. (2002). *When "work" comes "home": Coping strategies of teleworkers and their families*. Journal of Business Ethics, 41(4), 385–396.

Timonen, H. &. (2018). *Visibility of Work: How Digitalization Changes the Workplace. Hawaii International Conference on System Sciences*. Hawai.

Tohmatsu, D. (2016). *The 2016 Deloitte Millennial Survey: winning over the next generation of leaders*. Deloitte.

Trzupek. (2020). *PKI is key to securing a post-Covid remote workforce, Computer Fraud & Security*, vol. 2020, no. 10, pp. 11-13. Sciencedirect.

Vaithyasubramanian, S. C. (2016). *Access to network login by three factor authentication for effective information security*. The scientific world.

Verizon. (2020). Verizon report 2020. NY: Verizon.

Virwani, G. P. (2020). https://timesofindia.indiatimes.com/blogs/voices/co- working-has-cradled-indias-start-up-boom-the-support-it-now-seeks-is-well-deserved/. Retrieved from Times of India: https://timesofindia.indiatimes.com/blogs/voices/co- working-has-cradled-indias-start-up-boom-the-support-it-now-seeks-is-well-deserved/

Von Solms, B. (2006). *Information security–the fourth wave*. Computers & security, 25(3), 165-168.

von Solms, B. a. (2018). *Cybersecurity and information security – what goes where. Cybersecurity and information security – what goes where?*, Vol. 26 No. 1, pp. 2-9.

Vroom, V. H. (1964). *Work and motivation*. NY: Wiley.

Vroom. (2004). *Towards information security behavioural compliance*. Computers & Security, 191-198.

Ware, W. H. (1960). *Security Controls for computer systems*. Technical reportR-609,. California: The RAND Corporatin Santa Monica.

Ware., W. H. (1970). *Security controls for computer systems.* Technical Report R-609. CA: The RAND Corporation, Santa Monica, CA.

Weber, R. (1990). Basic Content Analysis. SAGE Publications.

Weiner, B. J. (2008). *Conceptualization and measure- ment of organizational readiness for change: a review of the literature in health services research and other fields*. Med Care Res Rev.

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

Weiner, B. J. (2009). *Using organization theory to understand the determinants of effective implementation of worksite health promotion programs*. Health Educ Res, 24:292-305.

Williams, C. R. (2020). *Cybersecurity Risks in a Pandemic.* Journal of Medical Internet Research , 1-4.

Woon, I. T. (2005). *A protetcion Motivation theory approach to home wireless security.* ICIS. ICIS Proceedings 2005.

Yeshasvini, .. R. (2022). *THE NEW AGE OF WORKPLACE CULTURE Insights from India's Great Mid-size Workplaces 2022.* Great Place to Work Institute.

APPENDICES

Appendix A – Guiding Questions For in-depth interviews for Data Collection

Instructions to participants, the researcher explained the below instructions to the participants before the interview and took their consent.

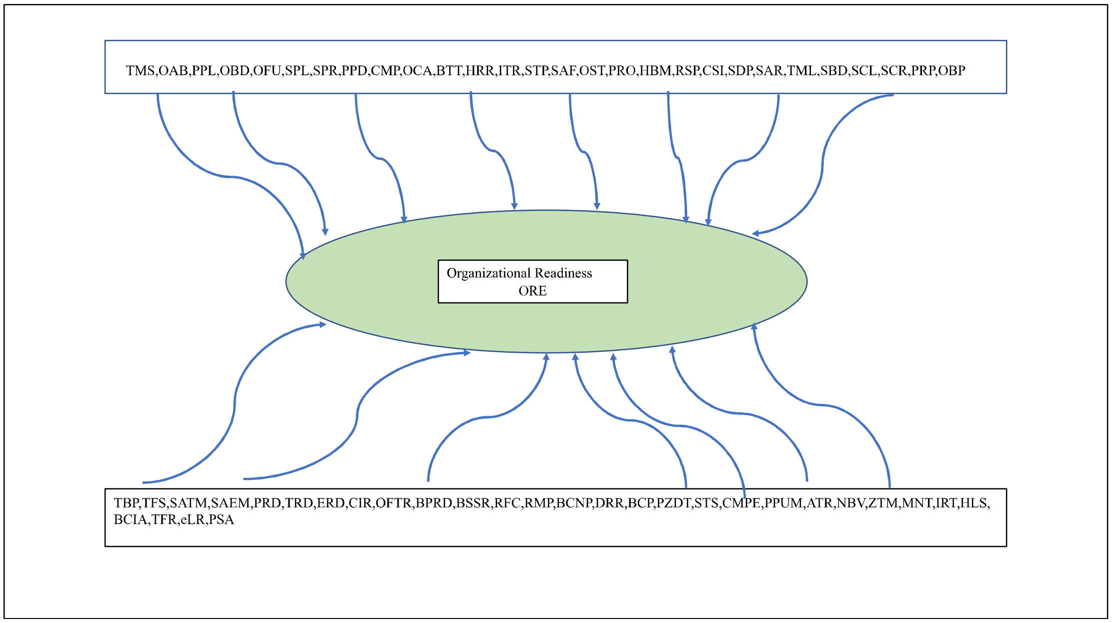
Dear respondents,

Thank you for your consent to be a part of our study.

We are trying to explore the challenges faced by organisations during work from home to safeguard against the information security threats and readiness to handle the security threats in this WFH context. Your response will help us in understanding multiple dimensions of the phenomenon. Please note that this is a pilot study to test the survey questions, hence your responses will help us fine tune the questions. We ensure anonymity and confidentiality of the responses. These responses would not be shared at an individual level, only aggregate findings will be shared while publishing the study. If interested, we would be happy to share the results with you. You can deny to answer any questions, responses are voluntary.

1. What is your present position, and how much information security experience do you have?
2. Just a thought... So, what comes to your mind when you think about information security? Just to make sure we're on the same page. What does it mean to you, or what do you believe it means to you?
3. Regarding work from home can you share your experiences? Earlier WFH and now any thoughts you can share?
4. Regarding security threats and WFH what is your experience? Why do think its risky to WFH
5. Regarding the organization policy was there a change why was it changed?
6. Regarding preparedness when I say "Organisational readiness" what are your thoughts?
7. Regarding your experiences during the pandemic and WFH can you shed some light?
8. If I mention Technology, Environment and Organisation , what are your thoughts and priority? Which one do you first prioritise?
9. What are the organisational activities which you feel are important while assessing organisational readiness?
10. We discussed on readiness earlier, can you elaborate any challenges to implement ,given a framework to your organization?
11. Outsourcing work to third party contractors, what is your experience on this from security adherence perspective? Do you have a security policy for contractors to adhere to? Do you see the contractors as a threat vector?
12. Have you seen any exposures due to contractors in last few years or in 2 years since pandemic started?
13. Do you classify information based on access you provide to employees? (The process of categorising data according to its level of sensitivity, such as open, partly open, or confidential)
14. What are the security standards your organization practices? Any certifications like ISO27000 ?
15. Is there anything further you want to say or clarify?

Appendix B - Content Analysis and coding



TMS,OAB,PPL,OBD,OFU,SPL,SPR,PPD,CMP,OCA,BTT,HRR,ITR,STP,SAF,OST,PRO,HBM,RSP,CSI,SDP,SAR,TML,SBD,SCL,SCR,PRP,OBP

Organizational Readiness
ORE

TBP,TFS,SATM,SAEM,PRD,TRD,ERD,CIR,OFTR,BPRD,BSSR,RFC,RMP,BCNP,DRR,BCP,PZDT,STS,CMPE,PPUM,ATR,NBV,ZTM,MNT,IRT,HLS,
BCIA,TFR,eLR,PSA

Appendix C Interview summary of RQ1

For our research question RQ1 on how different nWFH from earlier WFH scenario? We captured the responses from the participants which are presented below.
Question: Were you able to work-from-home due to the pandemic?
90% of the participants answered a "Yes" which was expected, as this is a global trend, mostly in the SME IT sector. But the other 10% could not WFH due to the nature of their work either in the manufacturing sector, Infrastructure, Data centre operations, medical profession and Banking sector.
Based on the empirical data gathered it is proven that 90% of the workforce worked from home which was a global trend as well.

We wanted to understand how the new-WFH is different from earlier WFH - during the normal situation. Following were the responses.
We have ordered the responses by People, Process (policies if the organizations had WFH as a practice), and Technology categories (Cates, 2005).

People Perspective

As per participant P1:
Ah! like when the WFH, they work at their comfort, and its more flexible, we can work anytime as long as the work gets done, we are ok.
Participant P2 elaborated his view as per the following narration
Given for me, when I was WFH, I had the flexibility of logging in and out ... what importantly matters to me was the added flexibility and a kind of .. you know, you can plan your day ahead. We as an organization we also ways believe in that like we do have business hours but at the same time, everybody in the org .. we have the flexibility to be available and at times even you know in case if you are not available due to any kind of personal work, you can always make it up in the next day by logging in early and complete the tasks. So yes, flexibility is one and number two would be you get to spend more time with family and all. You feel more energized and more motivated, saving a lot of time in traffic.
Participants P4, P8 says

I see the flexibility from an employee perspective, but at the same time flexibility from organization also as they too benefitted, I feel motivated when I started from home.

We work at our comfort and our organization provides proper access for our work hence I feel it's good.

So WFH is comfortable, we have meetings virtually and connected, even daily commute has reduced, the pros are more than the cons.

Participants P6, P7, P10 ,P20 shared their thoughts as

Because of flexibility offered to employees it helps to plan our WFH tasks, anywhere we work our philosophy is to get the work done.

Flexibility is what I see as a difference and over time people got adjusted, longer term impact when people work-from-home is already being assessed through surveys and how employees feel! It is just flexibility I guess, because WFH gives the flexibility in the hands of employees to plan their day. Whereas in office we have a time bound schedule to login and log out, So I would say flexibility to reflect on this!

There is a massive difference and before pandemic WFH - it was not an organized aspect of working, because it was rare. but now over the past 2 years its part of life, it has become an organized workforce at home ... they have made it a pat of life and to make it part of life its better organized and I would add here if anyone is working from it would not add or reduce the value ... we have learnt to deliver from home.

It is the same, the only difference is the number of days per week. Earlier it was less and now its 5 days a week.

WFO (work from office) - Group discussion helped us better understand the concepts

WFH - Peace of mind, travel can be avoided, tasks can be completed on a priority basis, and discussions can be conducted over MS teams, and we are ok with this arrangement.

The following categories emerged from the people perspective

Flexibility, less travel, peace of mind, better work organization, comfort of working at home emerged predominant expressions and had more number of citations.

Process Perspective

We explored the process perspective by asking – what was the impacts of nWFH on the organizational routines during pandemic? Did you change organizational policies, process, ex - security policy WFH policy etc?

What were some of the challenges you faced?

As participant P6 says

Enforcing the Policy was difficult for our organization when people worked from home as we did not have earlier a policy for WFH in normal situation.

Participant P9 being technical and hands on manager adds his technical expertise narration as below

We always had WFH earlier, but we had to change the process of IAM (Identity and Access management, this was a bigger process change in the new model of WFH.

Participant P16 being CISO(chief information security officer) adds his perspective

The process of more access to data and servers was encountered in the current pandemic situation and we had to tweak this process, and this was a huge difference from earlier to now!

The process is driven through a WFH policy and security policy of our organization, the do's and Don'ts when people work-from-home.

The process for procuring internet connectivity, where people did not have a home Wi-Fi in remote areas, VPN connectivity and all had to be done from scratch.

P20 shared his views on how they reworked

The whole organizational routine work with respect to the WFH conduct had to be re-worked within first few days before we announced WFH.

One of the interesting facts revealed by most of the participants is about "Moonlighting"

P11,P8,P7,P20,P4 opened up their grievances about their employees "Moonlighting".

P11 says we suspect some of our employees is doing more than two day jobs. This is eroding and we can't really check this, this is one of the pain points in work from home.

P8 puts the moon lighting as an ethical issue , employees should not do this as their commitment to our work is derailed !!

P7 says , we have lost trust on few employees as we came to know they are doing other company's job, whatever their goals are !!

P20 – Moonlighting is not a new thing , if they accept another job which is outside of our work hours.

P4 says apart from technical or organizational constraints , the employee's ethical aspects of moonlighting has to be understood !!

Technology Perspective

Technology in general was cited next highest to Organizational routines! We asked how important was technology when people WFH? What are the challenges faced? Does technology alone help?

I see a difference in the way infrastructure is planned when we WFH. Access to servers and data is more now compared to earlier days as everyone needs access to data and servers, the VPN, the central management infrastructure etc, hence from technical standpoint organizations should be able to afford all these new costs !!

Yes. Home and office it can happen in both. The only difference is that, at least when you are connected to the network right, Kind of controlled by the company in terms of whether it is using a secure connection versus an open connection, those kind of things. Generally, also not acknowledged, not like that, but many companies do have a laptop being taken out of office. They don't even have laptops. They have only had desktops from most of the employees once they are working from home Pretty much everybody has a laptop connected over the Wi-Fi, which might not be secured. The scope of compromise increases when working from home for whatever, for a lot of reasons that are getting security vulnerabilities, earlier that a small percentage of working for a company from work-from-home. It would impact only a small percentage. I mean, the entire company's working from home, then you have the chances of a security breach happening is more chances of eavesdropping a conversation into employees when it happens in an office, the chances are less because for example, in our XXX office, outsiders are not followed so easily and say the office or somebody comes like even family members give not a lot beyond setting time to be instead of after an hour or something, it's fine.

If he does have to log, now at home, I told him you're not logging anybody on a laptop is open, right? You have no control of who is eaves dropping. You would be talking and sharing a conversation. That could mean some suppose a friend outside sitting, hearing to the conversation, right? It is very, you cannot basically information leak can happen completely, both in terms of a social thing. And then the social engineering thing.

Your laptop itself is not over a secure connection right. The chances of somebody else using the laptop increases, knowing some family member using the laptop increases, you are using personal devices increases, the intention of some malicious user he's, he's more brave enough if he's doing it in the company of his own, he could not insert a

USB. Not everybody has all the mechanisms to protect it. he could insert with USB, take out code, all that can happen, in the office.
It was very tough, but now, the chances of that increases. It's basically protecting the data for the company, becomes a lot bigger problem, but what was a network security problem, which was like in office, you have to worry about network security, the entire world is a network now, security, but now it's like. you are worried it's not an office network anymore. People are connected to the laptop, or the public internet and they can connect from different locations and different timings. You cannot even monitor properly in office sometimes, so you can monitor for some activity, but since in office is somebody doing something, but going out to the internet and all that, we cannot actually monitor everything which goes out. It doesn't go through your firewall. It, for example, my connections from my laptop, obviously it might be going through the VPN with them, accessing some internet resources. It can go directly not able to split and link and it does not go away.

All your monitoring thing has been reduced. Now you cannot really monitor everything. What happens on my laptop when I'm working from home, these are the problems?

If, I mean, this are the things, information security when WFH is a about that, for example, it may not be a VPN for me. Somebody can physically say steal it, somebody can eavesdrop. Somebody can be just sitting behind a laptop and looking at it. If they are working on a, a coffee shop or something that is also about information security for me when WFH or anywhere right, they are not actively monitoring, but that's the only way there are a lot of things where somebody's laptop gets stolen. That can cause a security issue.

Even though we say WFH, do we really know people are connected from their homes? as the situation relaxed a bit, people started going to resorts etc so where is the security? that difference is very difficult to manage.

I see this question related to more work-from-home as a global trend but in terms of control and security I see the differences from earlier WFH, server access, data access has to be controlled and monitored.

Ah currently when people WFH, or even then people were taking laptops to home though they work from office , the same kind of vulnerabilities exists, so that does not change with people WFH, So the other extra thing that has creeped in is accessing servers and all , previously it was all routed through the office network now we might have to give people individual access, it all depends on how well your security management or access management to different servers or other application servers are done and managed.

No not more access privileges , just your authentication has to be more expanded and more robust like if you are working from office you can say access to AWS server can be only from this IP , now we have to give individual access to all people who need access to servers, one might be their home WI-FI is not static IP , it keeps changing, you might have to keep changing IPs for giving access so that has brought in little more effort on the management side because at the end of the day people still need access , this is the difference from technical perspective

Earlier WFH was allowed only in special circumstances and after approval. Since it was special circumstances, it was probably not required for employees to be available at all times during work hours. Now, since WFH is the norm, employees must be available at all times during business hours. The conduct of an employee is expected to be identical as if heor she is co-located with colleagues.

Our business is a hybrid operational model. Operationally we have not faced any issues as of now so not much of a difference from earlier WFH and new WFH.

WFH infrastructure like WI-FI, VPN, Encryption, etc were planned for secured remote work during the first few weeks after the announcement of WFH was made.

None - no difference we had always had WFH

Appendix D Interview summary of RQ2

To understand the influence of nWFH on IS Threats we started by asking few questions as follows

Q: what are your thoughts on WFH and its impacts to information security of an organization?

Q: Have you seen any differences in the information security threats like its more now than earlier?

Q: Do you think the hazards of IS threats has changed while working from home?

Q: When people work from, what are the information security measures you follow?

Responses:

No necessarily... it's the same, as before we did not notice any increase in IS threats in our organization, however I have seen reports worldwide of increase in certain types of threats like ransomware, falling to SPAM mails - which has shown increase trend, and I feel it's due to WFH.

No nothing as of now, nothing was reported during the pandemic period earlier like one year, we were WFH continuously. Now we are in Hybrid mode and so far, no issues reported

No, I don't think so, when we had permissions to WFH like earlier I said there were certain functions were allowed to WFH, so we already had a very robust VPN setup. we had VPN and cloud technology that ensured access, security policies and even for an employee working from remote location, access and security was already setup.

Access to malicious sites, clicking unidentified emails can help the hackers crack the network that needs to be avoided. We have a few steps all employees need to follow - should not entertain anyone else to use our laptops, they should not discuss any of our company confidential information with anyone at home it's a violation.

Spam emails having Covid-19 as the subject or in the mail body has to be filtered out in email protection gateway.

I guess that the first thing you know.... that causes a .. ah people use their internet access, so they are private networks, right?

So, sure there will be issues, on the contrary here in office we are in a closed network. So we only we can even monitor like who are joining and who are leaving in Realtime, but when it comes to WFH we really don't know .. like because it's not a closed network anymore. like an employee can use a hotspot or a fixed line connection. These are the issues ....

Hazard, I see from my experience, more access to our online drives like google drives had to be given to our employees and that was vulnerable.
we had a ransomware attack, but was contained, can't provide more information on this, but we had a ransomware issue last year.
we saw the term "Covid-19" being used in the spam mails which caught people's attention and many of our people clicked on those spams thinking it was real!!

We did see more malware issues in the pandemic situation, and I say we were vulnerable from people WFH. Yes, we had a ransomware attack and data breach attempt once, but impact was less. After this event we have upgraded our encryption method and the situation has improved, but we cannot relax, we are on high alert and have set up alerting mechanisms!

Appendix E Interview summary of RQ3

What are your thoughts when I say Organizational readiness with respect to safeguarding against IS threats?

How do you define readiness in organizations to safeguard against IS threats?

P1 – "See with or without an emergency, organizations should be ready, I see the budget as a constraint as I have seen in various organizations in our SME sector...But the basic protection should be enabled, and we should not allow compromises to happen. But also, I have seen less ransomware attacks in SMEs as compared to larger organizations... I also want to add the "Top Management support" is critical and I expect this to be "Direct from Board Room"".

P4 – 'Readiness to me is always be ready with your basic defence, secured VPN, with protective walls I mean Firewall, encryption and data loss prevention (DLP), IP Whitelisting, of course from people perspective its training and awareness not only with developers but with all functional organizations like HR, Finance, Quality teams etc basically everyone in the organization should have the awareness and this can be practically said to be readiness expected ..."

P3 – "This situation increased awareness among all players about the importance of data and systems security and paves the way for standard practices on security to be adopted by all.

Organizational readiness to me should comprise of Security Policies, process, updates, awareness, compliance, training., continuous audits, tools".

P6 – "The people should be aware of the things happening, they should be well educated in security, I mean even with the best talent and technology we can't achieve the required security without people being aware of security policies of the organizations and operate accordingly".

"I see readiness as multifaceted like readiness from finance department, HR department, culturally also HR should ensure they are preparing the employees towards the readiness, there should be a strategy team as a part of readiness, IT teams should be gearing up, and other than all everyone in the organization should have an affinity to keep themselves and their organization secured, these defines the readiness..."

P8 – "From IT perspective our org readiness includes − Data breach prevention - can be achieved by Data loss prevention (DLP) software applications".

P9 - Threats via browsing sites - Can be managed by monitoring browsers with AV and cloud proxy checking for vulnerabilities on all machines and closing them Getting the organization ready for WFH is a continuous process".

P10 – "During this process, we need to ensure the following from IT and organization perspective 1. Stable VPN 2. A good AV product 3. Proxy 4. Data Loss Prevention Employees should have very little data on their devices, if its goes bad, immediately it can be replaced enough hardware resources"

P14 – "No use of persona device we can achieve basic readiness with the above and of course training and awareness should be on top of the readiness criteria".

P11 – "In our case it was a thorough process 1. when we heard about Covid-19, from that day itself we started working on it 2. Even we had asked many teams to WFH and collected their experiences With the above we had prepared better when actual WFH was announced later".

P12 –" No, we were not ready, as a learning we quickly put together our security policy and a manual which instructs the standard operating procedure that the organization *must follow when we were under such urgency for starting to WFH, it is better to lose 100 bucks instead of losing thousands bucks".*

P16 – "speaking on the readiness, we were not prepared at all, as did not have any WFH concept earlier, we are from Manufacturing sector, hence a total plant shutdown was the only solution, which lasted for 2-3 months beyond this I can't reveal more".

P17 – "I am from the pharmacy industry and work in marketing, we all had to connect to our clients from home and travel on need basis with permission as delivering medicines is an essential service, neither we worked from home or at office, we were always online and coordinating the delivery of medicines so no WFH for us. But I can talk about the online technology which helped us save our daily business, without technology like internet, mobile phones, online doctor consulting we would be nothing and could not serve anyone ...."

P20 – "I am from IT infrastructure organization we support both on-premises infrastructure and support on cloud, we have now come up with Hybrid support. But I would like to inform that we were not at all ready. But till all the organizations or Government announced the pandemic and asked all to be at home, we scaled up our support with an internal red team directing us. All I mean to say is we geared up our online support, deployed remote support group to continue to support our clients and still we had a percentage of infrastructure team on client premises as it was data centre to be managed, they were all in client's location".

P1 – "Most of the people who were contacted from Banking sector informed they did not have WFH at all, a chief manager of a reputed public sector bank informed it was a struggle to manage the banking operations, beyond that he could not reveal...."

P5 – "No question of readiness and it was a war like emergency for us ..., we just made everything possible to make the core banking, ATM and online methods more robust"

P19 – "In my view readiness can be scoping out the kind of threats an organization is vulnerable to, depending on the industry it is trying to cater to"

P4 "Having these threats documented and circulated among all the stakeholders, if employees are a part of it yes, we should include them as well ,Clearly not sacrificing on the security aspects of product development cost"

P12 – "Have the threat models built and analyzed to build secured products and hence protect the organization".

P17 - Organization should have a threat model with respect to internal and external threats and hence, I recommend readiness starts with Threat modelling the entire Organization by scanning the Organization's Technology, Environment with respect to People. This can be a better way to define ORE.

P1- " Organizational readiness to me is the "Total Commitment from the Leadership team , from the board, the board team should understand that keeping the organization ready is mission critical and the board should drive the readiness in the organization and from information security perspective the culture of the organization I mean the "security culture for the organization should start from the Boardroom".

P3 - "The budget for information security should be adequate , see spending on security today is better than after math of a security incident which spoils the reputation of the organization".

"I come from IT security core team, and I have few points to share on the readiness and proactive initiatives".

The Organization who are serious about their reputation should be always focussed on a continual improvement, means periodic improvement plans in place and should work on this plan implementation

Cybersecurity insurance is one which can help as a proactive measure, this is a worthwhile investment

I understand organizational readiness as the readiness of organizations and all their vendors (which is difficult to achieve), the readiness of the vendors or partners is critical to secured organization

when you mention organizational readiness with information security context, we should break it down into Organizational Functional team readiness, cyber security readiness, information security readiness then we can take each and review.

OR - It's about being prepared with a robust back system if the primary security system fails by chance, to ensure we secure our customers data at any point of time.

Can you provide your thoughts on readiness in organizations? How should they get ready?

P11 - "I think it's about risk forecasting and situation assessment that needs to be done on a proactive basis and also have a solid project plan to address those risks along with contingencies if they occur over a period of time".

In your opinion what are the activities an organization should do to get ready to safeguard against IS threats in such panic situations?

P6 – "Proactively put contingency plans and workarounds in place to safeguard customer data and organizational data for unknown risks like COVID-19 is needed for any organization to plan for threats in advance".

P8 – "Yeah. organizational readiness like I said, unless it's a mature company, I am sure in the current scenario everybody was caught off guard ok! no body and it literally happened suddenly like - OK starting next week we will all work-from-home. So that way Org readiness was not even there or was not even envisioned, the only people probably who were able to make it happen... some of those financial companies for those kinds of companies who literally planned for those DR - Disaster recovery, disaster continuity management, so those kinds of companies had something in place and make it smoother for them, but not anybody else".

P9 -"The idea is to be ready always, not when a situation arises. That is what the pandemic situation has shown. Be ready for zero-day threats".

How do you define readiness from Org perspective?

P6 – "Proper security processes, implementation of standard security tools, strict compliance enforcement, continuous patch updates, employee training, constant awareness of new breach vectors".

P1 - Assume Zero Trust (ZTM) and don't allow employees to use official laptops to personal use!!"

P3 –" For readiness I believe in having a proper monitoring tool which goes a long way".

P4 – "OR is the first line of defence in this case there are lot of layers within the system security and network, right? so that is the first layer to protect our network!"

P6 – "As a first incident response, we had enabled Hot lines in case if there is any issue, the employees should first reach out to the hot line provided to them".

P1 – "OK! OR means the organization is ready to take up any risks, and it can counter it! risk of cyber-attack - for countering it we have put in place a better firewall *protection, better AV – Anti-virus applications, and we should be working constantly on the bugs if any , the bug fixes will be from a good partnerships with the vendors who supply such applications Like McAfee etc".*

P2 – "I think in my initial response on OR, I mentioned CIA... So based on that if I want to, you know ensure that the organization is ready for information security threats,.. the first one is confidentiality, that is I think the biggest of these.. for that we already have a very experienced team in place.. when even before adopting a Technology like encryption , so what we did is like once we moved to WFH model, we realized that there is a greater of risk of people like misplacing the laptop and all , employees used to travel to their home towns etc .. , So we implemented the automatic encryption technology, which allowed us to mostly automatically lock the laptops whenever there was any unauthorized activity being reported. So this way .. and robust Firewall protection along with secured network access and VPN together we were able to dynamically prepare for any such malicious activities. But this was possible as we are a financial institution and hence budgets were not an issue!! we had the right infrastructure base, and we did not have much challenges technically and Technology plays very critical role in readiness!"

Readiness with respect to People, Process and Technology any thoughts on these?

P1- "The priority for me would be first Technology, second People and then the process, I will tell you why? First you should have ... what kind of technology do we implement, because based on the type of Tech you educate your employees, that why we have the e-Learnings right? Every employee has to mandatorily undergo e-Learning and these e-learnings are monitored by HR. So even if there is a non-compliance from any employee, the business head of the VP of that particular process is answerable to that, so we take this very seriously, we often conduct this, 2 days trainings to educate our employees about the Technology that we are using, what are the ups and downs what are we supposed to do in case of security breaches and then finally establishing a processes. I think once you know that your technology is correct, that your people are aware of it you can easily set up the process and you know working on it to improvise based on the needs of the business and data today change in environment".

P3 – "For readiness process - have the right kind of talent, I think in our country we do have lot of talents, who help set up these kinds of technologies. Be more proactive - know what is exactly happening in the world. Always tie-up with reputed vendors, if *you are taking a third-party service. To add with that I think, you know you can always go for a reputable system security software, encryption methods and implement proper Firewall protection levels".*

On readiness not all companies can afford right? your thoughts on this?

P7 – "Cyber security readiness - planning and implementation is a pretty elaborate affair, and expensive too. not all organizations will be able to invest on both resources and training for information security".

P2 – "I believe that information security is as much a Function of employee awareness and usage of best practices as the implementation of various tools in the computing infrastructure".

P6 – "Most of the orgs were not ready during COVID-19 for WFH - Readiness by training and awareness, your thoughts on this? for small and medium enterprises".

P10- "This, IMO - might have been true of most of the small and medium enterprises. But I believe larger enterprises were well prepared".

Appendix F Interview summary of RQ3

We asked this question - How organizations assess their readiness? what are the factors to consider for assessment?
Participants P10,P6,P8 expressed their views as below

"Readiness assessment? I would suggest like you know .... having access to the right kind of technology and having implementation plan, like people who know how to use the technology and implement it, making your resource planning like you should know how much resources to be deployed to maintain the particular security system and this way you can assess where you stand on readiness."

"Continuous security audits, compliance audits (implementation, training)".

"From Organization perspective for readiness assessment in any environment, primary components need to be how well it has equipped with safeguarding Technology? how to update or patches, because if the technology is outdated it may not have the capacity to protect itself against new threats. The people using the tech needs to be more updated and aware, so knowledge and training coupled with updates or patches to the latest versions needs to be monitored and assessed."

"Assessing readiness in organizations to safeguard against IS threats – Ah.. I view this as a comprehensive process which can have a checklist from People, Process and Technology view".

Appendix G Interview summary of RQ4

Challenges to implement ORE

Narration by participants P2,P4,P6 ,P7 is provided as below

"Yeah, Basically the degree of perception of people is one thing which I could make out from what you mentioned and the employee willingness itself, All right? Has one of the things and monitoring of those is mandated. I think in general these are the important challenges with people."

"In my experience I see employee adherence as an issue when any process change is implemented, so the change management process is what we need to be robust and communicated till the last employee is compliant."

"First of all I have not heard of a term called "organizational readiness" , or we might have used another term in our organization, hence if at all this term is used then we should begin by defining it and then communicating I can see this as a challenge in change management process."

"Challenges for implementation of any new process will be an impact to all the departments in our organization. Hence, I see people challenges, technology training etc, establishment of support groups and management support."

"I see apart from our people, process and technological impact of any new process implementation, I also believe that we have third party contractors who work with us, also have to be considered and assessed for the challenges to implement OR process, like onboarding them, training them sign required NDA and legal documents etc."

"I agree there will be challenges on implementing the readiness processor framework - would like to add employee attitude to adherence to the policies and OR process, security policy etc. is what I can think of."

"Instead of naming this organizational readiness, can we put this under the best practices for readiness? in this way we would not re-invent the readiness concept? Also, it would be easier if we add the readiness as a best practice in organizations and a critical Organizational characteristic, right?"

"The challenge in my organization is, people due to convenience of getting things done quickly, or lack of time, people feel any process as a burden! example even security policy adherence, people have lazy attitude, hence have a light weight and basic readiness process for a better compliance rate."

“hmm.. not really a challenge in .. for example, we had a change in security policy during the pandemic, we added a few user-friendly rules but a policy which is of highest standard which will ensure a secured culture. From Technology standpoint we built a new user interface which was welcomed by the employees, hence a security policy which is robust but having employee friendly usage helps a lot. Hence from the challenges perspective I say if we have to implement a change it should be user friendly.”

Appendix H Interview summary on Best practices - Organizational

One of the participants P1 says as follows, which reflects on organization's policy
"Some companies, I mean it, but I think some companies have gone to the extent of even ensuring that they give a box to the employee with a good connection, and then they've configured it for them in a way when at home".
"So, I am actually saying, there are some companies, are, really following a method where they kind of give a secure Wi-Fi connection and configured it in a way where they can monitor".
This can be affordable by bigger organizations but for smaller ones it's still a struggle, but as compared to a compromised device, it's better to have such best practices.

Organization's Monitoring policy

Participant P1's response:

"All your monitoring thing has been reduced. Now you cannot really monitor everything. What happens on my laptop when I'm working from home, these are the problems"?
"Monitoring is really important. Training all employees is very important and monitoring provides information on an insider to do something malicious is really important. If there's a chance of an insider causing a problem, it is most of the attacks happening from an insider, finding that bad element by monitoring is important and is a CISO's nightmare."
"In the office it was a controlled environment but now at home it's tougher"
Monitoring over a VPN and beyond enterprise firewalls is a challenge to this policy but as a best practice organization should take a tough stand to add this monitoring policy and use relevant technologies for preventing any security incidents.
Training and security awareness policy
Organizational policies should include training and awareness as a continual process and monitor its employees for completion of mandatory trainings and compliance and it's a kind of enforcement there is no other way to bring secure work culture!

As per participant P6

“Yeah. so the only thing that this situation has brought in, is some of the training and awareness nuances has to be formalized into work culture, because going forward you will face your challenges, similar challenges and the model of work is going to turn into hybrid model so this is not like task phase that you have just crossed it and everything will be back to old status , no this is the new normal now.”

This thought emphasizes the need for training and awareness policy to be of high importance.

“We can have organizational policies to include such important policies but in practice we see employees tend to deviate the policies and it’s a very difficult question to answer, as participant

P6 says so”

“So, the reason is that from a pure employee perspective most of them do or do not realize the repercussions of loss of data and loss of reputation. They are not too aware of the impacts of what happens, they feel that doing these things is burdening. In addition, when they are actually on official work that they are assigned to do, they are bound to cut corners.”

Also, same thoughts are from participant P5

“Extra burden on them. They think it infringes on their freedom.”

So, what practices can help here? As participant P5 reinforces the use of a visible tool, can help here.

“We have an internal wiki detailing Security Best Practices across different niches and domains (mobility, web application development). We keep this wiki updated. We also mandate employee training through LinkedIn learning courses”.

While wiki come from old school, but still its use as a mandatory practice of having wiki documented in organizational policy seems to be relevant in this situation too.

Other practices at organizational level can include as participant P5 asserts in strong voice

“Policies, procedures, manuals, therapeutics like security titbits popping up on people’s lap top , reminding them always helps in reinforcing .. security tips delivered through the screen savers etc matters a lot in as organizational practice and form security circles to implement at ground level in the organizations and a highly placed

peer reporting to avoid insider threats should get us better in readying the organization and adoption as a best practice .....”

These statements and novel thoughts of moving towards building security culture in

Organization from ground up, can help in employees owning the security and develops “security by habit”.

Zero trust management as organization’s policy

Trust no one or no device policy at organizational level seems to be the echo and voice of most of the participants.
Though the participants believed zero trust management as a policy can help, it brings out a very important point on “budget constraints” and return on investments (ROI).
Adequate security budget as organizational policy

Onboarding third party contractors: Security binding organizational policy

On this question what’s the best practice which can help prevent third party contractors or suppliers from breaching security?
To conclude on the third-party contractors to be bound by the organizational policy which lays down the steps the contractors to strictly adhere to and monitored by competent authority pays back to the organization, if not for creating separate offices for contractors for working or remote working.
At this point we reached a saturation on the responses for managerialor organizational practices hence we concluded.

As participant P5 puts with clear voice

“Laptop, VPN most important no BYOD, adopt zero trust ...”

As per participant P6
Zero trust? that makes sense, from a long run perspective it's a good answer but however to get it in practicality for every organization is next to impossible depends on

how big an organization or what is the kind of work they do I guess when its UI kind of work etc ,so is it worthwhile? what is the ROI to do all of these?..”

Though the participants believed zero trust management as a policy can help, it brings out a very important point on “budget constraints” and return on investments (ROI).
Adequate security budget as organizational policy

The security budget should be adequate enough to accommodate the costs of technology products which are of utmost relevance, not all technologies need to be procured!

P5 puts it like this

“Employee training, building internal security tool sets (if budget permits) - which our organization does.”

While allocating adequate budget is important as a policy, but as P5 puts it, it’s equally important to building internal tool sets, building them inhouse can be an organizational best practice call to employees, which can spring up innovation from employees to build their own tools instead of buying costly tools. Also, this is a very important managerial aspect of digging into their teams to unearth the hidden technical talent, which can help in developing inhouse tools for security.
Onboarding third party contractors: Security binding organizational policy

On this question what’s the best practice which can help prevent third party contractors or suppliers from breaching security?

P6 says

“Now the line is getting blurred, because a contractor or internal employee is legally bound by the contract, but he is not, he is no different from an internal employee or contractor.”

P1 says

“A lot of companies, what the clients(contractors), they do work for, we have some things in place. Best practice in place, the thing is, you have a good organizational environment that people are like outsourcing companies like Infosys, and Wipro. They create a separate office for a particular client. People come to office work and then go. Some of them even have a requirement that they leave mobile phones outside, it’s possible in big companies and not for small companies.”

To conclude on the third-party contractors to be bound by the organizational policy which lays down the steps the contractors to strictly adhere to and monitored by competent authority pays back to the organization, if not for creating separate offices for contractors for working or remote working.

At this point we reached a saturation on the responses for managerial - organizational practices hence we concluded.

Appendix I Interview summary on Best practices -Technical

Password rotation

Participant P6 asserts

"Forced password rotation , sometimes whatever that minimal password length all those kinds of password rotation , password strength you will have to enforce, there are things certainly it is not possible but to that extent possible, we should try to see what is the login logout time and what are being accessed, which will hold good even when you are at office but more so when its home , in office at least you had option of doing some firewalls via proxies for access we could prevent from certain sites to be accessed, but protect the systems within your organization because it can contain malware, phishing all of those, when people working from home all these firewall kind of endpoint security is left up to them which is difficult to enforce with this being the criterion its lot more challenging and lot more.. more potential of having security issues .."
"Yeah.it can be as simple as changing your password every month, nothing has happened in the last three years why should I change?"

While strict policy of password rotation should be enforced, the above statements bring out employee attitude towards the adherence to technical practices which has to be dealt with some form of deterrence policy, hence here we see a mix of both organizational, technical practices converge here and should be built into the work culture.
Technology driving the environments at home

P7 says
"The Technical environment I am assuming is more on software aspects some of the things holds good when you are in office or home depends on environment you are , while on one side of the it's more like a work life balance people at least tend to have a differentiation between office and home , now that has got blurred in the big picture , what you say office environment or home environment that has got blurred or merged now so that has also" happened somewhere like a mixed bag some of it were not expected some were good and some were not.."

Technology in this context means the software to be used when people work-from-home. The restrictions administered through endpoint management - to use only approved software on the laptops is one of major voices we heard. Even if you allow personal devices provide the OS and image which can be downloaded through your own private cloud. This can be the takeaway for small and medium organizations.

IP address, authentication, Identity and Access management (IAM)

"No not more access privileges you just. your authentication has to be more expanded and more robust like if you are working from office you can say access to AWS server can be only from this IP ,now we have to give individual access to all the people who need access to servers , one might be their Wi-Fi if it's not a static IP it keeps changing , you might have to keep changing IPs for giving access so that has brought in little more effort on the management side because at the end of the day people still need access."

"We have added the IP address management to the whitelisting best practice. 2 FA two factor authentication and multi factor authentication are preferred. While weighing the cost factor 2FA is not costly whereas MFA can be costly, hence weighing based on the ROI is important small and medium organizations. usage of IAM – identity and access management can be inhouse of through AWS amazon web services or GCP – Google cloud platform".

Individual device management

P1 points to the following narration

"Lock your systems if you are not working on them".
"No be it laptop or mobile phones all the same , that means more or less the similar, whether they work from office or not , and from software aspect is, everybody is a professional whose working for the company so ideally they say or it is said that if you not are in front of the system you lock it and go about doing your other work, in home you tend to be in a different kind of environment, so you may or may not lock your

computer which will also mean that it's a potential hazard and there will be others at home going and coming who are ideally not bound by the NDA or the confidential contracts of the organization.."

Managed Endpoints and Encryption

P6 says

"For example, we made sure that people take the laptop outside and all that, and if the laptop gets stolen. We did the endpoint security encryption, endpoint was encrypted, the laptop was encrypted."

"You use more stronger encryption method at home and that can be done is what we are following."

Endpoint encryption is a best practice, some organizations follow this but for small and medium organizations need to balance the costs.

Managed endpoints and usage of endpoint management software

P7 says

Oh, managed endpoint? Yes, that helps to the limitation of what it used to be in office, the same thing it does here in the new condition. It does help to some extent, I am sure there are challenges and then just managing it over a VPN connection for everybody, products like ePO e-policy orchestrator will help for sure but using this kind of products over VPN has to be explore or might have been solved by now."

"Now there are EDR (endpoint detection and response) solutions, right? Others are there, but I think for those, people have to install EDR solutions, which is an integrated solution that has both data collection in real time and continuous monitoring." "Might be costlier for small organizations."

P7 also talks on the same practice

"Being a product manager, I follow and promote best practices like, VPN,2FA, encryption and EDR solutions from Technology standpoint"

There are a number of tools which can help, but as said earlier the best practice is to develop internal tool sets which can overcome any budget constraints.

Software OS updates, security patches updates

What bubbles up as a common security issue?

P2 had responded as

“Not having good antivirus installed on business endpoints, not updating authorized OS patches, antivirus updates regularly, absence of multi-factor authentication, improper authorization implementation, not being aware of the usage context - personalor business.”

Strong enforcement through the endpoint management software to do routine health check if the OS patches, security patches, antivirus updates are done and force the updates is a deemed technical best practice.

Routine Security Audits

P2 says

“Continuous security audits, compliance audits (implementation, training), Proper security process, implementation of standard security tools, strict compliance enforcement, continuous security patch updates, employee training, constant awareness of new breach vectors.”

“Today, compliance is a standard procedure and can be outsourced. However, if costs are a factor, then one has to trust employee actions and remind regularly.”

The health check of all the endpoints are a must and this a healthy practice.

IP-whitelisting

P6 says,

“We can avoid security issues if the employee’s devices with proper authentication and authorizations policies are in place and there is a proper white-listing mechanism for consulting organizations.”

While the best practice of IP whitelisting for contractors is considered, organizations also can review if it can be applied for their employees?

Providing Laptops with organization's configured image

As P4 says

"All the laptops are VPN configured and secured organizational image is on all the devices and the employee will have no freedom or options to invite a threat."
This also applies to contractors as per participant P4
"All the contractor laptops and systems are secured as per the IS policies and standards with secured image and VPN configuration."
Monitor, Monitor, Monitor as a best practice

P7 says
"I believe in monitor, monitor and monitor!"

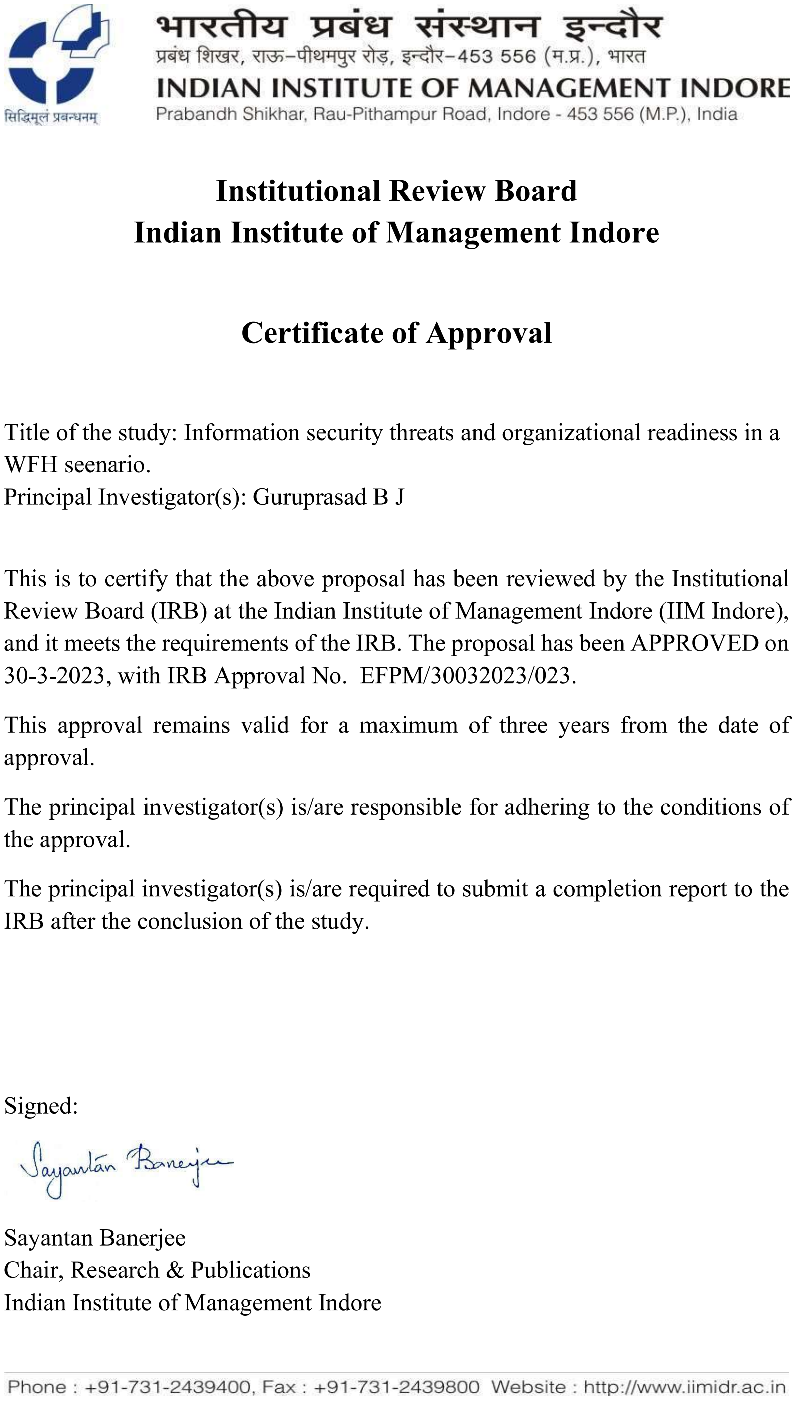
P3 echoes the same

"*Monitoring antivirus console on regular basis, Monitoring DLP breaches, is very critical apart from other monitoring for compliance".*
To conclude monitoring is very critical regardless of employees work location, more so when then work from remote. This needs support from top management on allocating budget required for such tools or for inhouse development is again reiterated here.
We reached a saturation on participant's responses at this point and hence we concluded.

Appendix J - List of Abbreviations

Abbreviation	Expansion
BYOD	Bring Your Own Device
BPG	Best practices guide
CIA	Confidentiality, Integrity, Availability
DDoS	Distributed Denial of Service
ISM	Information systems management
IAM	Identity and Access Management
ISA	Information Security Awareness
ISE	Information Security Education
IST	Information Security Training
IT	Information Technology
IS	Information Security
RBAC	Role Based Access Control
RDP	Remote Desktop Protocol
VPN	Virtual Private Network
ZTM	Zero Trust Model
nWFH	new Work-from-home
WFH	Work-from-home
MAM	Mobile Application Management
BPG	Best Practices Guide
TMT	Top Management
MDM	Mobile Device Management
MFA	Multi-factor Authentication
MIM	Mobile Information Management
NIST	National Institute of Standards and Technology
OT	Operational Technology
ORE	Organizational Readiness
OS	Operating System
SME	Small and Medium Enterprises
VOISM	Voice of Information Security Managers

Appendix K - Institutional review board approval letter



सिद्धिमूलं प्रबन्धनम्

भारतीय प्रबंध संस्थान इन्दौर
प्रबंध शिखर, राऊ–पीथमपुर रोड़, इन्दौर–453 556 (म.प्र.), भारत
INDIAN INSTITUTE OF MANAGEMENT INDORE
Prabandh Shikhar, Rau-Pithampur Road, Indore - 453 556 (M.P.), India

Institutional Review Board
Indian Institute of Management Indore

Certificate of Approval

Title of the study: Information security threats and organizational readiness in a WFH seenario.
Principal Investigator(s): Guruprasad B J

This is to certify that the above proposal has been reviewed by the Institutional Review Board (IRB) at the Indian Institute of Management Indore (IIM Indore), and it meets the requirements of the IRB. The proposal has been APPROVED on 30-3-2023, with IRB Approval No. EFPM/30032023/023.

This approval remains valid for a maximum of three years from the date of approval.

The principal investigator(s) is/are responsible for adhering to the conditions of the approval.

The principal investigator(s) is/are required to submit a completion report to the IRB after the conclusion of the study.

Signed:

Sayantan Banerjee

Sayantan Banerjee
Chair, Research & Publications
Indian Institute of Management Indore

Phone : +91-731-2439400, Fax : +91-731-2439800 Website : http://www.iimidr.ac.in