Barriers to the Implementation of Work from Home in the Indian BPO Sector

Permindersingh Manjeetsingh Bandesha
School of Art and Creative Technologies
The University of Bolton
Deane Road, Bolton, BL3 5AB

Thaier Hamid, PhD
School of Arts and Creative Technologies
The University of Bolton
Deane Road, Bolton, BL3 5AB

Anchal Garg, PhD
School of Arts and Creative Technologies
The University of Bolton
Deane Road, Bolton, BL3 5AB

ABSTRACT
The digitalization of workplaces has contributed to a load of new strategy models and management options in recent years. Even though India has seen a spectacular rate of ICT (Information and Communication Technologies) adaptation, impacting millions of lives in the process, working from home is a new concept in the Indian BPO sector, with incomplete academic and professional research on the topic. This study will discuss the extremely likely elements that are potential loopholes in a BPO company's decision to implement Work from Home and discusses the importance of management in maintaining security infrastructure and attempting to prevent the BPOs' database from becoming infiltrated and misappropriated used at any given time. Because it is critical that everyone in an organization works together and comprehends one another, the research is carried out to analyze and suggest modifications in the way data and formal communication should be communicated between the management and distant employees to encourage transparency and minimize misunderstanding in the organizational system, as well as to help in saving time and reduce the likelihood of compromise on accidental exposures and data security.

Keywords
Data Security, Business Process Outsourcing (BPO), Work from Home (WFH), Working from Remote Locations, Data Vulnerabilities.

1. INTRODUCTION
Data security risks have long been a source of concern for multinational corporations and have been thoroughly investigated. It is widely acknowledged that data security risks in Business Process Outsourcing (BPO) are continually rising and require an ongoing evaluation and relative upgradation in existing security systems whenever needed.

It is the company's duty to maintain its clients' data safe and secure. However, with time the amount, quantity, and quality of data generated by various techniques have increased, and the vulnerability to data theft has seen a massive and ongoing upsurge. [1]

India has traditionally provided a hub for outsourcing from most Western countries. Aside from foreign countries, Multinational Companies in India outsource a large portion of their work to BPOs throughout India. While outsourcing minimizes the client company's extra burden by delegating tasks to the BPO company, it also increases the likelihood of data security breaches because the information from the parent organization must be shared through data-sharing agreements with the agent (BPO) company, even though there is a written agreement between the corporates, but the possibility of misunderstanding and potential loopholes cannot be eliminated. The introduction and a potential increase in the trend of working from home in India is a cause for concern to be researched regularly, as India's BPO handles a large share of the world's business process outsourcing business.

Even though WFH was largely adopted due to corporates' inability to manage their offices due to the current crisis, companies are keen to continue with the WFH even after the crisis has passed, as corporates with previous WFH Provisions proved sturdy throughout the massive and unexpected socioeconomic crisis, Previously, investments in WFH infrastructure were seen only in multinational corporations; however, the necessity of WFH in the BPO sector has been seen in recent years as working from a conventional office seemed to be inconceivable. This resulted in a struggle to adapt to WFH and the technological development and infrastructure required for the purpose. [2] [3]

With recent developments in business models, the phenomenon of the remote workplace and working from home seems to be having a huge impact on companies, but the degree of concern related to the notion of WFH in India has not gained the attention it deserves in professional Literature and is an important area of questioning for many reasons. Primarily with massive amounts of sensitive data moving outside of the boundaries of the worksite across a wide range of devices and borderless teams spanning entire cities, states, and frequently countries, it is critical to investigate this issue. [4] [5]. The misuse of remote work alternatives must be secured in every way possible because the risk of an unknown person accessing company information without being detected by the CSO, CISO, or other cyber security professionals will always exist, but with WFH, the risk increases as stealing IP addresses and credentials is not a new problem, [6].

It would also be beneficial to comprehend how management illustrates its effectiveness by keeping fair treatment in mind when allocating work, analyzing, and reviewing the productivity of remote employees.

2. BARRIERS TO THE IMPLEMENTATION
With the acceleration of the adoption of work-from-home (WFH) practices across the globe, the barriers to implementation deferred in various countries and locations, and developing countries like India have faced many technical challenges that affected the smooth implementation of work-from-home. From being able to obtain reliable and affordable

internet connectivity to limited availability of appropriate technology and equipment that may lead to bigger threats such as the increased risk of cyber-attacks, data theft, and data breaches as cybersecurity is a major concern in WFH. while WFH has become the new normal, it is critical to recognize the challenges that India has been facing in putting this model in place. The research is focused on highlighting the major barriers to the implementation of WFH in Indian Business Process Outsourcing (BPO) as an integral part of keeping client data secure while providing quality service from home and other remote locations.

2.1 Technological barriers due to demography.

Companies must ensure that employees have been equipped with the appropriate equipment to work remotely and help them transition from the office to working from home. not only by securing the data in the clouds and servers but also by providing new equipment in the form of secure and high-speed Wi-Fi connections during the initial stage of the hasty implementation of WFH. As the companies would have to allow confidential information access in employees' homes, they would have to invest a large amount in providing the right security software and technologies to keep updated the computers, laptops, and all other electrical gadgets being used to access the client's data [7]. According to the Economic Survey 2016-2017, an estimated 9 million people migrated within India, primarily to metro cities such as Delhi and Mumbai, followed by Bangalore and Chennai from smaller cities and towns and even villages, and approximately 144.4 million people are employed in the service sector, with the Indian BPO sector employing over 4.5 million people [8] [9]. It is comprehensible that, with the reverse trend in migration and employees desiring to work from home, the investment to provide secure solutions for work along with up-to-date technology in a brief timeframe would be a massive task and would remain a challenge in the future with advancement in work from home due to India's uneven demography.

2.2 Finding reliable Wi-fi.

Companies must ensure that employees have been equipped with the appropriate equipment to work remotely and help them transition from the office to working from home. not only by securing the data in the clouds and servers but also by providing new equipment in the form of secure and high-speed Wi-Fi connections during the initial stage of the hasty implementation of WFH. As the companies would have to allow confidential information access in employees' homes, they would have to invest a large amount in providing the right security software and technologies to keep updated the computers, laptops, and all other electrical gadgets being used to access the client's data [7]. According to the Economic Survey 2016-2017, an estimated 9 million people migrated within India, primarily to metro cities such as Delhi and Mumbai, followed by Bangalore and Chennai from smaller cities and towns and even villages, and approximately 144.4 million people are employed in the service sector, with the Indian BPO sector employing over 4.5 million people [8] [9]. It is comprehensible that, with the reverse trend in migration and employees desiring to work from home, the investment to provide secure solutions for work along with up-to-date technology in a brief timeframe would be a massive task and would remain a challenge in the future with advancement in work from home due to India's uneven demography.

2.3 Security on BYOD and mobile devices is uncertain.

Employees are more susceptible to vulnerabilities in BPOs in which they are permitted or advised to choose their own devices for work. Reduced BYOD and mobile device security is a persistent danger that businesses face. Some of the constraints with using personal devices are ambiguous guidelines of usage, insufficient knowledge about remote access, limited security control, and fear of privacy breach, and all these can be instrumental in the occurrence of malware, phishing, or any other form of social engineering attacks [12]. The possibility of using a personal device and a public Wi-Fi network raises the possibility of a potential vulnerability, which can expose vital data to threats. The use of personal devices expands an organization's security perimeter and has a negative impact on its security policy; therefore, organizations must keep everyone informed about the risks and threats associated with the use of personal devices for office work. These personal devices can be double-edged swords; despite their potential benefits, they also raise issues that outweigh their benefits [13].

2.4 Inadequate data access, backup, and recovery systems.

The BPO's security policy helps determine the rights and limitations for data access from servers based on job responsibilities and the organizational security policy. It prevents employees from accessing data they do not need, and so it helps to keep intruders from unethically accessing resources. However, the software as a service should be sufficiently flexible to enable the company to keep the data secure while also offering access to the data to multiple employees at various remote locations [14]. Because of the large number of remote connections, it is difficult to keep track of the exact location from which the data is accessed. Similarly, if a cloud service provider is hired, data centers in more than one geographical location are maintained, resulting in several security challenges and threats. Traditional security features such as firewalls, host-based antivirus systems, IDS, and IPS are not always capable of providing adequate security in remote working [15].

2.5 Double the burden of investment in 0n-premises and off-premises security.

Data assets are more valuable and vulnerable than it has ever been, and incidents involving data security harm companies' reputations, disrupt operations, and are exorbitant; consequently, such security breaches and vulnerabilities have raised data security to the top priority of the CIO. While providing access to data through the cloud helps reduce capital and operational spending, in the long run, security breaches remain a major concern in the WFH scenario, as the negative impact of one data breach can result in reputational, moral, and financial damages to the BPO [15]. As a result, the burden of protecting and securing data in the office and with employees working from home becomes an additional burden for the BPO. The highest priority would be to train employees to recognize and report security breaches as it is essential to assure customers, client companies, stakeholders, and other affiliates that the critical data handled by the BPO will be secure and that they can trust the BPO with the information and its ability to keep it secure even in remote locations. As a result, the BPO must inform and educate not only the employees but also the customers.

2.6 Collaboration and communication

It is a significant challenge to maintain those in a company connected through a secure communication channel in Work from Home because in earlier circumstances meetings in office spaces were secure because meetings were done physically and therefore any misconceptions and confusions were easier to clear but with changing situations, it is practically impossible to work from home except if employees are given a secure and reliable videoconferencing and briefing channel [16]. Even as keeping agents connected is essential, this does not mean meeting them virtually daily but instead ensuring that they are kept up to date with all the information and knowledge that they need to be cognizant of. Unnecessary conferences will not only adversely affect them Psychologically, but also increases the likelihood of data security breaches; therefore, it is advised to reduce the number of unnecessary meetings with employees, and this needs to be planned as precisely as possible [17]. Effective communication is a major necessity of any establishment, and every organization has a different and complex communication pattern, and the communication behavior among the employees makes a huge impact. It is particularly important during organizational restructurings, such as the adoption of a new work culture, because the communication process has a significant impact on employees' comprehension, mindset, and commitment to the changes in an organization and its functioning [18]. Communication in physical proximity is very simple, quick, and reasonably secure because all communication is secure between the people entitled to know it, but due to the physical distance between WFH employees, an encrypted communication solution is very important. Because virtual communication through

3. METHODOLOGY AND IMPLEMENTATION

It is critical to understand and use the appropriate research methodology, as the methodology chosen must be capable of supporting, facilitating, and helping in the completion of the research with accurate and factual results. The ability to choose among various methods, the best blend that would fulfill all the research needs is the key to excellent research [20]. The data will be collected using semi-structured Interviews and questionnaires, interpretivist approaches will be crucial in the research. A comprehensive and In-depth analysis of the gathered data will be possible with the mixed approach, and it will also help to illustrate a clear view of the key factors related to the security risks in WFH in outsourcing and its implications [21]. To test the hypothesis, data collected through semi-structured interviews and semi-structured questionnaires can be analyzed using inductive coding on the Qualitative Data Analysis Software "NVivo." The Student T-test method will be used.

4. FUTURE SCOPE OF STUDY

Where WFH has provided benefits in certain areas it has also brought major concerns towards data security in the BPO Sector of India. This research related to the barriers in implementation will play a pivotal role in further investigation of the major security problems and challenges (Technical and Non-Technical) related to WFH post-implementation of WFH across India because data security and human behavior are a perennial concern and there is always a possibility of new threats at any time. Therefore, understanding the barriers to the implementation of WFH will help in researching the undermining threats that can adversely affect the concept of WFH in the future and this in turn will further help in researching and suggesting solutions to tackle the threats and vulnerabilities while conducting WFH.

5. CONCLUSIONS

At the completion of the research and analysis of this study, this research will be useful in a sector that employs over one million people in India and more so in other countries. Remote work or WFH processes will be Investigated and evaluated more carefully, critically, and frequently. Because WFH is a relatively new concept in India, research on this sensitive subject is limited.

6. REFERENCES

[1] Lobschat, L. et al., 2021. Corporate digital responsibility. Journal of Business Research, Volume 122, pp. 875-888.

[2] Bai, J. J. et al., 2021. Digital Resilience: How Work-From-Home Feasibility Affects Firm Performance, Cambridge, Mass: National Bureau of Economic Research.

[3] George, G., Lakhani, R. K. & Puranam, P., 2020. What has changed? The Impact of Covid Pandemic on the Technology and Innovation Management Research Agenda. Journal of Management Studies, Volume 57, p. 1754–1758.

[4] Yasir, S. & Kumar, H., 2020. Indian Call-Center Plot Fooled Americans into Paying Over $14 Million, New Delhi: The New York Times.

[5] Kamurthi, R. T., Chopra, S. R. & Sharma, R., 2021. Confrontation-Wi-Fi Risks and Data Breach. Pune, India, IEEE.

[6] Lund, S. et al., 2021. The future of work after COVID-19, Place of publication not identified: McKinsey Global Institute.

[7] Kaushik, M. & Guleria, N., 2020. The Impact of Pandemic COVID -19 in Workplace. European Journal of Business and Management, 12(15).

[8] Anoop, K., 2020. Impact of Migration of Labour Force due to Global COVID-19 Pandemic with Reference to India. Journal of Health Management, 22(2), pp. 181-191.

[9] Ammachchi, N., 2020. India's IT/BPO Industry Faces Large Scale Layoffs. [Online] Available at: https://nearshoreamericas.com/indias-it-bpo-industry-faces-large-scale-layoffs.

[10] Borkovich, D. J. & Skovira, R. J., 2020. WORKING FROM HOME: CYBERSECURITY IN THE AGE OF COVID-19. Issues in Information Systems, 21(4), pp. 234-246.

[11] Wang, L. & Alexander, C. A., 2021. Cyber security during the COVID-19 pandemic. AIMS Electronics and Electrical Engineering, 5(2), p. 146–157.

[12] Alotaibi, B. & Almagwashi, H., 2018. A Review of BYOD Security Challenges, Solutions and Policy Best Practices. 1st International Conference on Computer Applications & Information Security (ICCAIS), pp. 1-6.

[13] Palanisamy, R., Norman, A. A. & Kiah, L. M., 2020. Compliance with bring your own device security policies in organizations: A systematic literature review. Computers & Security, Volume 98, p. 101998.

[14] Ghani, A. et al., 2020. Issues and challenges in Cloud Storage Architecture: A Survey. Researchpedia Journal of Computing, 1(1), pp. 50-64.

[15] Subramanian, N. & Jeyaraj, A., 2018. Recent security challenges in cloud computing. Computers and Electrical Engineering, Volume 71, pp. 28-42.

[16] Parthasarathy, A., 2020. Coronavirus Challenge-Propelling a New Paradigm of Work from Home., s.l.: Science Reporter.

[17] Hancheng, C. et al., 2021. Large Scale Analysis of Multitasking Behavior During Remote Meetings. s.l., Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems, pp. 1-13.

[18] Zito, M. et al., 2021. Does the End Justify the Means? The Role of Organizational Communication among Work-from-Home Employees during the COVID-19 Pandemic. International Journal of Environmental Research and Public Health, 18(8), p. 3933.

[19] Khandelwal, M., 2020. Work from Home: Meeting the Change in Workplace. Research Reinforcement, 8(1), pp. 82-89.

[20] Dźwigoł, H., 2019. Research methods and techniques in new management trends: research results. Virtual Economics, 2(1), pp. 31-48.

[21] Khaldi, K., 2017. Quantitative, Qualitative or Mixed Research: Which Research Paradigm to Use? Journal of Educational and Social Research, 7(2), pp. 15-15.