IRO Journal on Sustainable Wireless Systems (ISSN: 2582-3167)
www.irojournals.com/irosws/

Future of Secure Remote Workforce Perspective - What's Next?

Duraisamy Balaganesh

Lecturer, Faculty Computer Science and Multimedia, Berlin School of Business and Innovation GmbH, Potsdamer Straße, Berlin, Germany

E-mail: duraisamy.balaganesh@berlinsbi.com

Abstract

Recently, finding a connection between changes in work habits and the controls put in place to handle cyber security threats is an innovative area of study. Surveys and conversations with subject matter experts are utilized to gather data. Since many employees struggle with the psychological and emotional aspects of working remotely, employers and information security managers are expected to continue to devote more resources to mitigating human-factor threats, which have multiplied during the COVID-19 epidemic. Consequently, the research has focused on approaches to manage or enhance security in the light of the COVID-19 pandemic's impact on present cyber threats and issues. Moreover, this article consists of various perspectives such as remote work environment, privacy authentication procedure and future security procedure.

Keywords: Cyber-security, phishing, work from home, remote work, authentication privacy

1. Introduction

Recently, companies throughout the world have implemented massive remote workforce relocation in response to the COVID-19 epidemic. What was once a "nice to have" for workers and employers is now a necessity, with many businesses throughout the globe moving their whole staff to distant locations. In response to the shift, businesses rethought their cyber-security strategy, implemented new safeguards, and revised their rules to ensure that remote workers had secure access to the data and systems they needed to do their jobs [1-5].

Uncertainty has been the theme of 2018, but one major trend has emerged: the rise of the hybrid workforce of the future. Employees who have worked remotely for a while anticipate being able to do so when COVID pandemic gets over. This includes being able to

DOI: https://doi.org/10.36548/jsws.2022.3.002
Received: 01.07.2022, received in revised form: 11.08.2022, accepted: 25.08.2022, published: 05.09.2022

do so from any location and using any device. Because of this, it's more important than ever for companies to re-evaluate their cyber-security measures, particularly if their executives are striving to create robust organizations. For organizations, security may serve as a vital link in the chain of resilience by allowing them to operate with more agility and a focus on protecting the cutting edge and the future. A person working from home has been shown in figure 1.

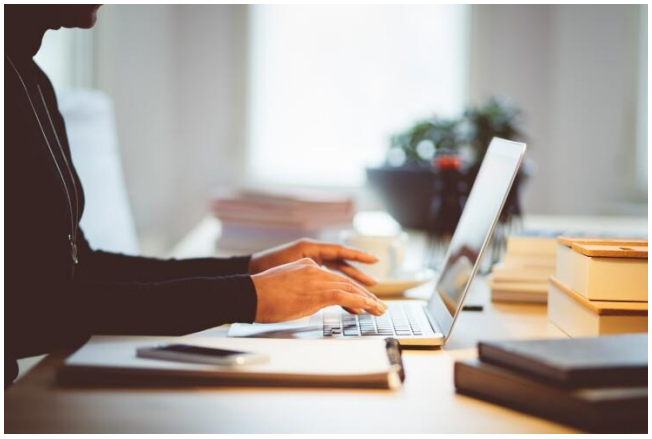

Figure 1. Work from Home (WFH)

To a large extent, many of us are able to work as usual, thanks to today's state-of-the-art technology. The availability of affordable computer power, cloud services, and high-speed Internet connections makes remote employment a viable alternative that might help mitigate the global health issue.

Since the coronavirus has disrupted regular habits, the next several months will be difficult practically for everyone on the planet. Teachers and students will work together from afar. Employees will carry out their duties from the comfort of their own homes, and CEOs will make decisions from the sofa rather than the conference room.

The cyber workforce is growing, but it must be cognizant of the new threats face. It also needs to be on the lookout for any suspicious activity online, since remote work is becoming the norm in businesses of all sizes. Important measures to take for our internet security are outlined below.

1.1 Privacy password

To this day, passwords are still the first line of defences in preventing unauthorized access to vital computer systems and programs. However, things become much more complicated when it has to trust on the safety of every worker's own wireless network. It is

made sure that the home router's password is difficult to guess and does not include any identifying information. As often as feasible, two-factor authentication (a password and another piece of information, such a text message) is used. Because of this, users of cloud-based apps that facilitate the sharing of data and documents have access to the information they need.

1.2 Phishing

More people going online means more opportunities for scammers, social engineers, and phishers. Criminals and hackers utilize people's fears about viruses and their voracious need for news to deceive them. An email should never be opened without first hovering the mouse over the sender's name to verify its legitimacy. When it comes to ransomware, most emails are bogus. Before replying to any emails, a security professional has to look them over. It is important for businesses to designate a single point of contact for all employees to report phishing or ransomware incidents. These efforts at education and dissemination will help staff members become more familiar with the methods currently being used by cybercriminals.

Managers have taken an interest in remote work since the advent of modern ICTs. This kind of employment goes by a number of different names [1–5]: remote work, telecommuting, virtual work, mobile work, and flexible work. The term "Remote Work" (RW) refers to a flexible work arrangement in which an employee is permitted to perform their job duties from a location other than the company's headquarters or production facilities, while still maintaining contact with their co-workers using electronic means of communication [6].

Despite the various drawbacks, researchers suggest that flexible work arrangements, such as remote employment, will continue [5]. Employees gain from remote work, but it may have both good and negative consequences on an individual's well-being [7 - 10].

2. Secure Remote Work Force

2.1 Monitoring remote worker performance

The necessity for continuous monitoring of remote worker performance and the pursuit of novel remote work efficiency techniques has arisen. More monitoring has shown to be counterproductive for distant employees [11, 12], but information exchange and other types of engagement are found to be just as effective in achieving the desired outcomes.

Evidence suggests a major role for the situational leadership style, popular in the USA since the late 1960s. Leaders may use it as an acceptable technique to influence their staff outside the office to boost productivity [13]. However, studies also reveal that not all management techniques result in optimal performance from either remote workers or supervisors.

2.2 Cyber-security strategies

There is a need to adapt to the demands of a more mobile workforce in the near future. The concept that workers may remain connected and productive despite spending significant time away from the workplace has been mainstreamed. Thus, many companies will probably adopt a hybrid approach to the workplace that accommodates both on-site and off-site workers. Increased diversity in the workplace and better business and human capital options are two outcomes of this. Cyber security issues, such as keeping organization operational in a drastically altered setting or safeguarding access on a larger scale than ever before, have emerged as a result of the sudden transition.

Workers are gaining access to business apps in the cloud through their personal devices, connecting to them via their homes' Wi-Fi or other external networks. The security and IT departments are being placed under intense pressure to handle an increasing number of remote employees and their devices in a secure manner.

2.3 Administration and management

The employee is now responsible for having access to all policies and controls, regardless of whether they are in the company's headquarters or not. However, there is a downside to having the option to work from home i.e., cybercriminals have ramped up their phishing attempts in an effort to steal sensitive information from users, infect the systems of the new remote workforce with malware, and take advantage of any resulting security holes.

Flexible hybrid workforces thrive when there is enough time for planning, teamwork, and employee agency. The problem of how well-balanced businesses have adjusted to the recent overnight shift to remote employment is a key takeaway from the last eight months. The same holds true for the possibility of an increase in the quantity and kinds of cyber security assaults; however, improved cyber security measures that enable these arrangements, have made it simpler for enterprises to cope with this possibility [14-18].

Recently, the remote workforce IT departments must ensure that all employees may securely and reliably access all company resources whenever they need them. No longer can

it treat security, networking, and collaboration as separate entities. They need to cooperate to achieve their goals. Along with these duties, leaders must also establish new enforcement methods and strengthen cyber security rules. Because investing in a strong security culture is so important, that this must be accompanied with a solid staff education program.

The resilience of businesses must be built on the foundation of stronger cyber defences that are both targeted and effective. Long-term remote work has raised the profile of cyber security inside companies, and this is likely to result in structural changes to how those companies approach cyber security in the long run. A lot of people have also said they want to boost their cyber security budgets in the future, which is encouraging. When it comes to leading a digital transformation, security must be at the forefront of IT executives' minds. By doing so, it can guarantee the safety, scalability, and flexibility of these initiatives. When trying to lessen the possibility and severity of a cyber-security breach, businesses should also look for methods to simplify their cyber security procedures. Simplifying the path to better security assures that it will be a business enabler, rather than a barrier to meeting current and future demands [19].

2.4 Limitations

According to the authors, there are several caveats to the provided findings. The poll was done at a time of epidemic. Companies that had to rely on telecommuting or other forms of remote employment during the epidemic were represented in the study. But that time, the constraint was temporary and didn't prompt business owners to rethink their approach to telecommuting. For instance, economies of scale could not be realized at this time owing to inadequate office space. Another drawback is that big corporations, which often have fewer limitations, such as financial circumstances connected to remote work assistance, were overrepresented in the survey sample. Results may have been impacted due to the sample size.

3. Securing Home Network

The security of home networks is not intrinsically weaker than that of commercial networks. A lot of individuals don't bother with the basic precautions necessary to keep their home networks safe. There isn't much use in doing so for individual usage rather than securing the account with a password. However, there are certain extra safety measures to be taken while utilizing a home network for professional purposes. The default router password should be changed to something more secure. An Internet Service Provider (ISP) could

provide a configuration page where it can make these changes. If it does not, then it may reach the router's configuration page by entering IP address into any browser's address bar. This page may also be used to enable network encryption. It should be avoided letting friends and family use work computer. It's possible that family members have set up a home group so that various computers and gadgets may freely exchange data and software. This is a security risk if use personal computer or laptop for professional purposes.

3.1 Restricting Access to Unauthorized Users

And this brings us to the central problem of working from home i.e., limiting access to outsiders. People might be fooled into thinking that home office is safer against intruders. In the best of circumstances, it may be challenging to keep children out of a home office. But this is a very real problem for commercial enterprises. Data security regulations mean it can't just hand out passwords to loved ones at home. As an extra layer of protection, a home router may be set up to only allow connections from authorized MAC addresses. Companies should treat each request for access from the outside as if it was the first one they've ever received and verify the identity of the user every time.

3.2 Remote Monitoring Security Apps

An effective antivirus and anti-malware suite must be installed on all company-issued devices. Scheduled updates from main server are recommended. In addition, internal systems should verify the security of a device before allowing it to access. Some workers may see remote monitoring applications favourably, while others may view them as Big Brother-like surveillance tools. However, they may be useful for employers that want to make sure their staff members aren't jeopardizing the security of the company network in any manner. By opening potentially dangerous emails or visiting potentially malicious websites, they provide a back door for attackers. When an employee utilizes corporate hardware, it has a far greater leeway in installing and using such surveillance software. Employees who are informed in advance and given an explanation for the change are more likely to accept it.

4. Observation and Inferences

4.1 Key Findings

There is still some variation in the degree to which hybrid workplaces are being adopted throughout developed countries. The worldwide average of firms using a remote workforce before the pandemic was 12%; however, when the epidemic struck, that number

has jumped-up to 60%. Many businesses of nearly 33%, in many developed countries, are planning to maintain a remote workforce after COVID-19. This number is the double of what it was before the epidemic.

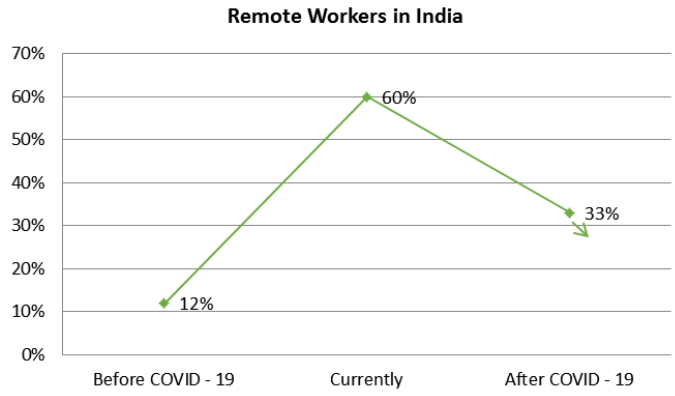

Figure 2. Remote Workers in India

4.2 Challenges of Cyber-Security in a Remote Work Environment

There are only a few potential dangers that office's IT security staff can prepare for. The hazards increase when it brings that setting inside someone's house, and the odds are less consistent from one instance to the next.

However, acquiring a home office is not an insurmountable challenge. This only indicates an increase in the variety of dangers that must be taken into consideration. It is usually a good idea to start with a clear cyber security policy for remote personnel to follow.

4.2.1 Cyber security

As more people working from home are on the go, businesses in India are facing a new wave of cyber-security threats. The majority of businesses propose that ensuring secure access to their networks is their biggest cyber-security concern. Concerns over data privacy, which may have an impact on security as a whole, and the controls and enforcement policies in place are also on the rise.

4.2.2 Endpoint security protection

Nearly half of the Indian organizations were vulnerable to endpoint security risks because employees took company devices home and used them for personal use, therefore evading standard cyber security protections that were not designed to accommodate remote workers. The majority of remote workers and remote workers' personal devices are the most hardest to secure, which is consistent with a worldwide trend [20 – 24].

Around 45% of Indian businesses found it difficult to secure client data while working remotely, and 25% found it difficult to secure cloud apps. Although these numbers were lower than the worldwide average, they were nonetheless respectable. The percentage levels of security risk concern faced by Indian companies during WFH are shown in figure 3.

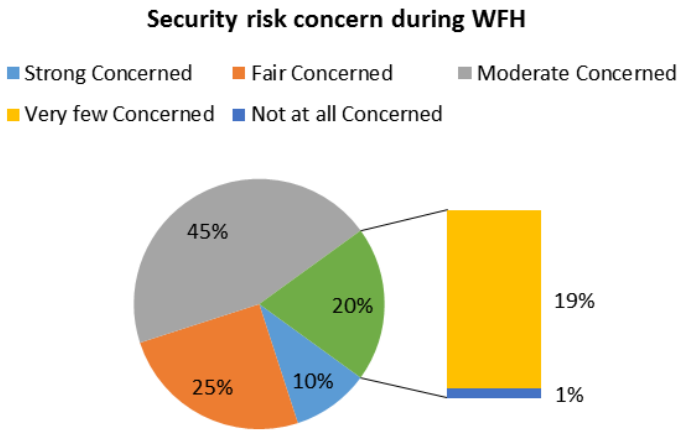

Figure 3. Security risk concern during WFH

4.3 Future Security Procedure

Considering workplace, many of the IT security measures it takes as a matter of course may be just as effective when it is not physically there. Example: Good data security measures are effective everywhere they are implemented.

4.3.1 Create a policy to protect data

Starting with a well-defined cyber-security policy is essential, as discussed before. It's likely that operate under some kind of IT policy that all recruits are required to sign off on. A matching record may be made for the off-site setting.

Staff members' attention may be maintained on security measures if they are aware of what is expected of them. The more relaxed setting of a home office might make people less careful with their data. The workers will be more secure if the steps of policy's implementation are planned out.

4.3.2 Safeguard Webcams

The security of a system may be compromised by the use of an external device, such as a camera. With regards to webcams in particular, it is recommended that always keep the lens covered while not in use. If need more specific guidance is required on additional external devices, organization's IT security staff may be contacted.

4.3.3 Virtual Private Network (VPN)

The use of a Virtual Private Network (VPN) for security purposes is becoming a normal practice in the IT industry. When workers do so from off-site locations, additional precautions must be taken to protect the confidentiality of the VPN connection. Undoubtedly, already there is a system in place wherein workers need to provide login information (usernames and passwords) before they can access the network. An extra layer of protection must be added by using two-factor authentication in conjunction with this. Then, the staff may use VoIP phone systems or something similar to double-check logins.

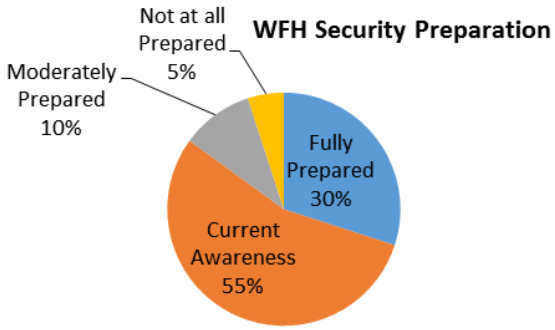

Figure 4. WFH Security Preparations

4.3.4 Securing Information Centrally

It should be made sure that the working staff isn't putting critical information elsewhere except in centralized repository. Always remote backup options, such as the cloud or a server must be available. Staff members should be aware that they should never keep company information on their personal computers. It needs to be periodically updated.

4.3.5 Continuing dedication to cyber security policies

The majority of companies will need to quickly adapt their cyber security policies to accommodate this significant transition as they continue to safeguard remote employees. Despite being the lowest of the three areas compared to the worldwide average, 93% of Indian businesses have reported updating their cyber security plans.

4.3.6 Increasing cyber security expenditure in a methodical but preventative manner

Most of the Indian businesses (56%) said that the COVID-19 incident will lead them to boost spending on cyber security in the future. Despite having the lowest percentage of firms wanting to increase such investments, this is a positive development. Therefore, the

biggest percentage (30%), of firms in India said they would make no changes to their expense on cyber security which is shown in figure 5.

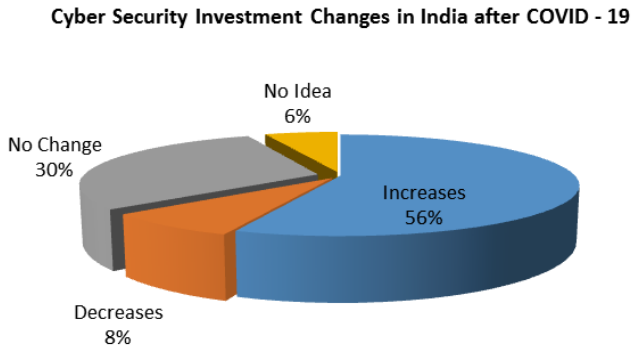

Figure 5. Changes in Cyber security Investment

4.4 Future Authentication Procedure

This is the first logical step in safeguarding a remote workforce, since it allows verifying the identities of workers requesting access to company resources.

4.4.1 Connect to a Virtual Private Network

It creates a protected channel between the user and the software, allowing remote employees to keep working and communicate with their office. It also helps in ensuring that only authorized users have access by providing an adequate degree of security without negatively impacting the user experience [25].

4.4.2 Make use of Domain Name System

The DNS layer is the first line of protection since most security breaches occur at the endpoint. This foundational layer prevents access to known harmful sites and can even detect and quarantine malware that has already made its way onto the network.

4.4.3 Endpoint security software

While the goal of endpoint security is to prevent cyber-attacks, it may also be used to quickly identify, contain, and remove dangerous files that have breached other layers of protection and made their way towards endpoints.

4.4.4 Increase the use of cloud-based security measures as a strategic priority

The security of workforce is ensured by this solution's ability to provide a consistent connection to apps regardless of the user's physical location or operating system. Greater

advantages can be gained from current product set by adopting a platform strategy. By doing so, it can view all security solutions in one place and integrate them with those of other providers.

4.4.5 Automation of the Security Operation Centre

To improve productivity and accuracy while decreasing operating expenses, this process is utilized for threat research, hunting, and remediation. This further facilitates security teams' ability to respond to shifting business and technological requirements and remain ahead of an ever-evolving threat scenario.

4.4.6 The human element is often the strongest part of any defence

Employees should be encouraged to learn more about cyber security and given more responsibility. Workers need to be made more aware of the need of adopting security-centric habits including being able to recognize phishing attempts, using strong passwords, and updating software. It's not enough to have a yearly, mandatory, and unpopular cyber security course that nobody attends. It has to be institutionalized as well.

5. Conclusion

The cyber-security must be at the core of every IT expenditure if organizations are to provide employees with the freedom to work safely from any location using any device. A platform-based strategy that offers top-notch security at every level of the network, the endpoint, and the cloud is required. This research article has discussed many challenges in various fields such as remote work environment, privacy authentication procedure as well as the future security procedure.

References

[1] Popovici, V.; Lavinia-Popovici, A. Remote work revolution: Current opportunities and challenges for organizations. Ovidius Univ. Ann. Econ. Sci. Ser. 2020, 1, 468–472.

[2] Allen, T.D.; Golden, T.D.; Shockley, K.M. How effective is telecommuting? Assessing the status of our scientific findings. Psychol. Sci. Public Interest 2015, 16, 40–68.

[3] International Labour Organization. Defining and Measuring RemoteWork, Telework,Work at Home and Home-BasedWork. COVID-19: Guidance for Labour Statistics Data Collection. 2020. Available online: https://www.ilo.org/global/privacy-policy/lang--en/index.htm

[4] Soga, L.R.; Bolade-Ogunfodun, Y.; Mariani, M.; Nasr, R.; Laker, B. Unmasking the other face of flexible working practices: A systematic literature review. J. Bus. Res. 2022, 142, 648–662.

[5] Mustajab, D.; Bauw, A.; Rasyid, A.; Irawan, A.; Akbar, M.A.; Hamid, M.A. Working from Home Phenomenon as an Effort to Prevent COVID-19 Attacks and Its Impacts onWork Productivity. Int. J. Appl. Bus. 2020, 4, 13–21.

[6] Sutarto, A.P.; Wardaningsih, S.; Putri, W.H. Work from home: Indonesian employees' mental well-being and productivity during the COVID-19 pandemic. Int. J. Workplace Health Manag. 2021, 14, 386–408.

[7] Klopries, T. Discussion of "Working from Home—What is the Effect on Employees" Effort? Schmalenbach Bus. Rev. 2018, 70, 57–62.

[8] Sarstedt, M.; Ringle, C.M.; Hair, J.F. Partial least squares structural equation modeling. In Handbook of Market Research; Homburg, C., Klarmann, M., Vomberg, A., Eds.; Springer: Berlin/Heidelberg, Germany, 2017; Volume 26, pp. 1–40.

[9] Yang, L.; Holtz, D.; Jaffe, S.; Suri, S.; Sinha, S.;Weston, J.; Joyce, C.; Shah, N.; Sherman, K.; Hecht, B.; et al. The effects of remote work on collaboration among information workers. Nat. Hum. Behav. 2022, 6, 43–54.

[10] Parker, S.K.; Grote, G. Automation, algorithms, and beyond: Why work design matters more than ever in a digital world. Appl. Psychol. 2020.

[11] Carroll, N.; Conboy, K. Normalising the "new normal": Changing tech-driven work practices under pandemic time pressure. Int.J. Inf. Manag. 2020, 55, 102186.

[12] Manko, B.A. Considerations in the use of work- from-home (wfh) for post-pandemic planning and management. Management 2021, 25, 118–140.

[13] Adamisin, P.; Sindleryova, I.B.; Cˇ ajková, A. Coronavirus vs. real cause of the European Economic Crisi—Comparing Slovak and German national model example. Online J. Model. New Eur. 2020, 37, 178–1010.

[14] Sull, D.; Sull, C.; Bersin, J. FiveWays Leaders Can Suport RemoteWork. 2020. Available online: https://sloanreview.mit.edu/article/five-ways-leaders-can-support-remote-work/

[15] Father, R.S. Reflections on actual situation of collective bargaining for the public servants and public services in Romania and in Europe. A theoretical and practical approach. Jurid. Trib. 2021, 11, 251–261.

[16] Peracek, T. Human resources and their renumeration: Managerial and legal backround. In Proceedings of the 13th International Scientific Conference on Reproduction of

Human Capital—Mutual Links and Connections 2020, Prague, Czech Republic, 5–6 November 2020; pp. 454–465.

[17] Camacho, S.; Barrios, A. Teleworking and technostress: Early consequences of a COVID-19 lockdown. Cogn. Technol. Work 2022, 1–17.

[18] Arunprasad, P.; Dey, C.; Jebli, F.; Manimuthu, A.; El Hathat, Z. Exploring the remote work challenges in the era of COVID-19 pandemic: Review and application model. Benchmarking Int. J. 2022.

[19] Arunmozhi, M.; Kumar, R.K.; Srinivasa, B.A. Impact of COVID-19 on global supply chain management. In Managing Supply Chain Risk and Disruptions: Post COVID-19; Springer: Cham, Switzerland, 2021; pp. 1–18.

[20] Lewis, S.; Cooper, C.L. Work-Life Integration: Case Studies of Organisational Change; John Wiley & Sons: Chichester, UK, 2017.

[21] Yao, X.; Li, X.; Zhang, C. An experiment of the impacts of workplace configuration on virtual team creativity. In International Conference on Human-Computer Interaction; Springer: Cham, Switzerland, 2019; pp. 153–160.

[22] Choudhury, P.; Foroughi, C.; Larson, B. Work-from-anywhere: The productivity effects of geographic flexibility. Strateg. Manag. J. 2021, 42, 655–683.

[23] Richman, A.L.; Civiana, J.T.; Shannona, L.L.; Hillb, E.J.; Brennan, R.T. The relationship of perceived flexibility, supportive work—Life policies, and use of formal flexible arrangements and occasional flexibility to employee engagement and expected retention. Community Work. Fam. 2008, 11, 183–197.

[24] Bhattacharyya, S.S.; Thakr, S. Coronavirus pandemic and economic lockdown; study of strategic initiatives and tactical responses of firms. Int. J. Organ. Anal. 2021, 29, 1240–1268.

Author's biography

Duraisamy Balaganesh is currently working as a Lecturer in Faculty Computer Science and Multimedia at Berlin School of Business and Innovation GmbH, Berlin, Germany. His area of research includes web mining, IoT, data science, machine learning, blockchain, signal processing and data mining.