

Security vs. Flexibility : Striking a Balance in the Pandemic Era

Vaishali Soni

Department of Information Technology
Netaji Subhas University of Technology
Delhi, India
vaishali.it19@nsut.ac.in

Deepika Kukreja

Department of Information Technology
Netaji Subhas University of Technology
Delhi, India
deepika.kukreja@nsut.ac.in

Deepak Kumar Sharma

Department of Information Technology
Netaji Subhas University of Technology
Delhi, India
dk.sharma1982@vahoo.com

Abstract—

An organization's reputation is largely dependent on the work culture it provides to its employees. This is the reason, "flexibility" is becoming an inherent part of an employer's support to its employees. Due to the unprecedented outbreak of novel corona virus (COVID-19), most companies have adopted flexibility of working from anywhere, for their employees. This digital transformation took place almost instantaneously. Hence, neither the employees, nor the employers were fully prepared for this situation. This definitely makes our lives convenient. But there exists another side of the coin which is concerned with the security issues pertaining to use of personal networks and devices. The home network devices have not been configured to be secure in line with the employer's requirements. That is the reason, attackers have a larger surface to get their hands dirty on. This paper exhaustively describes the holistic view of security issues and challenges faced by employees as well as employers in remote working paradigm. This paper emphasizes on the cybersecurity threats which have emerged in this pandemic era. The work presents the challenges faced by the employees as well as their employers in these tough times. Then this paper discusses the sudden rise in volumes of cyber-attacks between January 2020 to March 2020. The company's evaluation of critical threats in the on-site working paradigm versus the remote working paradigm have also been described. Next, it describes the risks which might occur in the near future of the COVID-19 impacted world. Finally, the paper proposes some of the ways in which employers can strike an efficient balance between flexibility for employees and security of their assets.

Keywords— *cybersecurity, pandemic, COVID-19, threats, attacks, flexibility, remote working*

I. INTRODUCTION

In January 2020, World Health Organization (WHO) declared the COVID-19 outbreak a Public Health Emergency of International Concern (PHEIC) [1]. It has impacted the society significantly in many ways and brought about a digital transformation. As working remotely is the new norm, "security" has become more critical than it has ever been in the past. The pandemic era has changed the way the security is perceived and implemented by the organizations.

The initial form of flexibility introduced by organizations was by using the concept of Bring Your Own Device or BYOD. With this paradigm, employees are allowed to use their personal devices to access not only the corporate networks but also the confidential business data [2]. However, new security risks and challenges are raised with the use of BYODs [3]. Devices used under BYOD can easily be lost or stolen. Many threats and attacks including spoofing, phishing,

sniffing, spam, and denial-of-service have also been found targeting BYODs [3]. Corporate data can be leaked when accessing BYOD within or outside of emails [4]. Hence, organizations need to put proper security controls in place in order to secure themselves as well their data [2].

Flexibility in the workplace has been defined in [5] as "the opportunity of workers to make choices influencing when, where, and for how long they engage in work related tasks". It enables the employees to choose when and where they work. Thus, giving them time flexibility as well as location flexibility. However, the flexible work environments unknowingly raise new risks for the organization.

Security has always been an important aspect for the technology infrastructure of any organization. Earlier, managing the security was relatively easy, as all the critical data and applications were safe inside the data center. The aim was to protect the technology infrastructure, so that attacks could be prevented.

It is considered that the data inside the secure walls of the IT infrastructure set up by the organization is protected. Due to the outbreak of COVID-19, perimeter is dead and the organization needs to work towards security without boundaries. As more employers provide their employees with the option to work remotely, creating a secure pervasive technology infrastructure has become very important. In these testing times, the organizations must create a strong security culture and train the employees so that they can adapt to the rapidly evolving cyber security landscape.

This paper dives deep into the cybersecurity threats posed by the pandemic to the employees as well as employers. Then the digital transformation mechanisms adopted by the employers to deal with the situation are discussed. Further, the work highlights the cybersecurity issues that have emerged with this digital transformation mechanism. Next, some of the related work in this area have been discussed. Also, it delves into the types of risks which can be foreseen for the near future. Finally, the paper proposes the ways in which organizations can strike an efficient balance between flexibility and security.

II. OVERVIEW

A. Cyber Threats posed by COVID-19

When the World Health Organization declared COVID-19 a pandemic, organizations worldwide were faced with an unprecedented, sometimes nearly instantaneous, transition from on-site workforces to remote ones [6].

This digital transformation which was adopted by organizations was very much related to the sense of speed. The

aim was that the show must go on and the productivity of the employees should not be affected. Thus, this led to hastily developed authentication mechanism and missing some regulatory requirements which has unwantedly given birth to new risks. The aim was to maintain the continuity of work, and thus security of the assets took a back seat.

From the employee's perspective, the situation changed drastically without much time to prepare. Employees were not trained to understand the cybersecurity landscape. Employees had to make adequate arrangements so that they could continue to work remotely. The target was to be connected to the organization's network and obtain necessary remote access. In the urgency of getting the system into an up-and-running state, employees forgot about the security related concerns.

Fig 1. shows the threats posed by COVID-19 in terms of security for employees as well as companies [7].



 For Employees	 For Companies
Working Remotely , with access to company's data and application anytime, anywhere	Increased reliance on third party service providers and applications to assist transition to remote work environment
Connecting through home routers/wireless devices , without adequate security capabilities	Cybercriminals launching new phishing attacks to exploit the panic caused by COVID-19
Using the same device for accessing personal accounts as well as doing enterprise's work	Inability to perform security tasks and real time monitoring

Fig. 1. Threats posed by COVID-19 to employees and companies in context of security [7].

Thus, although flexibility to work remotely provides convenience to the employees, but it poses a lot of risks for the companies.

B. Challenges Faced By Employees

This section describes the problems that the employees are facing in this unprecedented situation of working remotely.

Lack of technical background: Many employees have limited technical background and hence found it challenging to understand the use of new tools like virtual meeting platforms.

Lack of preparedness: The employees were not prepared with security enabled routers/networking devices to securely access their office network from remote locations.

Restriction to use Virtual Private Networks (VPNs): In some hotels, or public places the use of VPNs is restricted, hence forcing the employee to use personal email account for corporate communication, which exposes the risk.

Using personal applications on their devices: The employees have the tendency of using personal applications like social media accounts or game playing applications on their devices, which increases the chances of injecting malware into company's data or programs.

Lack of awareness: Many times, the employees are not aware of the cyber security risk that might emerge due to their activities. For example, use of same password for personal social accounts as well as corporate accounts makes the corporate account vulnerable. Similarly, if the data is exchanged between an insecure ISP and the company's server, then there are chances of Man-in-the-Middle attack.

C. Challenges Faced By Companies

As mentioned in [8], the most valuable resource is data. Hence a majority of organizations in 2019, were spending 12% of their IT budget on Cyber Security [9]. This shows that the companies have understood the importance that the security of technical infrastructure plays in their success.

Just as the companies thought they had cracked the code and reached the level of securing their gems inside tall security walls, the unparalleled outbreak of COVID-19 has shaken the world of cyber security.

The major challenges that the companies are facing are mentioned below:

Shortage of Cyber Security Experts: The companies did not have adequate number of experts to instantaneously create a secure pervasive technology infrastructure which can prevent attack on their data.

Dependency on Third Party Tools: The companies did not have their own solutions for all requirements. So, they had to rely on third party applications for various tasks like organizing virtual meetings. This exposed the company's data on third party applications which is involves tremendous amount of risk.

Use of heterogenous devices: As employees are working remotely, the variety of devices being used has increased. With use of heterogenous devices, remotely enabling the same security standards on all of these devices is not possible for the experts as many of these devices are incompatible with the security enabled networking devices used by the company.

Lack of Employee's Training: With the sudden advent of events, companies did not have sufficient time to educate their employees with cyber security rules and regulations or train them for precautions required when working remotely.

Lack of IT Support staff: As the number of users increased manifold, the company did not have sufficient IT staff available to support other employees.

Lack of Security policies: Organizations do not have proper documents which state the rules and regulations related to secure ways of working remotely. Employees really don't know where to find answers to their concerns.

III. IMPACT ON CYBER SECURITY LANDSCAPE

Coronavirus pandemic has completely shaken the cybersecurity infrastructure across the globe. As can be observed from the previous section, neither the employees nor the companies were prepared to deal with this situation. Thus, this has given an opportunity to the attackers to exploit the vulnerabilities in the technological structure.

COVID-19 has expanded the horizons for the attackers as they have exposure to more devices and vast spread of network to experiment with. As organizations have moved their people to their home networks, hackers have adapted and moved quickly so that they can exploit the confusion. The cybercriminals are misusing the human's quest to read global news to spread malware and ransomware through fake websites.

There has been a steady rise in the cyber-attacks since the outbreak of pandemic. The various kinds of attacks include:

- *Corona Virus themed MalSpam Emails* were used to distribute malware and Trojans e.g. the Emotet banking Trojan [10].
- *Spam Emails* were designed to be from Centers for Disease Control and Prevention (CDC) to steal email credentials
- *Malware inside Interactive Map*: The cybercriminals exploited the users' quest for latest news related to COVID-19 by implanting an AZORult malware inside an online application masquerading as an interactive map showing spread of the pandemic across the globe [11].
- *Vishing (or phishing) Attacks*: Advance technology was used to use voice as a medium to execute the phishing attack. The target was to convince the receiver to give away their credentials.
- *Ransomware Attack*: A new ransomware strain dubbed as CovidLock was disguised as a coronavirus tracking app and distributed [11].

Fig 2. shows the kind of security attacks that are being used by the attackers to exploit the situation [11].

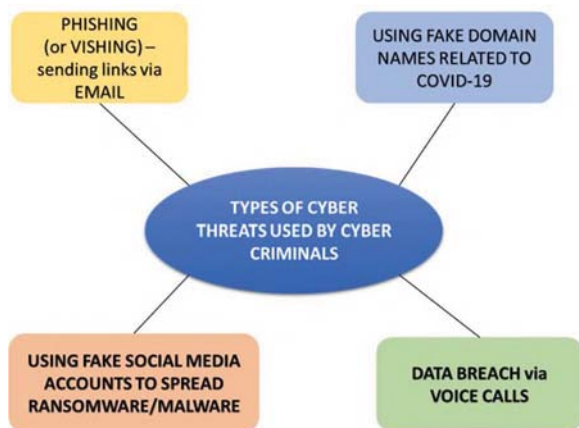


Fig. 2. Threat landscape in COVID-19 World[11].

As the COVID-19 outbreak reached India, the number of cyberattacks on Indian organizations doubled in March 2020 from January 2020[11]. This is depicted in figure 3.

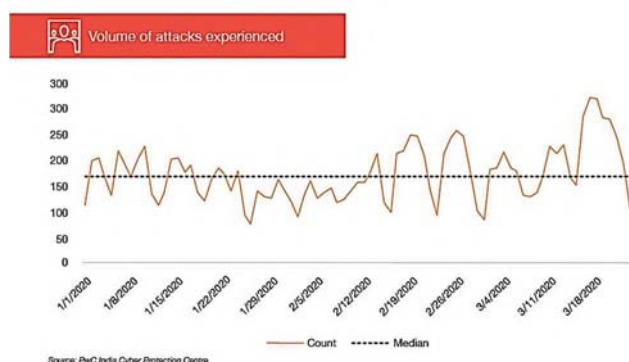


Fig. 3. Volumes of cyber attacks experienced by Indian Organizations in Q1 2020[11].

As per a survey conducted by Netwrix Research Lab which has been published in Cyber Threats Report 2020 [12], the remote work culture has brought about new trends in the threat landscape and thus, organizations need to re-assess their priorities to adapt to the new work-from-anywhere paradigm.

Fig. 4 shows how the critical cyber threats have changed for the organizations from the pre pandemic era (physical-office working culture) to the post pandemic era (remote working paradigm) [12].

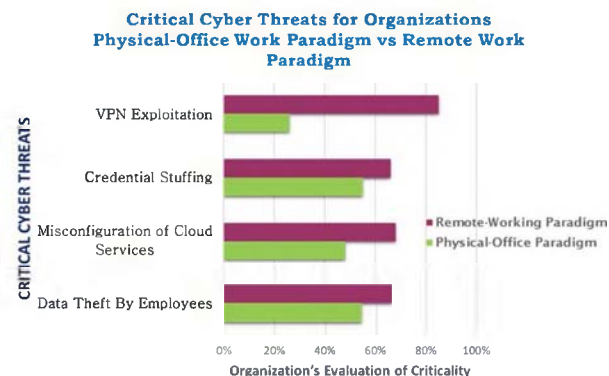


Fig. 4. Critical Cyber Threats in Physical-Office working paradigm vs. Remote-working paradigm [12].

Thus, it is observed that in order to protect their assets, organizations need to work toward inculcating a strong security technological infrastructure to deal with the frequently changing cyber-attacks landscape.

IV. RELATED WORK

As the change from on-site working to remote working took place almost overnight, not much preparation was possible for the organizations. However, the researchers have proposed some ideas which can help the organizations to appropriately cater to the need of the hour – remote working model.

Some of the mechanisms which can be used by organizations to be better prepared for managing few of the anticipated cybersecurity risks are :-

- *Phishing Detection Engine*: organizations can use machine learning techniques to create an engine which detects phishing emails and prevents them from reaching the employee's inbox. Scrum-based implementation to detect phishing has been discussed [13]. However, this is just a proof of concept using MATLAB, the same needs to be deployed and tested using open-source mechanisms like Python so that more organizations can benefit from it.
- *Build a Cyber Resilient Framework*: as discussed above, a lot of cyber attacks seem to be unavoidable in remote working paradigm, hence organizations must focus on designing a framework which focuses on being resilient to cyber attacks[14]. The infrastructure should be able to recover appropriately in case some security failure occurs.
- *Proper Incident Reporting Tools*: organizations must create proper Incident Reporting Tools which can help them to manage the security incidents efficiently. The tool would allow the organizations to reduce the time to detect the incidents and take appropriate corrective actions.

The above mentioned mechanisms are urgently necessary for organizations and research community must diligently work to find solutions to enable secure

remote work options for employees, which are convenient for employers also.

V. UPCOMING RISKS

The fact is that cybersecurity is an ever-evolving field and hence nobody can never reach the end of the tunnel. As the technology to defend attacks evolves, attackers find new tools to conduct their trials with.

This is an ongoing clash between the attackers and defenders. However, with the understanding of the present situation, the companies and workers can be prepared for the future risks which can be foreseen for the post pandemic times.

Here few known risks are highlighted which exist and can be used by attackers in near future.

- *Malware spread through deployed devices in deserted work spaces:* As the work spaces and buildings are deserted due to pandemic, attackers may attempt to use deployed devices like surveillance cameras, temperature monitoring sensors etc. in order to inject malware into the networks.
- *Data breach via Virtual Platforms:* Due to travel restrictions, organizations are dependent on virtual platforms for meetings and events, hence increasing the dependence on third party applications. Thus, it is possible for attackers to obtain critical information through these applications.
- *Intruders intercepting data due to improper authentication mechanisms:* The companies must adopt Multi-factor authentication mechanisms for securing their critical applications. This will help keep a track of the devices on which corporate data and applications are being accessed.
- *Ransomware attacks using Mobile Applications:* As the popularity of mobile applications increases, there are chances that hidden malware can be embedded inside mobile applications in order to launch ransomware attack on the network.

Organizations must aim to find ways to enhance their technology platforms and tools so that the security can be strengthened. Companies must plan adequate trainings for their employees so that they become watchful.

VI. TOWARDS SECURE FLEXIBLE WORK ARRANGEMENTS

The cybersecurity landscape is rapidly evolving and so the companies need to be prepared and well equipped to adapt to the changing scenario. In the pandemic era, attackers have been able to successfully exploit the vulnerabilities to some extent. Thus, it is important that companies wear their thinking hats and start developing new ways to protect their assets from being compromised.

Here are some points which if inculcated can help the companies to securely transition towards creation of secure flexible work arrangement.

- *Realize the importance of Cybersecurity and set up a secure network with the help of experts.* An organization may end up losing its assets if it underestimates the

consequences of a ransomware attack. Hence, cybersecurity must be prioritized in these testing times.

- *Access the security of each BYOD device before granting access to the enterprise's network [5].*
- *Use Mobile Device Management [MDM] tools like IBM MaaS360 to manage BYOD devices used by employees. [15].*
- *Use standardized secure remote access solutions like ZScaler [16]:* These solutions enable end to end security while using remote access.
- *Multifactor Authentication mechanisms while using remote desktop connections:* Use of hardware tokens or software tokens enable multifactor authentication for company's data and applications. This can be helpful when the device on which corporate access was being done is stolen or lost.
- *Configuring session timeout for sensitive applications:* In case of long period of inactivity, the session must be timed out so that unauthorized access can be prevented.
- *Categorize critical data to be accessible only via Organization's VPN and segregate it from data which is downloadable on personal device [17].*
- *All employees must undergo mandatory cybersecurity training* so that they are aware of the ways in which they might be attacked. Teymourlouei[18] provides a quick reference guide which helps users to identify and prevent cyber-attacks on their devices.
- *Ensuring adequate infrastructure setup to backup data periodically* – this will help in retrieving the important data in case of ransomware attack. Cloud-based services ease this task[19].
- *Proper policies must be created for creating efficient "flexible work arrangements".* Employees must be well-aware of the company's policies related to working remotely.
- *Proper platform to report phishing incidents:* Companies must have a platform through which any type of security breach incidents like phishing can be reported. Experts must provide possible solutions to deal with such scenarios. This helps in making other employees aware about existing threats.

In these challenging times, security becomes a shared responsibility. Hence, employees and companies must work together to be vigilant to secure the company's vital assets.

As companies provide flexibility to employees, their share of responsibility also increases. People are the most important resource for any organization. Thus, employees must make sure that they do their bit to contribute towards security of company's data and applications.

Employees can take care of the following aspects to make their contribution towards secure working environment.

- *Use Strong Passwords:* Most of the applications require authentication through passwords. Hence using strong passwords will prevent hackers or bots to be able to penetrate into the system

- *Always reset the default password provided by device manufacturers:* Nearly all routers come with default user name and passwords. The bad guys use this as the entry point to access the network configuration page. Hence using a different strong password protects the network manipulation by unwanted entities.
- *Keep different passwords for personal accounts and corporate accounts:* Many employees tend to use the same password for personal email accounts, social media profiles as well as corporate email address. If one account gets compromised all others are also at risk, hence employees should secure accounts using different passwords.
- *Don't click on unknown links:* Cybercriminals are well aware that people tend to click links when presented lucratively. Hence, you must avoid clicking links in emails or text messages which are sent by unknown senders.
- *Keep your software up to date:* Employees should always install important security updates immediately as outdated software are the backdoors for the cybercriminals

VII. CONCLUSION AND FUTURE SCOPE

The paper discusses the threats which have emerged in the pandemic era and the challenges faced by employees and companies worldwide in adapting to the digital transformation. It describes the cyber-threats landscape that has emerged in the first quarter of 2020. Further it highlights some of the risks that can be foreseen for the post-pandemic future. In the end, this paper mentions the techniques which can help the organizations manage security as well as flexibility. In order to change the future, humans must accept the challenges posed by the pandemic and make relevant changes to drive the technology around that. Cybersecurity is actually a problem of resilience. No system can be fully secure at all times, but the experts must think of ways in which it recovers in case of an attack. Organizations must formulate special teams to deal with adverse situations. The idea of "flexibility" is fascinating and convenient, but employees need to ensure that this does not "compromise" the security of the organization. With proper strategic planning, secure pervasive technology infrastructure can be built which will strike an efficient balance between flexibility and security. Success in cybersecurity is not the eradication of cyber threat or the corona virus, but it is about making sure that life can go on despite the challenges posed by the cyber threats or the virus. Thus, employees and employers must collaborate with each other to safeguard the flexible work arrangements.

In future, a ubiquitous secure technological system model needs to be developed which safeguards the company's network infrastructure as well as access to the confidential data. The model must take into consideration the use of heterogeneous networking devices used by Internet Service Providers as well as those personal devices used by employees. It must protect the devices from the predominant cybersecurity attacks and the known threats. New security related protocols and standards must be developed to provide end-to-end security from user's device to the company's network. This will help organizations to provide secure flexible work arrangements in the true sense.

REFERENCES

- [1] "COVID-19 Public Health Emergency of International Concern (PHEIC) Global research and innovation forum", by WHO [Online]
- [2] M. M. Ratchford and Y. Wang, "BYOD-Insure: A Security Assessment Model for Enterprise BYOD," 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ), Miami Beach, FL, USA, 2019, pp. 1-10, doi: 10.1109/MOBISECSERV.2019.8686551.
- [3] Y. Wang, J. Wei, and K. Vangury, "Bring your own device security issues and challenges," in *Consumer Communications and Networking Conference (CCNC)*, 2014 IEEE 11th, 2014, pp. 80-85: IEEE.
- [4] G. Disterer and C. Kleiner, "Using Mobile Devices with BYOD," *International Journal of Web Portals (IJWP)*, vol. 5, no. 4, pp. 33-45, 2013.
- [5] Bal, P.M. and De Lange, A.H. (2015), From flexibility human resource management to employee engagement and perceived job performance across the lifespan: A multisample study. *J Occup Organ Psychol*, 88: 126-154.
- [6] "Securely Transition to a Remote Workforce, A checklist to protect your employees", by Security Mentor, Inc. [Online] Available : <https://www.securitymentor.com/assets/site/assets/2020-Working-Remotely-White-Paper-Security-Mentor.pdf>
- [7] Chelly L. M. , Marsh Asia, "Session ID : SAO-W06V Managing security and flexibility in COVID-19 world" RSA APJ Conference 2020 [Online] Available : <https://www.rsaconference.com/apj>
- [8] "The world's most valuable resource is no longer oil, but data", *The Economist*, Report 2017. [Online] Available : <https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data>
- [9] Global Cyber Risk Perception Survey Report 2019, Marsh and Microsoft [Online] Available : <https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html>
- [10] KVN Rohit, Deccan Herald, February 2020, "Trojan alert : Hackers misuse coronavirus outbreak to spread PC malware" [Online] Available : <https://www.deccanherald.com/specials/trojan-alert-hackers-misuse-coronavirus-outbreak-to-spread-pc-malware-801155.html>
- [11] Gayal S., Maniar P., "COVID-19 Crisis The impact of cyber security on Indian Organizations", PWC Report April 2020 [Online] Available : <https://www.pwc.in/assets/pdfs/services/crisis-management/covid-19/covid-19-crisis-the-impact-of-cyber-security-on-indian-organisations.pdf>
- [12] "2020 Cyber Threats Report", Netwrix Research Lab, July 2020 [Online] Available: https://www.netwrix.com/download/collaterals/2020_Cyber_Threats_Report.pdf [Accessed : 9 November 2020]
- [13] D. Oña, L. Zapata, W. Fuertes, G. Rodríguez, E. Benavides and T. Toulkeridis, "Phishing Attacks: Detecting and Preventing Infected E-mails Using Machine Learning Methods," 2019 3rd Cyber Security in Networking Conference (CSNet), Quito, Ecuador, 2019, pp. 161-163, doi: 10.1109/CSNet47905.2019.9108961.
- [14] "Remote Working - Protect against Cyber-Attacks" Online : <https://theconversation.com/with-the-increase-in-remote-work-businesses-need-to-protect-themselves-against-cyberattacks-138255>
- [15] "11 Best practices for mobile device management (MDM)", by IBM [Online] Available: <https://www.ibm.com/downloads/cas/NP9KAQ0>
- [16] "Securing Remote Work : Safeguarding business Continuity with ZScaler", by ZScaler Inc. [Online] Available : <https://www.zscaler.com/resources/white-papers/securing-remote-work.pdf>
- [17] "The future of cybersecurity in Asia, Pacific and Japan – Culture, Efficiency and Awareness", A TRA report sponsored by sophos, August 2019. [Online] Available : <https://www.sophos.com/en-us/medialibrary/Gated-Assets/white-papers/sophos-the-future-of-cybersecurity-in-apj.pdf>
- [18] H. Teymourlouei, "Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users," *World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering*, vol. 9, no. 3, 2015.
- [19] C. Adams, "How to protect against ransomware," *bdtechtalks.com*, 22 June 2018.[Online]