An Investigation of Cybersecurity Issues of Remote Work during the COVID-19 Pandemic in Saudi Arabia

Gaseb N Alotibi[1], Abdulwahid Al Abdulwahid[2]
Faculty of Computer Science and Information Technology-University of Tabuk, Tabuk, Saudi Arabia[1]
Department of Computer and Information Technology, Jubail Industrial College, Saudi Arabia[2]
Royal Commission for Jubail and Yanbu, Jubail Industrial City, Saudi Arabia[2]

***Abstract*—COVID-19 pandemic has dramatically changed the public life style as well as the daily work activities across the world. This indeed has led both public and private sectors to attempt to adapt thereby shifting to remote work and adopting and enabling new technologies and online services in order to sustain their businesses while saving people lives. Unfortunately, a decent number of those endeavors have been undertaken unwarily in a hurry without taking the due diligence of all relevant aspects including cybersecurity and privacy. This survey aims at exploring the current state of the practice during the Covid-19 pandemic lockdown and the revolving challenges of using and publishing online services in Saudi Arabia. It also investigates the needs for investment in the cybersecurity field which would increase the trust on and reliability of them; and thus encouraging organizations to move confidently towards the real digital transformation.**

Keywords—Cybersecurity issues; investigative survey; remote work; COVID-19 Pandemic; Saudi Arabia

I. Introduction

COVID-19 pandemic has changed the life style of people in many aspects including social and work perspective. Indeed, the reliance on the Internet has become one of the daily life activities since the internet services have been used in most of the world countries. These activities include a variety of fields such as social network, entertainment, shopping, studying, and working. Therefore, about 4 billion users access the Internet, spending an average of 170 minutes daily – the majority of which was on social media [1]. However, the COVID-19 lockdown has forced the countries and their organizations in public/private sectors to empower remote working to keep their organizations running. Remote work is the means that allow employees to perform some or all of the work from home or any location other than their work site.

According to the statistical survey conducted by [2] to measure the remote system experience of epileptologists before and after the pandemic, they found that those who experience remote system have dramatically increased from about 63% to 86% within few months. In the UK, the remote working hits about 38% of the employees during the lockdown raising from 21% in 2019 [3]. This unforeseen noticeable changes in the policies and procedures of working that permeate over countries have made some challenges. These issues might be related to different aspects such as place, technology, and security. The Forbes survey of remote workers showed that 72% of employees are not working from a dedicated office place [4]. In addition, the majority of them (56%) has faced a difficulty to bring their work equipment to their homes. In the report published by Global advisory and accounting networks [5], cyber security concerns were raised thereby showing that nearly 65% of organizations announced they have been either breached or exposed to cyberattacks during remote work. On the other hand, about 13% of the organizations were not prepared at all, compared to 45% somewhat prepared and 42% claimed they have prepared very well for the transformation in the work manner. Consequently, the damage of their income was incredibly hard in the majority of organizations across the world. According to the Office for National Statistics (ONS), the UK economy is still not close to the pre-corona virus output levels [6]. The report anticipated that the damage of the lockdown just in April 2020 might hit 15 billion to 20 billion GBP. Globally, the crisis could lead over 2020 and 2021 to an overall loss of around 9 trillion USD which is greater than two countries’ economies such as Japan and Germany [7].

The cyber security aspect has been considered as main pivotal pillar in the remote work status. The struggle becomes clearer with the technology and security in response to the quick transfer in the work environment and probably paradigm. Indeed, the number of cyber attacks has dramatically increased to those organizations whilst processing information about the pandemic. For instance, during the pandemic crises, the World Health Organization (WHO) has mentioned that the number of cyber attacks to its staff and emails have surged more than five times compared with the same period a year before. Consequently, it is moving to a more secure authentication system after a leakage happened in its system [8].

Generally, the studies about the remote work have focused on the services that can be remotely provided. For example, [9] emphasized on some of the security challenges that need to be considered in each level of the cloud to secure the remote access to the site such as implementing and managing Identity and Access Management (IAM) systems. However, the pandemic incidence has forced organizations to think for a reasonable manner that can help in this partial or complete shift in their daily work. The author in [10] carried out a study focused on using PKI certificate and mobile device management platform to secure the organization system during this accelerating change.

In this work, we investigate the challenges that have faced organizations within Saudi Arabia during moving to the remote work. In addition, it is going to concentrate upon the cybersecurity aspect and to what extent it might be limiting and/or enabling remote work transformation. The subsequent section explains the design methodology of the conducted survey. The Results Analysis Section presents a detailed illustration of the responses received and then followed by exploring and discussing them and succeeded by some drawn conclusions with a set of relevant future directions.

II. Methodology

The survey was designed to explore and assess the maturity level of the organizations run in Saudi Arabia and its surroundings when they have moved to the remote work and challenges they have faced. Furthermore, it sought to explore the encountered information security breaches and utilized techniques during the COVID-19 pandemic. This was to answer the following research-related questions:

- What is the current state of the practice in the Saudi public and private sectors during the COVID-19 pandemic lockdown in relation to the growth of using and publishing online services and the revolving challenges and issues?
- Are cybersecurity concerns one of the vital issue(s) that may delay the digital transformation to online services?

A number of questions were devised and piloted with a number of specialized academic colleagues in order to obtain their perceptions on whether they are understandable and serve the purpose. After a few revisions based on the received inputs, the final version contained 28 questions and divided into four sections and structured as follows:

1) Personal demographic: Exploring the participants' demographic characteristics, related to gender, age, qualification, and job level.

2) Organization information: Establishing background of the organizations at which the participants work, in term of the type, field, size and location.

3) Exploration of the current state of the practice: Understanding technologies that were utilized into moving to remote work and during it, in addition to what extent online services have met the demand and requirements of stakeholders.

4) Investigation of cyber security related issues: Studying the reason(s) that has/have hindered or may hinder the growth of/ transformation to the remote work as well as security techniques that were used during it, their vulnerabilities and potential solutions.

The survey was set to be conducted over the Internet via an online questionnaire hosted by survey monkey website. Public users were targeted with three conditions: they are 18 years and above as well as were employees and worked in any means during the COVID-19 pandemic in Saudi Arabia. Those were recruited via e-mail besides other social media, such as WhatsApp, Twitter and LinkedIn from acquaintances and professional societies and groups.

III. Results and Analysis

A total of 300 participants completed the survey over a period of eight weeks, during which the survey was active. Table I depicts that the majority of them (49%) belonged to the age group of 30-39 years, followed by 26% from the age group of 40-49 years. A huge gap between the proportionality of male and female participants was observed. About 89% of the partakers were male, reflecting the unequal participation of the different genders. However, as the investigated aspects of this research related to the organizations' employees, it is more likely to be common practices regardless of the genders. With respect to educational qualifications, the majority of the participants held bachelor's degree, followed by Master's, and Ph.D. – indicating high literacy levels of them and hence high probable informed responses.

Moreover, the majority of the participants assumed high job positions including mid-senior (41%), director (21 %), and executive (7%) – showing good work experience and exposure with various areas of business operations. Accordingly, most partakers were working on the area of technology (30%), followed by 27% in education sector, and 12% in industrial field.

Fig. 1 shows that the participants were from diverse fields of work, representing more realistic and reflecting results.

TABLE I. Summary of Participants' Demographic Characteristics

Demographic Factors	Characteristics	Relative Frequency
Age	18-29	16.79%
	30-39	49.38%
	40-49	25.68%
	50 and above	8.15%
Gender	Male	89.38%
	Female	10.62%
Qualification	High School/ Diploma/ Associate Degree	6.91%
	Bachelor	39.75%
	Masters	30.12%
	PhD	23.21%
Job Position	Entry Level	11.60%
	Associate	19.01%
	Mid-Senior	40.99%
	Director	21.23%
	Executive	7.16%

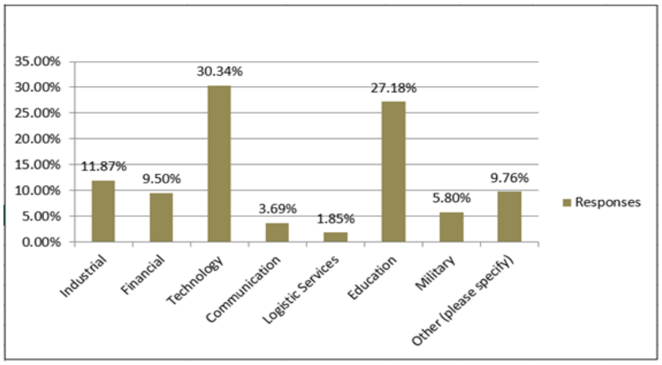

Fig. 1. Distribution of participants fields of work.

In addition, two thirds of the participants worked in public enterprises, while a third worked in private enterprises, indicating the distribution of participants in the two main sectors of the economy. In terms of the size of participants' organizations, 53% of the participants' organizations employed a thousand employees or more; 21% had between 100 and 999; and 19% had less. Thus, the size of the participants' organizations reflects the consideration of different small, medium, and large scale organizations, thus improving the analysis coverage of the results of this study.

Focusing on the strong technical infrastructure of the organizations that meets the needs of participants, it was identified that more than 77% of the participants stated that their needs were met. However, considerable number of participants (18%) were neutral, and about 5% stated that their needs were not met as illustrated in Fig. 2. Therefore, it can be a cause of concern for enabling and maintaining remote working conditions, suggesting a need for improvement in the technical infrastructure of the organizations.

Analyzing the use of devices in remote working conditions (as demonstrated in Fig. 3), it is identified that the majority of the participants relied on personal devices. 48% were using personal laptops, 17% personal desktop, besides 40% used personal smartphones/tablets for remote working. On the other hand, organizational laptops, desktops and smartphones/tablets were also being used by 48%, 23% and 10%, respectively. This increase in the use of personal devices for remote working may reflect the escalation in the security threats, as personal devices may be more prone to security attacks if proper security configuration is not maintained. Additionally, the diverse platforms usage indicates that most of the current remote workers probably own/use many digital devices with different operating systems and configurations –emphasizing the need to consider universal applicability as a crucial aspect in any proposed mechanism/solution.

Moreover, Fig. 4 represents the type of network connection utilized during remote working. The majority of the participants relied on private Wi-Fi connections (61%), indicating a more secured network compared to public Wi-Fi that was used by 6%. This may probably lead to potential security attacks that might affect the organizations and result in huge losses. Whilst 43% utilized Fiber Optic and 12% relied on broadband services, 44% used mobile internet services. The latter indicates the possibility effect on the work flow due to mobile low speed or loss of connection. In this context, only 22% of the participants strongly agreed and 49% agreed that their internet service provider has met their expectation in terms of speed and connectivity. In addition, almost 13% of the participants stated that their internet service provider did not meet their expectations, while 17% were neutral. These results indicate that the internet and communications infrastructure was not fully upgraded/reliable in order to meet the requirements of remote working system.

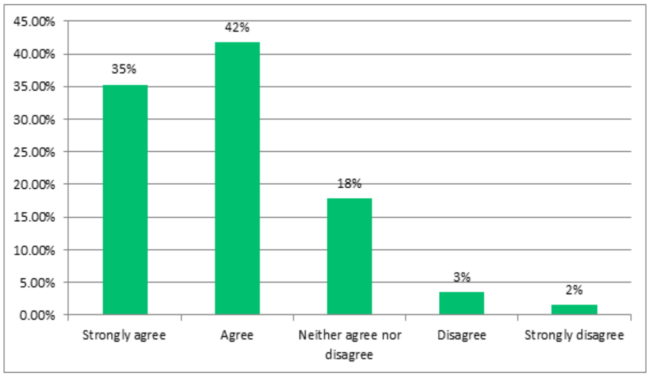

Fig. 2. The extent to which participants' organization meet their needs.

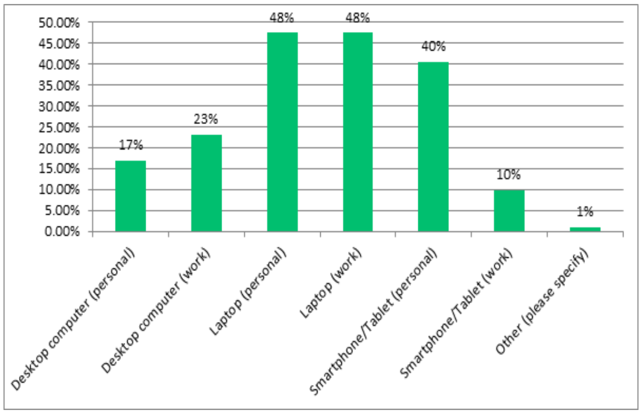

Fig. 3. Usage of digital devices during remote working.

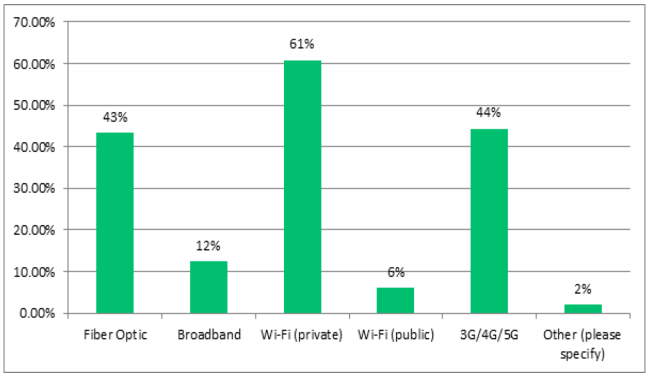

Fig. 4. Types of internet connections in use.

Considering the cloud services usage illustrated in Fig. 5, only 7% of the participants indicated that they do not use cloud services. Corporate cloud email services (60%) were the most preferred option by the participants, followed by the generic cloud file sharing services (34%) such as Google Drive, One Drive, Dropbox, iCloud, Nextcloud. As more than 90% of the participants used cloud computing services, it is likely that sensitive information may be accessed and updated during the remote working, leading to potential rise on privacy concerns. This, in addition to considering the diverse devices and network connections (from Fig. 3 and Fig. 4) used by the participants, cloud services may be more effective as they offer broad spectrum of universality and acceptability.

Regarding the security practices during remote working, Fig. 6 shows that only 5% of the participants did not use any authentication or security methods. Password/PIN/Pattern is the most commonly used authentication method adopted by the majority of participants (52%), followed by using VPN (39%) for remote working, and OTP (28%) for remote authentication. Face recognition and hardware token are other practices used by few participants. These results indicate that participants have adopted a range of security methods reflecting the use of multiple or a variety of security methods (44%) which adds an additional security layer for various activities during the remote working. Such practices improve security and privacy, thereby avoiding potential online security threats or loss of data.

Analyzing the impact of lockdown on the daily work of the respondents illustrated in Fig. 7, it can be identified that half of them stated that their daily work was affected, with 31% not affected and 19% was neutral. The results clearly indicate that lockdown has severely impacted their daily work routine while working remotely, indicating a greater influence of external factors (not internal to organization) on the daily work. Lockdown has not only affected the employees, but also the organizations, and their work culture. Most of the organizations shifted to remote working model in a far larger way than ever before. In this context, 76% of the participants stated that home Lockdown (Curfew) has encouraged or pushed their organizations to publish or enable more online services; while only 5% stated that it had no impact on their organizations in enabling more online services. Therefore, it can be inferred that there is a significant impact of lockdown on the organizational work paradigm, steeping more towards remote work.

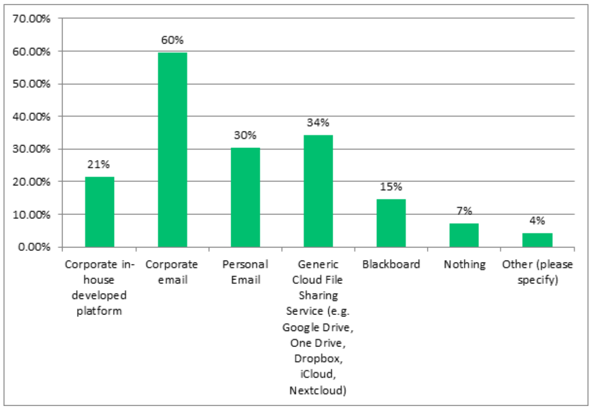

Fig. 5. Types of cloud file sharing services.

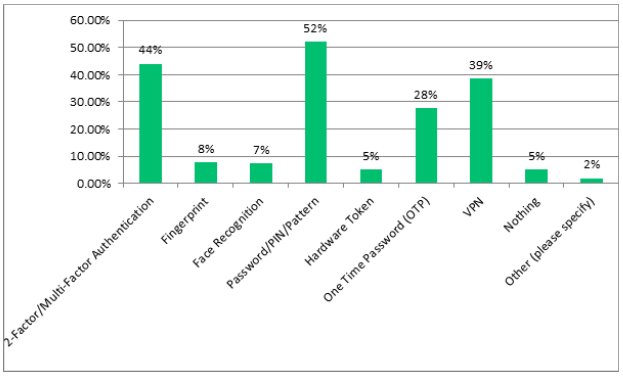

Fig. 6. Types of security / authentication practices.

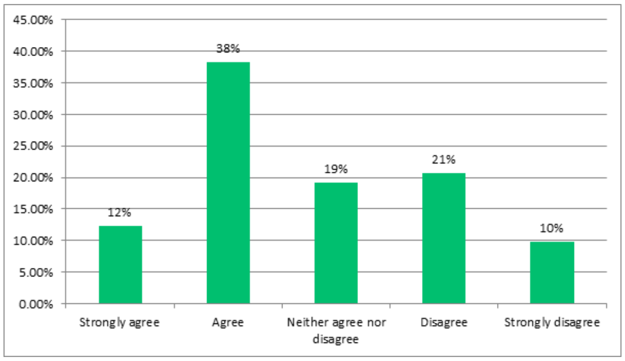

Fig. 7. Impact of lockdown on the daily work of the respondents.

Due to the sudden change in work culture, it is common that there could be many issues that might have to be dealt with by employees and organizations in shifting towards complete online services. In this context, Fig. 8 demonstrates the various challenges encountered by the participants and their colleagues during the remote working from home. The lack of high speed or quality connectivity infrastructure was the most common challenge identified by many participants (37%). These findings can be correlated with the earlier mentioned low satisfaction about their ISPs. Thus, it is evident that the lack of high-speed internet infrastructure in some areas of Saudi Arabia [11] and other states in the Middle East [12] was one of the major challenges affecting the remote working culture in the organizations. In addition, other major challenges included the lack of appropriate software (27%), the lack of appropriate hardware (23%), and the lack of appropriate skills/awareness (23%). These results indicate the lack of readiness of the employees and organizations in handling the unexpected change. However, it is unsurprising to note that 26% of the participants mentioned that they could not identify any challenge related to remote working during the lockdown, indicating an effective change management practices adopted by few participants and organizations during the lockdown.

Considering these sudden changes in the work culture, it is essential to compare the offline and online practices in order to improve the online services. Therefore, participants were asked to compare the organizational outcomes of online and offline services of their organizations. It is interesting to note that 62% of the participants reflected their opinion that online services used by their organizations delivered better outcomes than their counterpart offline services. Only 6% of the participants indicated that offline services delivered better outcomes than online services. The results signified that adopting the online services and remote working culture resulted in better outcomes compared to offline practices - implying the advantages of remote working. Aspects such as flexibility, convenience, saving travel time and transport expenses might probably have contributed to the improved work efficiency of the participants while remotely working from home during the lockdown.

Fig. 9 indicates that Zoom was identified to be the most commonly used platform, followed by Cisco Webex, Microsoft teams, Blackboard, Skype for Business, and Google Meet. Due to its easy-to-use feature with limited required resources or memory, applications such as Zoom might have been preferred over other commercial applications such as Skype. Availability and adoption of various platforms for online meetings, as illustrated in Fig. 9, may improve the communication and interactivity among the various employees and entities within online environment resulting in improved process and operational efficiency leading to better outcomes. On the other hand, it was identified that password security method was the most commonly applied authentication technique by the majority of participants (58%) for joining online meetings. In addition, other authentication techniques used included OTP, VPN and multi-factor authentication. These security practices adopted online meetings can be correlated with the adopted general security practices (Fig. 6), reflecting similar practices.

Focusing on the various factors that may hinder the transformation from traditional work practices to online services, various important issues were identified by the participants. Cybersecurity, lack of infrastructure, and lack of trust were the three major issues identified for transforming traditional services into online services, as illustrated in Fig. 10. In addition, the lack of staff and users' skills and awareness were the succeeding key challenging factors identified in this study against moving towards digital teleworking. Accordingly, 82% of the participants held an opinion that cybersecurity may be adversely affected by the online services.

In this context, the participants were asked about the probable vulnerabilities that might occur due to the increase in online services and remote working. Fig. 11 presents that information/data leak was identified to be the most important vulnerability by the majority of the participants (76%). Furthermore, identity theft (55%), and unauthorized information access (41%) were the following most vulnerabilities identified.

In view with the use of different devices with different configurations, and the increased usage of personal devices illustrated in Fig. 3, the potential risk of security attacks would be higher. Accordingly, information leak/theft, unauthorized accesses are some common vulnerabilities that could occur, but can have huge impact depending on the type of data loss. Thus, the results indicate that there is a high probability of security attacks or vulnerabilities in remote working process. In reference to the probability of vulnerabilities occurrences, the participants were asked if they had experienced any security incidents during working from home. Even though 73% indicated they did not experience any security incident, a non-negligible number of participants (16%) indicated that they did. This result can be in line with the level of cyber incidents in the Middle East, which may not only affect the remote working infrastructure, but also affect the organizations in a number of aspects. Moreover, 10% of the participants stated that they do not know if they have experienced any security incident. Unawareness about cyber incidents is another major issue, which may result in continuous exploitation by the attackers/hackers without being detected.

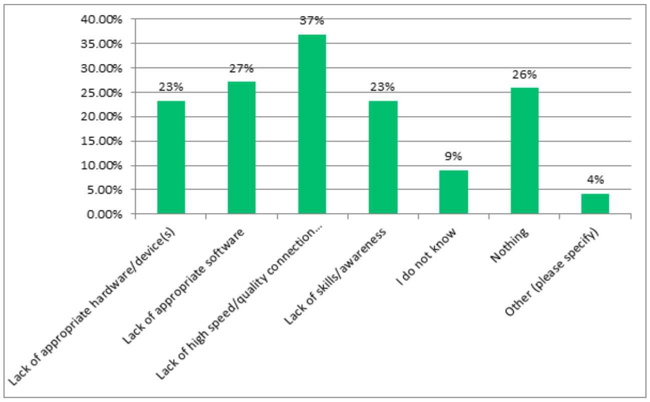

Fig. 8. Challenges faced by the participants in remote working during the lockdown.

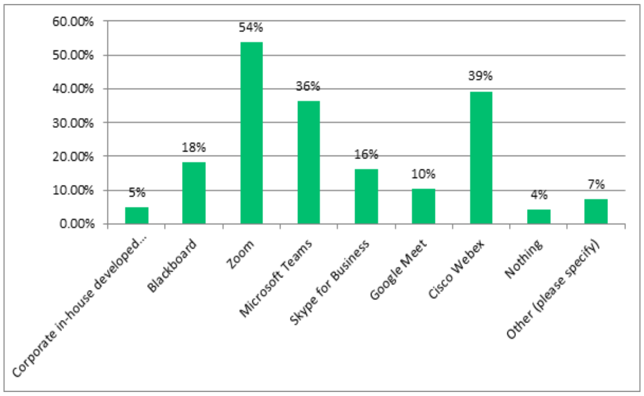

Fig. 9. Types of platforms used for online meetings.

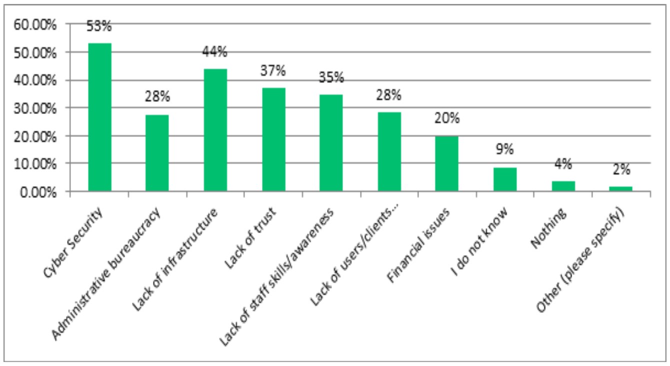

Fig. 10. Challenges in moving towards online services during the lockdown.

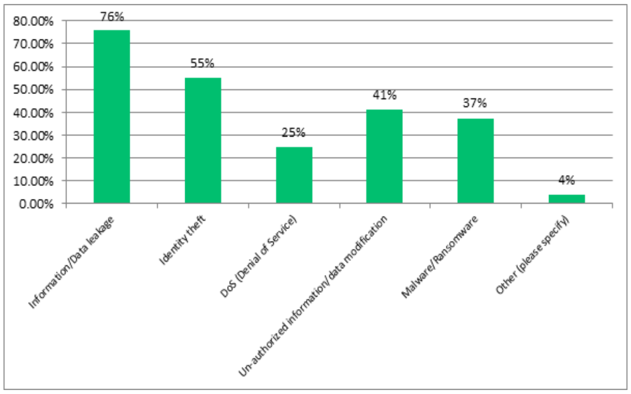

Fig. 11. Types of vulnerabilities that may occur during remote working process.

Considering the risk of security incidents during the remote working, it is important to analyze if the organizations are ready to invest in more effective cyber security solutions. Fig. 12 elucidates that over 80% of the participants strongly agreed and agreed that their organizations would invest more in cyber security solutions, indicating a growing importance for deploying effective security infrastructure in the process of transformation to online services. From the employees' perspective, it is essential to assess the impact of investments in cyber security solutions on trust and reliability in shifting to online services. In this context, over 87% of the respondents strongly agreed and agreed that the growth of investment by organizations in cyber security solutions will increase their trust and reliability in the growing online services and remote working.

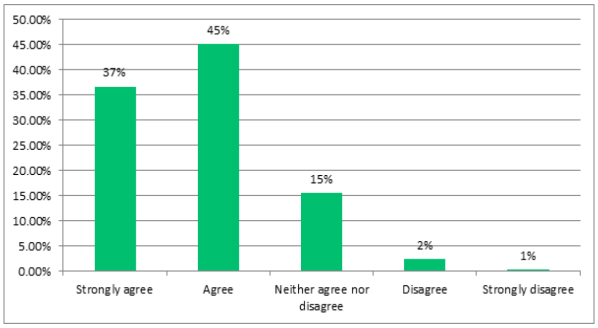

Fig. 12. Organizations' Readiness to invest more in cyber security solutions.

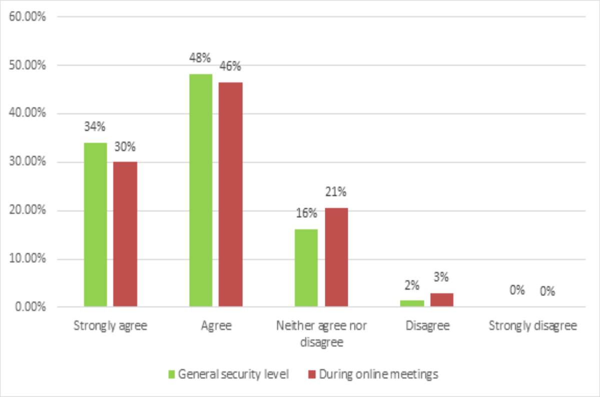

Fig. 13. Influence of transparent continuous authentication on enhancing the security levels.

With regard to the use of transparent and continuous authentication, participants' opinions were gathered whether it could enhance the security level in general and during online meetings specifically. Fig. 13 demonstrates similar results in both conditions, indicating a greater expectation and acceptance of transparent continuous authentication process.

IV. Discussion

The respondents of the survey were from a diverse population with respect to age, qualification, job position, work field and enterprise sector and size, making it quite representative in relation to the investigated issues. Despite the overwhelming belief on the strong technical infrastructure of the organizations, there is an apparent increase in the use of personal devices for remote working, leading to potential surge of security threats due to the usual relaxed security practices while interacting with personal devices. Nevertheless, employing proper mobile device management (MDM) solutions would lead to more suited security measures and maintenance, hence alleviating cybersecurity vulnerabilities and attacks.

It is apparent that most of the current remote workers own/use a number of digital devices with different operating systems and configurations. This is coupled with the evident adopted several online meeting platforms and cloud services, emphasizing the need to consider universal applicability and interoperability as a crucial aspect in any offered security mechanism.

Given the fair range of applied security authentication practices, still the knowledge-based methods outweigh the others, rendering the remote working susceptible to its well-known shortcomings that affect the security level. This prevalence can be attributed to the fact that these approaches are the main provided ones by the majority of platforms, portals and services besides other low accurately configured and more intrusive alternatives such as the biometrics of fingerprint and facial recognition. Users' inclination to the ease of use may yield to apply the PIN/Pattern method, for example, at the expense of a further layer of protection that is introduced with biometrics as a single factor or an additional factor. However, implementing them in a usable and robust manner would lead to a resilient online working environment with less effect on the day to day tasks than what was declared. This can also be aided by better early preparedness in terms of appropriate devices, applications, quality internet connections, and staff skillsets and awareness in order to have improved smooth transition of processes and operations leading to efficient online remote or hybrid work paradigm.

It is observed that cybersecurity and the lack of infrastructure and trust are the major challenges of digital work transformation. This also can be seen by the respondents' perceptions regarding the wide range likely vulnerabilities during remote working including data leakage and unauthorized modification and identity theft. Therefore, an intelligent security solution that balance the higher protection and usability is required and can be provided by continuous and transparent authentication approach which gained high acceptability and expectancy by participants, stemming to a potential success. This is also supported by the anticipated increase in investment in cybersecurity solutions by respondents' organizations.

V. Conclusion

The survey findings were derived from a fair range of participants' backgrounds with regards to demographics, employments, as well as organization types, fields, sizes and somewhat locations. Exploring their state of the practice, it was found that a variety of technologies were adopted and operated into transforming to remote work and during it, in terms of devices, connectivity, Cloud File Sharing Services, and online meeting platforms.

Despite the acceptable level of satisfaction about the used and offered online services in meeting the demand and requirements of stakeholders, still a number of challenges were raised and needed to be tackled, such as cybersecurity and the lack of high speed/quality connection infrastructure, appropriate software/hardware/device(s), and technical skills/awareness.

With reference to issues that hindered or may hinder the growth of or the transformation to the remote work, cybersecurity had the highest concern including confidentiality, authenticity, integrity, malware and availability (in order). Moreover, the lack of infrastructure, trust, and financial support were of those matters to be considered with potential solutions for better remote work experience. Although many organizations have moved relatively fast to the remote work and to some extent fulfilled their tasks, many of them have faced difficulty to offer appropriate scale of online services. Therefore, more investment in cybersecurity techniques and employee training could be an incentive towards a more effective, efficient and smooth remote work environment.

References

[1] Statista, "Internet usage worldwide – statistics & facts," available on https://www.statista.com/topics/1145/internet-usage-worldwide/, accessed on 29 November 2020, 2020.

[2] M. Kuchenbuch, et al., "An accelerated shift in the use of remote systems in epilepsy due to the COVID-19 pandemic," Epilepsy Behav. ;112:107376, 2020.

[3] L. Elliott, "Number working from home in UK rises after government U-turn," available on, https://www.theguardian.com/business/2020/oct/01/number-of-people-working-from-home-in-uk-rises-following-government-u-turn, accessed on 29 November 2020, 2020.

[4] C. Westfal, "Statistics show remote workers are frustrated, many still unprepared for working from home," available online, www.forbes.com, accessing on 29 Jan 2022, 2020.

[5] Hlb, "Global advisory and accounting networks," available on, https://www.hlb.global/press-room/remote-working-leads-to-increases-in-cyber-attacks/, accessed on 29 Mar 2021, 2020.

[6] ONS, "Office for national statistic," available on, https://www.ons.gov.uk/economy/grossdomesticproductgdp/articles/internationalcomparisonsofgdpduringthecoronaviruscovid19pandemic/2021-02-01, accessed on 1 April 2021, 2021.

[7] G. Gopinath, "The Great Lockdown: worst economic downturn since the Great Depression," available on, https://blogs.imf.org/2020/04/14/the-great-lockdown-worst-economic-downturn-since-the-great-depression/, accessed on 1 April 2021, 2020.

[8] WHO, "WHO reports fivefold increase in cyber attacks, urges vigilance," available on, https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance, accessed on 12 Apr 2021, 2020.

[9] F. Shahzad, "State-of-the-art survey on cloud computing security challenges, approaches and solutions," in Procedia Computer Science, 37, 357-362, http://dx.doi.org/10.1016/j.procs.2014.08.053, 2014.

[10] B. Trzupek, "PKI is key to securing a post-Covid remote workforce," in Computer Fraud & Security, vol. 2020, no. 10, pp. 11-13, October 2020.

[11] H. Alshehri and F. Meziane, "Current state on internet growth and usage in Saudi Arabia and its ability to support e-commerce development," in Journal of Advanced Management Science, vol. 5, no. 2, pp. 127-132, 2017.

[12] Houcheimi, "The key e-tail opportunities and challenges in the Lebanese e-commerce market," Journal of Information System and Technology Management (JISTM), vol. 7, no. 26, pp. 13-31. 10.35631/JISTM.726002, 2022.