European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.12.04.2

ISMC 2021
16th International Strategic Management Conference

CYBER SECURITY RISKS AND CHALLENGES IN REMOTE WORK UNDER THE COVID-19 PANDEMIC

Līga Atstāja (a), Didzis Rūtītis (b)*, Sintija Deruma (c), Eduards Aksjoņenko (d)
*Corresponding author

(a) BA School of Business and Finance, Riga, Latvia, liga.atstaja@ba.lv
(b) BA School of Business and Finance, Kr.Valdemara iela 161, Riga, Latvia, didzis.rutitis@ba.lv
(c) BA School of Business and Finance, Riga, Latvia, sintija.deruma@ba.lv
(d) BA School of Business and Finance, Riga, Latvia, eduards.aksjonenko@ba.lv

Abstract

The COVID-19 pandemic is having a negative impact on corporate cybersecurity in terms of workforce habits and digital skills, awareness of cyber hygiene, and the rapid shift to remote work solutions. It has also reiterated the importance of employer-led risk management practices in line with employment habits. During the COVID-19 pandemic the remote workforce has diversified and increased in numbers, offering employees the opportunity to continue working, the availability of which is also facilitated by the national approach to improving the epidemiological situation, which mandated wider use of remote work for those whose work specifics allow it. The study analyzed the current cyber risks and challenges affected by the COVID-19 pandemic, as well as risk management approaches or security controls. The novelty of research relates to the identification of changes in working patterns and their correlation with applied control measures for the management of cybersecurity risks. Data collection tools such as questionnaire and interviews with experts were used. Research conclusions reflect that the approach of companies and organizations to cyber risk management, providing a form of remote work organization is tailored to the industry, the nature of the information processed, the computer skills of employees, and pre-COVID-19 investments in corporate cybersecurity and digital transformation. Employers and information security managers are likely to continue to pay increased attention to limiting the risks associated with the human factor, which has become more multi-faceted during the COVID-19 pandemic, given the psycho-emotional challenges of remote work experienced by a large proportion of workers.

Keywords: Cybersecurity, covid-19, risks, remote work

https://doi.org/10.15405/epsbs.2021.12.04.2
Corresponding Author: Didzis Rūtītis
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

During the COVID-19 pandemic, a significant increase in the number of employers who offer employees the possibility to work remotely has also been facilitated by national approaches to improving the epidemiological situation, which prescribed remote work for all whose work specifics allow it. At the same time, cyber threats have increased during the pandemic, which highlights the need to adjust the approaches of employers to cyber-risk management.

This paper analyses the cyber risks and challenges raised by the COVID-19 pandemic and extended use of remote work, as well as risk management approaches or controls introduced. The research aims to analyze cybersecurity risks and challenges for companies and organizations associated with changing employee habits while working remotely during the COVID-19 pandemic.

Given the changes in the availability of remote working because of the COVID-19 pandemic, the authors have focused on the cyber risks and challenges posed by changing the daily and work organization habits of remote workers, as well as the use and popularity of the most common types of risk management (security controls). The study focuses on humans as the weakest link in cybersecurity. When working remotely, not only the protection of work information is important, but also the protection of personal information. The study analyses the cybersecurity risks associated with changing employee habits in the transition to remote work during the COVID-19 pandemic.

Research problem: the COVID-19 pandemic is negatively impacting companies' cybersecurity in terms of workforce habits and digital skills, awareness of cyber hygiene, and the rapid shift to remote working solutions, forcing employers to adapt organizational cyber-risk management practices to employee habits.

Research hypothesis: remote working during the COVID-19 pandemic has increased the risks to cyber security for companies and organizations.

2. Literature Review

The form of remote work organization was introduced in the 1980s and has so far been used to motivate and reward employees within the bonus system, reduce traffic congestion and the time it takes an employee to commute. Given the important role of information and communication technologies in the performance of their duties, this is also called telecommuting, but the definition also applies to jobs not related to ICT solutions. Due to the possibility of working from anywhere, remote working is also called mobile work, as its performance depends only on the availability of portable hardware such as wireless internet and a laptop (Ross, 2018). The utilization of remote work can be divided by regularity:

- permanent or full-time;
- part-time (as needed, for example, by determining the frequency or amount of work to be performed remotely);
- occasional (less than once a week).

Conceptually, remote work is different from “working from home” and also from “forced working from home”. Information system development research (O’Connor et al., 2021) highlighted that not only do remote workers perform work tasks from their homes or official workplace, but also other places. The

https://doi.org/10.15405/epsbs.2021.12.04.2
Corresponding Author: Didzis Rūtītis
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

work from home concept foresees the individual choosing entirely how the work from home is organized; however, in contrast, forced working from home is described as transition to remote work in the impact of the COVID-19 pandemic. Therefore, it is necessary to separate voluntary remote work and COVID-19 forced remote work, where choice in favour of remote work is associated to epidemiological safety and restrictions introduced by governments. Furthermore, bearing in mind the swift shift towards more available remote work during the pandemic, there is a considerable influx of cyber incidents. Which have been observed in most of the enterprises in the Cisco (2020) study, where, depending on size of the company, most small and medium-sized companies (55%), and 60% of large companies perceived a growing trend of cyber incidents.

The employee must obey orders from the employer and the established agenda, which is also true when working remotely. This indicates the possibility of flexibility to adapt the work conditions for part-time or full-time remote work, but specific agreement must be arranged so the employee is aware of the work conditions, subordination, specific training, policies, and control (International Labour Office, 2013). Personal devices are permitted for performing remote work, but contracts regarding use of private equipment (depreciation costs) must be in place. Common worldwide practice and local laws may state that specific costs can be stipulated in the relationship (for example: internet connection, use of a mobile phone, electricity and other). Otherwise, there is a substantial capital investment by the worker – an interpretation of local labour laws in various countries may support the finding that the worker is an independent contractor, who may raise concerns about responsibility.

Similar labour laws regarding device use can be applied in countries worldwide with various customization and need to adapt for critically important and specific examples, such as in the European Union, where data processing, accountability, right of information and data security must comply with General data protection regulation (Koch, 2020), availability of employee and working time control.

There are four groups of operational cyber security risks in the Carnegie Mellon University classification (Cebula et al., 2014) that ought to be considered when introducing and providing remote work while creating policies, standards and ensuring that those are communicated with employees:

- *System and technology risks* – especially risks associated with third party platforms (relatively easy to modify information, capture data). Therefore, data encryption for communication and exchange of data is needed and a stricter policy for use of free services.
- *Non-compliance with internal procedures* – also includes internal organization culture and behavior of users (Ayereby, 2018).
- *Risks associated with human behavior and human factors* – there may be errors in programs, systems, lack of security awareness and mistakes such as connections made in an incorrect and unauthorized or unsecure way (Verizon, n.d.).
- *Risks from external influences* – referring to Georgiadou et al. (2021) - society and businesses are often affected by cybercrime growth that includes social engineering and attacks, which are even more possible because of a new-normal mode of the way how we live and work. It also means that massive events like pandemic can help cyber-criminals to exploit the situation for crafting cyber-crime campaigns.

In the context of remote working, companies and organizations must consider that employees may need to obtain and work with information classified higher than the systems by which the remote work is performed. To adapt for work in higher cyber-risk circumstances (for example vulnerability of IT systems), it is necessary to incorporate the requirements of a cyber-security document as a policy in general (Ahmad, 2020). In addition, during remote working companies need to find confidence in the compliance of the employee's physical workplace which can be achieved via specific requirements and guidelines that can be also called workspace standards (Hou et al., 2021).

To foster cybersecurity during remote work companies should consider using wider multi-factor authentication methods, choosing not to use certain communication platforms, safe use of virtual private networks (VPN), and enhancing responsiveness to information technology security incidents (Škiljić, 2020). Moreover, mention should be made on the environment in which remote workers are conducting their respective tasks, as, during more strict epidemiological restrictions, workers are more susceptible to cyber incidents, which are less likely during informative and awareness-bringing campaigns (Buil-Gil et al., 2020).

To be productive, effective, and cooperative as an individual it is crucial that companies implement successful change management by promoting teamwork and cooperation by using real-time communication tools (Lallie et al., 2021). Moreover, for many companies it seems to be the momentum to revisit business continuity plans, cybersecurity resilience approaches, as well as risk appetite (Institute of Risk Management, 2021).

3. Research Methods

Both quantitative and qualitative research methods were used to collect the data for research tasks. The data obtained was analyzed using a triangulation approach, where the data sets obtained with different research methods were compared, identifying overlaps or correlations. Data collection tools such as questionnaire (quantitative research method) and interviews with experts (qualitative research method) were used.

3.1. Expert selection

To correlate survey data with qualitative experience, a series of partially structured expert interviews were conducted. Interviews were individual and conducted remotely. Experts interviewed hold positions such as CEO (Chief Executive Officer), CTO, information security manager, solutions architect, and data protection officer in fields such as ICT (Information and Communication Technology), financial services, and healthcare sectors. Interviews covered topics relevant to research on companies' response to the COVID-19 pandemic, introduction and preparations for remote work solutions, risks and challenges related to more widespread use of remote solutions, observations on changes in attack surface related to the pandemic, as well as digital transformation and cybersecurity risk management controls introduced recently, and additional support provided for remote workers in response to the pandemic. The qualitative data gathered from interviews were analysed anonymously, in a codified way, and used to provide trends and examples related to qualitative research.

3.2. Survey methodology

The sample of the study included a Latvian workforce who worked remotely full time or partially, due to the COVID-19 pandemic. Although 323 people were surveyed, the sample size consists of 313 respondents, since respondents who were not employed at the time of completing the survey and thus did not classify for the study were excluded from the sample.

To determine the average age of the respondents, the questionnaire included a question on the age group of the respondents (up to 25 years of age, from 25–40 years of age, 41–60 years of age and over 60 years of age). Although the ratio of population counting as labour force is defined in the legislation in the range from 15–64 years of age, a large part of young people are not actively involved in the labour market, naturally the majority of respondents are in the age group 25–40 (57.6%) and 40-60 (26%), but the smallest share of respondents - in the age groups under 25 and over 60 (Official statistics portal, 2021).

Most of the respondents can be perceived as experienced specialists as their largest proportion have been employed for more than 3 years (56%), and their self-evaluation on computer proficiency when using a Likert style scale from 1–5 averages at 3.5. Respondents were employed in various industries, but the majority were employed in education, IT and communications, public sector, financial and insurance activities, administrative and support services, and scientific and technical services.

4. Research Results

Data collection via questionnaire (quantitative research method) and interviews with experts (qualitative research method) provided the basis for the aim of the research.

4.1. Expert interviews

The analysis of expert interviews shows that the availability of remote work in organizations and companies is influenced by:

- choice of employees in favour of remote or full-time work in pandemic conditions;
- customer requirements and restrictions specified in the agreements to ensure information protection, as well as field-specific regulations;
- conditions for compliance with epidemiological requirements (limited space, need for long-term use of personal protective equipment when working in person);
- ability to provide the necessary technical support, devices for remote work, and support employees in creating an ergonomic workplace at home.

Experts indicated that most cybersecurity risks during remote work are related to the human factor – attitude, habits and security awareness of employees, as well as stress factors they experience. This aspect must be taken into consideration when developing prioritization for investments in cybersecurity and risk management approaches. Regarding information security, when working with restricted information, the employer must not only provide appropriate technical solutions, but also inform employees about the physical security requirements and responsibilities in the event of disclosure during remote work. Working remotely at home raises the issue of the Internet of Things (IoT), where smart home devices can analyze work-related information by listening to telephone conversations and video conferencing without users' awareness. Also, for information protection, employers may need to introduce new technical solutions or modify the information protection system, which is resource-intensive and not feasible in a short period of time, therefore employees may have limited opportunities to fully perform their duties remotely especially during the early stages of the pandemic.

The use of private devices for work purposes provides the employee with flexibility and mobility, and to conveniently perform various activities regardless of location, as well as allowing the employer to save money on the purchase and maintenance of devices. However, it involves cyber risks that are difficult for an employer to manage. Cybersecurity management challenges are particularly important when employees access work-related resources from unmanaged devices through uncontrolled Internet connections, thus limiting the scope for dealing with incidents that may pose data leakage or compliance risks. To find out the use of bring your own device (BYOD) among the respondents, quantitative data were obtained on whether the respondents use private devices for work (computers, mobile phones, tablets) and whether employers allow the use of private devices.

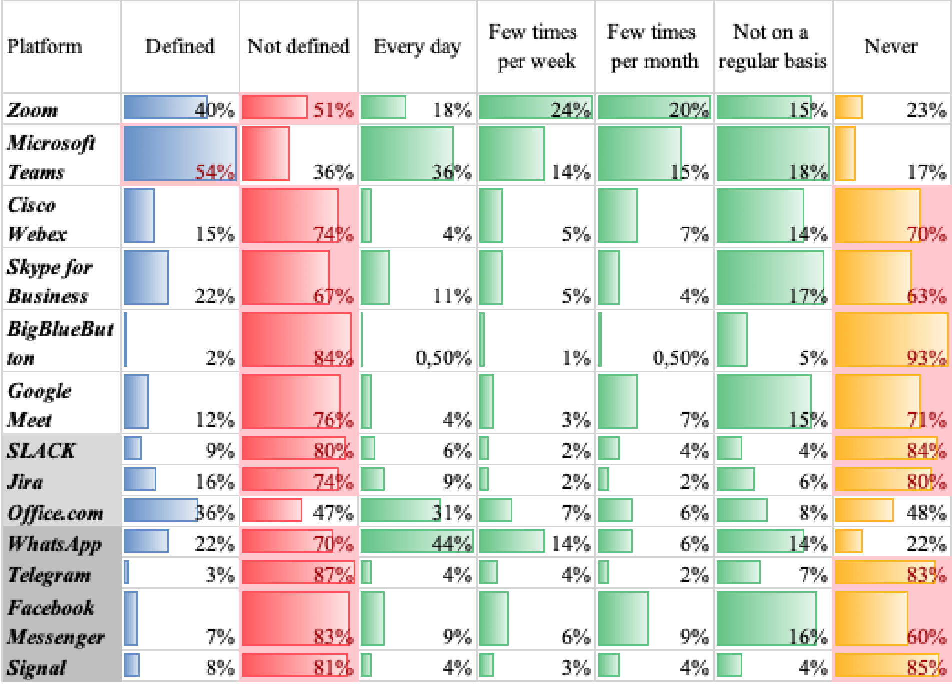
4.2. Survey results

Survey results provided insight into respondent habits while working remotely, support provided by employers, and the most common cybersecurity controls introduced for remote work during the COVID-19 pandemic.

During the COVID-19 pandemic a larger proportion of workers have become accustomed to remote work. As per survey conducted during this research before the pandemic, only 10% of respondents worked remotely every day, in contrast to 59% during the pandemic. Although the frequency of remote work varies among remote workers, during the pandemic more workers opt for remote work daily or a few days per week, thereby proving it to be the safest and most convenient choice during the pressing epidemiological situation.

The behavior of employees when working remotely also includes the use of work equipment for private purposes. The use of work equipment, for example, for checking personal email, entertainment, social networking, and other purposes, can pose cyber risks as well as risks to an employee's private information (such as sensitive information about the employee's private life and health). Synchronization of personal social networks (e.g. Google, Facebook) with devices provided by the employer is undesirable, which creates the risk of unauthorized processing of work information. Although employers can install software for device management and control, as well as for obtaining information on hourly recording and productivity (such as keyloggers), a balance needs to be struck between employee control and job tracking. The survey indicated that although employers permit the use of certain social networking sites or platforms for official work communications, employees still use them (see Figure 1).

https://doi.org/10.15405/epsbs.2021.12.04.2
Corresponding Author: Didzis Rūtītis
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330



Platform	Defined	Not defined	Every day	Few times per week	Few times per month	Not on a regular basis	Never
Zoom	40%	51%	18%	24%	20%	15%	23%
Microsoft Teams	54%	36%	36%	14%	15%	18%	17%
Cisco Webex	15%	74%	4%	5%	7%	14%	70%
Skype for Business	22%	67%	11%	5%	4%	17%	63%
BigBlueButton	2%	84%	0,50%	1%	0,50%	5%	93%
Google Meet	12%	76%	4%	3%	7%	15%	71%
SLACK	9%	80%	6%	2%	4%	4%	84%
Jira	16%	74%	9%	2%	2%	6%	80%
Office.com	36%	47%	31%	7%	6%	8%	48%
WhatsApp	22%	70%	44%	14%	6%	14%	22%
Telegram	3%	87%	4%	4%	2%	7%	83%
Facebook Messenger	7%	83%	9%	6%	9%	16%	60%
Signal	8%	81%	4%	3%	4%	4%	85%

Figure 1. Survey results: use of software tools for remote work and whether the employee has allowed their use (Developed by the authors)

Regarding the use of work equipment for private purposes, comparing age groups, in the age group over 40 it is observed that respondents are more likely to use work mobile devices for private purposes. In the age group over 41 years of age, 38% of respondents use work equipment for private needs every day, while in the age group under 40 years of age – only 22%. Of the respondents who have worked in their workplaces for a relatively longer period, the majority use a work computer for private purposes: 41% do it every day, 32% – less often (once a week or once a month), but 10% of respondents do not provide devices for remote work. The majority (68%) of respondents who do not use work computers for private purposes indicate that they also do not use work mobile phones for private purposes. Comparing the approach to the use of work equipment for private purposes, it can be found that men use work equipment for private purposes more often than women (36% of men indicate that they use it every day, but women – 24%). 21% of men and 25% of women never use a work computer for private purposes.

Although the use of work equipment for private purposes is not always associated with reckless and unproductive behavior, nor can it be completely eradicated, it is important that the employer addresses best practices and potential risks in policy documents and in relation to the employee. The employer may impose restrictions on certain actions with work devices, for example, by restricting the use of certain websites, as well as stipulating that the acquisition of non-work-related information must be performed in another browser.

Third-party access to work equipment involves the risk of work-related information leakage and accidental compromise of equipment. As the COVID-19 pandemic increased the range of services received remotely and the need for additional equipment for remote working and training (school, university), and for entertainment purposes and for household work, the need for additional equipment often increased. To identify whether the respondents pass on the devices used for work to peers (third parties), the survey included the question of whether the respondents allow such practices, potentially endangering the devices used to perform work duties. Although only 16% of respondents indicated that a device used for remote work is used by another household (e.g. for distance learning, browsing the Internet), it poses risks of unauthorized access to work resources, access to high-risk Internet resources, etc. Respondents who indicated that devices for remote working are also used by peers use both work and private devices for remote working.

The results of the survey show that from the point of view of employees there are significant challenges during remote work (see Figure 2), which can be classified as the ability to self-organize, communication quality, psycho-emotional factors (loneliness, lack of socialization), ergonomic and work environment factors, as well as technological factors (internet connection quality, access therefore, when designing a set of cyber risk management measures, companies need to take into account the challenges faced by employees, which are only partially solved technologically, but point to a significant need for organization-wide involvement, for example, organizational culture, personnel management, training activities that can tackle human-factor related challenges.

Bearing in mind the fact the challenges that employees meet when working remotely could be managed and addressed by direct action by the employer, respondents were also surveyed on the support means that are provided during the remote work. In this respect, provision of devices for remote work (68.7%) and IT helpdesk (78.7%) can be identified as the most attainable support measures. In contrast, only 35.2% of respondents indicated that their employer supplies office equipment for remote work ergonomics, including desks, chairs, and other items. Furthermore, only 9.4% of respondents stated that their employer compensates for costs related to the remote work. As such, although support activities have become more widespread during the pandemic, there are no best practices yet in place, nor are there industry standards for support that must be provided for remote workforce, since there were no correlations between industries and availability of support measures. The COVID-19 pandemic has made many companies revisit their cybersecurity investments and budgets, as was stressed in expert interviews in the realm of this research, as well as other research (Cisco, 2020; Institute of Risk Management, 2021).

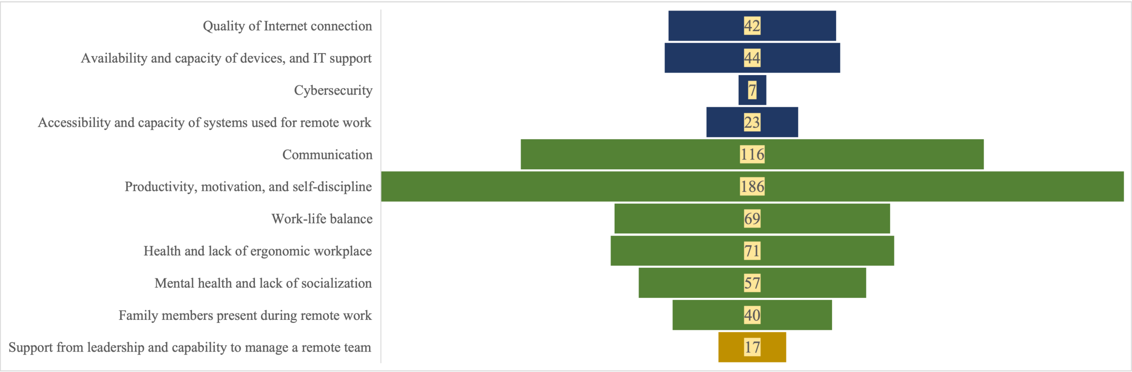


Figure 2. Survey results: challenges of remote work. Developed by the authors.

In respect to cybersecurity risk management practices commonly used by employers who provide remote work, they vary by the earlier investments in cybersecurity, capacity and resilience of systems, application of standards and best practices, and other factors. The survey proved that although some of

https://doi.org/10.15405/epsbs.2021.12.04.2
Corresponding Author: Didzis Rūtītis
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

the cyber-risk management controls used are more widespread, during the pandemic employers have not prioritized the introduction of a cybersecurity policy, training, and technological controls (see Figure 3). When asked to reveal the existence of a policy for remote work (including cybersecurity), 66.1% of respondents admitted that there was one, and 69.7% – that a policy for secure passwords was in place, but only 49.4% indicated that there were guidelines for setting up secure connections when working remotely. As for securing connections used for remote work, only 57.4% of respondents use VPN (virtual private network) to connect, and 47.7% use multi-factor authentication. Moreover, when asked if the employer had organized educational activities for remote work during the last year, only 41.3% responded affirmatively. It is therefore clear that although the COVID-19 pandemic influenced a hectic shift towards remote work, neither the introduction of technological controls nor policies were prioritized by employers who provide the remote work, and most of the awareness-raising campaigns were conducted on ad-hoc basis.

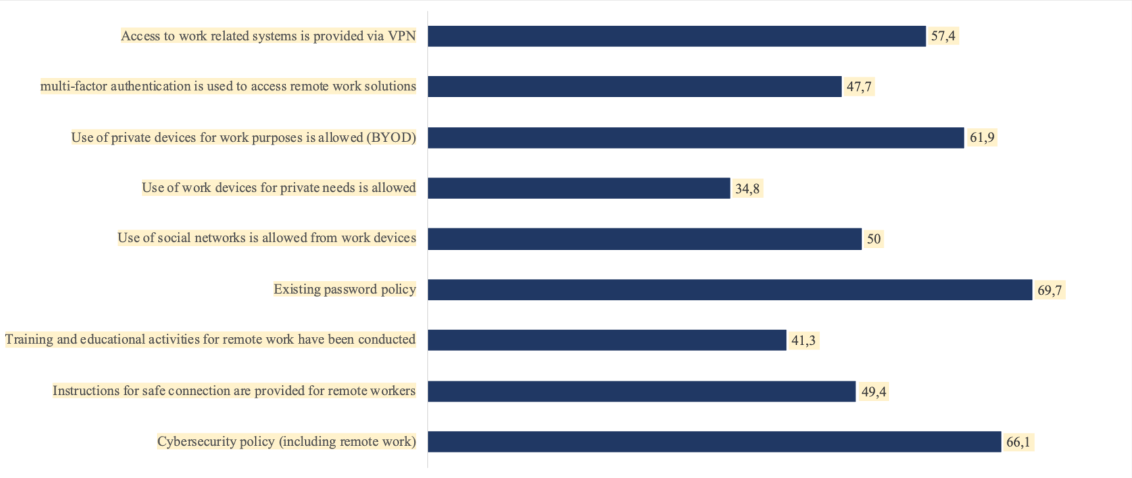


Figure 3. Survey results: cybersecurity risk management controls by popularity (Developed by the authors)

It has also been concluded that employers do not prioritize the development of requirements and instructions for remote working, which concern both the performance of work responsibilities remotely and the protection of information, as well as secure connection to the Internet and access to work systems. The use of private equipment for remote work is quite a customary practice among remote workers in Latvia; however, employers do not use opportunities to establish additional technical security controls to limit cyber risks in private devices and most do not develop policy documents or training activities for such an approach.

5. Conclusion and Discussion

The COVID-19 pandemic was a "stress test" for the transition of companies and organizations to remote working, for the secure implementation of remote working solutions, enhancing cyber resilience and capacity-building for employees, as not only did they need to be able to perform their duties remotely, but cyber-attacks increased. The organization of remote work due to the emergency caused by the COVID-19 pandemic is different from the planned and gradual implementation of the solutions and procedures required for remote work. The availability of remote work is not self-evident in many sectors of the economy, although it is slightly influenced by industry trends, driven by business initiative, solutions implemented so far, the degree of digitalization and centralization and the ability to manage remote work risks.

The cyber risks of remote work are linked to phishing and social engineering campaigns, including the COVID-19 theme, the possibility of compromising work systems and work equipment with malware and spyware, and the challenges of the working environment of workers affected by working conditions at home, such as negligence, third party access, connectivity issues, etc. These cyber risks are intensified by human-factor related insecurities such as negligence, insufficient digital skills, and stressors related to changed working conditions during the pandemic, as well as ill-adjusted configuration of work systems.

The approach of companies and organizations to cyber risk management, providing a form of remote work organization, is tailored to the industry, the nature of the information processed, the computer skills of employees, and pre-COVID-19 investment in corporate cybersecurity and digital transformation and IT team capacity and budget. Employers and information security managers will continue to pay increased attention to limiting the risks associated with the human factor, which has become more multi-faceted during the COVID-19 pandemic, given the psycho-emotional challenges of remote working observed by a considerable proportion of workers.

Technical controls for remote work cyber risk management are more accessible to employers but are not widely used in companies and organizations. During the COVID-19 pandemic, the use of secure video conferencing and communication tools became especially important; however, the results of the survey show that a significant part of respondents use private social networks daily to exchange work information, which is also allowed by employers.

As employers' approaches to providing the equipment and facilities needed for remote working and to compensating for remote working costs vary widely, good practice approaches in the sectors are expected to develop in the coming years in determining the range of support that remote workers receive. Considering the experience gained during the emergency caused by the COVID-19 pandemic, employers will be able to analyze the experience of business process continuity, information exchange, secure remote work organization, which will allow improvements and change management practices, approach to cyber risk management, as well as to identify areas where digitization needs to be improved.

Acknowledgments

The study has been funded by the Latvian Council of Science project “The Impact of COVID-19 on Sustainable Consumption Behaviors and Circular Economy (Nr. lzp-2020/2-0317)”.

References

Ahmad, T. (2020). *Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity*. SSRN. https://doi.org/10.2139/ssrn.3568830

Ayereby, P. M. P. (2018). Overcoming Data Breaches and Human Factors in Minimizing Threats to Cyber-Security Ecosystems. [Doctoral dissertation, Walden University]. Walden Dissertations and Doctoral Studies. 6163. https://scholarworks.waldenu.edu/dissertations/6163

Buil-Gil, D., Miro-Llinares, F., Moneva, A., Kemp, S., & Diaz-Castano, N. (2020). Cybercrime and shifts in opportunities during COVID- 19: a preliminary analysis in the UK. *European Sociological Association*, 47-59. https://doi.org/10.1080/14616696.2020.1804973

Cebula, J. J., Popeck, M. E., & Young, L. R. (2014). A Taxonomy of Operational Cyber Security Risks Version 2. 1-26. https://doi.org/10.21236/ADA609863

Cisco. (2020). Future of Secure Remote Work Report. https://www.cisco.com/c/en/us/products/security/future-secure-remote-work-report.html#download_report

Georgiadou, A., Mouzakitis, S., & Askounis, D. (2021). Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*. https://doi.org/10.1057/s41284-021-00286-2

Hou, H. C., Remoy, H., Jylha, T., & Putte, H. V. (2021). A study on office workplace modification during the COVID-19 pandemic in The Netherlands. *Journal of Corporate Real Estate*, *23*(3), 186-202. https://doi.org/10.1108/JCRE-10-2020-0051

Institute of Risk Management. (2021). Risk Management Response to Covid-19 Results of the 2nd IRM Pandemic Survey Dec 2020 – Jan 2021. Retrieved 12 May, 2021, from https://www.theirm.org/media/9314/risk-management-response-to-covid-19-1.pdf

International Labour Office. (2013). Regulating the employment relationship in Europe. A guide to Recommendation No. 198. https://www.ilo.org/wcmsp5/groups/public/---ed_dialogue/---dialogue/documents/publication/wcms_209280.pdf

Koch, R. (2020). Data protection and working remotely. Retrieved 4 August, 2021, from https://gdpr.eu/working-remotely-data-security/

Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *Computers & Security, 105,* 102248. https://doi.org/10.1016/j.cose.2021.102248

O'Connor, M., Conboy, K., & Dennehy, D. (2021). COVID-19 affected remote workers: a temporal analysis of information system development during the pandemic. *Journal of Decision Systems*, 1-27. https://doi.org/10.1080/12460125.2020.1861772

Official statistics portal. (2021). *Official statistics of Latvia*. Retrieved 24 August, 2021, from https://stat.gov.lv/en/

Ross, S. J. (2018). Information Security Matters: I Left My Security in the Office. *ISACA Journal, 4,* 1-3.

Škiljić, A. (2020). Cybersecurity and remote working: Croatia's (non-)response to increased cyber threats. International. *Cybersecurity Law Review*, *1*, 51-61. https://doi.org/10.1365/s43439-020-00014-3

Verizon. (n.d.). *Analyzing the COVID-19 data breach landscape*. Retrieved 10 March, 2021, from https://enterprise.verizon.com/resources/articles/analyzing-covid-19-data-breach-landscape/#