Fwd: UKS31093

by Alui Arh

Submission date: 17-Apr-2023 08:48AM (UTC-0500)
Submission ID: 2067210089
File name: Fwd__UKS31093.edited_pla.docx (33.85K)
Word count: 2694
Character count: 14867

Research methods - Challenges and best practices In managing remote work security

Introduction

Remote work security is the new branch of cybersecurity which is established to protect the corporate data and the other assets of the organization, while the employees of the organization are working from a remote location. Remote cyber security is important in remote working as it will help the employees to have better control of their work and on the other hand, the sensitive data of the organization can be protected in this remote environment (Georgiadou *et al.*, 2022). The biggest challenge in such a scenario is that the cyber-security tools used by the organization have a limited scope as management had prepared them to be efficient in the office scenario only. The employees working remotely from their homes or airport or hotels the sensitive data of the organization are exposing to unprotected wifi networks. This can result in big cyber security threats for the organization (Furnell and Shah 2020). The employees are accessing the office data from their own personal computers which is exposing the critical data of the organization to malware and trojans in the personal devices. Another challenge is the human factor, which means the employees in remote work situations unknowingly expose the organization's data to phishing scams which can have a serious dent in the cyber-security of the organization. The organization can make use of strong security protocols that are tailor-made to handle remote work cyber-security issues. The organization can also train the employees of the organization about the issues related to cyber-security and cyber threats. This will help the employees to protect the data related to the organization from cyber-security threats when working in a remote location.

Literature review

Description of search results

The search result was selected with the use of various filters. The filter of 2019 to 2023 was applied so that the relevant documents of the present years will be included in this research. A number of documents and articles were found in the database. Relevant documents were selected as per the requirement of the research. The relevant documents and articles on the Scholar were selected as per the requirement of the research. To select the appropriate documents that will be useful for this research was the most challenging task of this research. The articles which presented information to be used for academic purpose were used in this

research. Mostly general articles or the document having too much technical information was found in the database. Consequently articles were selected with utmost care to be used in this research.

Number	Keywords	Filter	Results	Assessment
1	Remote work security	2019-2023	70	Too many articles on Google Scholar cover the topic broadly.
2	Challenges in managing remote work cyber security.	2019-2023	64	Articles having an in-depth analysis of the topic related to various other fields also.
3	Remote workforce cyber-security management.	2019-2023	91	Articles are fit for academic writing.
4	Practices in managing cyber security	2019-2023	54	Relevant articles that will increase the knowledge of the issue
5	Cyber-security issues	2019-2023	75	Too many irrelevant articles related to the different fields.

6	Cyber-security issues in the post-pandemic period.	2019-2023	32	Less number of articles are available in this search criteria.
7	Management of the cyber-security threats in remote work.	2019-2023	80	A good number of relevant articles will be helpful in academic writing.
8	Practices to address cyber security.	2019-2023	30	Irrelevant documents that will not be useful for the report.
9	Remote work and the cyber threats	2019-2023	45	Good articles that provide in-depth analysis of the topic.
10	Remote work practices to counter cyber threats.	2019-2023	51	Articles are providing additional information to the existing knowledge on the issue.

Appropriate searching techniques

The documents that are relevant to the research study was considered in this research. The documents which were not relevant to the research were excluded in this research. Different search word were tried to find the relevant information that can be used in this research.

1	**Google Scholar**	Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees
2	**Google Scholar**	Working from home during COVID-19 crisis: a cyber security culture assessment survey
3	**Google Scholar**	Cybersecurity and remote working: Croatia's (non-) response to increased cyber threats
4	**Google Scholar**	Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap.
5	**Google Scholar**	Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy
6	**Google Scholar**	Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems*
7	**Google Scholar**	IT risk and resilience—Cybersecurity response to COVID-19
8	**Google Scholar**	Cybersecurity and Countermeasures at the Time of Pandemic.
9	**Google Scholar**	The impact of the pandemic COVID-19 in the workplace. *European Journal of Business and Management*
10	**Google Scholar**	Understanding the cybersecurity challenges of telecommuting and video conferencing applications in the COVID-19 pandemic
11	**Google Scholar**	The State of Industrial Cybersecurity in the Era of

		Digitalization.

Review of literature

Challenges and best practices In managing remote work security

According to Hijji and Alam, (2022), cybersecurity has become a prominent part of computing and information technology. This is due to the threat it poses to different organizations and their sensitive data. The cyber-security issues are harming the data of governments and organizations alike. The advent of the covid-19 and the subsequent work-from-home culture that followed during the period has exposed the data of the organization (Škiljić 2020). This has resulted in an increase in cybercrimes. The poor Information and technology infrastructure of the organizations has added to the graveness of the situation. According to Hijji and Alam, (2022), 47% of the employees working from home have faced issues related to cyber-security in some form.

Challenges in managing the cyber security threats

Lack of employee training - The employees working remotely are not properly trained about the cyber security threats and the cyber security issues that can cause a serious dent in the organization's data and their personal data. This has led to the employees unknowingly exposing the organization's assets and data to various malware (Dhirani *et al*., 2021).

Poor Information and technology infrastructure of the Organizations - The information and technology infrastructure used by the organizations are not fit to handle the cyber-security issues related to the work from home environment. This is one of the biggest challenges that organizations are facing in managing cyber-security-related issues of the organizations. The Information and technology infrastructure was prepared in the pre-pandemic time which is focused on providing security in the offices. This infrastructure has proved to be ineffective against the challenges that are faced by the organization in the remote working (Borkovich and Skovira, 2020).

Lack of proper visibility - The employees of the organizations are working in remote work locations. The IT staff of an organization lacks proper visibility about the tools, procedures and work behaviours that are adopted by the employees which is also harming the cyber-security of the organizations.

Evolution in ransomware and the malware - The malware and the ransomware have also evolved with the use of new advanced technology which has made it capable of exploiting the cyber-security of an organization. Malware and ransomware are locking the user systems of the organization and demanding money to unlock the systems of the users. This malware is easily able to disable the security of the data and corrupt the data which is affecting the organization's performance and efficiency.

Social engineering or phishing - Social engineering or phishing is used by cyber-security attackers to trick the user of the organization to expose sensitive data related to the organization. Social engineering or phishing is done in the form of emails to the users. These emails may seem to come from legitimate sources such as banks and government organizations. Once the user clicks the link on those Emails the system user gets attacked by the Phishing (Kaushik and Guleria 2020). This is a form of deception that the employees fall into and ends up exposing the data of the organization and the network exposed to malware.

Cloud computing issues - The organization is making use of cloud computing services in the remote working. In Cloud computing sensitive information of the organization is getting stored in the cloud which is helping the employees to use that information while working remotely. This has also increased the vulnerability of the data of the organization as a number of parties have access to the data of the organization which is stored in the cloud (Weil and Murugesan, 2020).

Best practices in managing the cyber-security

Proper training of the employees on the policies and the practices of the organization - The employees of the organization must have proper training on the practices and the policies that are used by the respective organization and adhere to those practices while working remotely (Ramadan 2021). The employees have to use the tools and devices that are only approved by the organization. The employees should not use personal devices to access the data related to the organization or the portals of the organization.

Proper security infrastructure on their own devices and computers - In the remote working it has been noticed that most organizations want the employees to work with the help of their own computers. This increases the risk of cyber-threats, consequently, the company should

install proper Information and technology infrastructure in the personal computers so that the risk associated with the issue can be addressed (Okereafor and Manny 2020).

Use of virtual private networks - The organization should make arrangements for the use of the VPN for the computers of the users working remotely for the organization. The use of the VPN will help the users to maintain security and privacy while accessing public wifis and networks. With the use of the VPN, the fear of being monitored and the fear of cyber threats will subside. Organizations are trying to transform themselves to manage and control the issues related to cyber security (Menze 2020).

Avoidance of use of third-party applications - The organization should try to avoid the use of third-party applications that may lead to the breach of the security of the sensitive data related to the organization. Avoidance of third-party applications will limit the access of organization data to third parties which will eliminate the chances of security breaches while working remotely for the organization.

Database search -

The articles in google scholar have been thoroughly reviewed to find out the relevant information to be presented in this report. The articles were searched with the help of different search words which would have helped to find out relevant and proper information about the research issues. The filter of the last 3 years 2019-2023 was applied in the database search which helped the report to find the latest information about the issue. The different variables in this report were used as search words to find information and articles to make in-depth findings about each of the variables and establish relationships with the different variables to conduct the literature review in this research. The database search was done in an orderly or structured form so a proper flow of information can be maintained in this report.

Limitation of the literature review

This research was carried out with greater efficiency, however, there were still some limitations and challenges that the research faced in the course of this research. The filtering of the information from the various articles available in Google Scholar was a big challenge. A number of articles from the available articles were selected which was a time-consuming process to find the relevant information about the research was also a challenge and the limitations of the literature review. There were a lot of available articles however to find relevant information specific to the research topic was the biggest limitation of this research which may also hamper the quality of the literature review in this research. In the activity of

searching the database of Google Scholar, important articles which would have helped in making a good analysis may have been ignored as searching for the correct articles was a tedious task.

Inclusion and exclusions

Cybersecurity awareness in the context of the industrial Internet of Things.	Excluded	This article seemed irrelevant to the research issue.
Remote working pre-and post-COVID-19: an analysis of new threats and risks to security and privacy	Included	This article had all the relevant information to be included in this research issue.
Cyber security of online proctoring systems	Excluded	This article was also totally not relevant to the research topic.
Understanding the cybersecurity challenges of telecommuting and video conferencing applications in the COVID-19 pandemic	Included	Useful information
Home working and cyber security–an outbreak of unpreparedness?	Included	Relevant information
Developing a cyber security culture: current practices and future needs.	Excluded	The information provided is too general to be used in this research work.
IT risk and resilience—Cybersecurity response to COVID-19	Included	Proper and relevant information is required for this study.

Cyber security attacks on smart homes during covid-19 pandemic.	Excluded	This article is not relevant to this study.
Balancing cyber security after the pandemic (tips and tricks)	Excluded	This article is full of technical knowledge which is not useful in this research.
Working from home during COVID-19 crisis: a cyber security culture assessment survey	Included	This article is good to find out the challenges faced by users and organizations in terms of cyber-security in the remote work environment.

Conclusion

With the advent of the pandemic, the work culture has completely transformed as most people preferred to work from their homes to decrease physical contact with people to stay safe from the pandemic. This work culture has offered many challenges in the form of cybersecurity threats for organizations and users. Cyber security threat such as phishing has become common in the remote working. The organizations have also undergone various transformations in their cyber security practices and procedures to enable the organization to handle the issues related to cyber security. The organizations made their IT department more effective and more informed to handle the issues related to cyber security. In this research report the challenges that are faced to manage the issue related to cyber-security are discussed with the help of the articles and journals that were available in the database of Google Scholar. The new practices that the company can adopt to handle these issues to handle issues related to cybersecurity are also discussed in this research. The organization should try to keep a backup of all the data so that data omission due to cyber security issues can be managed by the organization. Companies have to make investments in cyber security solutions to empower the organization to handle the issues related to the cyber-security.

References

Borkovich, D.J. and Skovira, R.J., 2020. Working from home: Cybersecurity in the age of COVID-19. *Issues in Information Systems*, *21*(4).

Dhirani, L.L., Armstrong, E. and Newe, T., 2021. Industrial IoT, cyber threats, and standards landscape: Evaluation and roadmap. *Sensors*, *21*(11), p.3901.

Furnell, S. and Shah, J.N., 2020. Home working and cyber security–an outbreak of unpreparedness?. *Computer fraud & security*, *2020*(8), pp.6-12.

Georgiadou, A., Mouzakitis, S. and Askounis, D., 2022. Working from home during COVID-19 crisis: a cyber security culture assessment survey. *Security Journal*, *35*(2), pp.486-505.

Hijji, M. and Alam, G., 2022. Cybersecurity Awareness and Training (CAT) Framework for Remote Working Employees. *Sensors*, *22*(22), p.8663.

Kaushik, M. and Guleria, N., 2020. The impact of pandemic COVID-19 in workplace. *European Journal of Business and Management*, *12*(15), pp.1-10.

Menze, T., 2020. The State of Industrial Cybersecurity in the Era of Digitalization. *Online, https://ics. kaspersky. com/media/Kaspersky ARC ICS-2020-Trend-Report. Pdf*.

Okereafor, K. and Manny, P., 2020. Understanding cybersecurity challenges of telecommuting and video conferencing applications in the COVID-19 pandemic. *Journal Homepage: http://ijmr. net. in*, *8*(6).

Ramadan, R.A., Aboshosha, B.W., Alshudukhi, J.S., Alzahrani, A.J., El-Sayed, A. and Dessouky, M.M., 2021. Cybersecurity and Countermeasures at the Time of Pandemic. *Journal of Advanced Transportation*, *2021*, pp.1-19.

Škiljić, A., 2020. Cybersecurity and remote working: Croatia's (non-) response to increased cyber threats. *International Cybersecurity Law Review*, *1*, pp.51-61.

Weil, T. and Murugesan, S., 2020. IT risk and resilience—Cybersecurity response to COVID-19. *IT professional*, *22*(3), pp.4-10.

Fwd: UKS31093

ORIGINALITY REPORT

9%	9%	2%	7%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	pure.royalholloway.ac.uk Internet Source	2%
2	erepository.uonbi.ac.ke Internet Source	1%
3	www.semanticscholar.org Internet Source	1%
4	www.mdpi.com Internet Source	1%
5	Submitted to University of York Student Paper	1%
6	Submitted to Global Banking Training Student Paper	1%
7	www.researchgate.net Internet Source	1%
8	www.hkjoss.com Internet Source	1%
9	ijcnis.org Internet Source	<1%

10	www.theseus.fi Internet Source	<1%
11	lup.lub.lu.se Internet Source	<1%
12	Zhiran Huang, Becky P.Y. Loo, Kay W. Axhausen. "Travel behaviour changes under Work-from-home (WFH) arrangements during COVID-19", Travel Behaviour and Society, 2023 Publication	<1%
13	www.utupub.fi Internet Source	<1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		