doi:10.20944/preprints202208.0513.v1

THE INCREASE IN SECURITY BREACHES THROUGH REMOTE WORKING

Syed Adnan Jawaid

University of Maryland-College Park, MD 20742, United States

Email: adnan.jawaid@hotmail.com

Abstract:

Background: The rise of cloud computing has led to the increasing number of organizations that rely on it for various tasks and services, such as education, healthcare, and e-commerce. Unfortunately, many security threats can be caused by the sudden use of cloud platforms.

Objective: This paper aims to provide a comprehensive overview of these threats and how they can be mitigated. Many companies are moving toward cloud computing to sustain their business growth and provide their employees with the best possible work environment.

Results: Due to the rise of cyber security threats and the unprecedented number of breaches of data, small and medium-sized enterprises are also starting to take a huge leap. The outbreak of COVID-19 has affected the lives of people all around the world.

Conclusion: Due to the seriousness of the situation, the WHO has declared the COVID-19 pandemic a public health emergency. To minimize the spread of the virus, the entire world has started adopting social distancing.

Keywords: Increase in Security Breaches through Remote Working, Security Breaches, Remote Working issues, Remote Working Challenges, Vulnerability issues while Remote working

1. INTRODUCTION

The following paper has been dealing with the issues that have been faced by people during the COVID-19 outbreak mainly due to the factor of data breaching. The paper discusses how data was compromised on Cloud, which is widely used by people worldwide to keep their work safe. Due to the increasing number of people using cloud storage and software-as-a-service (SaaS), the need for more effective and efficient data handling has become more prevalent. This is also reflected in the increasing number of organizations using the cloud for various functions such as education, healthcare, and e-commerce. Due to the emergence of the COVID-19 pandemic, various cloud services have been affected. This has increased the risk of cyber threats and breaches. In addition to data breaches, other factors such as network breaches are also common targets for attackers. As a result, it is important that the security concerns of organizations are continuously reviewed [1].

A survey conducted by Verizon in March to June revealed that there were 474 data breaches reported globally. Most of these incidents were caused by hackers and thieves, with 80% of them happening in the form of brute force attacks and hacking. The number of confirmed data breaches also doubled from the previous survey [2]. The survey was conducted by 81 global contributors. In March, a similar survey was conducted by Microsoft. It revealed that the number of people using cloud services in Italy increased significantly following the lockdown [3].

The article further highlights the causes and the issues that are faced by people mainly due to working remotely, this included students studying online and impact on the companies as the employees were majorly working from home. The database of education institutions is a treasure chest of potential. It can be exploited by criminal groups to gain access to sensitive data, which is very valuable for their purposes. Schools and universities are also very vulnerable to attack because they store reams of data that are essential to society and the economy [4].

doi:10.20944/preprints202208.0513.v1

2. REASONS FOR CYBER ATTACKS

Without proper authorization and authentication, remote workstations can't use enterprise resources for their intended purpose. This is typically the main reason why attackers use biometric methods to access corporate networks. The rapid emergence and evolution of cloud services has created a huge opportunity for both the private and public sectors. However, it is important to note that the increasing number of people using cloud services has led to a rise in the number of security vulnerabilities. This is because the lack of proper security policies can allow attackers to access the data stored in the cloud [5].

3. TECHNIQUES FOR CYBER ATTACK

One of the most common ways that attackers can access an organization's cloud services is through a home network. This method allows them to connect to the company's network without any privacy protocol. When connecting to an untrusted network, attackers can cause various types of attacks, such as IP spoofing and distributed denial of service (DDoS). Besides being able to access the data stored in the cloud, attackers can also perform various attacks on the system through a network connection. Some of these include DNS hijacking, cache spoofing, and DNS snooping [6].

The lack of proper training and policies regarding the use of cloud services has made employees vulnerable to security breaches. Due to the lack of proper budget support for the implementation of security policies, the number of dedicated budget slots for remote working decreased during the fiscal year. One of the most common types of cyber-attacks that can be carried out during a health crisis is social engineering. This type of attack involves tricking people into divulging their sensitive information. Due to the nature of this attack, it can be used to take advantage of the remote working situation [7].

In recent days, there has been a rise in the number of severe phishing attacks, which are mainly caused by the sharing of sensitive information through social media platforms such as WhatsApp. This type of attack usually occurs when an attacker sends an email with a link that imitates an official email [8].

Another common type of cyber-attack that can be carried out is phishing, which involves tricking people into clicking on a link that is sent by a fake email. This type of attack usually involves making the victims fall for a fake authority. One of the main reasons why people use cloud services is to keep track of their hobby or passion. They are more likely to follow the latest trends in social media. With the help of cloud services, people can easily access various applications, such as music, video, and photos. One of the most common ways that attackers can access a person's account is by sharing a window with the working platform [9].

5. **CRITICAL ANALYSIS**

The article highlights the different kinds of cyber attacks that have been happening due to the increase in remote working. But the article does not majorly discuss how these problems can be solved. The cyber attacks have been a major concern for every company having remote users, they know why they are being attacked and how they are attacked the issue is how to resolve such issues. Another thing that the article lacked was that even if people were not using the cloud or they were using something much safer the reasoning of those cyber-attacks. The preventions are given in the section 4 of the article which are quite limited and a reader would expect more of them to be briefly described in steps. Other than this the article was informative and well-versed while being referenced properly [10]. The few guidelines on how the prevention of cyber-attacks should be minimize were to have a strong password policy is required for all workstations and hosts to ensure that they are protected. Multi-authentication policies should also be implemented. The use of a shared file system such as Google Drive, Dropbox, or even an email address is required for employees to communicate. However, it is not allowed to share files through social media or any other free email address. Also, make sure that all the files are back on the hard disk before sharing them. Before downloading a certain application, make sure that the source of the information is known. Also, keep in mind that the latest security patches are released every time. To prevent the spread of email spoofing attacks, use DMARC, SPF, and DKIM protocols [11].

6. ADVANTAGES OF TECHNOLOGY

One of the many advantages of technology is that it allows people to work from home. Until recently, it had been relatively rare for people to experience this practice. In 2020, the Covid-19 pandemic forced many organizations to close their doors and send their staff home. This change was largely due to the emergence of the standard advice about home working. The rise of technology was also the driving force behind the changes [2].

The rise of the Covid-19 pandemic has changed the way people think about home working. This paper aims to provide a comprehensive analysis of the various factors that affected the way organizations and their staff members were prepared for the outbreak. Although home working is not a new concept, it is not always a priority when it comes to security [12]. In 2006, a study revealed that many people were not well-equipped to handle the various security threats that can affect their operations at home. This issue is now ten years later, and it is important to see if the situation has changed. In addition to being able to identify and implement effective safeguards, it is also important to consider if there are still adequate provisions in place when it comes to dealing with unexpected situations [13].

Although home working has been the norm for some workers, it has not been the case for a large portion of the workforce. For instance, on March 16, 2020, only 15% of the UK's workforce was working from home. By April 13, this figure had doubled, and it is estimated that approximately 6.8 million employees were working at home during the peak of lockdown [14].

7. HIERARCHICAL PREPARATION OF WORKPLACES

The review provides an overview of the extent to which organizations and their staff members were prepared for the unexpected emergence of home working and the subsequent cyberthreats that were presented in parallel. While the discussion is focused on the UK, other regions are also likely to have similar issues. Due to the data collected by the authors, the overall picture is likely to be similar [15]. The findings of the CSBS 2020 survey revealed that businesses have a number of actions they can take to improve their cyber security. These actions are aligned with the recommendations of the National Cyber Security Center's 10 Steps to Cyber Security. The 10 steps were established in 2012 to provide a comprehensive view of the various aspects of cyber security [16].

Around 12% of businesses have already taken action against all of the steps that were outlined in the 10 Step Plan. This figure varies depending on the size of the organization, with the small firms having fewer than 1 employee having fewer than 9% compliance, while the large companies with 250+ employees have 42% [17].

Companies of all sizes are expected to have the necessary resources and skills to perform at their best in the 10 steps of the security assessment. However, larger firms also have more complex needs when it comes to cyber security. This is why it is important that they do more to address these issues [2]. Most small businesses do not need advanced monitoring tools or network security. The 10 steps provide a framework for addressing the various aspects of cyber security for all sizes of organizations. They help us identify which parts of an organization have invested in this area [18]

8. RESULTS

The results of this survey suggest that many businesses do not take the necessary steps to educate their employees about the importance of mobile and home working. Only a quarter of the respondents said they have addressed these issues. The level of compliance with the 10 steps is more granular, considering the various aspects of security that are included in the survey. However, there is a notable drop-off in the number of firms that are focused on the people-centric aspects of security. This is consistent with the survey's previous releases [19].

Despite the complexity of their cyber security needs, many small businesses do not need advanced monitoring and security tools. This is why we have created a comprehensive framework that aims to help small and medium-sized enterprises identify their current state of cyber security and invest in the necessary resources to improve their operations [20].

The proportion of employees working in large companies has increased significantly over the past couple of years. It is now 42% in large firms with over 250 employees, and 9% in micro firms with less than a hundred workers. This suggests that larger firms have the necessary resources and skills to do better at certain steps [21].

The results of this study article suggested that although the prevalence of home and mobile working has remained relatively low in the UK, companies are still not overly concerned by these issues. This suggests that they have not learned the lessons of past experiences. Mobile working and home working were also not considered risky at this point [22].

There's also indirect proof that businesses with home-based cyber policies tend to have more charitable organizations than those who rely on external help. There's also evidence to suggest that many of the lessons that have been learned in the past have not been implemented. For instance, according to a study conducted by CSBS 2020, the most common response to a cyber-attack is to provide additional staff training. However, this suggests that the support that is being provided is not being proactively maintained [1]

CSBS series findings have generally suggested a variety of schools of thought regarding cyber security among those in charge of the security department. Most of the time, those in charge of security think that end user awareness is very important. However, they also feel that they have a hard time convincing the management boards to support their efforts. Some of the people who believe that cyber security is an issue of common sense are those who believe that end users should take the necessary steps to protect themselves. This is a less common view in the past couple of years [2]

Despite the various factors that affect the development and maintenance of cyber security, it's still common for people to dismiss security education and awareness as a waste of time. This is because the assumption that people will not notice or take any notice of the warnings is often the reason why people do not take action [2].

9. **DISCUSSION**

The research article covers every aspect of the cyber security issue due to remote working. Even though the remote working was majorly seen during the pandemic, the article covers the issue from 2004. The initial phase of the cyber security being compromised due to remote working was lack of knowledge. Over the years this scenario has changed even with vast security breaches the security is still not strong enough to work remotely. The article also gives an overview of the issues that are faced by companies due to these breaches [23]. Upon further reading, the article discusses to resolve such issues and the study and its findings were reliable as per the quantitative data collected. The main thing that a reader will catch the eye of the reader is the increasing number of people choosing to work from home has created a new opportunity for employers to adopt secure home-working practices. There is a wide variety of resources available to help staff develop effective strategies, but they need to be directed towards it and are also certain that they cover the bases that they need to. It is important to note that many businesses have not taken the time to seek out the necessary guidance on how to effectively implement home-working practices. According to a survey conducted by CSBS 2020, only 54% of businesses have sought out external information about cyber security [24].

The number of people who are aware of the importance of securing their personal data has increased significantly since the introduction of the GDPR in 2018. However, it still means that many businesses are not able to access the necessary resources to help them implement this strategy. The Covid-19 pandemic provides businesses with an opportunity to take advantage of the various government initiatives that are aimed at supporting the development of effective home-working practices. For instance, by providing support through business-support schemes, the government can help direct companies toward the appropriate cyber guidance. In the UK, there is potential for businesses to find out about the various resources that are available to help them implement home-working practices through the gov.uk's Covid-19 support. This could also be done through other organisations [25].

CONCLUSION

This article aimed to discuss the security concerns faced by different sectors of the healthcare industry, such as IT, education, and banking. During the period of March to July, there have been several cyber security attacks that affected the healthcare industry. The article also presented a literature study that describes the various attacks that occurred.

The graph of social engineering attacks has increased significantly over the previous year. This issue is considered a serious threat that requires the establishment of a comprehensive security policy. Besides changing the policies, users also need to be aware of the various precautions that they can take to prevent their workstations from being attacked. In order to address the security concerns of remote workers and distance learners, people will develop a security protocol that will allow users to control the access to their cloud resources.

Regardless of the nature of Covid-19, the security of flexible working remains an issue that employers need to address. This is because the increasing number of people working in the gigantic economy will inevitably lead to them being placed in different roles. To ensure that their employees are aware of the proper practices and policies when it comes to cyber security, organisations will need to make sure that they are regularly updated. This can be done through the establishment of a clear understanding of the various roles and responsibilities of gig workers. The effects of Covid-19 are likely to have a long-lasting impact on the lives of individuals. Although the issues discussed here are relatively minor compared to the loss of life and the consequences of the pandemic, they still remain significant.

Bibliography

(1)

Mandal, S.; Khan, D. A. A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic https://ieeexplore.ieee.org/abstract/document/9215374. https://doi.org/10.1109/ICOSEC49089.2020.9215374.

(2)

Furnell, S.; Shah, J. N. Home Working and Cyber Security – an Outbreak of Unpreparedness? *Computer Fraud & Security* **2020**, *2020* (8), 6–12. https://doi.org/10.1016/S1361-3723(20)30084-1.

(3)

Kurpjuhn, T. The SME Security Challenge. *Computer Fraud & Security* **2015**, *2015* (3), 5–7. https://doi.org/10.1016/s1361-3723(15)30017-8.

(4)

Alexei, A.; Alexei, A. Cyber Security Threat Analysis in Higher Education Institutions as a Result of Distance Learning. *repository.utm.md* **2021**, *4* (3).

(5)

Williams, M. L.; Levi, M.; Burnap, P.; Gundur, R. V. Under the Corporate Radar: Examining Insider Business Cybercrime Victimization through an Application of Routine Activities Theory. *Deviant Behavior* **2018**, *40* (9), 1119–1131. https://doi.org/10.1080/01639625.2018.1461786.

(6)

Curran, K. Cyber Security and the Remote Workforce. *Computer Fraud & Security* **2020**, *2020* (6), 11–12. https://doi.org/10.1016/s1361-3723(20)30063-4.

(7)

Parmar, B. Protecting against Spear-Phishing. *Computer Fraud & Security* **2012**, *2012* (1), 8–11. https://doi.org/10.1016/s1361-3723(12)70007-6.

(8)

Saura, J. R.; Ribeiro-Soriano, D.; Zegarra Saldaña, P. Exploring the Challenges of Remote Work on Twitter Users' Sentiments: From Digital Technology Development to a Post-Pandemic Era. *Journal of Business Research* **2022**, *142*, 242–254. https://doi.org/10.1016/j.jbusres.2021.12.052.

(9)

Venkatesha, S.; Reddy, K. R.; Chandavarkar, B. R. Social Engineering Attacks during the COVID-19 Pandemic. *SN Computer Science* **2021**, *2* (2). https://doi.org/10.1007/s42979-020-00443-1.

(10)

Ncubukezi, T.; Mwansa, L. Best Practices Used by Businesses to Maintain Good Cyber Hygiene during Covid19 Pandemic. *Journal of Internet Technology and Secured Transactions* **2021**, *9* (1), 714–721. https://doi.org/10.20533/jitst.2046.3723.2021.0086.

(11)

Opara, E.; Soluade, O. Straddling the next Cyber Frontier: The Empirical Analysis on Network Security, Exploits, and Vulnerabilities. *International Journal of Electronics and Information Engineering* **2015**, *3* (1), 10–18.

(12)

Johns, E. DCMS: Cyber Security Breaches Survey 2021. *Network Security* **2021**, *2021* (4), 4. https://doi.org/10.1016/s1353-4858(21)00036-2.

(13)

Hina, S.; Panneer Selvam, D. D. D.; Lowry, P. B. Institutional Governance and Protection Motivation: Theoretical Insights into Shaping Employees' Security Compliance Behavior in Higher Education Institutions in the Developing World. *Computers & Security* **2019**, *87*, 101594. https://doi.org/10.1016/j.cose.2019.101594.

(14)

Tawalbeh, L.; Muheidat, F.; Tawalbeh, M.; Quwaider, M. IoT Privacy and Security: Challenges and Solutions. *Applied Sciences* **2020**, *10* (12), 4102. https://doi.org/10.3390/app10124102.

(15)

Wiafe, I.; Koranteng, F. N.; Obeng, E. N.; Assyne, N.; Wiafe, A.; Gulliver, S. R. Artificial Intelligence for Cybersecurity: A Systematic Mapping of Literature. *IEEE Access* **2020**, *8*, 146598–146612. https://doi.org/10.1109/access.2020.3013145.

(16)

Priestman, W.; Anstis, T.; Sebire, I. G.; Sridharan, S.; Sebire, N. J. Phishing in Healthcare Organisations: Threats, Mitigation and Approaches. *BMJ Health & Care Informatics* **2019**, *26* (1), e100031. https://doi.org/10.1136/bmjhci-2019-100031.

(17)

Eian, I. C.; Yong, L. K.; Li, M. Y. X.; Qi, Y. H.; Z, F. Cyber Attacks in the Era of COVID-19 and Possible Solution Domains. *www.preprints.org* **2020**. https://doi.org/10.20944/preprints202009.0630.v1.

(18)

Palanisamy, R.; Norman, A. A.; Mat Kiah, L. BYOD Security Risks and Mitigation Strategies: Insights from IT Security Experts. *Journal of Organizational Computing and Electronic Commerce* **2022**, 1–23. https://doi.org/10.1080/10919392.2022.2028530.

(19)

Faraj, S.; Renno, W.; Bhardwaj, A. Unto the Breach: What the COVID-19 Pandemic Exposes about Digitalization. *Information and Organization* **2021**, *31* (1), 100337. https://doi.org/10.1016/j.infoandorg.2021.100337.

(20)

Hicks, M. Why the Urgency of Digital Transformation Is Hurting the Digital Workplace. *Strategic HR Review* **2019**, *18* (1), 34–35. https://doi.org/10.1108/shr-02-2019-153.

(21)

Dolezel, D.; McLeod, A. Managing Security Risk. *The Health Care Manager* **2019**, *38* (4), 322–330. https://doi.org/10.1097/hcm.0000000000000282.

(22)

Bello Garba, A.; Armarego, J.; Murray, D. Bring Your Own Device Organizational Information Security and Privacy. *ARPN Journal of Engineering and Applied Sciences* **2015**, *10* (3), 1279–1287.

(23)

Khando, K.; Gao, S.; Islam, S. M.; Salman, A. NEnhancing Employees Information Security Awareness in Private and Public Organisations: A Systematic Literature Review. *Computers & Security* **2021**, *106*, 102267. https://doi.org/10.1016/j.cose.2021.102267.

(24)

Babiceanu, R. F.; Seker, R. Cyber Resilience Protection for Industrial Internet of Things: A Software-Defined Networking Approach. *Computers in Industry* **2019**, *104*, 47–58. https://doi.org/10.1016/j.compind.2018.10.004.

(25)

Chauhan, P. S.; Kshetri, N. CSDL | IEEE Computer Society

https://www.computer.org/csdl/magazine/co/2021/08/09504500/1vJVwMtqeWY.