Security Breaches of Remote Working

Tanvi Saini (209301610)
Department Of Computer Sciences and Engineering
tanvi.209301610@muj.manipal.edu

Aditya Sharama (209202224)
Department Of Electronics and Communication Engineering
aditya.209202224@muj.manipal.edu
Manipal University Jaipur, Rajasthan, India

Abstract- In recent years, remote working has become a popular mode of work arrangement for many organizations, particularly with the advancement of technology that allows people to work from anywhere at any time. The COVID-19 pandemic further accelerated the trend. One of the most significant risks is the increased likelihood of data breaches, which can result in loss or theft of sensitive information such as customer data, financial records, and intellectual property targeted by Hackers and cybercriminals.

The purpose of this research is to analyze the security risks associated with remote working and explore the potential solutions to mitigate those risks. As the COVID-19 pandemic forced a significant shift towards remote work, cybercriminals have found new opportunities to exploit vulnerabilities in remote working environments.

This research aims to provide insights into the causes of security breaches in remote working environments and identify the best practices that can be implemented to improve security. It will also examine the impact of security breaches on organizations, their employees, and their customers.

The significance of this research lies in its potential to help organizations and individuals understand the risks associated with remote working and adopt effective security measures to protect themselves..

Moreover, the research will explore the impact of remote work security breaches on various industries, such as healthcare, finance, mental health and consequences, and education, and how these industries can improve their security measures to prevent future breaches. The study will also analyze the role of technology in facilitating remote work and how advancements in technology can help organizations enhance their security measures.

Keywords- hacker, cybercrime, security, remote work, COVID-19, security breach

1.INTRODUCTION

With the advent of technology, remote working has become increasingly popular in recent years. Many organizations have embraced remote working as a way to provide flexibility to their employees and reduce their overhead costs. However, the rise of remote working has also brought new security challenges for organizations. The security breaches of remote working can have significant consequences for both individuals and organizations. In this research paper, we will explore the security challenges of remote working and examine the impact of security breaches on organizations and individuals.

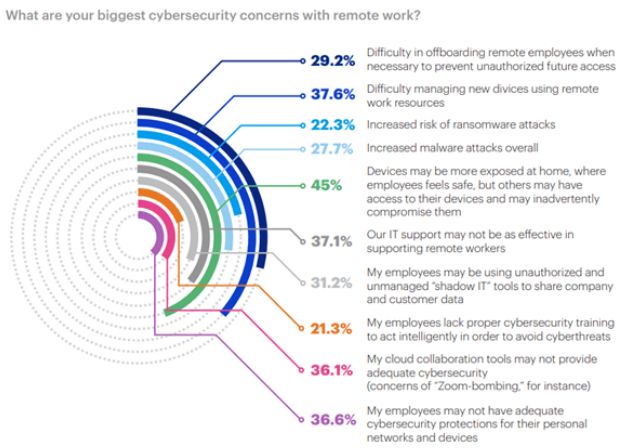
The COVID-19 pandemic has accelerated the trend towards remote working as organizations have been forced to adapt to new working conditions. With remote working becoming the norm, organizations are increasingly concerned about the security of their systems and data. Cybercriminals are taking advantage of the vulnerabilities of remote working tlaunch attacks on organizations. They are exploiting weaknesses in the security protocols of remote working to gain access to sensitive data and systems. Remote workers may also inadvertently compromise the security of their organizations through their actions, such as using unsecured networks or devices.

The security breaches of remote working can have a range of consequences for organizations. The loss of sensitive data can damage an organization's reputation and lead to financial losses. In some cases, security breaches can lead to legal action being taken against the organization. The impact of security breaches can also be felt by individuals. Remote workers may have

their personal information compromised, which can lead to identity theft or financial fraud.

As per the second edition of the International Labour Organization (ILO) Monitor released on April 7th, 2020, almost 81% of the global workforce, which accounts for approximately 2.7 billion workers, are currently affected by complete or partial lockdown measures (ILO Monitor: COVID-19 and the world of work. Second edition 2020). Due to the COVID-19 pandemic, it is projected that around 195 million full-time workers, or 6.7% of working hours worldwide, will be lost in the second quarter of 2020. Consequently, losses incurred by different income groups are expected to surpass the impacts of the financial crisis of 2008-2009.

Various Cyber Security Centers and experts across the world have provided suggestions and advice to help people protect themselves from cyber crimes and fraud. Due to the growing number of countries advocating for citizens to stay, study, or work from home, the need for cybersecurity has become even more crucial. Given the current situation, it begs the question of how the COVID-19 crisis has impacted the cybersecurity practices of both individuals and organizations.



2. LITERATURE REVIEW

A) Overview of Remote working and its prevalence

Remote working, also known as telecommuting or teleworking, refers to the practice of working outside of a traditional office environment, typically from home or another remote location. The concept of remote work has been around for many years, but it has become increasingly prevalent in recent years due to advancements in technology and the growing demand for flexible work arrangements.

Remote work has become particularly widespread during the COVID-19 pandemic as many organizations have been forced to adapt to remote work to comply with social distancing guidelines. In fact, a large number of employees are expected to continue working remotely even after the pandemic has subsided. The benefits of remote work include increased flexibility, reduced commuting time and cost, and greater work-life balance. However, the shift to remote work has also created new challenges and risks, particularly in the realm of cybersecurity. The use of personal devices and home networks can make organizations more vulnerable to security breaches and data theft.

As a result, it is important to understand the prevalence of remote work, its benefits and challenges, and the security risks associated with it in order to develop effective strategies for addressing these risks and ensuring the security of organizational data.

B) Challenges and Impact

Remote working comes with various challenges that organizations and employees face. One of the main challenges of remote working is maintaining data security. With employees working from different locations and using different devices, it can be difficult for organizations to maintain proper security measures. This can lead to an increased risk of cyber-attacks, data breaches, and other security threats. Additionally, employees may not have the necessary equipment or infrastructure to work securely from home, which can make them vulnerable to cyber-attacks.

Another challenge is the impact on employee mental health and wellbeing. Remote working can cause employees to feel isolated and disconnected from their colleagues, which can lead to feelings of stress and anxiety. Additionally, the boundaries between work and personal life can become blurred, leading to

work-related stress and burnout. This can also lead to decreased productivity and poor work performance.

Effective communication can also be a challenge in remote working. With employees working from different locations and time zones, it can be difficult to ensure everyone is on the same page and working towards the same goals. This can lead to miscommunication, delays in projects, and ultimately impact the organization's bottom line.

Research conducted during the COVID-19 pandemic has shown that remote working has had adverse effects on employee well-being and mental health. Studies suggest that remote working can lead to an "always-on" work mode, resulting in mental and physical fatigue. For instance, research by Hernandez (2020) and Molino et al. (2020) support this claim. Moreover, qualitative interviews with 50 newly working from home employees indicate that remote work can negatively affect productivity, according to Mustajab et al. (2020). Participants cited reasons such as multitasking, decreased motivation, childcare responsibilities, and psychological issues for the decline in productivity.

Overall, while remote working has many benefits, it also comes with its own set of challenges. It is important for organizations to address these challenges to ensure the security and wellbeing of their employees, while maintaining the productivity and efficiency of the organization.

C) Security Risks and threats

Remote working has become a treding these days, but it has also led to an increase in security risks and threats. One of the major risks associated with remote working is the use of unsecured networks, such as public Wi-Fi, which can be easily compromised by hackers. Attackers can exploit vulnerabilities in the network to gain access to sensitive data, including passwords and financial information.

Another security threat associated with remote working is the use of personal devices for work-related activities. Personal devices may not have the same level of security as company-provided devices, leaving them vulnerable to attacks. Additionally, employees may unintentionally download malware or other malicious software on their devices, which can then spread to the company's network.

Phishing attacks are also a significant risk associated with remote working. Cybercriminals often use social engineering tactics to trick employees into revealing sensitive information, such as login credentials or financial information. These attacks can be particularly effective against employees who are not used to working remotely and may be more susceptible to social engineering tactics.

According to a survey conducted by Verizon from March to June, there were 474 reported data breaches globally, with the majority being caused by hackers and thieves. Of these incidents, 80% were attributed to brute force attacks and hacking. The number of confirmed data breaches had also doubled compared to the earlier survey. The survey was conducted by 81 global contributors. In March, Microsoft conducted a similar survey that showed a significant increase in the number of people using cloud services in Italy following the lockdown.

Lastly, the lack of physical security measures is another challenge of remote working. Company data may be accessed or stolen if an employee's device is lost or stolen, or if unauthorized individuals gain access to the employee's workspace.

Overall, it is essential for organizations to recognize these security risks and take measures to mitigate them in order to protect sensitive data and prevent security breaches.

D) Types and Causes of Security Breaches in Remote Working

There are various types and causes of security breaches that can occur in remote working. One of the most common types of breaches is phishing attacks, where attackers send fraudulent emails, messages or calls to trick employees into divulging sensitive information

such as login credentials. Other types of breaches include malware attacks, where attackers use malicious software to gain access to a system, and unauthorized access to sensitive information by insiders or external attackers.

The causes of security breaches in remote working are varied and can include weak passwords, unsecured networks, and outdated software. In many cases, employees are not aware of the risks associated with remote working, and they may not be following best practices for securing their devices and networks. Another cause of security breaches in remote working is the lack of proper security measures in place, such as firewalls, antivirus software, and encryption.

Moreover, the use of personal devices and unsecured Wi-Fi networks by employees can also increase the risk of security breaches. Remote workers often use their personal devices to access company data, and these devices may not have the same level of security as company-issued devices. Additionally, unsecured Wi-Fi networks can be easily intercepted by attackers, putting sensitive data at risk.

It is important for organizations to be aware of the types and causes of security breaches in remote working and take proactive measures to mitigate these risks. This can include implementing strong password policies, providing secure remote access to company networks, and conducting regular security training for employees.

As per the CNBC cyber report, Phishing attacks are growing in frequency and sophistication, posing an increasing threat to internet users. According to a study conducted by messaging security provider SlashNext in October 2022, which analyzed billions of link-based URLs, attachments, and natural language messages in email, mobile and browser channels over a six-month period, over 255 million attacks were identified. This marks a 61% increase in the rate of phishing attacks from the previous year. The research also revealed that hackers are increasingly targeting mobile devices and personal communication channels, with a 50% increase in attacks on mobile devices. The study identified scams and credential theft as the most commonly used tactics. This shift towards mobile devices and personal communication channels as a means of attack has made it easier for hackers to reach potential victims, making it critical for individuals and organizations to take steps to protect themselves from these evolving threats.

E) Impact of Security Breachs

Security breaches have significant impacts on both organizations and individuals, especially in the context of remote working. For organizations, a breach can result in financial losses, reputational damage, and legal implications. The cost of repairing the damage caused by a breach can be significant, ranging from recovery of lost data to fines and legal fees. Additionally, customers may lose trust in the organization, resulting in a loss of business and damage to the company's reputation.

For individuals, security breaches can result in identity theft, financial losses, and emotional distress. Breaches can compromise sensitive personal information, such as social security numbers, bank account details, and medical records. This information can be used by cybercriminals for fraudulent activities, leading to financial losses for individuals. Moreover, the emotional toll of having one's personal information stolen can be significant, causing stress and anxiety.

As per the reports, the healthcare sector is suffering the most due to data breaches, with an average cost of $9.23 million per incident - the highest cost among all industries surveyed. Similarly, data breaches are also causing significant financial losses for the financial sector, with an average cost of $5.27 million, which is the second-highest after healthcare.

The US is the country that is most targeted by attackers, with a staggering 7,221,177 incidents per million people. France is a close second with 6,488,574 breached records per million citizens. Canada and the UK are also attractive targets for attackers due to their large population and advanced digital infrastructure.

If we talk about UK, according to a recent survey conducted by the UK government, 39% of businesses in the country experienced a cyber attack in the last year. Among these businesses, 31% claimed to have faced attacks at least once a week.

Table 1.1: Proportion of UK businesses identifying cyber attacks each yea

2017	2018	2019	2020	2021	2022
46%	43%	32%	46%	39%	39%

One out of five companies reported negative outcomes following these attacks. The estimated average cost of the cyber attacks was £4,200, but medium and large-sized businesses incurred a higher average cost of £19,400.

Also, the risk management report was also drawn by UK government, in which they found Slightly more than 50% of businesses have taken steps to recognize cyber security threats in the last year, with various measures taken, of which security monitoring tools (35%) were the most frequent. However, interviews with industry experts revealed that due to inadequate board comprehension, the responsibility for mitigating risks was often delegated to external cyber vendors, insurance providers, or an internal cyber professional.

Table 1.2: Proportion of UK businesses acting to identify cyber risks each year

2017	2018	2019	2020	2021	2022
57%	56%	62%	64%	52%	54%

3.OVERVIEW OF THE DATA COLLECTED

For the research on the topic of Security Breaches of Remote Working, data was collected from various sources including academic journals, industry reports,

and surveys conducted by reputable organizations. The data collected covers a wide range of topics related to remote working security, including the prevalence of remote working, challenges of remote working, security risks and threats associated with remote working, types and causes of security breaches in remote working, and the impacts of security breaches on organizations and individuals.

4.CONCLUSION

It is challenging to overstate the significant impact that COVID-19 has had on societies globally. Analyzing the effects of remote working on employee mental health, wellbeing, and cyber security behaviors uncovers a complex and intricate set of consequences on employee performance and attitudes. The literature on employee cyber security practices during the pandemic, combined with existing research on remote working and employee behaviors, reveals a wide array of outcomes. These include employee exhaustion, decreased productivity, insufficient awareness of cyber security principles related to remote working, and multiple implications for the psychological contract. An examination of employee relationships through the psychological contract concept highlights the need to reassess implicit agreements and understandings between employees and organizations in the new remote working context. Moreover, it underscores the importance of researching how leadership styles may need to be altered. From the literature, several recommendations emerge that could provide valuable guidance for organizations seeking to alleviate the pandemic's impact on employee well-being and mitigate insecure cyber security practices. Effective leadership styles, unambiguous communication, comprehensive risk awareness training, and flexibility to enable employees to avoid 'zoom fatigue' may help organizations fulfill their obligations within the psychological contract.

5.REFERENCES

[1]Review Article - (2022) Volume 19, Issue 7 "The Increase in Security Breaches Through Remote Working" By Syed Adnan Jawaid : Department of Health Sciences, University of Maryland-College Park, United States.

[2]Forbes Article by Benjamin Laker (Contributor)

[3]Article on Remote Working and Cyber Security Literature Review By: Nadine Michaelides, University College London

[4] CNBC Cyber Report By Bob Violino(2023)

[5] Report from nibusinessinfo.co.uk

[6] Report from gov.uk for statistics of cyber crime, security breach, and management

[7]Blog by Venkatesh Sunder at IndusFace(2022)

[8]Security Issue Blog by Pratik Dholakiya at Keap(2022)