Research conducted prior to the creation of new protocol for virtual operation

Secure remote working practices

Mahdi SarikhaniFard

Table of Contents

[Table of Contents 2](#_Toc135220135)

[Abstract 3](#_Toc135220136)

[Introduction 4](#_Toc135220137)

[Research Methodology 4](#_Toc135220138)

[Analysis 4](#_Toc135220139)

[Findings 4](#_Toc135220140)

[Discussion 4](#_Toc135220141)

[Conclusion 4](#_Toc135220142)

[Recommendation 4](#_Toc135220143)

# Abstract

Here in this report, we have been trying to discover and examine different strategies for enhancing cyber safety and communication practices in virtual environments of our organization. Our key objectives are as find an understanding of secure and effective protocols for virtual teamwork and its establishment. Research findings will further aid us in identifying critical areas we need to focus on its security such as accounts, data, network security, and web conferences being held. Later, we will try to integrate these best practices into organizational policies through updating our best practices and protocols.

## Introduction

Virtual environments have been recently getting a place where we will have our organizational operations in it. At the same time, we have got similar trend in the public, that every company is giving more attention to remote work and digital collaboration. These environments have been described as places where usually have their unique challenges, particularly around maintaining their security in communication channels and safeguarding sensitive information being used in them. As we have got a business which is aiming to continue to get more dependent on virtual tools for their team collaboration, we need to ensure about our quality and compliant of our cyber safety and communication protocols. This research aims to help us in developing effective guidelines that ensure secure interactions while performing communication among teams within operations. By addressing these areas mentioned, the focus will be on ensuring their compliance with industry standards. After that, we will have integration of our findings into organizational frameworks made previously for future reference. The outcome of this research will provide our organization with actionable strategies where we can mitigate cyber risks and improve virtual communication, assuring about efficiency and security in virtual environments.

## Research Methodology

I do believe we need to use a combination of both qualitive, and quantitative research strategies based on the given scenario and outlined objectives. In order to understand practices and techniques, sometimes interviews (as an example) can provide us in depth insights into recent industry cyber safety practices and communication techniques used by staff. Sometimes there are opportunities in this kind of research which can’t be find in quantitative research. So, these interviews need to be conducted with employees from different companies we are affiliate with. In these interviews we will receive their valuable experience and suggestions on our virtual communication and collaboration, ensuring thar our protocols outcomes are friendly and meet user needs. For quantitative research method, we can collect information by surveys and data analysis, which can provide you with measurable outcomes and statical evidence requested. Quantitative methods can be beneficial as it allows us to evaluate performance and reliability of our communication and collaboration tools using numbers its holding in its data. Quantitative data also can help us in understanding of trends in the industry about virtual communication and collaboration tools.

## Analysis

|  |  |
| --- | --- |
| Analysing and Synthesising Research Data  Secure remote working practices | |
| Steps | Analysis and Synthesis |
| 1. Review research objectives | We are supposed to perform research on cyber safety (and partly communication techniques) to find the latest measures for virtual environments where we can attach discovered effective communication methods in virtual environment between teams. So our objectives needed to obey a series of defined merits such as being up to date, reliable, guaranteed measurable outcomes and compliant with accepted industry strategies. After research and data collection, we need to gather all together to conclude to cyber safety protocol along with a Virtual Meeting Protocol. |
| 1. Review research data organisation (e.g., themes, categories) | I have created a template for organizing my data collected which I do believed can be used to feed an analyser platform if we wanted to go further. In this template, I have dedicated two separate tables for each topic and created each one 10 columns which are Source title, Author(s), publication date, publisher/Journal Name, Link, Type of source, Relevance to Research, Notes /Observations and Citation. |
| 1. Discover patterns, themes, trends and practices | All of data collected from each website had similar pattern, but as we put them next to each other they have potential to structure a theme based on how they are organized. In path to completing this mentioned, we also faced trends. Below is a summary: **Key Patters and Themes**  1. Strong Emphasis on Account Security:  We have got multi-factor authentication which has been highlighted multiple times as critical measure to prevent unauthorized access while using our devices and accounts for virtual communication. Moreover, there are recommendations for creating and maintaining strong, unique passwords and passphrases are consistently suggested, including the use of passport management tools.  2. Device and Data security:  There are a series of suggestion and essential security tips associated with devices being used for virtual communication. Suggestions can be like locking devices when unattended, keeping software updated, and performing regular data backup. Further, we found suggestions about safeguarding against risks associated with external devices being used and shared among staffs. Moreover, there are good practice suggestions to be implemented while using cloud storage along with encryption transfer as an encouraged alternative secure file transfer and storying method.  3. Network Security  We found recommendations including secure connection practices while being connected to the Wi-Fi network such as altering default settings and also avoiding public Wi-fi unless necessary. In addition, there are emphasise on importance of VPN usage for secure connections while working remotely.  4. Awareness of Surroundings and Potential Scams:  In our data collection, we observed that they have been stating the need for individuals to be cautious about their surroundings when accessing sensitive information, they usually handle while they are communicating virtually in a remote working area prevent data breach. Moreover, there are awareness regarding scams and the techniques used by cybercriminals, including identity theft, phishing and more hazardous threats they may face. These awarenesses mentioned can help us enrich our practices for mitigating such threats.  5. Use of remote Desktop Client  There are lots of industry guidelines associated with secure configuration of remote desktop clients to mitigate risk we face with remote access. In this case, we have found data on leading our path in the handling sensitive data within remote sessions with organized guidance provided by industry and government’s frameworks.  6. Web Conferencing Security  We have also collected data associated with guidelines on how to select and implement web conferencing solutions where provider has got strong encryption practices, and the ability to accommodate privacy and legal requirements for its users. It gives recommendations on how to securely conduct meetings on such solutions. |

## Findings

|  |  |
| --- | --- |
| 1. Summarise findings and recommendations | We were able to come to decision on usage of several key security practices those was highlighted in our collected data for virtual communication. In our data collected in last step, Account security was our priority which was almost main subjects of all of statements. In this case, we tried to address it with recommendations such as multi-factor authentication and implementing password management tools. We further decided to find a frame for our practices which was possible with having an understanding of our own device and data security industry requirement in framework they have presented. If we just want to state basic examples of advice can be possible outcome of our practices, we can state locking devices, updating software, and using encryption. Moreover, we decided to build a foundation which our employees can return to it for securing their connections. This will address their network security, where we can aid them in securing their Wi-Fi connections, asking them to prevent public network connections, and using VPNs for remote work. Lastly, we thought it is necessary to consider environmental elements and use data to tell them about importance of cyber awareness. This will help them in preventing including phishing attacks and identity theft. Finally, we came to conclusion that these data are acceptable for structuring best practices for securing clients, web conferencing tools and staffs. I do believe all these characters can aid each other to protect sensitive data and ensure privacy for each side. |
| 1. Share and distribute findings | In order to share it within the organization, I do believe that we first need to review the if there are existing security policies in this organization, using which we can ensure compliant with any specific requirements or protocols we may have missed. Based on the findings, I can establish a communication plan as a foundation for all of future communication among employees where they can find clear guidelines and best practices. This can be along with formal training sessions and learning materials. I need to identify internal channels such as email, the company intranet or the company’s Model learning platform. Additionally, we may need some regular reminders along with updates which need to be sent to them, and lastly a feedback mechanism will be helpful when it comes to addressing questions and concerns. Using distribution process, I can ensure that all staff are aware of these practises and adhere to the updated security protocols. |
|  |  |

## Discussion

## At the end of the research, we have got findings those are emphasizing the critical role of cybersecurity on communication protocols and how they are written out. Cybersecurity plays a vital role in virtual environments, especially in the context of remote work. The research highlights several key practices that ensure secure interactions among teams on virtual environments. These findings are compliant with industry standards, supporting all security necessities for safeguarding sensitive information in virtual settings.

## Additionally, the research helped us on the importance of integrating mentioned practices which found to be standard into organizational frameworks. This can be done later using structured training, clear guidelines, and consistent communication channels. Practices such as multi-factor authentication, VPN usage, and secure device management are not only essential to be implemented for avoiding unauthorized access but also for fostering a culture of awareness among internal actors such as employees.

## Moreover, we had emphasis on user awareness, especially regarding scams and phishing attempts, encouraging organization towards ongoing education to mitigate cyber threats. While the current study is mostly focus on establishment of security measures, I do believe that future exploration could affect our practices and will make us see a need of implementation new practices within organizations and explaining why employees need adherence to new protocols.

## Conclusion

Our study is concluding that a series of effective cyber safety measures and communication protocols are essential for starting operations in virtual environments. Mentioned secure practices, enhanced awareness processes, and utilized technologies if all being used, they will reduce risks.

## Recommendation

* Formalize Security Protocols: Create clear, documented guidelines addressing account, device, and network security.
* Training and Awareness: Conduct regular training sessions
* Leverage Technology: Adopt tools such as password managers, and secure web conferencing solutions.
* Communication Plan: Use internal channels (e.g., email, intranet) for updates and feedback mechanisms to address concerns.
* Periodic Reviews: Continuously assess and update protocols to align with evolving industry standards.