The Impact of Covid-19 on Information Security in an Organisational Context due to Increased Levels of Remote Working

Dissertation Submitted as a partial fulfilment for the Degree

of

Master of Sciences

(Information Security)

Submitted By:

Anshul Arora

UNISE1667IT

Supervisor:

Dr. Salvatore Fava

SELINUS UNIVERSITY OF SCIENCES AND LITERATURE

Via Pompeo Scipione Dolfi, 4, 94277 Bologna BO, Italy

2022

CERTIFICATE

SELINUS UNIVERSITY OF SCIENCES AND LITERATURE

VIA POMPEO SCIPIONE DOLFI, 4,

94277 BOLOGNA BO, ITALY

This is to certify that **Anshul Arora** is a bonafide student of M.Sc. (Information Security) (Enrolment no: **UNISE1667IT**) of **Selinus University of Sciences and Literature**. The present dissertation is submitted to in partial fulfilment of the requirement of the degree of Master of Sciences (Information Security). This dissertation under my guidance entitled **"The Impact of Covid-19 on Information Security in an Organisational Context due to Increased Levels of Remote Working"** is an original piece of research work and no part of this dissertation has been submitted for any other degree of any other University to the best of our knowledge.

Date:

Dr. Salvatore Fava

(SUPERVISOR)

DECLARATION

SELINUS UNIVERSITY OF SCIENCES AND LITERATURE

VIA POMPEO SCIPIONE DOLFI, 4,

94277 BOLOGNA BO, ITALY

I, ANSHUL ARORA (Enrol.no.: UNISE1667IT) student of M.Sc. (Information Security) Selinus University of Sciences and Literature has completed the dissertation entitled "The Impact of Covid-19 on Information Security in an Organisational Context due to Increased Levels of Remote Working" which embodies my original work and is submitted towards the partial fulfilment of the requirement of the degree.

ANSHUL ARORA

M.Sc. (INFORMATION SECURITY)

Enrollment No.: UNISE1667IT

Selinus University of Sciences and Literature

Date:

ACKNOWLEDGEMENT

I am thankful to my supervisor, **Dr. Salvatore Fava** for his guidance and suggestions during my research. He helped me to design, implement, apply, criticize and clearing the paths towards thesis completion with his solution-oriented approach.

I would like to extend my heart filled gratitude to my wife and parents for their unconditional love, help and support.

ANSHUL ARORA

M.Sc. (INFORMATION SECURITY)

Enrollment No.: UNISE1667IT

Selinus University of Sciences and Literature

TABLE OF CONTENTS

LIST OF FIGURES

ABSTRACT

The World Economic Forum's Global Risks Report 2021, clearly states that cyber risks continue to rank among the topmost global risks. The COVID-19 pandemic has further created a perfect environment to expose cyber vulnerabilities and unpreparedness. The new adopted business models that have been adopted by the companies during the pandemic which has made Working from Home the “new normal”. With companies now accelerating their digital transformation, cyber security has become a major concern. Neglecting information Security could lead to increased reputational, legal, operational and compliance risks. This dissertation aims to study the impact of COVID-19 on cyber risks due to increased remote working. To understand and analyse the same a survey of 12 questions was conducted with 200 information security professionals working as Team Leads and above, belonging to companies of varying sizes across multiple industries. The results hence generated after careful evaluation state that there has been a considerable surge in cyber security risks with the increase in remote working.

CHAPTER – 01

INTRODUCTION

1.1 THE COVID-19 PANDEMIC

1.1.1 Description

No one could even think that a virus can do so much harm. Accepting and most importantly dealing with this pandemic has been an experience no one would ever forget. Born and raised in Wuhan, this has proved to be one of the most dreadful pandemic mankind has ever seen. It has greatly impacted the way humans had lived and how will they now continue to live post the birth of this virus. Coronavirus disease (COVID-19), an infectious disease caused by the SARS-CoV-2 virus is a highly transmissible disease that has impacted every inch of the world. In addition to the threat to public health, the economic and social disruption it has also threatened the long-term livelihoods and wellbeing of millions.

The first ever known case was identified in Wuhan, China in December 2019. The disease has since spread like a spider web clutching in its arms the entire world.

1.1.2 Signs & Symptoms

The symptoms could range from minor issues to major illness.

- Headaches
- Loss of smell & taste
- Nasal Congestion
- Runny Nose
- Cough

- Muscle & Joint Pain
- Fever
- Sore Throat
- Diarrhoea
- Breathing Difficulties
- Digestive Issues
- Fatigue

1.1.3 Transmission

It is mainly transmitted via respiratory route occurring when individuals inhale droplets or airborne particles that are exhaled by infected people as they breathe, talk, cough or sneeze.

1.1.4 Diagnosis

The diagnosis is usually done using nasopharyngeal swab. Although can be done through the nasal swab or sputum sample as well.

1.1.5 Prevention

- Vaccination
- Wearing Masks in public
- Staying indoors
- Avoiding crowded places
- Social Distancing
- Washing hands with soap often
- Sanitization

1.1.6 Treatment

- If infected with mild symptoms then home isolation under healthcare professionals' guidance for treatment

- If infected with major symptoms- contact healthcare professional and get admitted to the hospital for treatment

1.2 INFORMATION SECURITY (InfoSec)

1.2.1 Description

According to NIST, Information Security refers to "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

Information security (referred to as InfoSec) covers the tools and processes that organizations use to protect information.

1.2.2 Principles

The canons of Infosec are –

i. **Confidentiality:** This principle aims to keep personal information private while ensuring that it is visible and accessible only to those individuals who own it or the ones who need it to perform organizational operations.

ii. **Integrity:** The purpose of this principle is to ensure that the data is true and dependable, and it is not modified incorrectly, neither accidently nor maliciously.

iii. **Availability:** The goal of this principle is to make the technology infrastructure, data, and the application available as and when needed for an organizational process.

It is crucial that every element of Infosec program must be designed to fulfil one or more of these principles. In combination they are referred to as the **CIA Triad**.

1.2.3 Goals

- To ensure that only authorized persons have access to the data.
- To make sure that data contained is accessible only to specific users who have the right to use such information.
- To block unauthorized changes to information
- To ensure completeness and general accuracy of information
- To determine the source or authorship of information.

1.2.4 Standards

There are certain information security standards that have been developed to protect the system and the users in several ways. Based on the type of data that needs to be protected, there are different standards.

Below mentioned are a few standards:

i. ISO 27001

- Typically, one of the common benchmarks that follow to the organization to actualize Data Security administration framework.
- It is comprised of the set of strategies that states the rules and perquisites which should be fulfilled in arrange to urge the organization certified with this standard.
- As per this standard, the organization is supposed to keep all the technology up to date, the servers ought to exist without vulnerabilities and the organization has got to be reviewed after the desired interim to remain compiled to this standard.

- It is a worldwide standard and each organization that serves other organization that complies with this standard is assumed to comply with ISMS approach that's secured beneath ISO 27001 hone.

ii. PCI DSS

- PCI DSS stands for Payment Card Industry Information Security Standard.
- This could be considered as the standard that must be selected by the organization that acknowledges accepts payment through their gateway.
- The businesses that store client information like their name and card related data must embrace this standard in their organization.
- As per this compliance, the technologies utilized by the organization ought to be up-to-date and their framework ought to persistently experience the security evaluation to guarantee that it isn't having any vulnerability.

iii. HIPPA

- HIPAA stands for Health Insurance Portability and Accountability Act.
- It is the standard that the hospitals must follow in order to guarantee that their patient's information is fully protected and not spilled at any cost.
- To comply with this standard, the hospital must have a strong network security team to take care of all the security occurrences, their quarterly security reports ought to be solid, all the transaction should be done in encrypted mode and so on.
- This standard guarantees that the basic health-related data of the patient will stay secure so that the patient can feel secure around their health.

iv. FINRA

- FINRA stands for Financial Industry Regulatory Authority.

- This standard is all around making things secure for the financial bodies that handle the funds in monetary exchanges.
- In this standard, the framework is gathered to be profoundly secured and to comply with this standard, different measures got to be considered in terms of information security and the user's information assurance.
- It is one of the foremost fundamental measures that all the organizations based on finance are supposed to comply with.

v. GDPR

- GDPR stands for General Data Protection Regulation.
- It is a standard defined by the European government which is concerned about the data protection of all the users.
- In this standard, the body assigned must ensure that the user's data is secure and cannot be accessed without legitimate authorization.
- As the name states, this standard primarily centres on the security of the user's information so that they can feel secure while sharing it with any of the organizations that are complying with the General Data Protection Regulation.

1.3 REMOTE WORKING

1.3.1 Description

Popularly known as work from home (WFH) refers to a type of flexible working arrangement that permits an employee to work from a remote location that is outside the office.

The recent rapid spread of the novel coronavirus disease (COVID-19 infection) has led to a serious worldwide financial downturn. Governments forced add up

to lockdown, prohibiting non-essential travel, and requiring the closure of all non-essential services.

The strict government control measures driven to numerous badly designed working conditions. Conventional ways of working experienced genuine challenges. The effect of COVID-19 on the worldwide economy was comparable to that of the 2008 emergency, although its long-term results were more serious.

The effect on company execution is articulated in intensely affected regions and businesses, such as instruction and healthcare. Numerous companies have picked for adaptable work hones, such as working from home to diminish the spread of infection and misfortunes.

Amid the COVID-19 emergency, most individuals were as of now utilizing online commerce as well as work from home and digital businesses.

These locations could be- an employee's home, a co-working space, or a shared space. Typically, it could be any place outside the corporate building or campus.

It entails:

i. Policies governing equipment use
ii. Network security
iii. Performance expectations

1.3.2 Characteristics

i. **Strong & Reliable Connectivity:** Remote working requires and depends heavily on internet and mobile technology to support its intensive use.
ii. **Communication & Collaboration Tools:** Remote working requires secure and high-quality chats, video conferencing and other business needs.
iii. **Healthy Culture:** Remote working relies extensively on a supportive management that focusses more on culture of trust and teamwork.

1.3.3 Challenges

i. **Productivity Drains:** In the absence of clear guidelines and procedures, lower levels of motivation and reduced productivity can be a concern.

ii. **Unreliable Technology:** Inadequate technology and tools can greatly affect productivity.

iii. **Technological Constraints:** Unreliable technology can act as a major hinderance in effective work.

1.4 COVID-19 AND REMOTE WORKING

1.4.1 Description

Remote Working has by far been the biggest legacy of Covid-19. The pandemic has forced the companies to quickly shift from work from office to working from home. Many employees started to WFH full time. Companies believe that WFH will become more prevalent post the pandemic. Initiating remote working has become a policy priority for most governments. But it is also important that the policies so designed, were in tune with the practical aspects included both for employees as well as the employers. The WFH situation ga deeper insight and played a vital role in revisiting and re-shaping the future policies for more flexibility.

1.4.2 Impact on Businesses

The new crown pneumonia widespread caused far reaching destruction in nations around the world. Tens of millions of individuals were contaminated; the economy was in recession and numerous individuals lost their jobs. Governments implemented numerous controls. These measures slowed the spread of the plague, and a few businesses were extremely harmed.

- The issue faced by the company is that the aptitudes and skills of the workers are not adequate for the WFH design. The company needs highly skilled workers to carry out their work, but the office work abilities of the past are not adequate to meet the company's needs.

- The mental stretch caused by WFH to workers features a negative effect on the accomplishment of corporate goals.

- This struggle cannot be dodged due to the substitution of office space with domestic space. The company should consider relinquishing domestic space to meet the work needs of employees.

- The part of corporate culture is altogether debilitated by the loss of physical contact.

- It has also severely impacted the security perse of business; in the sense that WFH has imposed greater risks to information security & compliance.

1.4.2 Impact on Employees

Amid the COVID-19 widespread, the houses of employees suddenly got to be the main place of economic activity. Numerous nations utilized their homes as a buffer against economic downturns and took action to back this WFH.

We contend that businesses and governments saw housing as a supporting pillar for financial improvement.

However, some people used their houses as a workplace that can be used inexpensively in an emergency (e.g., COVID-19) but neglects its function as a place to live. As a result, employees were faced with corresponding challenges and problems:

- Firstly, the model required upgrading employees' WFH work skills. Employees needed to work and communicate online, which required special skills, such as new office skills and online communication skills. However, some specific industries, such as low-skilled services, couldn't adopt this model. In addition, network accessibility and online task suitability affected the feasibility of the WFH model.

- Secondly, internal psychological stress. Research showed that a lack of social support and the feeling of working alone gave birth to loneliness and stress as they are unable to communicate their anxiety to others. In addition, with uncertainty about the future, such as layoffs, pay cuts, and bankruptcies, lead to massive increase in the level of stress in employees.

- Lastly, this model reduced opportunities for intimate psychological interactions while reducing face-to-face communication to a large extent. The lack of enthusiasm for face-to-face interaction, and the failure to address the lack of interpersonal interaction ultimately led to employees feeling disconnected from the corporate culture and work environment.

1.5 IMPACT OF COVID-19 ON INFORMATION SECURITY

COVID-19 widespread has been the news all around the world. The medical fraternity as well as the government and citizens over the world are collating their efforts to contain the spread of this disease. In any case, indeed as healthcare administrations reinforce their resources to combat the COVID-19 crisis, they have ended up becoming the casualties of cyber-attacks.

1.5.1 Impact 1: Rise in Phishing & Ransomware Attacks

- A study released by the Cyber Insights Middle stated that there was a considerable increase in phishing attacks, malware spams and ransomware attacks.
- The study cites that the attackers used COVID-19 as a bait to imitate brands and in this manner misdirect employees and customers.
- Not as it were that the organizations were threatened, but the end users who downloaded the applications related to COVID-19 were frequently tricked into installing ransomware disguised as legitimate applications.

1.5.2 Impact 2: Increased Security Risks due to Remote Working

- Company Virtual Private Network (VPN) servers proved a life saver for businesses during the pandemic with numerous workers working from home.
- The businesses hence were exposed to risks that lead to security misconfigurations in VPNs, which uncovered the private data on the internet, and therefore uncovered the computers to Denial of Service (DoS) attacks.
- In addition, certain individuals used personal computers to conduct official tasks that posed greater risk to the organisations.

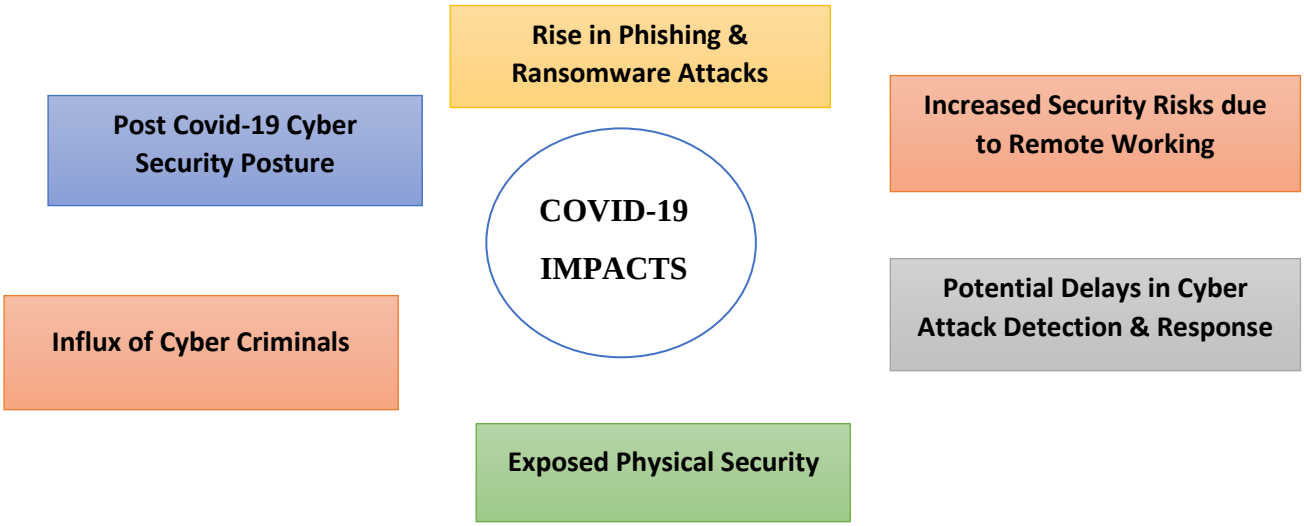

Figure 1: Depicting the Impact of Covid-19 on business Infosec

1.5.3 Impact 3: Potential Delays in Cyber-Attack Detection and Response

- Due to the COVID-19 pandemic, the functioning of several security teams was compromised, which made it difficult to identify malicious activities and even more difficult to respond to these activities.
- Problems in upgrading patches on devices were also prevalent due to the non-functionality of the security teams.
- It became mandatory for the organizations to assess the Security defences they had and initiate the use of co-sourcing with external consultants specifically in key human risks areas that were identified.

1.5.4 Impact 4: Exposed Physical Security

- The workers at times due to non-availability of proper internet connection relied on public spaces to access internet facilities.
- This led to the computer equipment and the sensitive information held by the device to be unwittingly exposed to theft or harm.
- Companies had to invest in making sure that working in public spaces was limited and employees were made aware of the potential risks to security of data.
- Also, the organizations educated their workers about the theft or injury, to ensure that sensitive information remained safe.

1.5.5 Impact 5: Influx of Cyber Criminals

- Organizations downsized their workforce to cope with the effects of COVID-19.
- Most of the professionals lost their jobs owing to the announcements of lockdowns by the governments across the world.

- This move encouraged the growth of cyber criminals as idle people with internet access who had lost their means of livelihood due of COVID-19 saw it as an opportunity to make a living out of this pandemic.

*1.5.6 Impact 6: **Post Covid-19 Cyber Security Posture***

- The COVID19 pandemic has placed a major strain on the global economy which has given rise to recession as its after effect.
- To cut down on the economic losses, the organizations downsized by cutting off business lines.
- It also included cybersecurity operations that were perceived to be non-critical.
- It has been predicted that in the long run, this short-term practice may prove to be "penny wise and pound foolish," as it would manifold the impact of attacks on the organization.

CHAPTER – 02

REVIEW OF LITERATURE

COVID-19 has been a roller coaster that has impacted lives of people worldwide. Not only has it impact lives but also greatly impacted the world on an economic front.

The pandemic gave birth to a new challenge for businesses as they struggled to adjust to the 'new normal' of working from home. Companies accelerated their digital transformation, while information security continued to be a major concern.

The research titled "Impact of Covid-19: A cybersecurity perspective" (2021) was given by Mohammed Baz, Hosam Al akami, Alka Agrawal, Abdullah Baz and Raees Ahmad Khan. This research is an attempt to measure and analyse the impact of COVID-19 pandemic on cybersecurity. It aims to focus on various aspects of cybersecurity that have been impacted by the pandemic have been ranked in the descending order of severity quantitatively by the help of multi-criteria decision-making problem-solving technique. The research is a thorough and conclusive analysis that added to the experts' efforts in estimating the extent of the effects of COVID-19 on cybersecurity. The in-depth analysis revealed in the results of the study depict that the impact of possible delays in the detection and response of cyber-attacks is highest among all the impacts that business had to bear during the crisis.

Another study titled, "Working from home during Covid-19 crises: A cyber security culture assessment survey conducted by Anna Georgiadou, Spiros Mouzakitis and Dimitris Askounis (2021). This research aims to evaluate the cyber security culture readiness of organizations

from different countries and business domains when teleworking became a necessity due to COVID-19 pandemic. The research designed a questionnaire and conducted an online survey addressing employees while working from home during the COVID-19 spread over the globe. The questionnaire contained n 23 questions. The data was then analysed from different perspectives leading to numerous findings regarding information security readiness and resilience of both individuals and organizations. The results were then presented and discussed in detail while focusing on future scientific routes and research paths that need to be explored. It also focusses on several cyber security recommendations address both the emerged vulnerabilities and the need for security culture evolution.

Research titled “Cyber Security Risks and Challenges in Remote Work Under the Covid-19 Pandemic” authored by Didzis Rutitis, Sintija Deruma and Eduards Aksjonenko (2021). The research states that as amid the COVID-19 far reaching the remote workforce has extended in numbers, offering specialists the opportunity to proceed working, the openness of which is additionally empowered by the national approach to making strides the epidemiological circumstance, which commanded more extensive utilization of inaccessible work for those whose work specifics allow it. The inquire about centres on analysing the current cyber dangers and challenges influenced by the COVID-19 far reaching, as well as danger organization approaches or security controls. Information collection instruments such as survey and interviews with specialists are utilized. Research conclusions reflect that the approach of companies and organizations to cyber hazard organization, giving a shape of inaccessible work organization is custom fitted to the industry, the nature of the information arranged, the computer aptitudes of agents and pre-COVID-19 ventures in corporate cybersecurity and digital transformation.

Another research titled, “Data loss prevention in a remote work environment” submitted by Stanley Ugochukwu Emenike (2021). The study gives a comprehensive overview of the hazard to organizational information due to the increment in remote work taking over the commerce scene. In looking for answers to the research question, the study applies topical investigation in analysing qualitative information from the interview of 6 respondents with over 5 years of experience in information security. The investigation recognized four topics (dangers, hazard, security occurrence and security pose) that are important. The discoveries show that there was a rapid hike in phishing, malware and DOS assault against the organization data resources since the initiation of the worldwide widespread which has led to information loss and influenced the organization’s competitive advantage and reputation. Also, the security posture before the pandemic was not effective in dealing with the increase in information attacks during the pandemic. The pandemic has led organizations to reassess their security posture to identify areas that need to be strengthened. The challenge in achieving an effective security posture is the attack surface is expanding and changing rapidly as well as the insufficient resources available (both human and financial). The organisation reassessed their security posture to identify gaps that need to be addressed. Employee training and awareness need to be done more frequently as well as implementing different technical security measures. Also, policies and procedures are implemented that outlines the acceptable use and management of the organization information assets. Moreover, the security posture before the widespread was not successful in managing with the increase in data attacks amid the widespread. The pandemic has driven organizations to reassess their security posture to recognize gaps that ought to be reinforced. The challenge in accomplishing a viable security pose is the attack surface is growing and changing quickly as well as the insufficient assets accessible (both human and money

related). The organisation reassessed their security posture to recognize crevices that must be tended to. Employee training and awareness ought to be done regularly as well as executing distinctive specialized security measures. Moreover, approaches and methods are executed that traces the acceptable use and administration of the organization data resources.

CHAPTER – 03

METHODOLOGY

3.1 Objective

The study is conducted to study the impact of Covid-19 on Information Security in organizations due to the increased levels of remote working.

The mode of data collection is a survey that has been specifically designed with questions that access the above topic on various essential parameters to give us a deeper insight.

The participants include 200 InfoSec related professionals working as Team Leads or above in varied organizations.

3.2 Hypothesis

Information Security related risks increase with increase in the levels of remote working during COVID-19.

3.3 Participants

With the means of purposive sampling, a sample of 200 InfoSec related professionals working as Team Leads or above in varied organizations participated in the study.

3.4 Inclusion Criteria

- Field: InfoSec related professionals

- Designation of professionals: Team Leads or higher

3.5 Exclusion Criteria

- Field: All other field related professionals

- Designation: Below Team Leaders

3.6. Procedure

A survey was designed with 12 questions accessing various parameters required to be studied and analysed. Professionals of various companies were approached virtually and explained about the purpose of the study while giving them a brief about the data and its relevance. They were then asked to carefully read the questions and the corresponding options and choose the option (1 or more) as per their understanding.

CHAPTER – 04

DATA ANALYSIS

The responses of 200 participants were studied carefully and each question was then analysed to generate a careful synopsis of the results.

4.1 Percentage of workforce working remotely/at home last year compared to during the COVID crisis

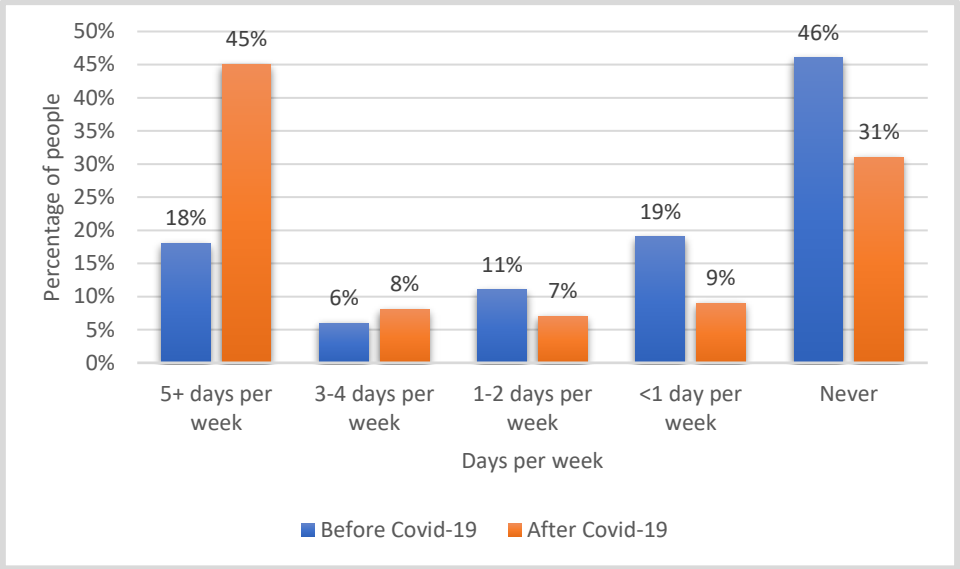

Figure – 2: Percentage of workforce working remotely/at home last year compared to during the COVID crisis

The above graph compares the no. of days employees worked from office and home before covid-19 as compared to the no. of days worked at home or from office post covid-19. The results show a drastic increase in work from home post covid-19.

4.2 Prior to the COVID-19 pandemic, how prepared were the organizations with a business continuity/disaster recovery plan that included a rapid shift from on-premises to a remote workforce.

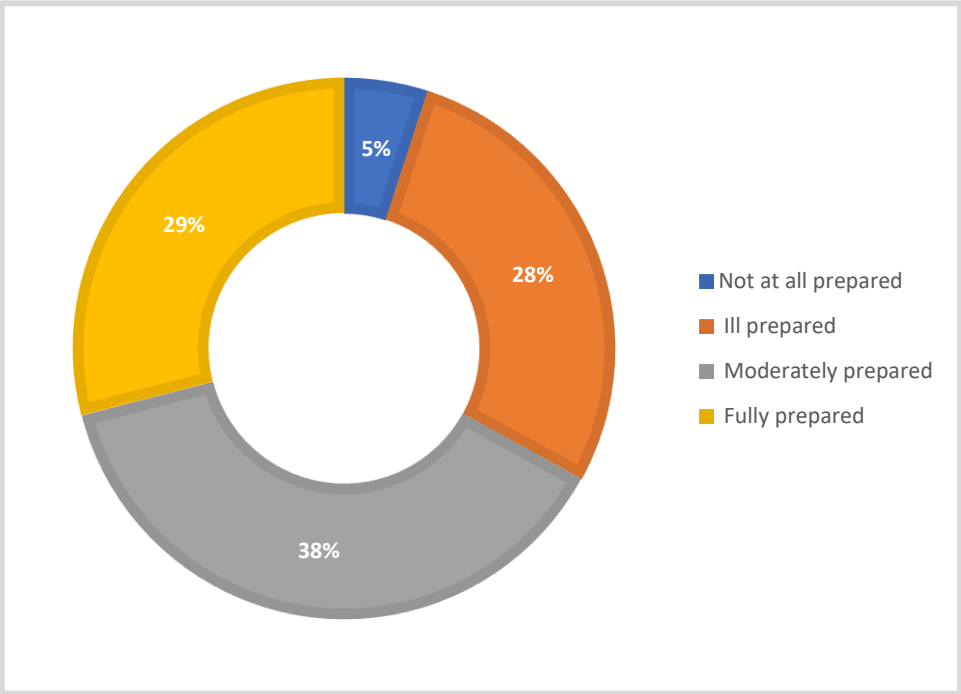

Figure – 3: Percentage of preparedness of the organizations with a business continuity/disaster recovery plan that included a rapid shift from on-premises to a remote workforce.

The above pie chart shows the percentage of preparedness companies had when they had to immediately shift from WFO to WFH. To put forward about 33% of the organizations were not prepared, while 38% were moderately prepared. Also, to see that a whopping 29% were not set out for the challenge.

4.3 Level of the leaders being concerned about the security risks introduced by users working from home

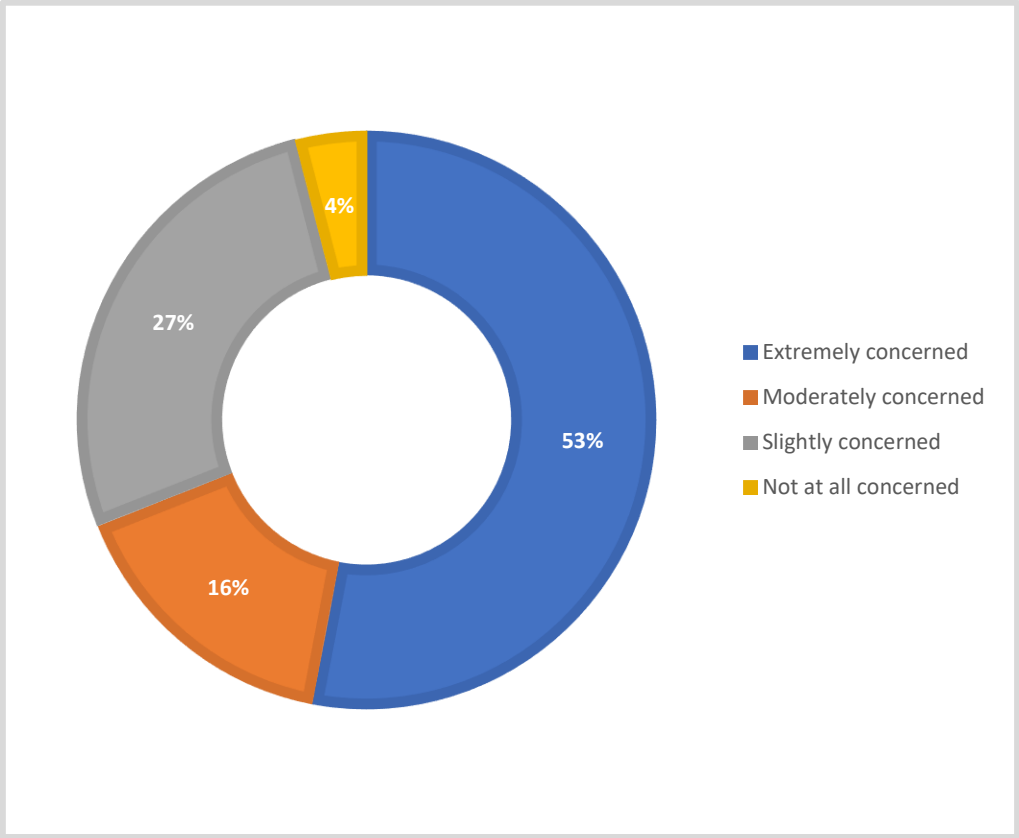

Figure – 4: Percentage of the leaders being concerned about the security risks introduced by users working from home

The above pie-chart clearly depicts that around 53% of the leaders were highly concerned about the WFH structure due to uncertainty, while a mere 4% seemed to be ok with it.

4.4 Level of the organizations being prepared for the shift to remote work from a security perspective

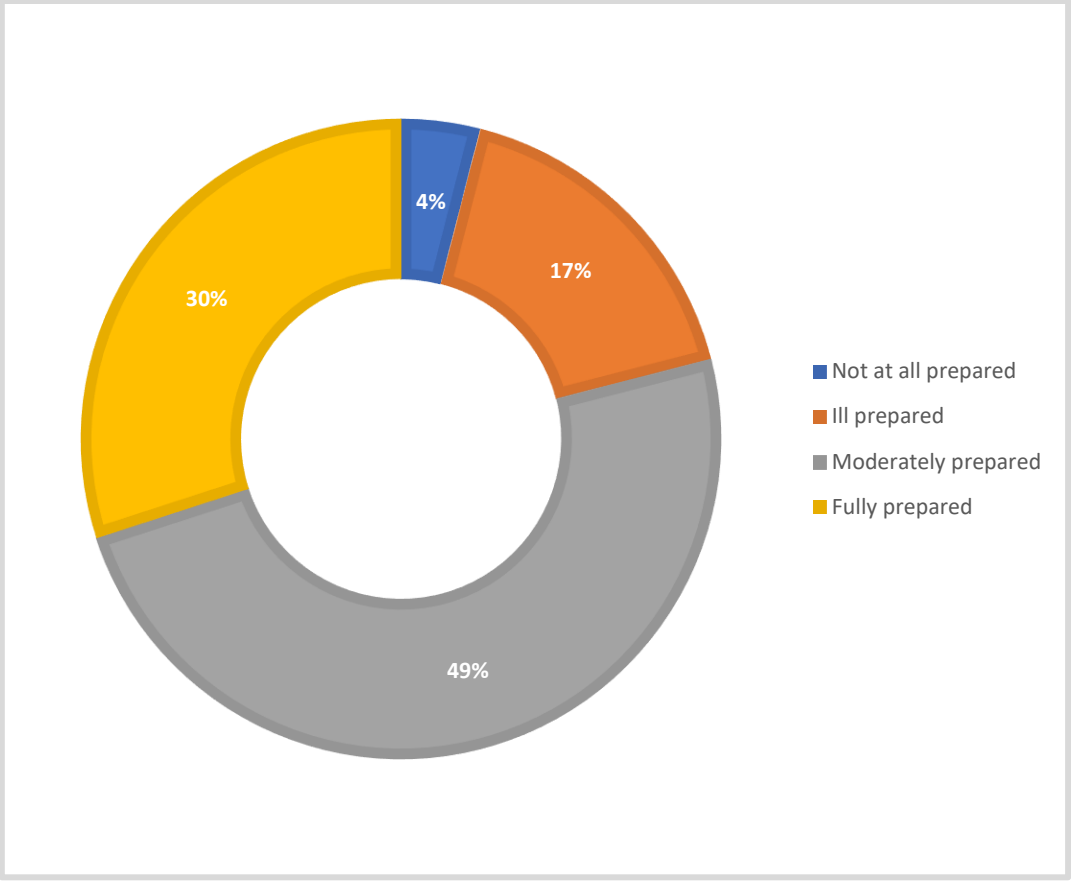

Figure – 5: Percentage of the level of the organization's preparedness for the shift to remote work from a security perspective

As per the above representation, we are clearly able to understand that only 30% of the organizations were fully prepared to start working from home at a short notice as compared to 21% being not prepared at all and 49% of them were moderately prepared which could lead to increased risks which the organizations weren't prepared for.

4.5 Types of security controls deployed by the organizations to secure remote work-home office scenarios.

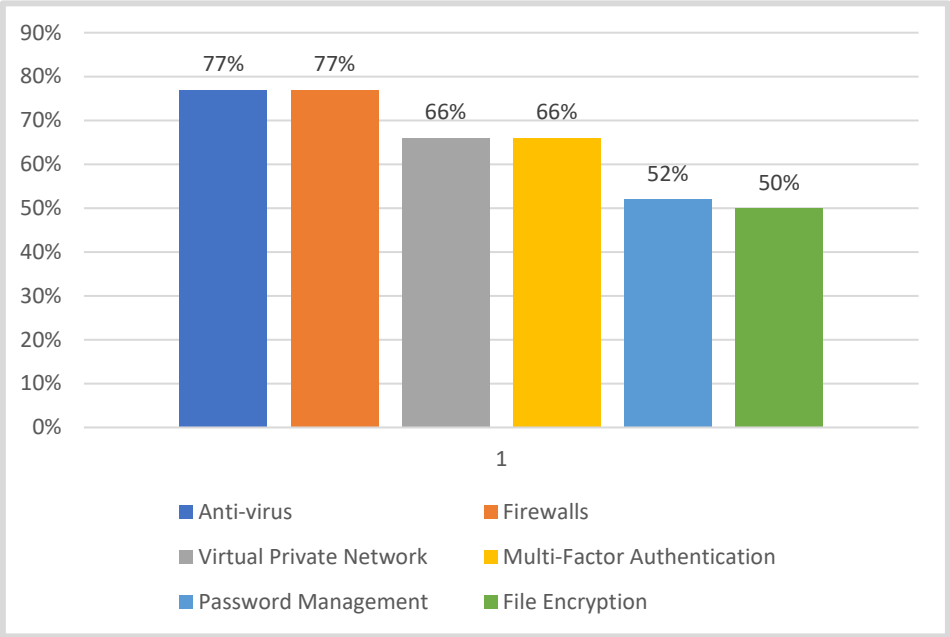

Figure – 6: Percentage of the types of security controls deployed by the organizations to secure remote work-home office

The above bar-graph depicts the percentage of different security controls that were deployed to secure WFH from any Information security threats-

Anti- Virus: Used by 77% of organizations

Firewalls: Used by 77% of organizations

VPN: Used by 66% of organizations

MFA: Used by 66% of organizations

Password Management: Used by 52% of organizations

File Encryption: Used by 50% of organizations

4.6 Organization's biggest security challenge regarding increasing the remote workforce.

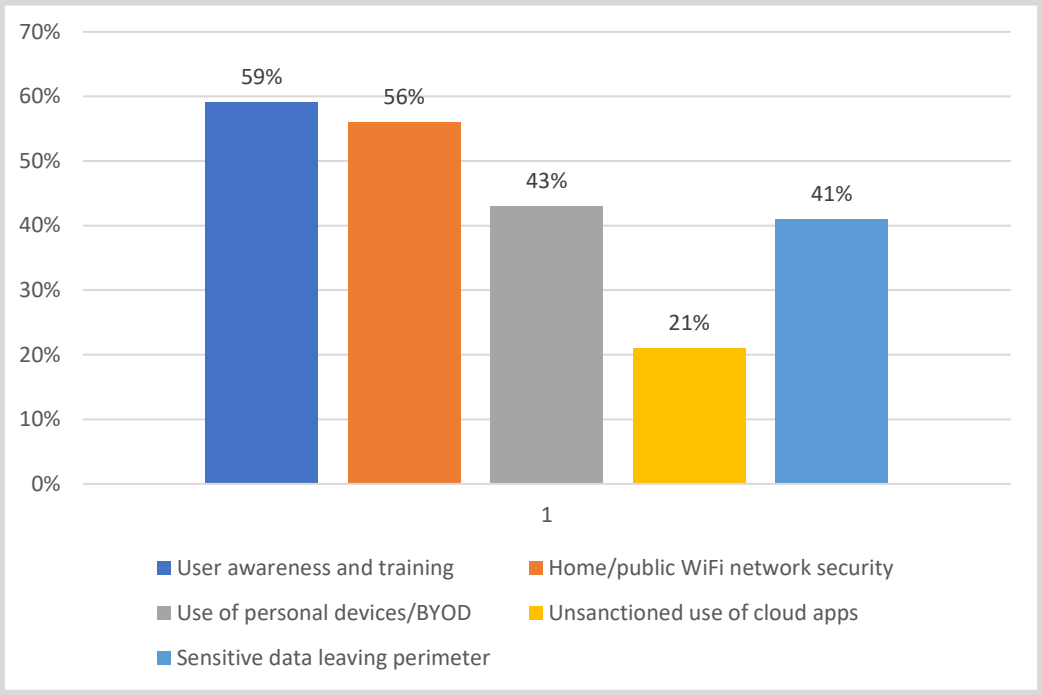

Figure – 7: Percentage depicting organization's biggest security challenge regarding increasing the remote workforce.

The above representation shows the areas posing biggest challenges to the organization's data security along with their percentages-

User awareness & training: 59%

Use of Personal Devices/BYOD: 43%

Sensitive data leaving perimeter: 41%

Home/ public WIFI network security: 56%

Unsanctioned use of cloud apps: 21%

4.7 Specific threat vectors that organizations were most concerned about with employees working from home

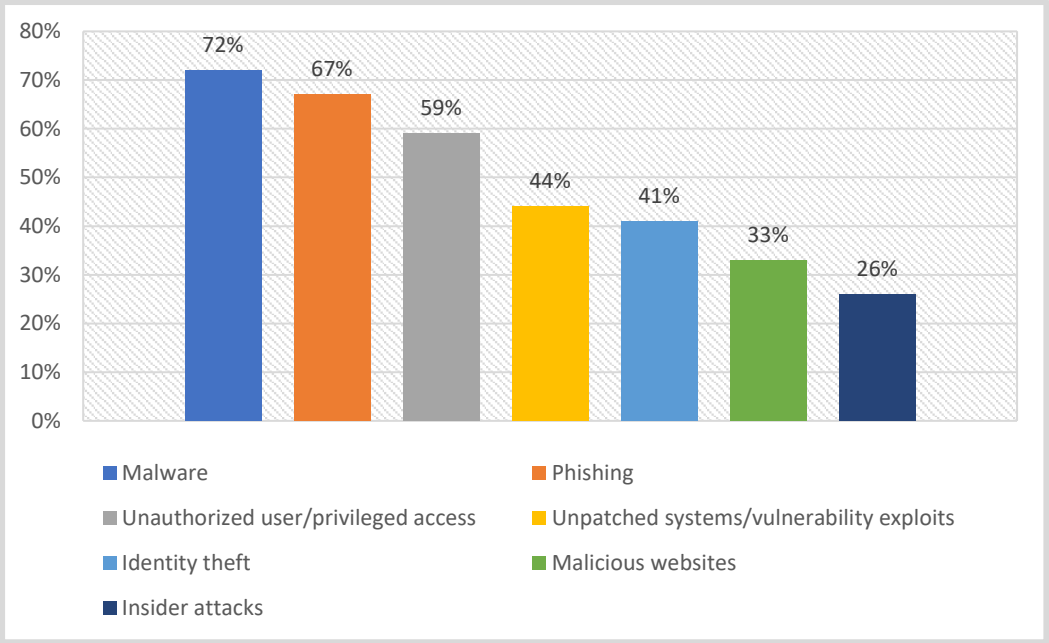

Figure – 8: Percentage of specific threat vectors that organizations were most concerned about employees working from home

With the maximum staff working from home, the bar graph above represents the specific threat vectors that the leaders were most concerned about –

Malware- 72%

Unauthorized user/Privileged access: 59%

Identity theft: 41%

Insider attacks: 26%

Phishing: 67%

Unpatched systems/vulnerability exploits: 44%

Malicious websites: 33%

4.8 Work applications used by remote workers that organizations are most concerned about from a security perspective

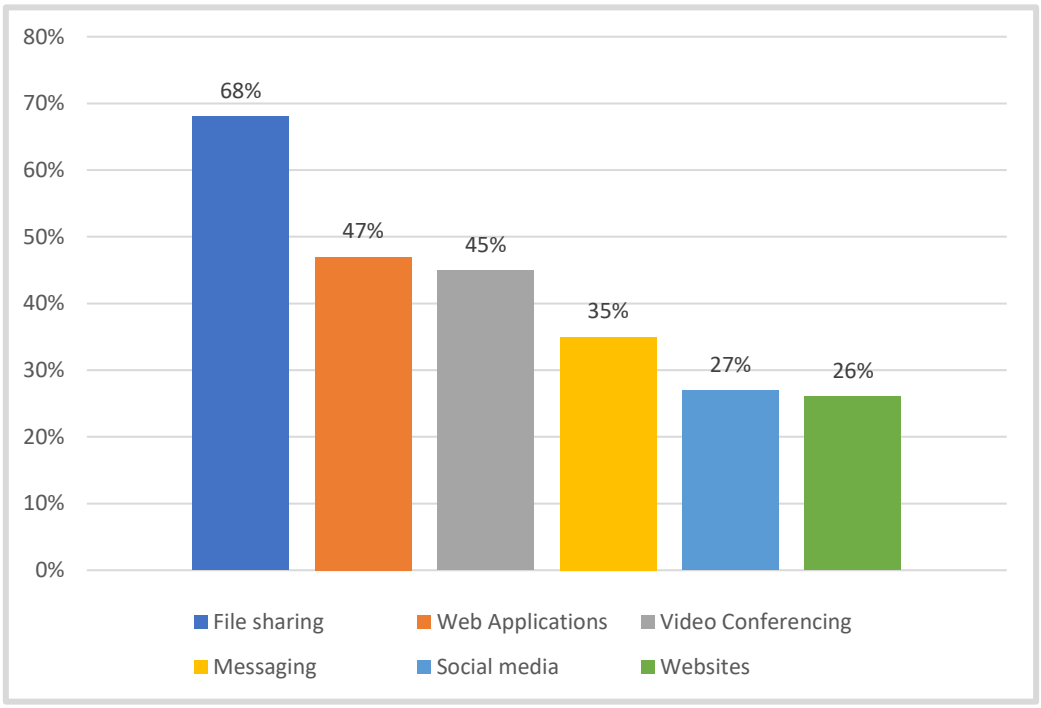

Figure – 9: Percentage of work applications used by remote workers that organizations are most concerned about from a security perspective

Herein, the graph is representative of the percentage of applications that could pose a security risk to organizations data-

File Sharing: 68%

Web Applications: 47%

Video Conferencing: 45%

Messaging: 35%

Social Media: 27%

Websites: 26%

4.9 Enforcing or not enforcing the same level of security controls and data management for all roles in the company as they access remotely

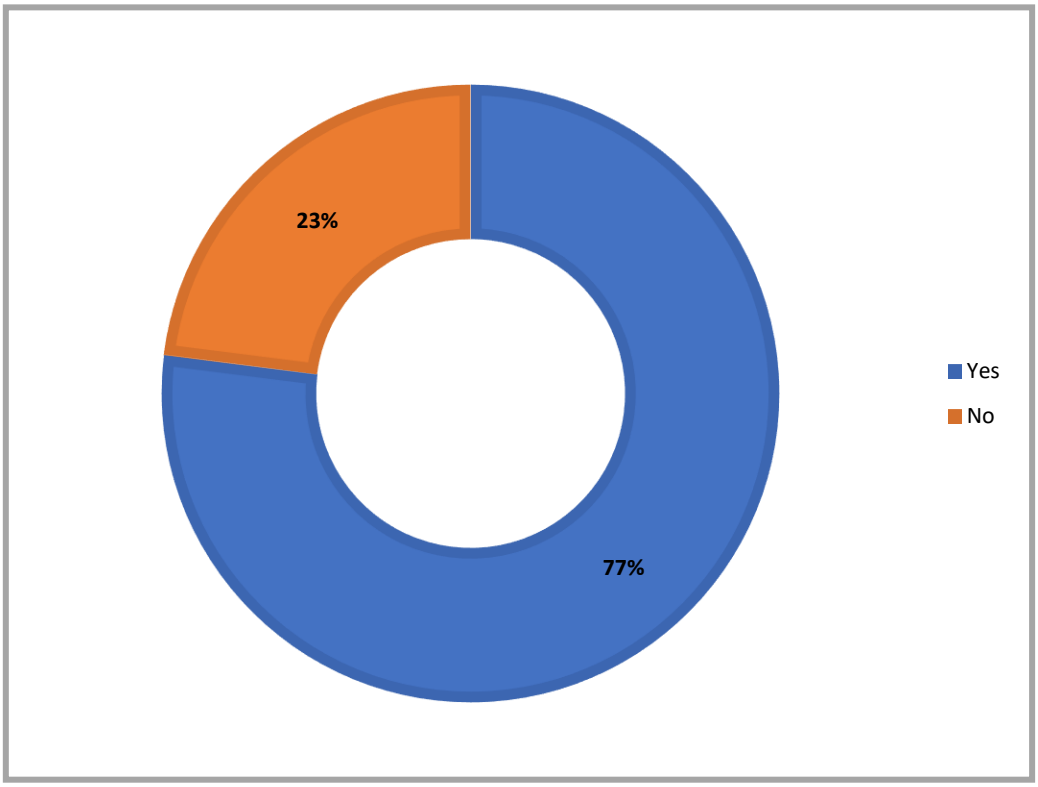

Figure – 10: Percentage of organizations enforcing or not enforcing the same level of security controls and data management for all roles in the company as they access remotely

The pie chart above represents that 77% of the organizations enforced the same level of security controls and data management for all roles in the company, while only 23% had different levels of security controls while the employees worked remotely.

4.10 Employees being able to or not being able to access managed applications from personal, unmanaged devices.

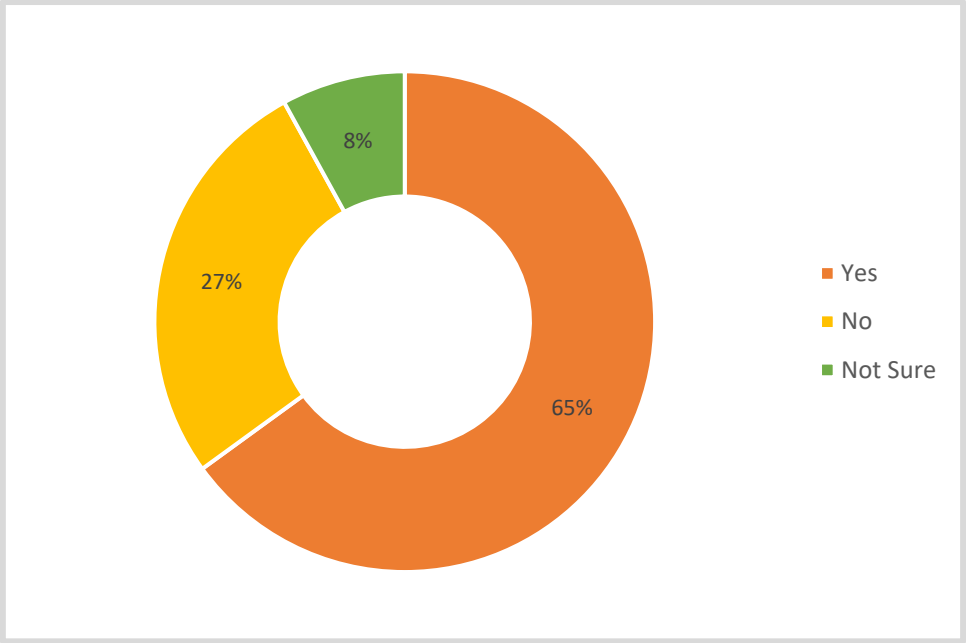

Figure – 11: Percentage of employees being able to or not being able to access managed applications from personal, unmanaged devices.

The diagrammatic representation above shows that about 65% employees were able to access managed applications from personal, unmanaged devices imposing a huge data security risk.

4.11 COVID accelerated/not accelerated the migration of additional user workflows or applications to cloud-based applications.

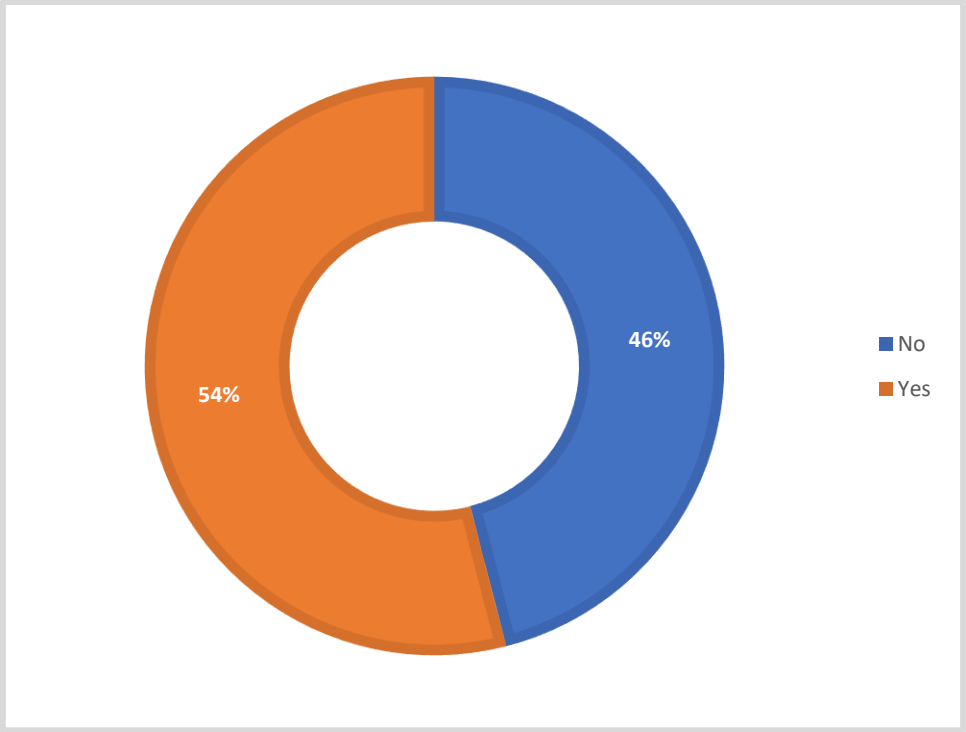

Figure – 12: COVID accelerated/not accelerated percentage the migration of additional user workflows or applications to cloud-based applications.

The pie-chart above states that Covid-19 had accelerated migration of additional user workflows or applications to cloud-based applications to 54%.

4.12 Remote work could/could not impact compliance mandates that apply to the organizations.

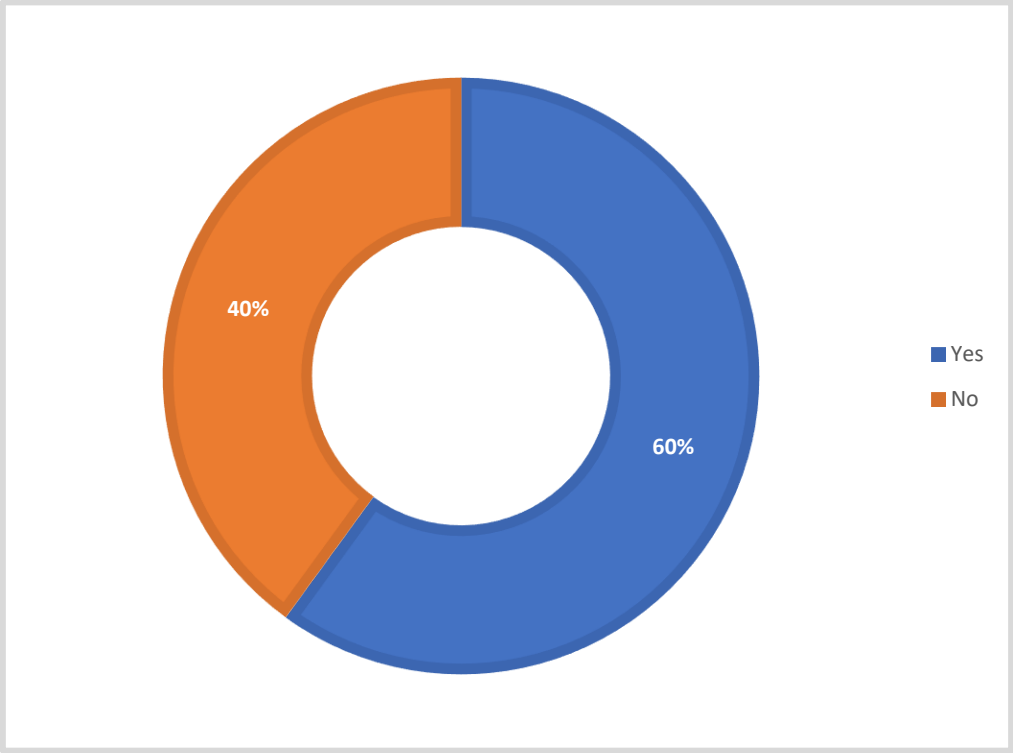

Figure – 13: Remote work could/could not impact compliance mandates that apply to the organizations.

The pie-chart depicts that remote work could impact compliance mandates that apply to organizations to up to 60%.

CHAPTER- 05

INTERPRETATION AND DISCUSSION

In the present chapter the results presented in the previous chapter have been interpreted and discussed.

The Covid-19 pandemic has greatly impacted the way humans had lived and how will they now continue to live post the birth of this virus. Coronavirus disease (COVID-19), an infectious disease caused by the SARS-CoV-2 virus is a highly transmissible disease that has impacted every inch of the world. In addition to the threat to public health, the economic and social disruption it has also threatened the long-term livelihoods and wellbeing of millions. The first ever known case was identified in Wuhan, China in December 2019. The disease has since spread like a spider web clutching in its arms the entire world.

The survey conducted on 200 Information Security professionals, with 12 questions in the survey that were designed to get in- depth information about the pandemic which led to remote working and how it has impacted information security. The hypothesis drafted was that:

- Information Security related risks increase with increase in the levels of remote working during COVID-19.

From the careful study and analysis of the survey results show clearly that there has been a drastic increase in work from home during and post covid-19.

Data received through Figure 2 gives us the percentage of preparedness companies had when they had to immediately shift from WFO to WFH. Figure 2 implied that to put forward about

33% of the organizations were not prepared, while 38% were moderately prepared. Also, to see that a whopping 29% were not set out for the challenge. We could also interpret through Figure 4 that around 53% of the leaders were highly concerned about the WFH structure due to uncertainty, while a mere 4% seemed to be ok with it.

Through Figure 5 we were clearly able to understand that only 30% of the organizations were fully prepared to start working from home at a short notice as compared to 21% being not prepared at all and 49% of them were moderately prepared which could lead to increased risks which the organizations weren't prepared for. Also, by reading figure 6 we got a fair idea on different types of security controls that were deployed by the organizations to secure remote work-home office scenarios which did involve huge operational costs.

User's awareness and training in respect to the information security was a big concern for the organizations, while working through home/public Wi-Fi further imposed a major challenge on organization's data security. Use of personal devices by employees also added to the peril.

Figure 8 gave the view that with the maximum staff working from home, there were specific threat vectors that the leaders were most concerned about such as Malware 72%, Unauthorized user/Privileged access accounted for 59%, identity theft for 41%, Phishing 67%, Unpatched systems/vulnerability exploits for 44% and Malicious websites accounting for 33%.

As shown in figure 9, work applications used by remote workers that organizations are most concerned about from a security perspective were File Sharing -68%, Web Applications- 47%, Video Conferencing- 45%, Messaging- 35%, and social media- 27%.

Through figure 10 we can see that about 77% of the organizations enforced the same level of security controls and data management for all roles in the company, while only 23% had

different levels of security controls while the employees worked remotely; that indeed poses risk on the data of the company due to the varied needs that at times cannot be met through same level of security controls.

Figure 11 shows that about 65% employees were able to access managed applications from personal, unmanaged devices imposing a huge data security risk.

Figure 13 also depicted that remote work impacted the compliance mandates of organizations to up to 60%.

Therefore, from the above interpretations, it can be concluded that the drastic increase in the level of remote working as a consequence of the pandemic had indeed imposed a greater risk on the data protection of organizations.

CHAPTER- 06

CONCLUSION

Through careful analysis of the inputs received as the survey results, it can be concluded that the drastic increase in the level of remote working as a consequence of the Covid-19 pandemic had indeed imposed a greater risk on the information security of the organizations.

The study clearly depicts the increase in work from home of employees due to the lockdowns and health concerns across the world due to the pandemic. Organizations were not prepared enough and lacked the required resources to fully protect its data.

Issues like unawareness, lack of training, use of personal devices by employees and the like posed a greater risk to the organizations. Collected data is also representative of the number of applications such as social media, websites, video conferencing and the like that posed an increased security risk to organizations data.

For the purpose of the study, a survey of 12 questions was conducted on 200 information security professionals working as Team Leads and above, belonging to companies of varying sizes across multiple industries. The results hence generated after careful evaluation state that there has been a considerable surge in cyber security risks with the increase in remote working.

LIMITATIONS:

However, the present study may have some limitations as it was carried out in a short period of time and with limited resources. Some important limitations are:

1. Size of the sample was small.
2. The sample was not representative of the whole population.
3. Although all possible efforts were made to elicit genuine data, a social desirability effect could have influenced the responses of some of the participants.
4. No control over other relevant variables.

SUGGESTIONS:

The following suggestion can be given for further research.

1. The sample size should be large, fairly representative.
2. Global comparisons to be studied further.

CHAPTER -07

REFERENCES

1. Khan NA, Brohi SN, Zaman N (2020) Ten deadly cyber security threats amid COVID-19 pandemic. TechRxiv Powered by IEEE: 394-399.
2. Meghisan-Toma GM, Nicula VC (2020) ICT Security Measures for the Companies within European Union Member States-Perspectives in COVID-19 Context. In Proceedings of the International Conference on Business Excellence 14: 362-370.
3. Mastaneh Z, Mouseli A (2020). Technology and its Solutions in the Era of COVID-19 Crisis: A Review of Literature. Evidence Based Health Policy, Management and Economics 4: 138-149.
4. J. G. Ronquillo, J. W. Erik, K. Cwikla, R. Szymanski and C. Levy, "Health IT, hacking, and cybersecurity: National trends in data breaches of protected health information," JAMIA Open, vol. 1, no. 1, pp. 15–19, 2018.
5. K. Sahu and R. Shree, "Stability: Abstract roadmap of security," American International Journal of Research in Science, Engineering & Mathematics, vol. 2, no. 9, pp. 183–186, 2015.
6. R. Kumar, S. A. Khan and R. A. Khan, "Analytical network process for software security: A design perspective," CSI Transactions on ICT, vol. 4, no. 2, pp. 255–258, 2016.
7. S. A. Khan, M. Alenezi, A. Agrawal, R. Kumar and R. A. Khan, "Evaluating performance of software durability through an integrated fuzzy-based

symmetrical method of ANP and TOPSIS," Symmetry, vol. 12, no. 4, pp. 1–15, 2020.

8. A. Agrawal, M. Alenezi, S. A. Khan, R. Kumar and R. A. Khan, "Multi-level fuzzy system for usable-security assessment," Journal of King Saud University-Computer and Information Sciences, pp. 1–9, 2019.

9. R. Kumar, S. A. Khan, A. Agrawal and R. A. Khan, "Measuring the security attributes through fuzzy analytic hierarchy process: Durability perspective," ICIC Express Letters-An International Journal of Research and Surveys, vol. 12, no. 6, pp. 615–620, 2018.

10. Anderson, N., & Schalk, R. (1998). The psychological contract in retrospect and prospect. Journal of organizational behavior, 19, 637-647