

Sri Lanka Institute of Information Technology

**Cyber Security Concerning Remote Working**

**Individual Assignment**

IE2022 – Introduction to Cyber Security

Submitted by:

|  |  |
| --- | --- |
| Student Registration Number | Student Name |
| IT21385414 | Gallage E.D. S |

Contents

**Acknowledgement**

**Abstract**………………………………………………………………………………………03

1.**Introduction**……………………………………………………………………………

* 1. Introduction to Remote work
  2. Cyber security Importance Regarding Remote Work
  3. Major Cyber security concerning Remote Working
  4. Advantages of strengthening Cyber security concerning Remote Working
  5. The Problems of lack of attention on Cyber security concerning Remote Working

2.**Evolution of the topic**

2.1. Evolution of Working Remotely.

2.2. Different application of strengthening Cyber security in Remote work.

2.3. Real-world examples of enhancing Cyber security for remote work and taking advantage of these improvements

3.**Cyber security trends in the modern world based on remote work and future developments in the area**

4.**Conclusion**

5. **References**

Acknowledgement

First, I would like to express my gratitude to the senior lecturer, Mr. Amila Senarathne, whose ideas assisted me in completing my report and assignment-related presentation. His guidance from the beginning to the end of the assignment was a major factor in my ability to complete it successfully. Also, the completion of this project would not have been possible without Mr. Amila Senarathne's instruction in IE2022- Introduction to cyber security. Regarding the success of the report, I would like to express my appreciation to the previous researchers who conducted excellent work in the fields of cyber security and remote work. In addition, I would like to thank everyone who assisted me during the duration of my assignment.

Abstract

The purpose of this report is to show the development of remote working impacts on cyber security and to discuss the risks and possible actions to be taken. Remote working is now a global increasing concept, which poses new cyber security risks. Due to the covid -19 pandemic that the whole world had to face almost all organizations had to adapt to working remotely. The covid-19 pandemic totally transforms the traditional working office environment. Remote working is convenient and has many advantages, and it also discloses individuals and businesses to a variety of cyber security risks.

With the evolution of the work-from-home concept and certain cyber security attacks in particular, phishing became more pervasive. The primary issue is that only the IT team in an organization will identify cyber security risks and propose solutions. However, given the high number of risks in the cyber environment, management and other employees must also contribute to minimizing cyber trends. Cyber security teams must not only overcome the global challenges imposed by this catastrophe, but also unique issues such as protecting a newly remote staff and preventing malicious attacks targeting remote users. This report will contribute to the existing understanding of cyber security in remote works. In the first chapter, this report focuses primarily on the report's introduction, which covers the introduction to remote work, the significance of cyber security, the major cyber security threats in remote work, the benefits of enhancing Cyber security in Remote work, and the problems associated with a lack of focus on Cyber security in Remote work. In the second chapter, I focused on the subject's development. Which covers the evolution of remote work, the emergence of cyber security in remote works, the various applications of strengthening cyber security in remote works, real-world examples of strengthening cyber security in Remote work, as well as the advantages and real-world problems encountered because of a lack of focus on cyber security in remote works. In the third chapter, I focused on future cyber security requirements for remote work and cyber security trends for remote work in the modern world. The report concluded with an executive summary and a conclusion.

1. Introduction

* 1. Introduction to Remote Work

Remote work is work done outside of a traditional office environment, also referred to as working from home or telecommuting. The concept of remote work is that employees can successfully execute projects and daily tasks without needing to commute to an office each day. Different levels of remote employment opportunities exist, but each type provides the benefit of flexibility in an employee's professional and personal life [1].

Remote Working (RW) is synonymous with telecommuting and working from home. Remote work refers to a professional environment where employees may work from home or from another location outside their physical office. Often, this requires the creation of a workspace at home. There are many advantages to working remotely, including the ability to work from anywhere. Employees can work from convenient work locations as their preference remotely [2]. Because of using this work from home concept organization top management and other leading parties had to re-arrange their working environment [3]. Working remotely necessitates the implementation of new policies within the organization, special training for the employees, governing mechanisms, achievement of the organization's performance goals, and, most importantly, network security and a heightened awareness of data confidentiality.

* 1. Cyber security Importance Regarding Remote Work

Cybersecurity is important because it protects all categories of data from theft and damage. This includes sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, and governmental and industry information systems. Without a cyber security program, your organization cannot defend itself against data breach campaigns, which makes it an irresistible target for cybercriminals.

With the proliferation of cybercrimes and frauds, information theft has become one of the costliest and rapidly expanding cybercrimes. Since information is considered to be the weapon of the 21st century, organizations must take appropriate measures against cybercrimes. With regard to working from home.

1.3 Major Cyber Security risks in Remote Work

Due to the growing popularity of remote work around the world, threats continue to arise. According to my research in area of cyber security concerning remote working, I identified below major risks.

The cyber security risks associated with remote work can be divided into two categories: risks associated with remote work for organizations and risks associated with remote work for employees.

Organizational Security Risks from Remote Work

* Email Scams (Phishing Attacks)
* Ransomware
* Cloud jacking
* Man-in-the-middle attack
* Distributed denial-of-service attack
* Weaker Security Controls
* Threats

Employee Security Risks from Remote Work

* Assessing to confidential data through unsafe connections (WI-FI)
* Using Personal Devices for Work
* Ignoring Basic Physical Security Practices in Public Places
* Unencrypted file sharing
* Using Weak Passwords

Remote Work Security Risks for Organizations

* Email Scams (Phishing Attacks)

The highest cyber security risk to remote working is phishing attacks. Phishing attacks are the practice of sending fraudulent communications that appear to come from a reputable source. It is mostly done through email. The goal is to steal sensitive data like credit card and login information, or to install malware on the victim’s machine [4].

When an organization is subjected to such an attack, it typically suffers severe financial losses as well as a loss of market share, status, and customer trust. Depending on the scope, a phishing attempt could turn into a security incident from which a company will struggle to recover.

Depending on the scope of the attack, it can result in significant entity breakdowns. To achieve the entities' objectives, well-built cyber security systems are required within the organizations.

Ex: - Email phishing

Email phishing is a well-known attack that is also known as

'Deception phishing.' Some parties use to send emails to other

parties with malicious intentions in mind and tend to steal most

confidential data and information to commit fraud.

They usually send some links with emails, and when the recipients open the emails and click on the links, they are directed to malicious websites that steal personal and very confidential data and information from that party or install malicious codes in that party's machines, which are known as malwares.

* Ransomware

A type of malicious software design to hold a computer system or data it contains captive until a payment is made. Targeted ransomware assaults are becoming more common by the day. Ransomware assaults increased by 92.7% in 2021 compared to 2020. 3 Ransomware assaults demand a ransom for an organization's essential data, and corporations pay millions of dollars to hackers each year because they do not want to risk losing their sensitive data. However, even if you pay the ransom, there is no guarantee that your files will be safe.

* Cloud Jacking

Cloud jacking has become a big issue as the cloud becomes a more sophisticated manner of storing data. These attacks are generally carried out in two ways: injecting malicious code into third-party cloud libraries or directly into cloud platforms. Simply said, a public cloud vendor is responsible for supplying the infrastructure, but users bear most of the responsibility for data protection. Remember that even though your data is on the cloud, you are ultimately responsible for its security.

* Man-in-the-middle attack

When a two-party transaction occurs on a public network, hackers can inject themselves into it. They may filter and take your info once they have access. Your remote working staff are exposed to these assaults if they utilize public networks to do official responsibilities.

* Distributed denial-of-service (DDoS)

A distributed denial-of-service (DDoS) attack disrupts network services and targets websites and servers. A DDoS attack attempts to deplete the resources of an application. The perpetrators of these attacks flood a site with erroneous traffic, causing it to function poorly or to go offline entirely.

A DDoS attack involves a network of bots flooding a website or service with HTTP requests and traffic. During an attack, multiple computers storm one computer, pushing legitimate users out. As a result, service may be delayed or disrupted for an extended period.

During an attack, hackers may also infiltrate your database and gain access to sensitive information. DDoS attacks can target any endpoint that is publicly accessible via the internet and exploit security flaws.

DDoS attacks can last for hours or even days. These cyber-attacks can also cause multiple disruptions within a single attack. They are dangerous to both personal and business devices.

* Weaker Security Controls

Multiple layers of current cyber protection will not apply to remote employees, and workers who suddenly take their work devices home will find themselves without defense as they replace the office network with their home Wi-Fi. These are just a few examples of the many ways that security controls are being weakened.

Due to the lack of NAC, IDS, and NGFW or proxy servers, client devices will remain unprotected and exposed to possible unsecured networks among potentially compromised devices. Furthermore, the security of the internal network could also be compromised. Remote workers may require access to resources previously only available on wired networks.

* Threats

There are security risks associated with remote work everywhere! Unfortunately, there will be people within own organizations who want to kick us while we're already down. For malicious insiders, sudden remote working is a boon. Sensitive data can now be easily stolen from a company device via USB from the comfort of their own home.

Security monitoring can be removed or turned off entirely. This risk is more difficult to address. It may not be a viable option, but it can be assessed against the requirement for productivity and data access.

People around us may also pose a risk. Yes, you read that correctly! Most of us believe we live with individuals we can trust, but from the perspective of the firm, their staff residences are zero-trust settings. Private conversations can now be heard, and intellectual property can be viewed on TVs and monitors in living rooms around the world. What is the solution? To work safely from home, we must educate all our employees.

Remote Work Security Risks for Employees

* Assessing to confidential data through unsafe connections (WI-FI)

In today's world, with new developments in the field of cyber security, many organizations place a premium on securing their remote employees' work on computers given by the entity. Many businesses have policies and sections dedicated to this aim. However, most of them lack a thorough understanding of how employees use their work devices and connections. This may expose you to cyber threats.

**Ex: -**

* People often update their mobile phones and personal PCs, but many do not consider updating their routers. As a result, it may expose the company to cyber risk, where thieves may acquire access to confidential data and information.
* Almost all businesses utilize utmost security for their workplace networks and connections. As a result, the dangerous conditions are reduced. However, many personal connections and routers lack such security measures and guardians.

* Using Personal Devices for Work

The majority of employees transfer data and information files from their personal devices to their official ones. This is extremely dangerous and exposes you to malevolent behavior. On the other side, there is a new trend that allows or requires employees to use personal devices rather than work gadgets given by corporations. This is known as 'BYOD,' or bringing your own devices to work.

**Ex: -**

* Some audit companies require audit trainees and employees to carry their own laptop computers to work.

These types of settings are very vulnerable to dangers, and companies must take maximal precautions against them.

**Ex: -**

* When employees leave their firms with sensitive and very confidential information that belongs to the entity or is related to the entity, it exposes the entity to risk. Some sensitive data and information were saved on devices used by employees during their working hours, and organizations should destroy them. Companies should also have a proper procedure in place to prevent those dangers and work on their secret information.

Furthermore, keeping employees' software up to date and seeking for upgrades is essential, as updates are critical in preventing cyber dangers. As a result, organizations should examine this issue and devote adequate attention to software updates. As a result, organizations should seek for changes and notify their employees about them to preserve a risk-free working environment.

* Ignoring Basic Physical Security Practices in Public Places

Organizations should put in place systems and policies to maintain basic security measures. Companies must educate their employees on simple security measures that they can implement and follow. And companies should review those measures on a regular basis to ensure that employees are following the basic actions. Organizations should remind their employees not to disclose sensitive information to third parties. This should be done in a pleasant manner. Because, even if cyber security is a priority, businesses must also prioritize physical security within the organization.

**Ex: -**

* They frequently leave their personal computers on without turning off the screens. This allows anyone to look at the screen and see the data displayed on it.
* Openly and publicly sharing sensitive data among various devices.
* Allow other people from outside the entity or other divisions of the entity to use work- laptops or personal laptops with confidential data related to work and workplace.
* Unencrypted file sharing

While organizations may consider encrypting information stored on their network, they may not think to encrypt data in transit.

Your employees share so much sensitive information daily, including client account information, files, and more, that your company cannot afford for it to fall into the hands of cybercriminals. If confidential company data is intercepted, it can lead to identity fraud, ransomware cyberattacks, theft, and other crimes.

**Ex: -**

* Daily, accounting, consulting, and auditing firms receive more information from clients regarding ongoing audits and other projects. Companies should be held accountable for protecting such information.
* Using Weak Passwords

This is a more prevalent issue faced by organizations. Even if an organization employs multiple cyber security solutions to protect against cyber threats, errors can occur when subordinates attempt to secure their accounts with weak passwords. Criminals and hackers in the cyber environment are aware that these types of mistakes make it easier for them to commit fraud by hacking passwords. Various techniques are employed by hackers and criminals to crack passwords. The most common method is to compile a list of commonly used passwords and try each one until they gain access to the systems and accounts of the other party.

Next common issue is reusing passwords across multiple purposes and platforms. This may allow criminals access to multiple platforms and accounts used by employees with the same password. Using the same password across multiple platforms and accounts is therefore extremely risky.

* 1. Advantages of strengthening Cyber security concerning Remote Working

Benefits for the Organizations:

* Since these conditions will reduce the amount of time wasted on roads and in other locations, employees working from home will be more productive.
* Reduced maintenance fee.
* Cost savings
* Reduce the rate at which employees leave the organization.
* Lead to improve the satisfaction of employees.
* Reduced overhead costs result in reduced salaries and wages. This ultimately results in hiring additional employees. The company can hire more workers and divide their responsibilities among them.

Benefits for the Employees:

* Help employees achieve a work-life balance.
* Increase career advancement opportunities.
* Reduce communication expenses
* This new setting will ultimately result in the hiring of more workers, who will have greater opportunities than before.
  1. The Problems of lack of attention on Cyber security concerning Remote Working

Even in the best of circumstances, with numerous benefits for both the organization and the employee, working from home can pose certain security risks.

1. Cybersecurity is not the responsibility of a single entity within an organization, but rather of all employees.

* Everyone in the organization, including managers and employees, has the same level of responsibility for cyber security, because everyone handles information.
* Occasionally, employees tend to focus solely on their work and work-related obligations rather than cyber security concerns, which may ultimately result in failures. Implementing an atmosphere in which each employee contributes to reducing cyber security threats is crucial for accomplishing corporate objectives.

1. Utilizing insecure networks such as public Wi-Fi

* Because they may lead to corruptions and malicious activities, employees should not use freely accessible public networks for office work.

1. Employees are lacking in understanding

* Without proper knowledge, employees may work without taking proper safety precautions. Therefore, proper comprehension is indispensable.

1. Occasionally, employees within an organization do not recognize the scams

* Email phishing is the most well-known example of this type of scams.

1. Using VPNs that are easily overloaded

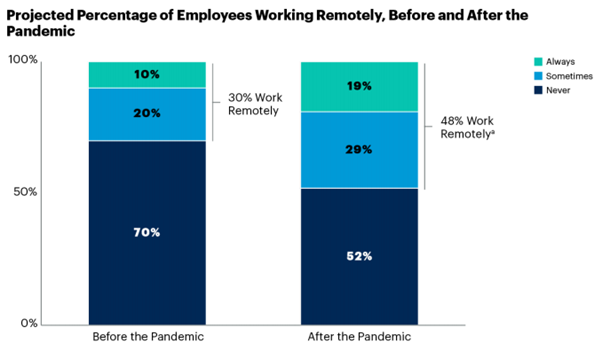
* Even though VPNs improve security, when more people use the same connection, it may cause a slowdown that hinders business operations.

1. The employees will lose focus of security priorities

* When most employees are required to work from home, the security team must focus more on these activities due to the potential for security difficulties.

1. Evolution of the topic

2.1. Evolution of the Working Remotely

[5].

* During the pandemic, nearly half of employees worked remotely full-time.
* 30% of employees worked remotely prior to the pandemic, compared to 48% currently.
* 48% of employees will continue to work remotely at least partially after COVID-19.
* Currently, 40 % of modern employees choose to work at home.
* 62% of employees anticipate that their employers will permit them to work remotely in the future.

2.2. Different application of strengthening Cyber security in Remote work

1. For preventing Phishing Attempts

* Conducting cyber security training and awareness sessions for employees
* Educate and train employees on how to protect themselves from phishing attacks, as well as how to recognize these types of attacks, etc.
* Educating individuals on best practices that can be implemented within organizations to reduce risky conditions and maximize the benefits of such implementations.

1. To prevent employees from using insecure connections and home Wi-Fi

* If the organization can afford it and representatives will be working remotely for a considerable length of time, consider providing every employee, or at least those who work with a great deal of sensitive information, with a firewall to protect their home Wi-Fi.
* Periodically refreshing the representative switch's product when free updates are available ensures that any current security holes are patched before a hacker can exploit them. Additionally, determine whether the switch has encryption features that can be enabled.

1. Employees who use weak passwords are penalized

* Encourage employees to adopt strong passwords by implementing a password policy within the organization. Take immediate action on password problems
* Which are created by stringing together phrases is one of the top network connection security recommendations offered by experts. Secure passphrases can be anywhere from four and twelve words, or even longer, with longer passwords being more difficult to crack and guess than shorter ones.
* For instance, a password might be "sir=Google!0og7redbird." To increase the security of a password, one can add accents, character shifts, and numbers.
* In the era of web-based media, personal information commonly used in passwords, such as a user's birthday, is readily accessible on the Internet. If a programmer reads a worker's Facebook profile, for example, they can use the photos, posts, and personal information section to find common password information. Consequently, the use of such extremely personal data is more dangerous.
* Security teams, including supervisors and upper-level management, should advise employees not to use the most common personal information as their passwords.
* When recording a secret key, regardless of whether it is on a tacky note or in the Notes application of a mobile device, leave the door open for a person with terrible intentions to discover it.

Expect to find a statement that impedes password recording in a secret key strategy. If employees need to record passwords to remember them, they should consider using a secure password storage program.

1. For prevents sharing unencrypted File

* Sensitive information transmitted over email or telephone should be encrypted.

Ex: - When it comes to email encryption, Outlook, a popular email platform, includes features that can transform plain text communications into cipher text, so that only the recipient with the key can decode the message.

* Organizations can also use email encryption platforms to obtain email data, links, and contact records.
* Voicemail data can be encoded when the appropriate business telephone scenario is present.

Ex: - Suppliers of business telephones offer features that encrypt and securely email voice message data to protect sensitive and confidential information.

* Using a secure file-sharing platform to encrypt data is also an option. These stages ensure that data is encrypted from beginning to end.

Ex: - OneDrive and Dropbox

1. Discourage the use of personal devices for work and encourage subordinates to utilize only company-supplied devices.

Methods to safeguard mobiles

* Sensitive data can undoubtedly be safeguarded with basic measures, such as enabling a strong password on the phone, but additional measures can also be taken. If the element's representatives conduct business on their home phones, the element can request that they refrain from doing so unless their phones are scrambled.

Ex:

- On Android phones, encryption can be enabled through the security settings.

- On iPhones, it is possible to enable a setting that erases the device after a predetermined number of failed login attempts.

* Voicemail data can be encoded when the appropriate business telephone scenario is present.

Ways to protect computers

* When it comes to securing the PCs of remote employees, the most reliable solution is to provide each employee with a work PC, so they do not need to work from a PC.
* DaaS can be used to transform a personal device, such as a PC or tablet, into a workstation, allowing access to all applications and documents on an organization's server. This is accomplished by leasing virtual workstations through a public or private cloud administration.
* With virtual work areas, if a representative's personal device is stolen, no company data is lost, as data is stored on the virtual work area rather than the actual work surface.

Ways to protect printers

* Home printers have a variety of insecure features that organizations should advise their employees to disable when working remotely.

Ex: - "print from anywhere" features enable users to print documents at home, even when they are away from the office. However, this feature has a low level of security because it requires an opening in the firewall to enable remote communication with the machine. Consider recommending that their representatives reduce this element.

* Another baffling home printer feature is a typical default setting that, when employees scan to the hard drive on their printer, permits them to access the folder from workstations within the organization.
* This configuration permits data to be written to and removed from the device from any location within the organization, typically with minimal or no security. Organizations must take steps to mitigate the data risks posed by this type of component.

Ex: - This element allows associations to consider suggesting that employees turn off printers.

* 1. Real-world examples of enhancing Cyber security for remote work and taking advantage of these improvements.

1. Google

* Google is one of the most well-known examples of using high security to mitigate and reduce cyber risks
* Google strives to transmit the most trusted mists in the industry.
* Google have committed groups like "project zero" who center around finding and fixing weaknesses across the web to make the web more secure for all the users all around the globe [6].

1. Facebook

* Recently, Facebook announced a revolution towards security with an extended focus on private illuminating, in any case, and after that building a phase around that. - In a post, CEO of Facebook Check Zuckerberg specified that [7].

Ex: - "I accept the eventual fate of correspondence will progressively move to private, encoded administrations where individuals can be sure what they say to one another stays secure and their messages and content will not keep close by for eternity."

* This quote demonstrates how the CE emphasized the need for cyber security in their business and what they are attempting to implement to reduce cyber security risks and increase business efficiency.

1. Amazon

* Amazon is a provider of cloud services. The company announced its "AWS - Secret Region," becoming the first commercial cloud provider to offer areas for government work.
* Additionally, the company is competing for the Joint Enterprise Defense Infrastructure (JEDI) contract, which would allow it to provide cloud services to the Department of Defense.

1. Microsoft

* Microsoft focused on ensuring information and network security, primarily because it has such a broad reach across enterprise frameworks.
* They considered placing a significant emphasis on advancing cloud security to protect their sensitive and classified data.

1. Apple

* As a major player in the telecommunications industry, Apple is increasingly concerned with cyber security. And they made significant changes to their business.
* Apple consistently considers client security and has no products under review by other companies.
* With the impact of data breaches, Apple is increasing its efforts to collect client information, particularly on the modern and ventures levels.

1. KPMG

* KPMG is one of the "big four" Therefore, it is one of the largest companies in the world. As one of the four largest companies in the Auditing, bookkeeping, and consulting industry, KPMG has considered network security and data protection. They provide digital security benefits from one end of the globe to the other. In addition, they promote the cyber security services they offer to businesses.
* KPMG assists organizations in developing a versatile and trustworthy presence in the modern world, despite evolving threats. KPMG offers a combination of technical expertise, in-depth business knowledge, and inventive professionals who are enthusiastic about securing and expanding businesses and preventing cybercrimes.

1. Cybersecurity trends in the modern world based on remote work and future developments in the area.

Remote work hopes to have the flexibility and capacity to work remotely while achieving the organization's goals. Previous research indicates that as technology advances, an increasing number of network protection threats will emerge. For instance, ransomware attacks, Distributed Denial of Service attacks, document attacks, Cloud malware attacks, zero-day attacks, swarm, and online media attacks. Numerous organizations must address the potential risk posed by each delegate in their hurriedly revised telecommute model. As technological advancements and business models have risen in the digital protection space and the world has gained control over a previously blocked-off area of work, previously unknown threats are also coming into focus. Thus, the world has progressed to consider more examples of protection in remote works.

* When workers leave for home, threats continue.
* Insider attacks
* Ransomware risks
* Zero Trust issues
* Attacks on the Supply Chain
* Service Access with Secure Access
* Companies with Special Purposes for Acquisition
* Abuse of Verification

1. Conclusion

Working remotely necessitates the implementation of new policies within the organization, special training for the employees, governing mechanisms, achievement of the organization's performance goals, and, most importantly, network security and a heightened awareness of data confidentiality. This report examined the necessity of cyber security for remote work. Especially in situations such as the Covid-19 pandemic. For the economy to function, businesses must maintain their functions. Therefore, many individuals were required to engage in work-from-home practices. Therefore, discussing this type of contemporary topic will enrich the existing body of knowledge. This report will contribute to the existing understanding of cyber security in remote works. In the first chapter, this report focuses primarily on the report's introduction, which covers the introduction to remote work, the significance of cyber security, the major cyber security threats in remote work, the benefits of enhancing Cyber security in Remote work, and the problems associated with a lack of focus on Cyber security in Remote work. In the second chapter, I focused on the subject's development. Which covers the evolution of remote work, the emergence of cyber security in remote works, the various applications of strengthening cyber security in remote works, real-world examples of strengthening cyber security in Remote work, as well as the advantages and real-world problems encountered because of a lack of focus on cyber security in remote works. In the third chapter, I focused on future cyber security requirements for remote work and cyber security trends for remote work in the modern world. The report concluded with an executive summary and a conclusion.

5.References

[1]. Indeed “Q & A: What is Remote work”,25 February 2020. Available: <https://www.indeed.com/career-advice/finding-a-job/remote-work/>.

[2] "https://www.gartner.com/," [Online].

[3] J. H. a. A. Adkins, "Harvard Business Review," [Online]. Available:

<https://hbr.org/2015/04/what-great-managers-do-to-engage-employees/>.

[4]. Cisco “What is phishing?” Available: <https://www.cisco.com/c/en_in/products/security/email-security/what-is-phishing.html/> .

[5].Instution.com,” Remote Working Statistics You Need to Know in 2022” <https://www.intuition.com/remote-working-statistics-you-need-to-know-in-2022/> .

[6]. K. Walker, "How Google supports today’s critical cybersecurity efforts," SVP of Global Affairs, 2021

[7]. b. tech, "How Big Tech Is Finally Tackling Cybersecurity," 210. [Online].