Sri Lanka Institute of Information Technology

Ensuring information security while employees work from home.

Group Assignment

Information Security Policy and Management - IE3072

Group Details:

Student ID	Name
IT20613518	Madhusanka D.N.V
IT20613372	Badullege P.H
IT20297404	Anuradha E.K.R
IT20618872	Thisitha K.L.D
IT20627928	Herath H.M.T.D

Date of submission

11th September 2022

Table of Contents

Content	Page No
Introduction	3
Significant	4
Critical Evaluation	5
Conclusion	10
Abstract	12
References	13

1. Introduction

1.1 What is Information?

Information is organized or classified data. It is a valuable asset in the modern world. Information is used to make decisions and take action. Business organizations are required to gather information and take action to grow their businesses. These actions are helpful for them to avoid risks and threats. So that information needs to be accurate, complete, and timeliness. Timeliness means the availability of information.

1.2What are Cyber Attacks?

According to NIST [1], Cyber Attack is "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information." There are various types of cyber-attacks. Malware, phishing, Man in the middle, DDoS, SQL injection, and cross-site scripting are some examples of cyber-attacks. So, Business organizations need to protect their information against cyber-attacks.

1.3What is Information Security?

Business organizations required some mechanism to prevent information from cyber-attacks. So that information security comes. Otherwise, someone or something can get business information and do unethical things. It can be a risk to those businesses.

According to NIST SP 800-209 [2], information security is "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."

2. Significant

2.1 Why is ensuring information security while working from home important?

Due to Covid 19 pandemic situation and economic crisis in Sri Lanka, most of the business organizations were started work from home concept to their employees. In this concept, organizations had huge challenges to secure their data and information. Because in this period, cyber-attacks were heavily increased.

Businesses and consumers are being cautioned by technology and industry experts about the growing threat of international cyberattacks. The FBI claims that after the COVID-19 epidemic hit, the number of successful attacks has risen dramatically in the United States by 600% (Inglet, 2020) and globally by 300% (FBI IC3 Report, April 2020).
Due to the COVID-19 invisible danger, a significant rise in successful attacks is directly attributable to the number of people telecommuting or working from home. once more
By opening attachments, having more administrator rights than necessary, downloading sensitive information onto thumb drives, forwarding work emails to personal accounts, sharing documents they shouldn't, or having access to more data than is necessary,
people are exposed as the weakest link in organizations. [3]

Our study focuses on the cybersecurity challenges faced by remote workers and the ongoing battle to protect sensitive corporate data and individually identifiable information. To address and reduce these negative cyber influences on teleworkers and their companies, this study investigates the cyber risks and benefits to businesses and individuals when employees work from home.

3. Critical Evaluation

3.1 Practical

The COVID-19 pandemic was first reported in Sri Lanka in January 2020. So, most of the employees were not able to go to their working offices to do their work. Because people needed to maintain social distance and healthy manners to survive COVID-19. This made so many problems for people in Sri Lanka. Because they needed to maintain their family by doing jobs. According to the Department of Census and Statistics, Sri Lanka's labour force participation and job openings decreased. And also, the unemployment rate increased. So, the Sri Lankan government wanted to solve these problems a little bit. So, they advised implementing full or partial work-from-home (WFH) policies.
This WFH concept was a big challenge for businesses and workers. Because they had not had any experience with this. All the workers were not able to shape up to WFH. WFH in Sri Lanka depended on the following three factors.

1. **The possibility of conducting job-related activities from home (nature of the job)** [4]

There are various kinds of jobs in Sri Lanka. Only some of the jobs were suitable to work from the home policy. Because the jobs like masons, and carpenters were not able to do their work from home. Most ICT-related companies could do their work from home. This is the nature of work and the possibility of conducting work.

2. **The capability of the businesses and workers to adapt to WFH** [4]

All the business organizations couldn't be able to start work from home concept easily. Because they needed to give access to their company data. Business Organizations and employees have required the following tools to execute a work-from-home environment.

- **Cloud storage**

Cloud storage is a must thing to implement WFH. Otherwise, employees can't access company files and do their work. Google Drive, Dropbox, and OneDrive are some examples of cloud storage. [5]

- **Communication tools**

Employees and managers need to communicate with each other at work. And also, companies have meetings to discuss things. So, communication methods were a must in

that period. Skype, Zoom, Hangout, and Teams are some examples of communication tools that were used during the pandemic. [5]

- **Project management tools**

Project management tools did a vital thing during the pandemic for business organizations. Because organizations had to manage their work tasks among employees and give time to complete tasks. Trello, Asana, and Jora are some project management tools that were used by business organizations. [5]

- **Time tracking tools**

Time tracking tools helped to check the effective working and focus on work. [5]

Companies were required to increase their security. Because cyber-attacks were heavily increased during the pandemic situation. So, Security was a very important asset to organizations. Organizations recruited cyber security professionals to handle the security of their companies.

3. **The availability of ICT infrastructure and access to the internet for both workers and businesses**. [4]

Employees needed to access ICT infrastructure in companies to do their work remotely. Otherwise, they are unable to do their work. And also, employees required good internet connection for their homes.

3.2 Challengers to ensure security

Sri Lankan Business organizations faced multiple challenges when ensuring security in WFH.

Technical knowledge

- All the employees of Sri Lanka don't have proper technical knowledge. So, business organizations had to train their employees to shape up with WFH. [6]

Phishing Emails and Scams

- Phishing emails and scam attacks were increasing heavily at that time. So, employees had to get knowledge about phishing and scams to prevent it. [6]

Internet access

- Internet access for employees must be secure. Otherwise, attackers can easily launch attacks through an unsecured network. So, employees are required to use public WIFI. [6]

Personal devices

- Employees' personal devices are not fully secured. Because their devices can be used by their children or family members etc. Sometimes employee devices can have outdated software. That software can be vulnerable to attacks. And also, virus and malware attacks can happen to employees' devices. It may affect Business organizations. So, employees' personal device security is very important. [6]

3.3 Failures

- **Weak passwords**

Weak passwords are vulnerable to many attacks. Employees use of weak, insecure, or reclaimed watchwords and login credentials poses one of the largest hazards to businesses' remote workforces. Cybersecurity software and technologies like firewalls and virtual private networks are rendered useless if safe watchwords aren't used (VPNs). [7]

Hackers can now use software to access critical corporate data and crack account passwords. For instance, they can create extensive lists of popular passwords to get access to accounts or create computer code that correctly guesses login combinations using a variety of password variations. Another typical strategy is to try to access their corporate account logins by using passwords they are aware someone else has used for another account, like a personal email or social networking site.

- **The Custom of Sharing Unencrypted Files**

Associations might consider scrambling information that is put away in their organization, yet they probably won't remember to encode information that is being moved starting with one area and then onto the next. Your association can't bear to allow this data to stay powerless against being taken by a cybercriminal on the grounds that your workers convey such a lot of delicate data every day, including client account data, and documents, and the sky is the limit from there. Assuming private data is blocked, it might bring about the robbery, ransomware cyberattacks, personality extortion, and different issues. [7]

- **Accessing Private Information Through Dangerous Wi-Fi Networks**

Your staff members can be using unprotected public Wi-Fi to access their company accounts or connect to their home wireless network. This makes it simple for hostile individuals nearby to observe their connection and gather sensitive data. For instance, attackers may intercept and steal data provided in plain text form that is not encrypted. Due to this, you should forbid your staff from connecting to any unidentified Wi-Fi networks unless they are doing so using a VPN connection.

- **Using personal technology at work**

Whilst working from home, 46 of the labor force conceded moving data among their non-public computers and their place of work computers, that is a regarding exercise. At the identical time, an exercise called the" deliver Your particular tool" or BYOD policy — which permits workers to apply their particular bias to oils has surfaced.

You must be fully informed of the problems posed by your staff using their personal devices for business-related purposes. For instance, they can abruptly depart from the You won't have the ability to delete the private data that was kept on their smartphone while they were working for your firm and keep onto it. Additionally, they might not be updating their software, which exposes security gaps in your environment. We keep emphasizing how crucial it is to deploy software updates promptly, and with good cause. Because it would be challenging for you to oversee what happens on your employees' endpoints, we advise against allowing them to use their personal devices at work. [7]

- **Power cut problems**

Any moment of the day can experience a power outage, which often lasts a few hours. Depending on which employees are impacted, it might only be a little nuisance at most, but at worst, it might have a negative impact on daily operations and put your company's operations on hold. A power outage that lasts less than an hour has a completely different effect than one that lasts for the entire workday. Even though it can be challenging in these circumstances, try to estimate how long it might take to restore electricity by keeping up with the local news.

3.3 Laws

Because of the pandemic situation and the economic crisis in Sri Lanka, many employees couldn’t work as usual. Because of this, many companies introduced a work-from-home method. However, this new online work method created new threats regarding the security of their information.

Information is a crucial tool for an organization. Because of this, companies and organizations needed to protect their information. In helping protect the information, implementing security laws plays an important role. These security laws can be described as the laws governing the procedures, techniques, tools, and criteria necessary to secure information technology assets (IT Assets) and other types of data against illegal access, use, disclosure, modification, or destruction. So, with the pros outweighing the cons many companies decided to implement information security laws to protect their information.

Nowadays there are many security laws that are used to protect information organizations. For example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Children's Online Privacy Protection Act of 1998 (COPPA), the Fair and Accurate Credit Transactions Act of 2003 (FACTA), 1999 Gramm-Leach-Bliley Act, and the 2002 Homeland Security Act, etc. [8]

Nowadays in Sri Lanka using Computer Crimes Act, No 24 of 2007, and PERSONAL DATA PROTECTION ACT, No. 9 OF 2022 laws for Information security. Before the pandemic and the economic crisis in Sri Lanka, companies and organizations didn’t tend to use security laws. This happened because back then, companies rarely used their Information outside of their corporation and because many people were unaware of information security laws. But after many companies had to start using a work-from-home method, they needed a proper way to protect their information. Because of this, the usage of information security laws widened. As a result of this, both the information security of companies and the trust of foreign countries with our companies got stronger. [8]

4. Conclusion

According to our research, business organizations need to follow following things to ensure security in WFH. These things give better security for organizations.

- **Infrastructure protection:**

It's critical to have faith that corporate infrastructure is safeguarded by strict security standards. Making sure all work devices are equipped with the necessary endpoint security tools and a reliable VPN service for a secure connection to the corporate network is part of this. Home networks are by nature less secure than those that staff members connect to at work. Default passwords for Wi-Fi routers are frequently quite simple for hackers to guess. Remote workers should create a special password that they may change at any time by entering the router's address, such as "192.168.1.1," in their web browser to access the router's settings page.

Additionally, users have the option of changing the network's name or service set identifier (SSID) to make it more challenging for hackers to locate and access the network. Network encryption, which may be modified in the security settings of the router's wireless configuration page, should be used to fortify home networking. Wi-Fi Protected Access 2 is the most reliable encryption setting on the majority of routers (WPA2). By restricting access to particular media access control (MAC) addresses, Wi-Fi can be made stronger. Additionally, the router should always be using the most recent firmware version. [9]

- **Secure the network:**

Because of the unexpected rise in remote work, it is critical that companies take the required precautions to secure their network. This includes the implementation of software capable of running continuous viruses and suspicious connection scans. Antivirus software aids in ensuring the security of remote workers. Cybercriminals use sophisticated attack methods including distributed denial-of-service (DDoS), malware, ransomware, and spyware to target home networks. By automatically detecting, identifying, and stopping viruses, phishing schemes, and zero-day assaults from infiltrating the network, antivirus software aids in the fight against these dangers. [9]

- **Encourage employees to use the IT support team:**

Instead of attempting to resolve technological problems on their own, employees should be encouraged to consult the IT support teams. This could assist to prevent a bigger issue from occurring in the future and will guarantee that problems are treated as soon and safely as feasible.

- **Safe communication**

Make sure the instant messaging and video conferencing programs used for internal communications adhere to accepted security requirements. Although staying connected is important, security shouldn't suffer as a result. [9]

- **Make use of strong passwords**.

Employees need to have strong passwords for their business accounts. Though, Employees must have at least 12 characters with combination letters, symbols, and numbers. Those passwords must not be mostly used passwords like “admin". Employees also need to think about their password managers' security. [9]

- **Against the power cut**

Plan and prepare-

Make a strategy if you suspect terrible weather is headed in the direction of your employees. In case they lose internet connectivity, ask your staff to charge their devices and download or print off documents they can work on manually. If the internet is down, you might even wish to invest in a broadband USB stick.

- **Employee awareness training programs**

There are some employees who don’t have proper knowledge about how to secure their working environment. So, Business organizations can collaborate with security professionals and do awareness training programs. This may increase business security.

5. Abstract

Working from Home (WFH) presents a critical weakness to network safety dangers, like noxious programmers and social specialists, as we affirmed by tending to our examination inquiries through a significant and material writing survey of educated authorities and a little contextual investigation of telecommuters. Yet again the human perspective is distinguished as data security's most fragile connection (corporate and individual). [3]

Our exploration instructed us that, no matter what the sort or size of the association, or the position and job of an individual, going from latency to activity is certainly not a straightforward methodology. We likewise comprehended that bringing issues to light is just the most vital phase in making a contemporary digital guard in the distant working environment and that a strong specialized establishment and business congruity plan are basic to progress. Associations should try their insight by diminishing gamble to shield against an assortment of digital dangers.

The most elevated echelons of the association should uphold, purchase in, and store this WFH program. It likewise should be made accessible to all partners. Solid morals preparing and security training programs are the most important phases in furnishing telecommuters with network cybersecurity protection.

No matter where they work, users must be taught not to click on dubious links and to always guard their log-in information. It is crucial to choose a top-notch cybersecurity system that can both remove infections and pinpoint their source in the case that cyber assaults are successful (Pankov, 2019).

Regardless of where they work, all representatives should be responsible for keeping social specialists and programmers from taking advantage of the association. Leader and line supervisors, experts, specialists, providers, advisors, receptionists, and anybody with a console could be in every way focused on for misuse; nonetheless, telecommuters may be the generally underestimated and uncovered. We fight that the trouble of safeguarding against human-based digital and social designing weaknesses is huge and cannot be ignored any longer. Organizations will proceed to WFH for a long time to come as the US begins to recuperate from the COVID-19 pandemic. Regardless of where we are telecommuting, we should be generally careful about the pandemic of scrambled malevolent traffic from programmers and social designers on the grounds that covered phishing dangers, malware, and ransomware are on the ascent. [10]

6. References

[1] NIST, "COMPUTER SECURITY RESOURCE CENTER> Cyber Attacks," NIST, [Online]. Available: https://csrc.nist.gov/glossary/term/Cyber_Attack. [Accessed 30 08 2022].

[2] NIST, "COMPUTER SECURITY RESOURCE CENTER," [Online]. Available: https://csrc.nist.gov/glossary/term/information_security#:~:text=NIST%20SP%20800%2D209,confidentiality%2C%20integrity%2C%20and%20availability.. [Accessed 30 08 2022].

[3] H. N. Security, "Employees abandoning security when working remotely," 29 05 2020. [Online]. Available: https://www.helpnetsecurity.com/2020/05/29/abandoning-security-when-working-remotely/. [Accessed 05 09 2022].

[4] "Working Remotely in the Age of COVID: Who is Left Behind?," TALKING ECONOMICS, [Online]. Available: https://www.ips.lk/talkingeconomics/2021/03/08/working-remotely-in-the-age-of-covid-who-is-left-behind/. [Accessed 08 09 2022].

[5] D. Celebic, About.me, [Online]. Available: https://domain.me/remote-working-tools-for-any-business/. [Accessed 08 09 2022].

[6] U. I. Guys, "Security Challengers For Work From Home," [Online]. Available: https://www.ultimateitguys.com/content/four-security-challenges-working-home. [Accessed 06 09 2022].

[7] T. P. Security, "WFH Security Issues and Bad Employee Behaviors in Remote Workplace," [Online]. Available: https://www.third-party-security.com/wfh-security-issues-and-bad-employee-behaviors-in-remote-workplace/. [Accessed 06 09 2022].

[8] C. Bro, "Cyber Crimes and Laws in Sri Lanka," 2021.

[9] B. Busch, "How to Maintain Security When Employees Work Remotely," Hitachi solutions, [Online]. Available: https://global.hitachi-solutions.com/blog/working-remotely-security-tips/. [Accessed 07 09 2022].

[10] M. Apgar, "The Alternative Workplace: Changing Where and How People Work," Harward Business Review, [Online]. Available: https://hbr.org/1998/05/the-alternative-workplace-changing-where-and-how-people-work. [Accessed 08 09 2022].