Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond

Arnold Mashud Abukari and Edem Kwedzo Bankas

Abstract— The emergence of Corona Virus Disease (COVID-19) has threaten individuals, organisations and Government Agencies across the world and grounded almost everything to a halt. COVID-19 continues to spread rapidly asymmetrically around the world after it was first observed in Wuhan, China. Economies are crashing and businesses are at the verge of collapse. Individuals or employees are working from home in the form of teleworking others too have stopped working. Despite this challenge caused by this pandemic, Cyber Criminals (Social Engineers) are targeting unsuspecting individuals and organisations to gain access to their sensitive information through the activities of Social Engineering. In this paper, we present hygienic protocols that can help address the dangers of cybercrimes in the era of COVID-19. The education protocol, training protocol and policy protocols are outlined. The paper also revealed some defects that needs to be addressed when using VPN and desktop sharing. Our paper also reviewed the NIST standards on Teleworking and the Information Technology Lab (ITL, 2020) guidelines.

Index Terms— COVID-19, DoS, VPN, PAM, Teleworking, Cyber Security

1 INTRODUCTION

Corona Virus Disease (COVID-19) is a pandemic that has taken the world by storm. The pandemic has succeeded in striking fears across businesses and individuals across the globe as well as horrified medical practitioners in the world. Despite the pandemic stabilising in China where it was reported to have started from, other countries throughout the world especially United States Of America (USA), Spain, Italy and France are having serious challenges in controlling the pandemic. With over 1,720,000 confirmed cases and over 104,000 reported dead cases as at April 11, 2020 (WHO,2020), Some Governments and businesses have locked down their countries and restricted movements in their quest to combat the pandemic. Some Universities, government institutions as well as businesses have been tasked to work from home and this will largely be dependent on the use of the internet. These emergency measures however comes with challenges. The individuals and businesses operating from homes uses computer systems and virtual environments which is being exploited by hackers or cyber criminals. In an FBI Public announcement by the office of the Chief Information Security Officer, State of Texas captioned "Cyber Actors take advantage of COVID-19 Pandemic to exploit increased use of Virtual Environments", reveals that, Cyber actors exploit vulnerabilities in these systems to steal sensitive information, target individuals and businesses performing financial transactions, and engage in extortion. According to the announcement, the FBI's Internet Crime Complaint Center (IC3) received over 1,200 complaints related to COVID-19 Scams. Cyber criminals have recently engaged in phishing campaigns, Denial of Service(DoS) Attacks, fake news portals and applications to steal very sensitive information from unsuspecting individuals, Government Officials and Businesses. In this paper,we propose some cyber security hygienic protocols for teleworkers in the era of COVID-19 and beyond.

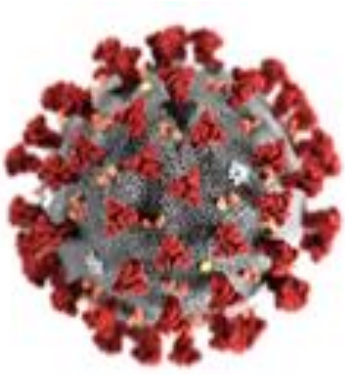

Figure 1: COVID-19 (www.gau.edu.tr)

2 TELEWORKING

The term Teleworking describes a working arrangement

- *Arnold Mashud Abukari is currently pursuing PhD programme in Cloud Computing Security in the University for Development Studies(UDS) and a lecturer at the Computer Science Department of the Tamale Technical University, Ghana. E-mail: amashud@tatu.edu.gh*
- *Edem Kwedzo Bankas is a senior lecturer at the department of Computer Science in the University for Development Studies, Ghana. E-mail:ebankas@uds.edu.gh*

where an individual works from home using computer systems and virtual environments (International Encyclopedia of Social and Behavioral Sciences, 2001). In teleworking, individuals or teleworkers will have to rely on self-reliance greatly and remote work self-efficacy (Staples et al, 1999). Despite the convenience it provides to teleworkers, administrators over the years have raised concerns about supervision and how to rate performances in terms of hours worked, satisfaction and perceived flexibility (B. Hesketh, 2001). However, (Jarvanpas and Leidner, 1999) argues that teleworking groups are able to maintain trust without contact and were better able to manage uncertainty and complexity.

"We don't even have a proper definition of what telework entails and as a result we don't have a legislation that governs telework. We would like the International Labour Organisation (ILO) to facilitate research to assist us with coming up with that definition and also with legislation because while there are advantages, there are also questions and challenges", South Africa's Deputy Minister of Labour, Nkosi S.P. Holomisa lamented in a Global Dialogue Forum organised by the ILO in Geneva from 24-26 October, 2016.

.

3 TELEWORKING AND CYBERSECURITY

The increase in the confirmed cases and deaths relating to COVID-19, a global pandemic, has led to many employers and Governments recommending telework to keep employees safe and productive thereby allowing their employees to work from home without necessarily considering the cyber security implications on their employees and businesses and the need to properly set up a secured environment needed for a safe teleworking. Information Technology devices at homes are generally perceived to be poorly configured compared to the work environment IT devices hence the IT devices at home are highly prone to cyber attacks especially in the COVID-19 pandemic era. Cyber criminals or hackers may take advantage of the unsecured off-site routers, modems, unsecured network devices and poorly configured home network devices to exploit the vulnerabilities associated with teleworkers and there compromising the security of the organisations and government agencies.

Recognising the dangers in terms of the possibility of increasing cyber crime on individuals and businesses in the wake of this COVID-19 pandemic, The Information Technology Laboratory (ITL, 2020) in March 2020, issued a news bulletin to reiterate the National Institute of Standards and Technology(NIST) standards for teleworking .

The following Information Technology security measures were outlined in the March 2020 Information Technology Laboratory (ITL,2020) news bulletin:

1) Developing and enforcing a telework security policy, such as having tiered levels of remote access
2) Requiring multi-factor authentication for enterprise access
3) Using validated encryption technologies to protect communications and data stored on the client devices
4) Ensuring that remote access servers are secured effectively and kept fully patched
5) Securing all types of telework client devices – including desktop and laptop computers, smartphones, and tablets against threats

(ITL,2020) further agrees that Telework and remote access technologies need addition protection due to their nature of being at a higher exposure to external threats compared to on-premise Information Technology Infrastructure. Major information Technology security concerns using teleworking were identified despite the NIST standards for teleworking. Below are some challenges informing the need for our research:

1) Lack of physical control
2) Unsecured networks used for remote access
3) New threats for organisations through allowing external unsecured access to sensitive resources
4) Teleworkers may be using their own unstructured and unsecured resources to access their organisation's valuable resources
5) The security measures assumes individuals uses computing devices from their employers which is not applicable in all cases.

There is no comprehensive telework security policy that protect teleworkers, Bring Your Own Devices (BYOD) and remote access for most organisations and Government Agencies

4 TELEWORKING AND REMOTE ACCESS METHODS

Remote access is the ability of a teleworker to securely establish a connection to systems or a computer through a network connection. Remote access to systems in the COVID-19 Pandemic has become a life saver for businesses and other organisations using computer systems. Despite remote access being one of the solutions to help individuals and organisations continue working, it comes with a lot of security concerns in the wake of the COVID-19 pandemic. Malicious internet users and hackers have started exploiting vunearabilities associated to the teleworker and this could compromise the security of the teleworkers and their organisations.

VIRTUAL PRIVATE NETWORKS

One of the tools of choice for teleworkers to connect to their organisation's computing systems is the Virtual Private Network (VPN)(Howlet, 2019). Teleworkers can remotely access their company files as well as upload files to their company's servers. According to (Howlet, 2019), VPNs are designed for teleworkers to have online privacy and anonymity by changing their public internet into a private network using a specific communication channel. The security in VPNs lies on the the

creation of a communication tunnel and protecting the connection by encrypting data.

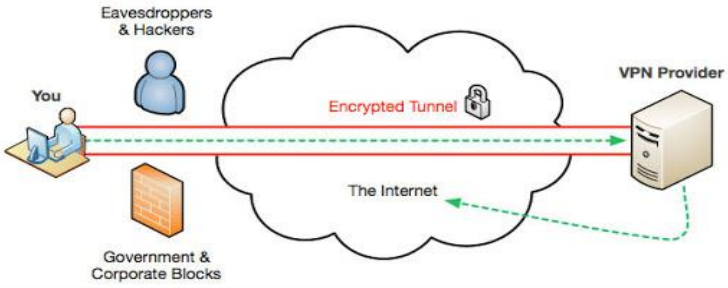

Figure 2: Overview of VPN (www.wirelessshark.org)

Teleworkers using unsecured WiFi networks at their various locations stands a chance of weakening the security provided by Virtual Private Networks (VPNs) since the privacy of the teleworker could be exposed to hackers snooping on that unsecured network and therefore compromising the security of the teleworker and his/her organisation in the process and this has informed our research in this paper. Even though VPNs have their own security challenges regarding data breaches as reported by (Swearingen, 2018) but that is not the focus of our research work.

DESKTOP SHARING

Desktop sharing is a remote access method that enable organisations to provide access to users for real-time sharing of files, presentations or application sharing. Remote support, online conferences and webnars can all use the desktop sharing concept. Desktop sharing comes with authentication risks that suggests security implication to the organisation. If the user's credentials are compromised then it means an unauthorised user can have access to the organisation's resources through the network. For the purposes of auditing, logging and audit trails are challenging with desktop sharing.

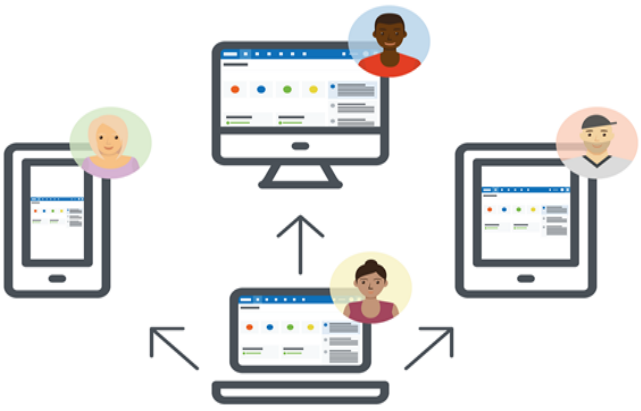

Figure 3: Desktop Sharing (www.placetel.de)

PRIVILEGED ACCESS MANAGEMENT (PAM)

Understanding the security challenges faced with the usage of VPNs and Desktop sharing technologies, the Privileged Access Management (PAM) was developed as a better enterprise level solution. The Privileged Access Management solution has a combination of tools and technologies that works together to secure, control and monitor user access to organisation's resources. This is possible through a privileged account to the organisations resources on their servers. A well implemented Privileged Access Mangement (PAM) can offer the following in terms of information secutiy defense:

1) Ensure advanced credential security, systems and data access control
2) Ensure credential obfuscation
3) Ensure user activity monitoring

Adhering to the full implementation and deploying of the Privileged Access Management (PAM) can lower the threats of unauthorised network access and administrators of information systems of an organisation can uncover suspicious activity on the network.

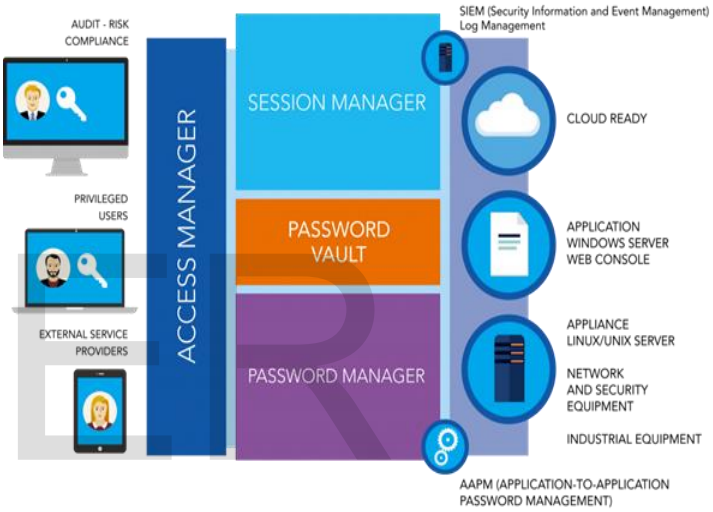

Figure 4: Privileged Access Management overview (www.mechsoftme.com)

5 CYBERSECURITY AND CRIME

Cyber Crime is the use of computing resources such as computers and networks to perform illegal operations online (Moore, 2005). In 2007, (Binitha et al, 2007) argues that cybercrimes also includes using computers as a means to perpetuate crimes or activities that contravenes any law. Cybercrimes are committed with malicious intention to harm individuals or groups of individuals using the internet (Warren and Jay, 2002). Spreading of computer related malwares, online bullying, unauthorised electronic transactions, child pornography and breach of privacy are some of the activities performed by cyber criminals. In a McAfee sponsored report published in 2014, it was revealed that an estimated damaged annually was $445 billion globally through the activities of cyber criminals (McAfee, 2014).

To combat cybercrimes, there is a need for a comprehensive and robust cyber security solutions. Cyber Security is a way of protecting computer systems, networks and individuals from

the malicious attacks from hackers. These attacks from hackers or malicious users damage hardware, software, electronic data as well as cause disruption of services (Schatz et al, 2017). Due to the increasing number of cybercrimes, cyber security is identified as one the major challenges confronting the world today (Stevens, 2018).

To fight against cybercrimes needs a multi-faceted approach as identified in the figure xxx. Attitude awareness, Ethics, Information Technology systems and Law enforcement should work together to combat cyber crime. In the wake of the COVID-19 Pandemic, cyber criminal activities are bound to increase and there is the need to enhance the cyber security measures currently being adopted.

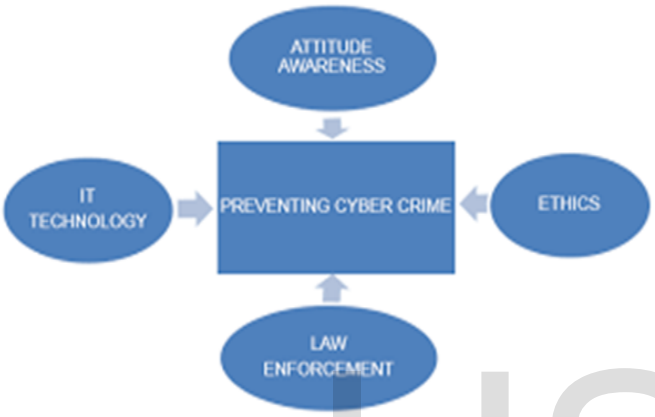

Figure 5: Preventing cyber crime

6 TELEWORKING AND SOCIAL ENGINEERING

One of the key strategies cyber criminals will be using in this trying times of COVID-19 is Social Engineering. This is a strategy employed by malicious hackers to manipulate people expecially teleworkers psychologically, to perform actions that will reveal confidential information. Cyber criminals use the concept of social engineering for the purposes of gathering information about their targets or for fraud or to gain access to computer systems (Anderson, 2008). Social Engineering is also thought to be any act that influences an individual or group of persons to take actions that may or may not be in their interest. In a research presented by (Andersson and Reimers, 2014), it was revealed that employees do not often see themselves as a major component of the organisation's information security. This makes employees take actions that ignores information security protocols of the organisation hence compromising their individual and organisation's security. (Schlienger and Teufel, 2003) suggested five(5) steps to help manage information security. These are:

1) Pre-Evaluation
2) Strategic Planning
3) Operative planning
4) Implementation
5) Post-Evaluation

(Breda et al, 2017) argues that as the digital era is maturing, cyber security has evolved with diminishing vulnerabilities in software and people are more exposed to cyber criminals than ever.

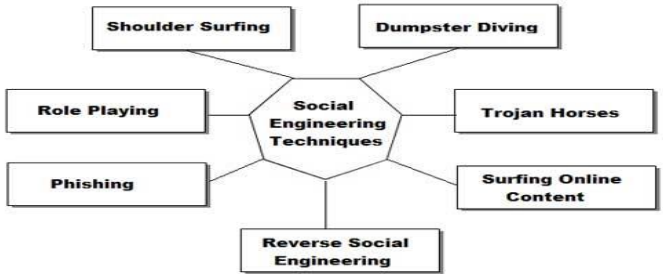

Figure 6: Social Engineering Techniques

Tailgaiting, impersonation, eavesdropping, shoulder surfing, dumpster diving, reverse social engineering, fake emails, fake applications (Some COVID-19 Apps), fake domain names etc are some the techniques cyber criminals use to compel unsuspecting individuals to reveal very sensitive information. Phishing, Baiting and watering hole are other socio-technical approach for Social engineering (Breda et al, 2017).

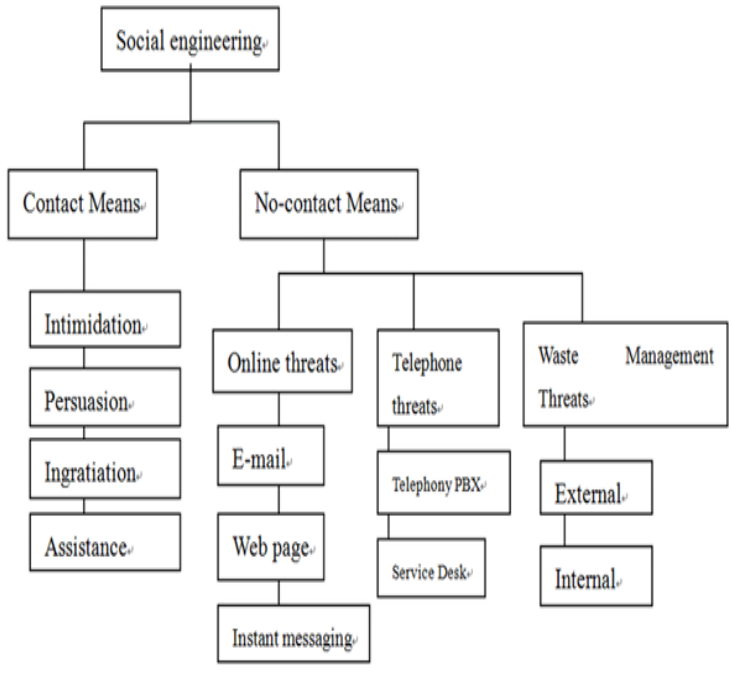

Figure 7: Social Engineering Classification

7 PROPOSED PROTOCOLS

We propose a comprehensive cyber security protocols for individuals, organisations and Government agencies who are using teleworking in the era of the COVID-19 Pandemic and beyond across different security domains such as social engineering, fake news and applications, encryption schemes.

7.1 TRAINING PROTOCOL (ORGANISATION LEVEL)

In this era of COVID-19 pandemic, Social Engineers (Hackers) are targeting unsuspecting individuals to get sensitive information from them for their malicious activities. We have proposed a training protocol for individuals and organisations to use to assess their employees who are teleworking in this era of COVID-19. Social Engineering awareness training is essential in combating cyber crimes during this trying time. Social engineering awareness, social engineering penetration strategies awareness, safe behaviours of teleworkers and reporting channels are key to ensuring secured systems in the quest to reduce cyber crimes and improve cyber security.

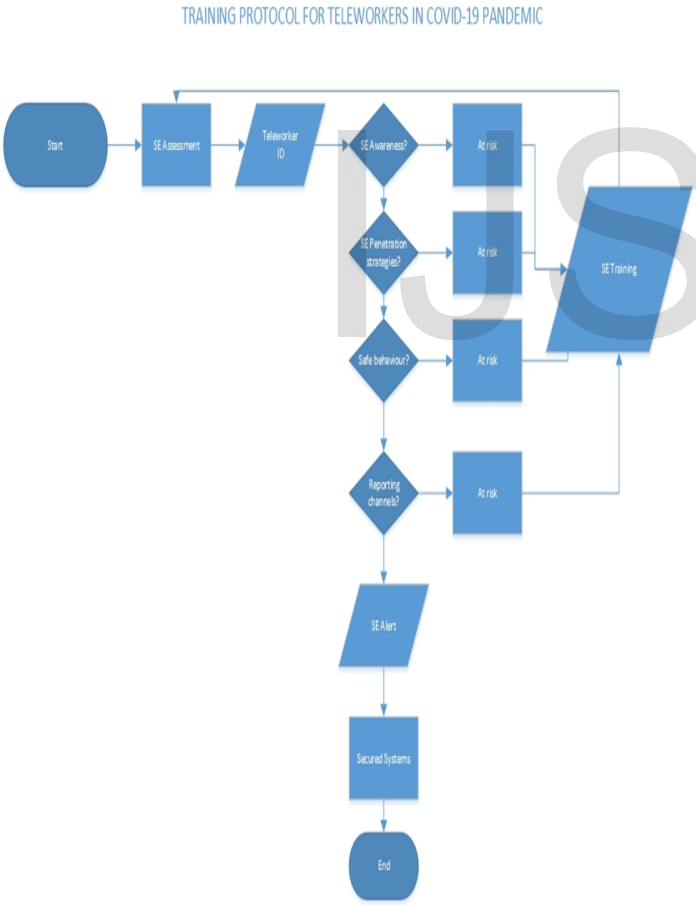

Figure 8: Training Protocol for Teleworkers in COVID-19 Pandemic

The proposed training protocol in figure 8 determines how risky lack of social engineering awareness, penetration testing and reporting channels could be to organisations and recommend Social Engineering Training for teleworkers.

7.2 EDUCATION PROTOCOL(INDIVIDUAL LEVEL)

There is always the need for individuals to get education in the use of internet, the internet ethics and knowledge on some deceptive approaches used by cyber criminals. There is therefore the need for organisations or the individuals themselves to go through some assessment using our proposed protocol before teleworking. This will ensure teleworkers are alerted about the proper use of internet and the best practices in using the internet. Identifying fake news, fake applications, fake email IDs and fake websites used to share information about COVID-19 are key in ensuring the reduction of cyber crimes in this pandemic. Against this background, we propose the education Protocol for teleworkers to be adhered to.

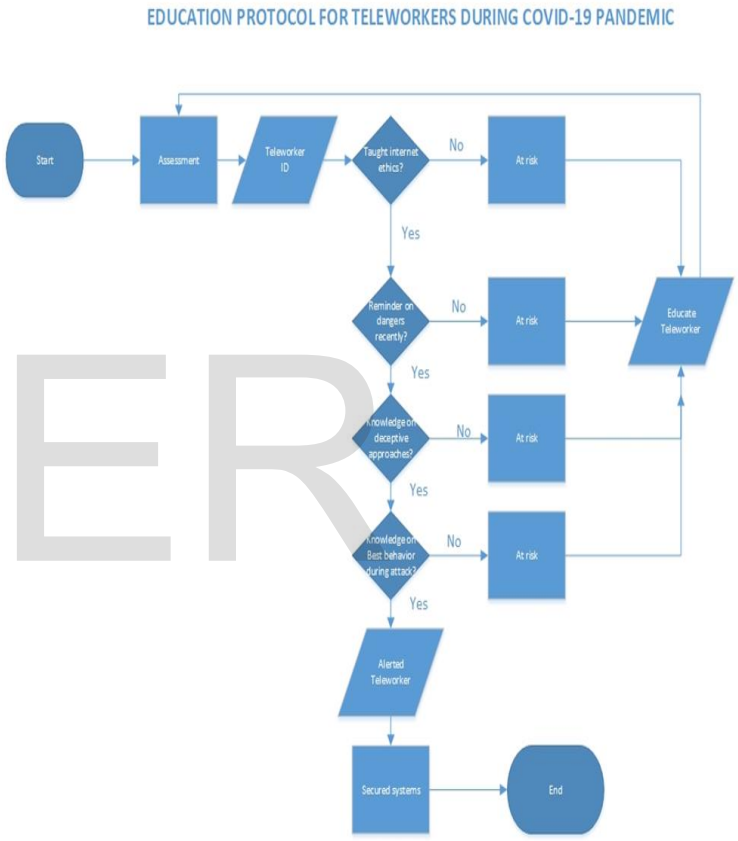

Figure 9: Education protocol for Teleworkers in COVID-19 Pandemic.

In our Education protocol, internet ethics, knowledge on deceptive approaches, knowledge on best behavious when surfing the internet and periodic reminders of the best practices are essential to safeguarding the organisation's vital information during this era of corona Virus Disease (COVID-19).

7.2 POLICY PROTOCOL

Organisations and Government Agencies usually use policy statements or Information Technology Policy document to help enhance their cyber security measures against social engineers and malicious hackers. Policy documents are usually used to streamline the behaviour of personnel against the expected behaviours in the policy document (Buckley et al, 2014). According to a research conducted by (Aldawood and Skinner, 2019),developing and instituting a comprehensive

cyber security procedures is one of the best security measures to reduce social engineering attacks.

Our Policy protocol took into consideration personnel behaviour, punitive measures, social engineering measures, preventive measures, desk policy, caller IDs, monitoring, social media, auditing and compliance. These are key components needed to be addressed in policy statements and Information Technology Security policy document.

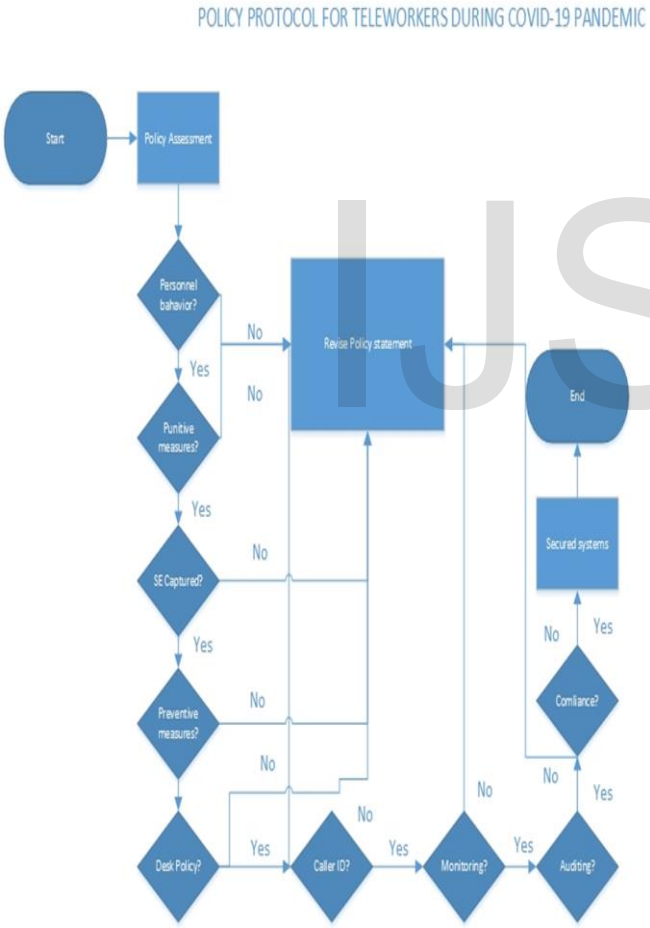

Figure 10: Our Policy Protocol for teleworkers in COVID-19 Pandemic

4 Conclusion

Despite the proposed protocols outlined in this paper, there is still the need for Information Security tools to be used to ensure optimum protection from cyber criminals. Updating network tools, installing and configuring Network-based Intrusion Detection Systems (NIDS), Proper mechanism to identify phishing attacks, email restrictions on attachments, reporting tools, proper configuration of firewalls and penetration testing are still required to compliment the protocols outlined in this paper in order to fight against cyber crime in the COVID-19 Pandemic era. Educating and training teleworkers is very important to equip them to identify potential threats and also prevent revealing sensitive information to unauthorised people through the activities of social engineering. Teleworkers, organisations and Government agencies must be very vigilant and work together to combat cybercrime in this COVID-19 pandemic era. Adhering strictly to our proposed protocols outlined in this paper will help reduce cybercrime.

Acknowledgment

.

References

1) Aldawood, Hussain & Skinner, Geoff. (2019). Contemporary Cyber Security Social Engineering Solutions, Measures, Policies, Tools and Applications: A Critical Appraisal. 2019-2020.
2) Anderson, D., Reimers, K. and Barretto, C. (March 2014). Post-Secondary Education Network Security: Results of Addressing the End-User Challenge.publication date Mar 11, 2014 publication description INTED2014 (International Technology, Education, and Development Conference)
3) *Anderson, Ross J. (2008). Security engineering: a guide to building dependable distributed systems (2nd ed.). Indianapolis, IN: Wiley. p. 1040.* ISBN 978-0-470-06852-6. Chapter 2, page 17
4) Binitha et. al. (2007). Cyber Crimes and Information Frauds. *Recent Advances in Information Science & Technology*, *Recent Advances in Information Science & Technology* Journal, pp 1-3.
5) Breda, Filipe & Barbosa, Hugo & Morais, Telmo. (2017). SOCIAL ENGINEERING AND CYBER SECURITY. 4204-4211. 10.21125/inted.2017.1008.
6) *Cyber crime costs global economy $445 billion a year: report". Reuters. 9 June 2014. Retrieved 15 April 2020.*
7) H. Aldawood and G. Skinner, "An Academic Review of Current Industrial and Commercial Cyber Security Social Engineering Solutions," in *2019 the 3rd International Conference on Cryptography, Security and Privacy*, Kuala Lumpur, Malaysia 2019.
8) Maziah M. Ali (2016). Determinants of Preventing Cyber Crime: a Survey Research. *Journal of International Business Research and Marketing, 2(7),* 16-24.
9) Moore, R. (2005) "Cyber crime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.
10) O. Buckley, J. R. Nurse, P. A. Legg, M. Goldsmith, and S. Creese, "Reflecting on the ability of enterprise securi-

ty policy to address accidental insider threat," in *Socio-Technical Aspects in Security and Trust (STAST), 2014 Workshop on*, 2014: IEEE, pp. 8-15.

11) Pal, P., & Jain, J. (2017). A Recent Study over Cyber Security and its Elements. *Journal of Advanced Research in Law and Economics*, *8*.
12) *Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017). "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law.* ***12*** *(2). ISSN 1558-7215.*
13) Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of Cyber Security. *IJARCCE*, *7*, 125-128. doi:10.17148/IJARCCE.2018.71127
14) *Stevens, Tim (11 June 2018). "Global Cybersecurity: New Directions in Theory and Methods" (PDF). Politics and Governance.* ***6*** *(2): 1–4. doi:10.17645/pag.v6i2.1569.*
15) *Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 978-0-201-70719-9.*
16) www.who.int/emergencies/diseases/novel-coronavirus-2019/events-as-they-happen
17) https://csrc.nist.gov/News/2020/telework-cybersecurity-itl-bulletin-blog-posts