Cyber security threats during the pandemic

Hassan Aljohani

Email: hes20201@gmail.com

Abstract

The aim of this paper was a systematic review of cyber security issues, types, causes, consequences and management and preventive steps. A total of 17 papers were shortlisted for a reviewed by focussing on the types of cyber threats, causes, mitigation and prevention. The findings were as follows: Generally, all internet activities are liable to cyberattacks of various types. The pandemic has exacerbated the threat in multiple manners. Government sites, healthcare sites, online learning platforms, work from home platforms and all other internet applications have been succumbing to cyberattacks of different types. These attacks have different targets, causes and consequences. Most of them occur due to some slippage or error in vigilant use of internet. Even the best protected sites are vulnerable to cyberattacks as hackers find new ways to penetrate the defence systems. The consequences of these attacks on Covid-19 related aspects have serious consequences on healthcare, trust and compliance of people with government measures to prevent its spread. Even people in authority have contributed to lack of trust on healthcare workers though their outbursts in social media. The only way to protect from cyberattacks is careful handling of internet access for any purpose. The findings from this work can be used as learnings for improving the quality of internet browsing.

Keywords: Cyber security threats, internet use, pandemic, review

Introduction

As Coronavirus has been spreading around the world with new strains appearing every now and then, there had been a significant secondary threat through a series of indiscriminate, a set of targeted, cyber-attacks and cyber-crime campaigns. In their article, Williams, Chaturvedi, and Chakravarthy (2020) noted that globally, cybersecurity threats have been estimated to cost about US $6 trillion a year by 2021 and there is a five-fold increase in the number of attacks after Covid-19 has hit the countries. Relaxations in the enforcement of the Health Insurance Portability and Accountability Act by the Office of Civil Rights has also resulted in relaxing the physical and technical safeguards to cyberattacks. About 90% of health care providers had already suffered from cyber-attacks on their data. Regular software updates, use of the best local area networks and frequent penetration tests are required to be done by the companies to prevent cyberattacks. Factors increasing vulnerability to cyberattacks need to be understood and controlled. Here, a review of cyber security threats of various types, causes, consequences and management and preventive steps are analysed using reported works. The findings from this work can be used as learnings for improving the quality of internet browsing.

Method and Results

The method used for this paper is a systematic review. A search of the first five pages of Google Scholar using the topic itself as the search term was done. All the available papers in English language discussing cyber security issues related to Covid-19 pandemic were selected. This method of search and selection yielded 17 usable papers. These are discussed one by one below.

Scams of various types impersonating public authorities like the WHO, supermarkets, airlines, support platforms, personal protection equipment and fraudulent claims of cures have been on the rise. Targets for these cyberattacks could be the general public, persons working from home or any other specifically targeted vulnerable groups. Fear, anxiety, stress and worry of individuals could drive them to seek desperate solutions for their problems chanced by the new situation. This becomes a golden opportunity for cybercriminals have to expand their attacks even using the traditional methods of trickery. Software vendors have been caught unawares and they have not been able to ensure security of their products against the new threats. Critical infrastructure, especially healthcare services are prime targets of cyber-attacks as the impact will be very high. Realising this, on April 8th 2020, the United Kingdom's National Cyber Security Centre (NCSC) and the United States Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) published a joint advisory on how cyber-criminal and advanced persistent threat (APT) groups were exploiting the current Covid-19 pandemic (NCSC, 2020). It contains details of different types of cyber-attacks, targets and mitigation methods. However, a broader assessment of the wide range of the pandemic-related cyber-attacks, is lacking in research as well as in practice. Extremely dispersed nature of reported attacks from various sources makes it difficult to develop response, protection and prevention methods. This information gap was addressed in the work of Lallie, et al. (2020) in which, timelines of cyber-attacks have been described. The timeline mapped the important cyber-attack events around the world against the spread of the virus and strategies like timing of lockdowns. This type of timeline mapping revealed a pattern of cyber-attacks follow events such as announcements of policy. This facilitates tracking of the rapidity with which cyber-attacks and crimes occurred in relation to the first report of the pandemic in the area was published. In some cases, these attacks even pre-empted implementation of these policies and strategies. Unfolding of cyber-attacks, method of attacks and impacts were analysed focusing on UK, but applicable across the world. Especially, the impact of these attacks on workforce and the risks to which they were exposed were also probed. The chronological sequencing of attacks and the representation of campaigns have been done using an accepted attack taxonomy. Some of the important data given by the authors are presented below. The timeline in Fig 1 has the data too crowded and it is difficult to provide any specific descriptions about the contents. It can only be said that several events related to corona pandemic led to challenging cyber-attacks. The X-axis provides the pandemic events and the lines terminating in statements are the different types of cyber-attacks reported in various countries.

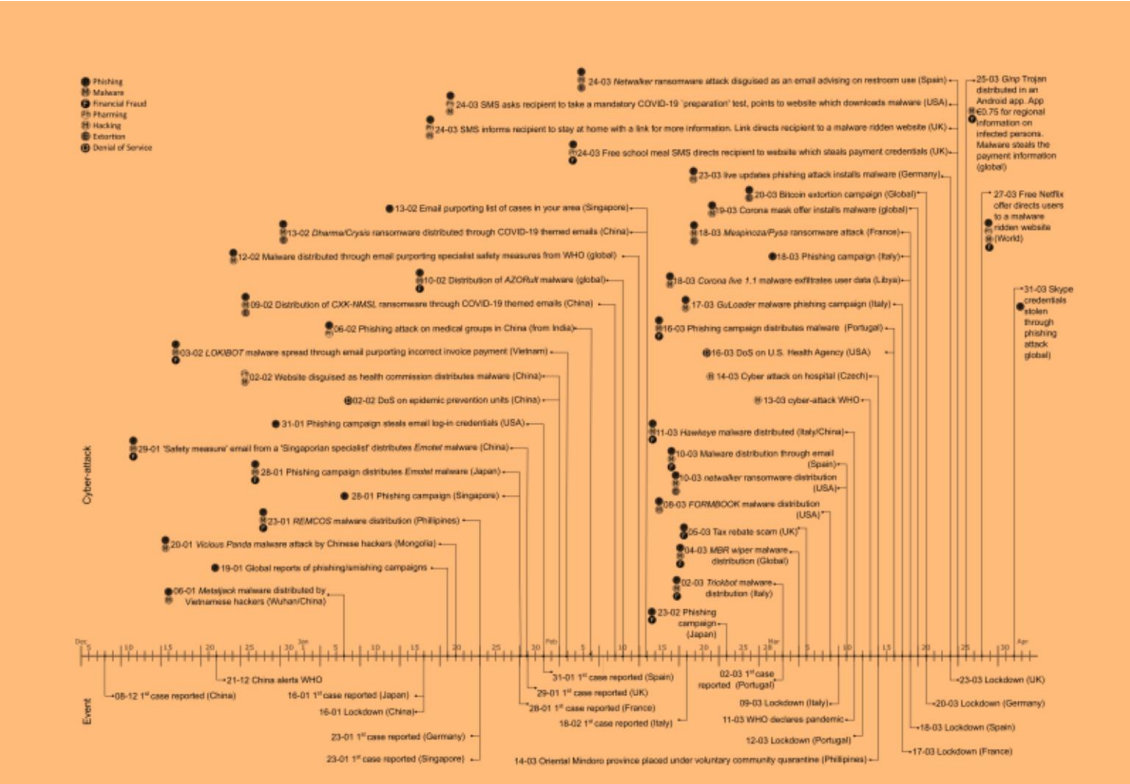

Figure 1 Timeline of Covid pandemic and cyber attacks (Lallie, et al., 2020).

A more useful list of cyber-attacks around the world has been tabulated by the authors. This is presented in Fig 2. In this table, a numbered list of cyber-attacks related to the pandemic, is provided. It contains details like the country from which reported, attack type, description of the attack and the dates of the attack and the article. In most cases, the report on the attack is published 3 to 4 months after the attack has taken place. This may be due to the time taken for the first priorities of mitigation measures, investigative procedures and preventive steps. China and USA were maximum reported countries. There were many global scale attacks also. A few instances where Covid-related event could be correlated with cyber-attacks have also been given. From the UK perspective, in the case of the first two attacks, the gap between the event and the attacks were 30 days and 14 days respectively. After this, the time gap continuously declined. From the same perspective, it was also clear that, phishing and smishing were most prevalent, followed by hacking, denial of service and hacking in that order of decreasing frequency. There were also some financial frauds and extortion. Different methods of attacks have been used for different purposes, the detailed instances of them provided by the authors. One of the most important aspect of cyber threat is the impact on workforce. The pandemic effect itself notwithstanding, the need to quarantine all staff at the workplace, facilitation of working from home and any need to upgrade security of current IT infrastructures as people to protect them may not be available in view of the timeline of attacks described above assume significance.

ID	Ref.	Country	Attack Type	Description	Article Date	Attack Date
1	[51]	China	P.M	Vietnam accused of launching a *METALJACK* phishing campaign against the Wuhan district offices	22/04	06/01
2	[74]	Global	P.M	International reports that both phishing and smishing campaigns are taking place	19/01	-
3	[75]	China, Mongolia	P.M	Chinese hackers accused of distributing the *Vicious Panda* malware to Mongolia through emails purporting to come from the Mongolian ministry of affairs	12/03	20/01
4	[76]	Phillipines	P.M.F	*REMCOS* malware distributed to Phillipino citizens	13/03	23/01
5	[77]	Singapore	P	Phishing campaign steals email log-in credentials	28/01	-
6	[78]	Japan	P.M.F	Safety measures phishing campaign distributes *Emotet* malware	28/01	28/01
7	[79]	China	P.M.F	'Safety measure' email from a 'Singaporian specialist' distributes *Emotet* malware	06/02	29/01
8	[77]	USA	P	Email purporting list of COVID-19 cases in victim's city takes user to website which steals credentials	11/02	31/01
9	[80]	China	H	DoS on epidemic prevention units	09/02	02/02
10	[80]	China	P	Phishing campaign steals email log-in credentials	09/02	02/02
11	[81]	World	P.M.F	First cases of *AZORult* a data theft malware	10/02	-
12	[82]	China	P.M	Email purporting specialist safety measures from WHO prompts malware download	12/02	-
13	[76]	Vietnam	P.M	*LOKIBOT* malware spread through email purporting incorrect invoice payment	13/03	03/02
14	[83]	China	P.Ph	Phishing attack on medical groups in China (from India)	06/02	06/02
15	[84]	China	P.M.E	Distribution of *CXK-NMSL* ransomware through COVID-19 themed emails	18/02	09/02
16	[84]	China	P.M.E	Distribution of *Dharma/Crysis* ransomware through COVID-19 themed emails	18/02	13/02
17	[76]	Italy	P.M	*Trickbot* malware distributed through email	13/03	02/03
18	[85]	Global	P.M.F	MBR wiper malware disguised as contact tracing information	04/03	-
19	[76]	USA	P.M	*FORMBOOK* malware distributed through email purporting parcel shipment advice	13/03	08/03
20	[86]	USA	M	Health systems in Champaign Urbana Public Health District (Illinois) affected by the *netwalker* ransomware	12/03	10/03
21	[76]	Spain	P.M	Email purports COVID-19 remedy as mooted by Israeli scientists days in advance	13/03	10/03
22	[87]	Czech	H	Cyber-attack on Czech hospital	14/03	14/03
23	[88]	USA	H	Denial of Service on U.S. Health Agency	16/03	-
24	[89]	Libya	P.M	Corona live 1.1 is the *SpyMax* malware which in this case is a trojanised app which exfiltrates user data	18/03	-
25	[90]	World	P.M	Corona mask offer installs what appears to be a harmless malware which distributes an SMS to all contacts. Presumably an update to the app will mobilise the malware	19/03	-
26	[91]	Global	P.E	Extortion campaign threatens to infect the recipient with COVID-19 unless a $4,000 bitcoin payment is made	17/04	20/03
27	[92]	Spain	P.M	*Netwalker* ransomware attack disguised as an email advising on restroom use	24/03	-
28	[93]	USA	P.M	SMS asks recipient to take a mandatory COVID-19 'preparation' test, points to website which downloads malware	24/03	24/03
29	[94]	UK	P.M	SMS informs recipient to stay at home with a link for more information. Link directs recipient to a malware ridden website	24/03	-
30	[95]	UK	P.Ph.F	Free school meal SMS directs recipient to website which steals payment credentials	25/03	24-03
31	[96]	World	M.F	*Ginp* Trojan distributed in an Android app. App charges €0.75 for information on infected persons in the recipients region. In actual fact, it steals the payment information	25/03	-
32	[52]	Global	P	Skype credentials stolen through a crafted phishing campaign	23/04	31/03
33	[97]	World	P.Ph.M.F	Free Netflix offer directs users to a malware ridden website	27/03	-
34	[98]	UK	M	Fake NHS website gathers user credentials	28/04	-
35	[99]	UK	P.M	Email purports to offer job retention payment as per the UK governmental announcement	30/04	19/04
36	[100]	Global	M	*Coronalocker* locks a computer and appears to cause rather more annoyance than any real damage	21/04	-
37	[101]	Global	P.M	Docusign recipients directed to fake website offering COVID-19 information	08/05	-
38	[5]	UK	P.M	Recipients are directed to a fake track and trace website which collects user credentials	13/05	-

key: P:Phishing (or smishing); Ph:Pharming; E:Extortion; M:Malware; F:Financial fraud; H:Hacking

Figure 2 Covid-19 related cyber-attacks described (Lallie, et al., 2020).

Risk conflicts created by the pandemic are difficult to solve. For example, GPs not getting access to patient records due to cyber threats conflicts with the essentiality of accessing the patient records during the pandemic to advise the patients suitably. Safe processing of patient record is another issue. Changes required in granting access to workforce to essential data required for their work may also create problems. An audit of threat sources, vulnerabilities, violation of policy or process and exposure of information assets to cyber threats need to be done regularly even when there is no pandemic, but becomes more critical during the pandemic. The requirement for rapid access to pandemic data can compromise the current legal protection of privacy of personal health data. Government interventions to reduce the spread like contact tracing, collection and processing of epidemiological data and testing results may require access to big data very often. This will conflict personal privacy versus public safety. These very acts also become fertile grounds for cyberattacks. Even the rapidly evolving R&D information on Covid-19 is vulnerable to cyber threats.

The assessment and addressing of the security and other risks the new operational environment due to the pandemic were discussed by Weil and Murugesan (2020). Pandemic events place

enormous stress on IT systems, tactical security measures and IT governance models leading to long term strategic disruption in the global digital canvass. There had been rapid development of massive work at home migration in business organisations. This has necessitated equipment and enabling IT systems for remote work and manage personnel in entirely different ways. The migration of several services and operations to online has caused many new vulnerabilities to cyber security. BYOD, unpatched routers, and open WiFi are becoming fertile targets for hackers and intruders. Many organisations have provided recommendations to address the cyber security issues arising from the pandemic situation.

Security issues to be addressed and methods of cyber protection for teleworkers were outlined by Abukari and Bankas (2020). In such an arrangement, individual teleworkers need to be self-reliant and display high degree of self-efficacy to perform well. IT devices at homes are not usually well configured compared to workplace systems. This makes home IT devices vulnerable to cyberattacks, especially during this pandemic period. Cyber criminals can take advantage of the lack of security of home IT services and use them to penetrate company data. These possibilities led The Information Technology Laboratory to issue a news bulletin in March 2020 reiterating the National Institute of Standards and Technology (NIST) standards for teleworking. The standards consist of five items from developing and enforcing a cyber security policy to securing all client-related devices. In teleworking, remote access is done to establish connections to systems or computers through a network connection. This facility is at once both a convenience for teleworking as well as a threat to cyber security to due to chances of greater exposure to cyberattacks and the threat is higher in the context of the pandemic. Teleworkers normally use virtual private networks (VPN) to connect with the organisation's computing systems. VPN security is due to its creation of a separate communication tunnel from a public internet into a private network and protecting the connection by encrypting data. But if unsecured Wi-fi is used, its security is also vulnerable. Desktop sharing is another method of data sharing and interactive communications. But there are authentication risks which may compromise the entire organisation's data systems. Another method is Privileged Access Management (PAM). Privileged account is given to the organisation resources on their servers. The organisation can, then, allot their own privilege accounts to select officers on absolute need basis. One of the main methods cyber criminals tend to use increasingly, is social engineering. This method consists of manipulating people psychologically, to perform some actions leading to revealing of confidential information. The method can be used to gather information, committing fraud or accessing the central information system. It can be targeted to ne individual or a group. Cyber criminals target those employees who may not be important for information security of the organisation, but sufficient to gain access to it. When these individuals are prompted, they may take actions ignoring information security leading the criminals to access the systems of the organisation. All these other preventive and response/mitigation methods are common for normal times also, but the increased threat of cybercrimes during the pandemic renders them especially critical for rapid deployment of defences. The authors proposed three protocols for employees training at organisational level, education protocol at individual level and policy protocol at both organisation and the government level. The diagrams of these protocols are presented in Fig 3 to 5.

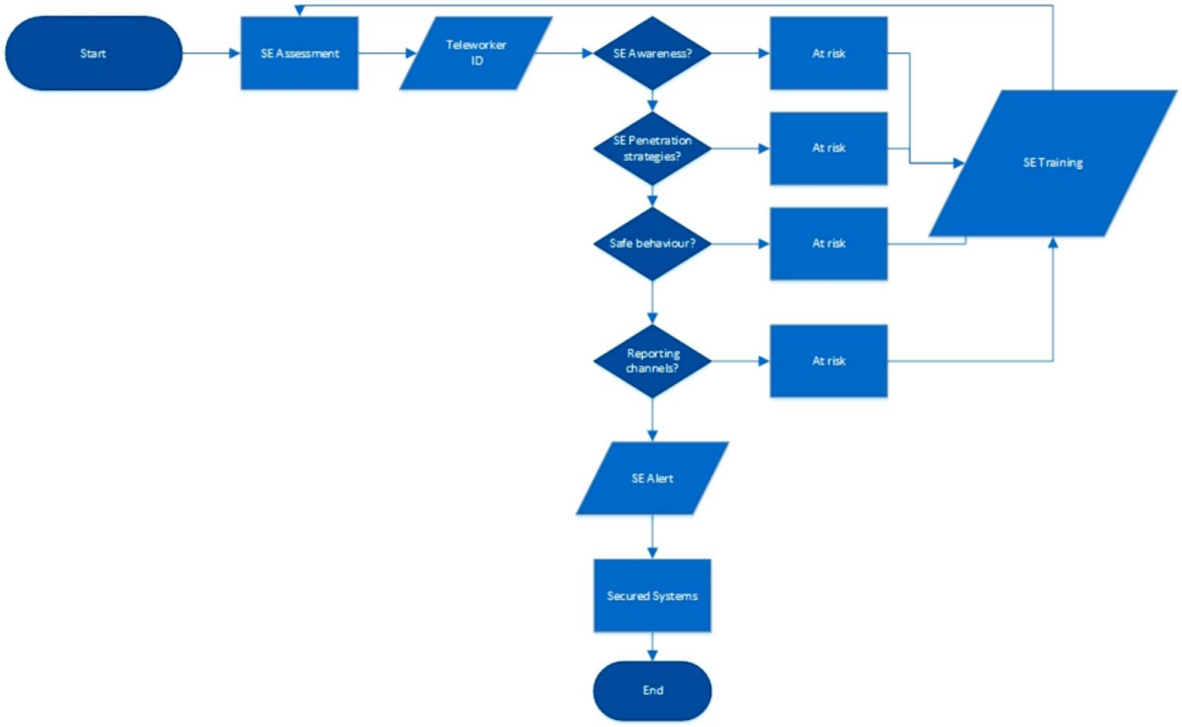

Figure 3 Training protocol for cyber security at organisation level (Abukari & Bankas, 2020).

The training protocol given in Fig 3 consists of topics on which training need to be given with stress on how the threats occur, what is the risk and how to avoid them. The risk due to lack of social engineering awareness, penetration testing and reporting channels to organisations are emphasized in this protocol.

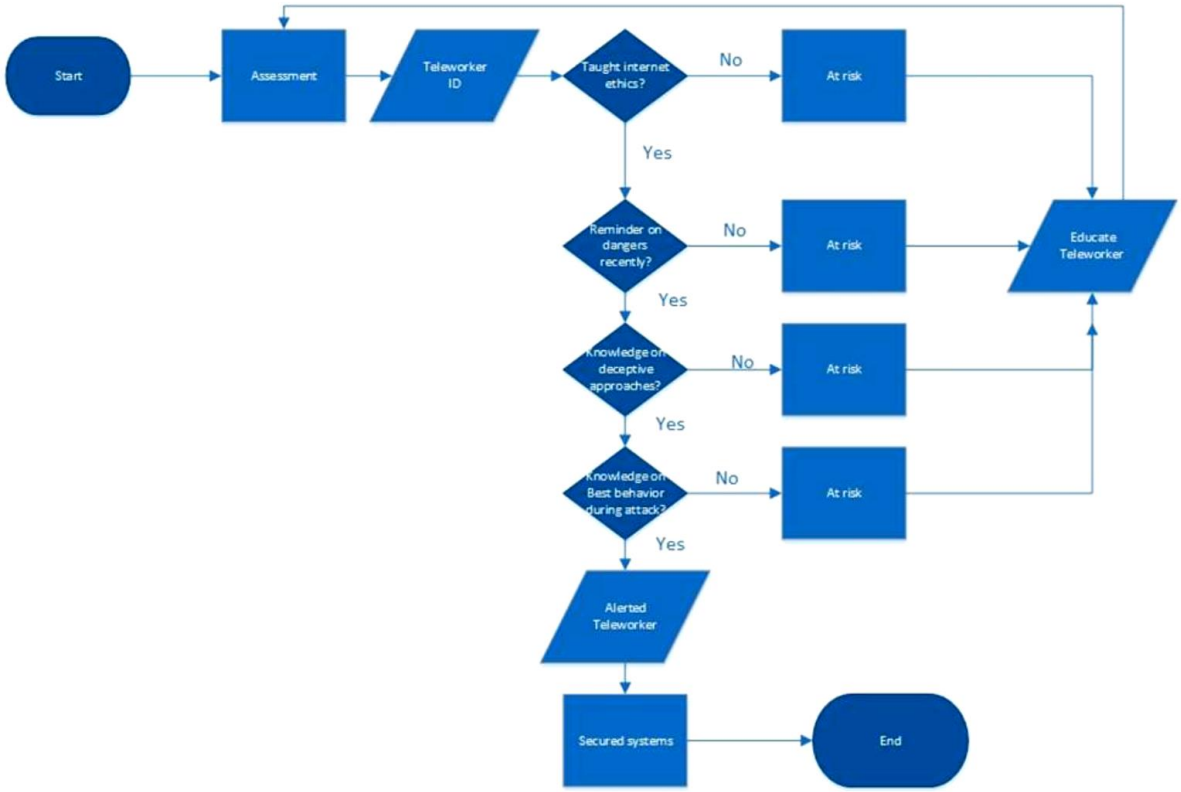

Figure 4 Individual education protocol for cyber security (Abukari & Bankas, 2020).

The education protocol for individual employees given in Fig 4 has internet ethics, knowledge on deceptive approaches, knowledge on best behaviours 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, as its vital components.

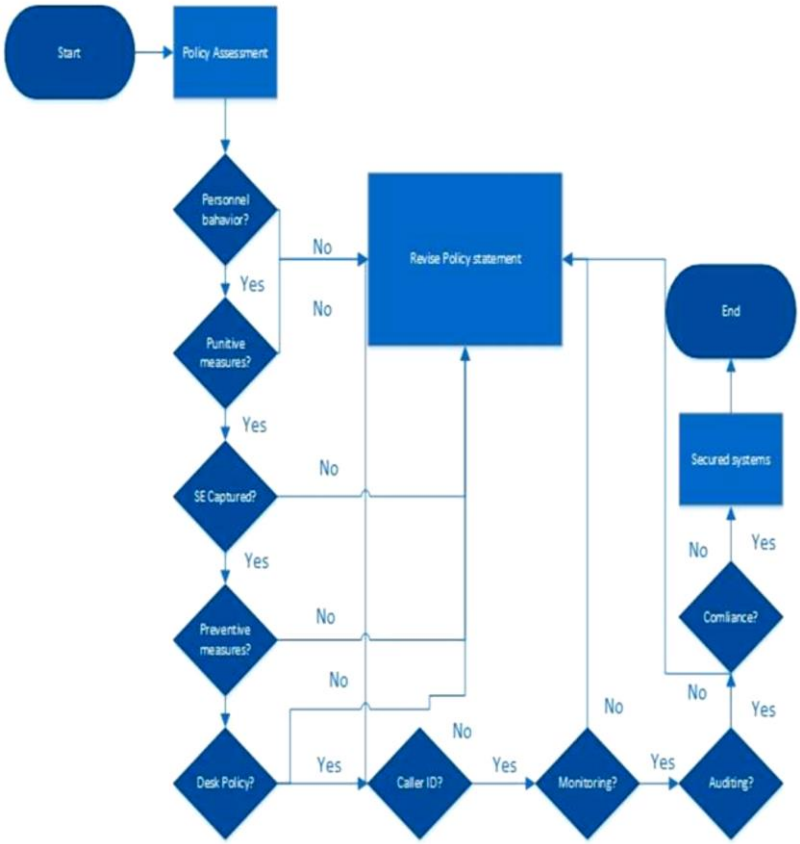

Figure 5 Policy protocol for organisations and governments to reduce the risks to cyber security (Abukari & Bankas, 2020).

In the policy protocols given in Fig 5, personnel behaviour, punitive measures, social engineering measures, preventive measures, desk policy, caller IDs, monitoring, social media, auditing and compliance are included.

In an article, Taddeo (2020) noted that ethical, legal, and social implication of digital systems have arisen as an issue of personal privacy due to the spread of the pandemic necessitated mass surveillance, contact tracing and others. Governments have put in place policies and protocols to address these issues. These measures at the same time reduce security threats, and mitigate the risks for mass surveillance by implementing decentralised protocols like Decentralized Privacy-Preserving Proximity Tracing (DP-3T).

The cyber security challenges of court proceedings during this pandemic were discussed by Baldwin, Eassey, and Brooke (2020). Most courts have opted for full virtual, limited in-person or hybrid (virtual and limited in-person) formats for their procedures. These formats are extended to representation of cases and attorney-client meetings and provision of off-site access to personnel records. When these alternative working systems are employed, it needs to be ensured all concerned can operate the technology and requisite equipment, confirm identities, obtain signatures and securely function in a new virtual environment. The problem of cyber security arises when records are to be accessed.

Employees working from home of various types and sizes of organizations seem to have only the minimal cybersecurity resources compared to the normally available ones to them. Hence, it the duty of the organisations, in their own interest, to ensure that their employees working from home are fully protected. The Absolute 2019 Global Endpoint Security Trend Report showed that 42 per cent of endpoints are unprotected at any given time. This report was before the pandemic. The situation could be much worse now even in the best of cyber security scenarios (Ahmad, 2020).

One of the cyber security problems is the dis/mis-information campaigns about Corona-19 pandemic in the social media. The EU cybersecurity policy changes in the context of the pandemic was determined, at least partly, by its pre-existing trends which were based on economic and security path dependence since the 1980s. The EU policy changes over the years leading to the current stage was traced and discussed by Carrapico and Farrand (2020). More specifically, online disinformation trends had the effect of splitting the levels of trust placed in different actors involved in providing cybersecurity. In this respect, social media platforms were perceived as not sharing the EU values regarding freedom of expression and harmful speech. This perception was aggravated by the multiplicity of conspiracy theories about the pandemic. The EU cyber security policy can be historically divided into a genesis phase of 1980-2010 and a formalisation phase since 2010. During the genesis phase, the focus was on safeguarding the EU single market and protecting its citizens. Formalisation started with the release of a policy paper Internal Security Strategy in 2010. Revisions and additions followed since then, to meet the changing needs of cyber security. Other related EU organisations were brought into the stream. The policy became full-fledged in 2013. The Cybersecurity Strategy component of it was a combination of the three former pillars of the EU to address online security issues comprehensively. It mirrored its pillar structure through steps to protect the internal market by combating cybercrime, ensure resilience for network and information systems and critical information infrastructures enveloped into a total cybersecurity framework. The concept of cyber defence was introduced as a common security and defence policy. Disinformation arose as a context for cyber defence since 2014 gradually gaining importance. Now private sector lost its prominence as a EU partner of expert status and became agents regulated by the EU. This change placed private parties like social platforms which exhibit trust deficit due to disinformation into a negative list. The EU policy trajectories in the Covid-19 scenario became a natural extension of the policies prior to the Covid-19 outbreak, the new normal reinforcing the earlier policies with stress on the vulnerability and protection aspects, especially the disinformation in social media as the focus. As a result, two discursive path-dependencies emerged. One consisted of the private sector providing cybersecurity is a trusted partner in governing cyberspace. The other consisted of social media platforms, which challenge the EU's security through its unwillingness or inability to effectively tackle disinformation, and thus need more oversight.

To address the trust deficit caused by disinformation and misinformation related to Covid-19, Khurshid (2020) proposed use of blockchain technology. The distributed trust networks and cryptography-based security of blockchain technology may solve data-related trust problems. Blockchain has a robust, secure, privacy-preserving, and immutable record framework to convert the nature of trust, value sharing, and transactions in positive ways. The author presented two diagrams of blockchain used healthcare supply chain systems of Covid-19. However, how it addresses trust deficit due to misinformation is not clear.

In their paper, Pranggono and Arabo (2020) reported a correlation between Covid-19 and the increase in cyberattacks targeting vulnerable sectors. The success rate of cyberattacks increased with growing anxiety and fear of the pandemic, as the very same weaknesses are used by cyber attackers. The prime victim of cyberattacks seems to be the healthcare sector. Security of work from home, stare-sponsored cyberattacks, phishing and ransomware are other issues. It is especially important for healthcare sector to improve their cyber security to the highest level by integrating different methods of prevention and protection.

Some security and privacy challenges involved in the use of 5G and internet of things to solve various problems related to healthcare and daily normal activities due to Covid-19 pandemic were discussed by Siriwardhana, De Alwis, Gür, Ylianttila, and Liyanage (2020). Sensitive data like video recording of telemedicine activities, automated collection of contact tracing data, 5G drones capturing additional information on bystanders, exposure to unknown parties by the use of internet of things and existence of several unconnected devices increase chances of cyberattacks when 5G and internet of things are used. Solutions for these security problems lie in built-in security systems in 5G, software-defined privacy and privacy retaining protocols. Light weight scalable security mechanisms can be used in mobile devices which use internet of things. Blockchain technology can be employed as was discussed above. A holistic security and privacy framework can be achieved by building upon and integrating these solutions into a smart and trustworthy security platform in the overall 5G ecosystem. Scalability, 5G connectivity and legal challenges still exist for which solutions can be found at the context level.

Personal data privacy and security concerns are applicable in the case of telemedicine services also as the data entry and access happen in the internet. Use of personal data on public interest and public health, without consent of the individual may be justified in pandemic situations, but it should not at the expense of compromising data security from hackers (Vidal-Alaball, et al., 2020).

Cyberattacks can be for political or financial gain, pointed out (Wirth, 2020). Cyber threats existing before were aggravated with the onset of Covid-19 pandemic. Some threats originated due to the pandemic as the attackers got an opportunity. Social engineering attacks used fake websites, malicious apps, phishing emails, and text messages taking advantage of the desire of users to be informed. They also exploited the reduced level of safety precautions when the crisis developed. Hackers promised not to upset healthcare. However, there were attacks affecting care delivery, testing and research. Even politically motivated attacks on organisations like WHO, healthcare departments of some countries and hospitals have happened. Work from home has compromised public IT infrastructure and tools, created large surfaces for attacks on hurriedly deployed several devices. IT infrastructure built urgently into new healthcare buildings, temporary structures or converted buildings was poorly equipped to handle cyber threats compared to the standards. The large scale deployment of healthcare facilities have increased vulnerabilities by the very numbers, in which human errors also contributed to security breaches. As never before, physical security and cybersecurity are converging. This leads to several devices being exposed, as they are handled by several people, hurried deployment of networks, telehealth and work-from-home infrastructures. Thus, traditional boundaries and controls are vanishing rapidly. These trends increase the opportunities for adversaries for more attacks. Both health professionals and common people are hungry for information. This provides opportunity for disinformation, misinformation and traps of fake websites. John Hopkins disease tracker has

been mimicked. The adverse experiences should be used as lessons to be learned for better management of the situation in future.

The problems faced in social cybersecurity due to hate speeches in bots were investigated by Uyheng and Carley (2020). Integrated analysis of Twitter conversations about the pandemic in USA and Philippines showed distinct relationships between bots and hate speech across datasets. These hate communications reflected the racially charged toxicity in the US and the political conflicts in the Philippines. But activity was related with higher hate in both countries and were higher among denser communities which were more isolated from others.

Increasing direct and through social media threats to health workers in USA could be attributed to misunderstanding of the pandemic, biased risk perception and a general decline in good behaviour attributes among the public. Some of these causes cannot be solved easily, but others can be worked around. People belonging to such groups resist wearing masks, closure of businesses and refuse to be vaccinated. In an information space filled with inconsistent information, there is confirmation bias, which allows some people dismiss evidence that are not in line with their pre-existing beliefs. Decision bias, omission bias, optimism bias and distance bias are some other types of biases discussed by the authors. In USA, Firefauci campaigns in social media like Twitter and Facebook, negative attitude of leading politicians (including Trump) about healthcare professionals. Elected local leaders and even judiciary directly attack and abuse local health professionals in more personal ways (Mello, Greene, & Sharfstein, 2020).

To reduce the spread of Covid-19 entire world has adopted social distancing, where working and learning from home is the new normal for this new world. To sustain the economical revenue and business growth companies that radically moves into cloud infrastructure to support employees, who work remotely. With the unprecedented growth of cloud, data breaches and cyber security takes a huge leap. Hackers penetrating not only the cloud resources it also hampers the hosts and device connected with it. Several security challenges in the cloud and generic preventive measures were outlined by Mandal and Khan (2020). Serious security breaches in cloud-based remote learning due to data breaches, unskilled usage, psychological effects of cyber security, attacks due to use of dark webs, attacks on video tutorials, phishing, email scams, attack on hosts, ransomware attacks were discussed. In the case of working from home, cyber threats arise due to improper authorisation and authentication, connecting through home network, upgradation problems, social engineering scams and phishing attacks of various types. Healthcare, Banking, E-commerce, Entertainment are affected due to e-banking and transfer of money, unskilled use of banking sites, attacks through Corona safety apps, spikes in online purchase of essential goods, dark webs and intruders. Extra preventive measures and use of strict safety protocols are recommended to enhance cyber safety in these types of attacks.

A very critical discussion on the security culture around the world and WHO in tackling the Covid-19 pandemic was done by Bjelajac and Filipović (2020) pointing out many instances of security threat in the form of misinformation of various types. WHO did not have its own verified principle to respect economic, cultural, social, and civilization attributes of many different countries hit or could be hit with the disease. So, it accepted unverified Chinese procedures, despite many questions on the scientific validity of such drastic measures prescribed by the Chinese. The spread of coronavirus posed both health and political threat to president Xi Jinping due to strong discontent on this issue. To suppress the truth, he punished Chinese whistle blowers. If the fact that bats in China had SARS-like coronavirus, it would have been much easier to isolate those viruses and develop drugs that blocked them much earlier.

Companies did not want this as they would like more profit from developing the drug after the threat becomes very serious. The number of cases reported in different sources is the number of persons who tested positive for coronavirus. But most of them had no symptoms or afflictions and therefore, are not diseased. There is confusion in reporting due to the lack of methodology or total ignorance. Media and other information sources were giving daily coronavirus statistics based on this. So, it is a type of misinformation risk. The number of deceased should be a fact and not estimation. However, in many countries, direct causes of deaths are not determined and all the deaths are attributed to coronavirus. This may be the reason for certain countries reporting high mortality rates compared to others. This is another misinformation risk. Share of Covid-19 deaths in the total number of deaths is another issue. Death statistics due to different causes, when Covid-19 is included, show that, dying is a natural process, even during an epidemic. The difference is that this year each person who died of Covid-19 is registered. The number of people who died from Covid-19 is only published and this creates panic reaction. For example, as on 6 May 2020, Covid-19 deaths-were 273795 and other deaths were 20750000 globally. There seems to be a certain kind of pressure of health authorities on citizens to justify some misgivings. Truly, it is poor work on the basics. There is a lot of confusing misinformation and false unsubstantiated claims about the origin of Coronavirus. All these are misinformation risks. It is not easy to explain why the disease hit hardest the countries where they have the highest level of health care, most Nobel prize winners in fields of medicine and pharmacy, the best hospitals, institutes, researchers and billions of dollars at their disposal and yet they were helpless. Many other countries with much less resources like these, out of sheer inability, could not do anything and they are better off than the advanced countries on healthcare. The WHO recommended strict hygiene and isolation measures. Many countries strictly followed these guidelines of draconian pressure on their citizens and economy. On the other hand, research conducted around the world showed that mass testing does not prove anything and isolation is not a good solution. For example, in New York, 66% of the new cases in isolation did not go anywhere. Despite being objected to harsh criticism for refusing to close the country and implement strict measures, Sweden came out well as it has a very strong public health policy. Sweden may be a model to reach a ‘new normal. Sweden had trust in their community in implementing social distancing measures. This statement further contradicts all the recommendations issued by the WHO earlier and adds to the confusion.

Conclusions

Many types of attacks on cyber security affecting many aspects of life during the Covid-19 pandemic have been researched and reviewed by various researchers. All these cyberattacks taking place during normal times are exacerbated during the current pandemic. The only solution appears to be greater vigilance and careful handling of internet for various purposes. Information purported to be coming from authentic sources should be double-checked for real authenticity. However, basically not showing excess anxiety or thirst for knowledge about the pandemic or recommended preventive measures is a good step against disinformation and misinformation through emails, social media and others. The findings from this work can be used as learnings for improving the quality of internet browsing.

References

Abukari, A. M., & Bankas, E. K. (2020). Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. *International Journal of Scientific &*

Engineering Research, 11(4), 1401-1407. Retrieved Jaanuary 7, 2021, from http://tutag.org/wp-content/uploads/2020/05/Some-Cyber-Security-Hygienic-Protocols-For-Teleworkers-In-Covid-19-Pandemic-Period-And-Beyond-1.pdf

Ahmad, T. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. *SSRN*, 3568830. doi:10.2139/ssrn.3568830

Baldwin, J. M., Eassey, J. M., & Brooke, E. J. (2020). Court Operations during the COVID-19 Pandemi. *American Journal of Criminal Justice, 45*(4), 743-758. doi:10.1007/s12103-020-09553-1

Bjelajac, Ž., & Filipović, A. (2020). Lack of security culture in facing the COVID-19 pandemic. *The Culture of Polis*, 383-399. Retrieved January 13, 2021, from https://www.researchgate.net/profile/Zeljko_Bjelajac/publication/342107074_LACK_OF_SECURITY_CULTURE_IN_FACING_THE_COVID-19_PANDEMIC_THE_CULTURE_OF_POLIS_vol_XVII_2020_no_42_pp_383-399/links/5ee2580d299bf1faac4b3d8f/LACK-OF-SECURITY-CULTURE-IN-FACING-THE-C

Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of Covid-19: the case of EU cybersecurity policy. *Journal of European Integration, 42*(8), 1111-1126. doi:10.1080/07036337.2020.1853122

Khurshid, A. (2020). Applying blockchain technology to address the crisis of trust during the COVID-19 pandemic. *JMIR medical informatics, 8*(9), e20477. doi:10.2196/20477

Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. *arXiv, 2006 (Vol 1)*(June), 11929. Retrieved December 31, 2020, from https://www.researchgate.net/profile/Xavier_Bellekens/publication/342377769_Cyber_Security_in_the_Age_of_COVID-19_A_Timeline_and_Analysis_of_Cyber-Crime_and_Cyber-Attacks_during_the_Pandemic/links/5ef3264d458515ceb2081841/Cyber-Security-in-the-Age-of-COVI

Mandal, S., & Khan, D. A. (2020). A Study of Security Threats in Cloud: Passive Impact of COVID-19 Pandemic. *International Conference on Smart Electronics and Communication (ICOSEC), 10-12 Sept. 2020, Trichy, India* (pp. 837-842). IEEE. doi:10.1109/ICOSEC49089.2020.9215374

Mello, M. M., Greene, J. A., & Sharfstein, J. M. (2020). Attacks on public health officials during COVID-19. *Jama, 324*(8), 741-742. doi:10.1001/jama.2020.14423

NCSC. (2020). *Advisory: COVID-19 exploited by malicious cyber actors.* National Cyber Security Centre, UK. Retrieved December 31, 2020, from https://www.ncsc.gov.uk/files/Final%20Joint%20Advisory%20COVID-19%20exploited%20by%20malicious%20cyber%20actors%20v3.pdf

Pranggono, B., & Arabo, A. (2020). COVID-19 pandemic cybersecurity issues. *Internet Technology Letters, In press*, 6 pp. doi:10.1002/itl2.247

Siriwardhana, Y., De Alwis, C., Gür, G., Ylianttila, M., & Liyanage, M. (2020). The fight against the COVID-19 pandemic with 5G technologies. *IEEE Engineering Management Review, 48*(3), 72-84. doi:10.1109/EMR.2020.3017451

Taddeo, M. (2020). The Ethical Governance of the Digital During and After the COVID-19 Pandemic. *Minds & Machines, 30*(June), 171–176. doi:10.1007/s11023-020-09528-5

Uyheng, J., & Carley, K. M. (2020). Bots and online hate during the COVID-19 pandemic: case studies in the United States and the Philippines. *Journal of Computational Social Science, 3*(2), 445-468. doi:10.1007/s42001-020-00087-4

Vidal-Alaball, J., Acosta-Roja, R., Hernández, N. P., Luque, U. S., Morrison, D., Pérez, S. N., . . . Vèrges, A. S. (2020). Telemedicine in the face of the COVID-19 pandemic. *Atencion primaria, 52*(6), 418-422. doi:10.1016/j.aprim.2020.04.003

Weil, T., & Murugesan, S. (2020). IT Risk and Resilience-Cybersecurity Response to COVID-19. *IT Professional, 22*(3), 4-10. doi:10.1109/MITP.2020.2988330

Williams, C. M., Chaturvedi, R., & Chakravarthy, K. (2020). Cybersecurity risks in a pandemic. *Journal of Medical Internet Research, 22*(9), e23692. doi:10.2196/23692

Wirth, A. (2020). Cyberinsights: COVID-19 and what it means for cybersecurity. *Biomedical instrumentation & technology, 54*(3), 216-219. doi:10.2345/0899-8205-54.3.216