IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

EXPLORING RECENT CHALLENGES IN CYBER SECURITY AND THEIR SOLUTIONS

Adiba Shaikh[1], Arshiya A. Khan[2], Syed Zebanaaz[3], Shazia Shaikh [4], Nazneen Akhter[5]
[1]Assistant Professor, [2]Assistant Professor, [3]Assistant Professor, [4]Assistant Professor, [5]Assistant Professor
[1]P.G.Department of Computer Science
[1]Maulana Azad College of Arts, Science & Commerce, A'bad. MS, India

Abstract: The running era can be termed as an era of the internet, as the use of the internet is increasing day by day. Every coin has two sides, so is the coin of the internet. One side shows the ease of communication, sharing information, marketing, and businesses, etc with the use of the internet. On the other hand, it brings a crucial concern on the security part. Cybersecurity is the field that promises to safeguard the network, data, electronic devices, servers, computers from malicious attacks. By cybersecurity, we mean staying ahead of hackers and preventing exploitation of the system. Hackers are getting smarter day by day, thereby bringing new challenges to cybersecurity experts. News about threats like ransomware, phishing, vulnerability exploits, IoT-based attacks, etc, run around us most of the time nowadays. The current study describes well-known common challenges and discloses some new challenges in cybersecurity and suggested possible solutions to overcome them.

Index Terms**: Cyber security, cyber criminals, Hackers, DDoS, Phishing, Malwares, Ransomware, Internet of Things, Artificial Intelligence, Cloud risks, countermeasures, technical skill gap, anti-security tools, anti-virus**.

I. INTRODUCTION

Cyber security ascribes to the process of providing protection to internet connected systems such as computers, servers, mobile devices, electronic systems, programs, and data from attack, damage or unauthorized access. In other words, Cyber security represent a collections of methods, technologies, and processes that help protect the confidentiality, integrity, and availability of computer systems, networks and data, against cyber-attacks or unauthorized access. Cyber security is sometimes referred to as information security. Cyber security is crucial because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices An eloquent fraction of this data can be sensitive information, whether it be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses. It is practiced by individuals, organizations and enterprises as it shelters all kinds of data including sensitive data, personally identifiable information (PII), protected health information (PHI), personal information, intellectual property, data and governmental and industry information systems from theft and damage. Without a cybersecurity program, it is almost impossible for any organization to safeguard itself against cyber attacks and threats. The need for cybersecurity is rising with the advent of new technologies such as cloud services like Amazon Web Services and many more. The current study outline some known common challenges and discloses some new challenges in cybersecurity and propounded solutions to overcome them.

II. WELL- KNOWN SECURITY CHALLENGES

The following are some well known cyber security challenges are discussed below

2.1 DDoS Attack:

DDoS Stands for Distributed Denial of Service attack. In DDoS attack, cybercriminals deluge a network with plenty of malicious traffic that is difficult to operate normally which in turn causes the site's normal traffic, commonly known as legitimate packets, to freeze. The purpose of a DDoS attack is to overload a server with access requests until it ultimately crashes that turns out to be denial of a service. Among all other attacks, the DDoS attacks are those which hinder clients, users to access all the advantages of services available to them from server side [1]. The DoS attack is an attempt by a person or a group of persons to cripple an online service which results in serious consequences, especially for companies like Amazon and eBay which rely on their online availability to do business [2]. The expansion of 5G, proliferation of IoT and smart devices, and shift of more industries moving their operations online have conferred new junctures for DDoS attacks as presented in McAFee consumer threat report. The cybercriminals are taking leverage, and 2020 saw two of the biggest DDoS offensives recorded ever that were launched on Amazon and Google.

DDOS attacks classified into two broad categories: flooding attacks and Flash Crowd attacks. Flooding DDoS attacks guzzle resources such as network bandwidth by overwhelming bottleneck link with a high volume of packets. Flash Crowd attacks use the predictable behavior of protocols such as TCP and HTTP to the attacker's advantage [2].

2.2 Phishing:

Phishing is the act of circumventing the security with an alias or the act is sending email that falsely claims to be from a legitimate organization [3]. This is usually combined with a threat or a request for information: for an example, that an account will close, a balance is due, or information is missing from an account. The email will ask the recipient to supply confidential information, such as a bank account details, Pins code or passwords; these details are then used by the owners of the website to conduct the fraud. The phishing website looks identical to the real website and the end user does not realize that they have been redirected. However, the hacking of data through the phishing can be avoiding by not clicking the unknown links from the strangers [4].

Phishing attacks have impact on organizations and individuals and confront a heavy loss which includes fines from information laws and regulation, the loss of reputation, the cost for recovery, and reduces productivity [5]. Phishing in other directions initiate the attacks such as phone calls, instant messaging, or physical letters beside emails. However, the technical method includes deceptive phishing, Phishing e-mail, spoofed website, phone phishing, social media phishing [6].

2.3 Malware:

It is software that has a malicious purpose (MALicious softWARE). Malware is uninvited from multiple sources, through different medium such as pop-ups on web pages, spam, emails, downloads from unknown sources [7]. The types of malware are spyware, Trojan horses, virus attacks, worms, adware, and logic bombs; are the most prevalent danger to systems [8].

A *computer virus* is designed to replicate and spread. The virus is spread by using victim's email account to everyone in his contacts. Due to virus replication, the network traffic turns out to be heavy causing network slowdown [9]. An electronic *Trojan horse* works similarly as the well-known story of Trojan horse used to gain access to the city of Troy. It is malicious software that is masquerading as legitimate program [10]. *Spyware* is a program which spies on the activities done on the computer system. When a website is browsed, spyware gets downloaded and create a simple text file by using the browser of the system and get stored on the hard drive. Later, any data saves flat file save can be retrieved by any websites, so the entire Internet browsing history of the computer can be tracked [11]. Another type of spyware is called as *keylogger* which records all the user's keystrokes. *Worm virus* is malicious, self-replicating software that can automatically spread and propagate through a network. *Adware* is advertising supported software.

2.4 Internal Misuse:

When insider dissipates their access privileges or steals data is termed as internal misuse. People leak secure data to public sources. Secure data may include strategy documents, customer data, and even proprietary source code. Insiders that perform attacks (insider's attacks) have a distinct advantage over external attackers because they have authentications to system access and also may be familiar with network architecture and system policies and procedures [12]. Employees have the authorization of a wide range of physical equipment inside of a company, with the only trust to prevent them from damaging or stealing it. Hardware such as hard drives that contained lots of crucial data can be destroyed or stolen physically from the company or data on a USB drive can be duplicated erased or transferred otherwise. In addition, misfortunes like floods, fires, terrorism, or power failure can destroy data stored.

III. RECENT CYBERTHREATS

3.1 Ransomware:

Ransomware is a malware family that using security techniques such as cryptography to hijacking user files and associated resources, then requests crypto currency in exchange for the locked data [13]. Some ransomware gets into the system utilizing social engineering, malicious advertisements, spamming, drive-by downloads, while others try to discover vulnerabilities to exploit it, using open ports or exploiting a backdoor to get inside [14]. The infection process begins by injecting malware into the networked computer by targeting human or technical weaknesses. Human weaknesses often emerge from opening and clicking spam messages, known as phishing emails. Whereas technical weaknesses rise from various factors such as using publicly accessible Wi-Fi networks, lack of firewall protection etc. After the infection process, cybercriminals change the file system by encrypting the whole computer files and allow a victim to see only their message and Bitcoin payment process [15]. When cybercriminals hack a computer, it is nearly impossible to decrypt the files unless having the decryption algorithm or a decryption key. For this reason, victims tend to pay cybercriminals to restore their hostage data from the criminals [16]. Ransomware is considered the fastest-rising cyber threat catching the attention. It either encrypts files or blocks access to the system or the network. If one is hit by Ransomware, the hacker demands money depending on the criticality of the data or the size of the organisation. In this case, victims at the edge of losing the data also suffer financial and productivity losses.

3.2 Cloud Risks:

Companies are moving their sensitive data from legacy data centers to the cloud, due to the flexibility & costs involved in the legacy data centre. Moving the data to the cloud needs proper configuration and security measures in place otherwise there are chances of falling into a trap. Cloud service providers are just securing their platform, securing the companies infrastructure from theft & deletion over the cloud is the company's responsibility. With cloud services, the traditional endpoint focused security operations tools do not work as the perimeter and security gradually move away from the endpoint to cloud security controls and much of the insights are lost [17]. The five most significant cloud risks are access management, data breaches & data leaks, data loss, insecure APIs, mis-configured cloud storages.

3.3 Artificial Intelligence:

Artificial intelligence is generally an associate of the humans that apply problem-solving techniques and learning for understanding activities' high levels in operation of the human-inspired elements, decision-making, and emotional cycle [18]. Artificial Intelligence runs in parallel to cyber-attack & prevention. AI has revolutionized the era by acting and defending. The fact cannot be ignored that besides defense, AI is also acting on the attacker side as well. Biometric login is one of the examples of Artificial Intelligence. AI after a lot of research and modeling can learn the anomalies in behavior patterns that can be used as a defensive tool. Unfortunately, these similar techniques can be used by attackers to execute a cyberattack.

Previous generations of cyber-attacks aimed mostly at stealing data (extraction) and braking systems (disruption). New forms of attacks on AI systems seek to gain control of the targeted system and change its behavior. To gain control, three types of attacks are particularly relevant: data poisoning, tempering of categorization models, and backdoors [19]. Each of these exploits the learning capability of AI systems to change their behavior. For instance, cybercriminals may introduce carefully designed, erroneous data among the legitimate data used to train the system in order to modify its behavior.

3.4 Internet Of Things (IoT):

Internet of things (IoT) is a collection of interconnected objects, services, people, and devices that can communicate, share data, and information to achieve common goals in different areas and applications [20]. Companies are becoming more dependent on technology, exposing them to attacks. With the rapid adoption of the Internet of things (IoT), security threats are also growing drastically. A commonly accepted architecture of IoT includes three layers namely, perception layer (PL), network layer (NL) and application layer (AL). PL using sensor, gathers information smart object in the environment. NL is responsible for transmitting & processing sensor data, establishing connection with other smart things, servers and network devices. AL delivers application-specific services to users and a notion of smart city, smart homes, smart healthcare, etc. Attackers can exploit IoT infrastructure by inducing vulnerabilities at each of these layers. IoT applications such as smart TVs, security systems, wearable health meters collect user information which may be accessed or shared by some hackers for illegal motives. Security challenges in PL are *eavesdropping, replay attack, timing attack*. Threats at NL include *DoS, RFID spoofing, sinkhole attack*. Lastly, at AL challenges are *phishing, cross site scripting, malicious vorm/ virus attack*

3.5 Technical skills gap:

Cyber attacks are advancing with the increasing number of sophisticated and successful targeted cyber attacks throughout the globe. There arises an urgent requirement for cybersecurity professionals with adequate motivation and skills to prevent, detect, respond, or even mitigate the effect of such threats. Recent research by the Department for Digital Culture, Media & Sport (DCMS) claims that around 48% of organisations in the UK are incapable of carrying out basic operations defined by the Govt Cyber Essentials Scheme like setting up the firewall, storing data etc. The report also claimed that 30% of businesses deprived the advanced cybersecurity skills like Pen Testing, forensics etc. Companies and organizations are constantly facing severe shortages in valued and highly-skilled cybersecurity professionals.

The lack of such expertise leaves them vulnerable to cyber threats, resulting in theft of sensitive information, financial loss, and reputation damage [21]. Rapid growth in technology and technical nature of cyber attacks broadens the gap between absence of appropriate security skills and faster growing for cybersecurity professionals.

IV. PROPOSED SOLUTIONS

4.1 DDoS Countermeasures:

One of the countermeasures for DDoS attack is predictive analytics. It helps IT personnel to examine the attack, predict its probability of occurrence, and source of origination. Predictive analytics software consumed by machine learning can collect significant information on known cyberattacks and can affix the results to existing security protocols. This is especially effective for active DDoS mitigation as it allows cybersecurity systems to identify threats and thereby takes proactive measures to redirect traffic before the system gets affected. Backing up critical data is another counter measure. There are some other countermeasures too.

Every single user who accesses your router should be given a username and password, make sure to have RPF on the interface of every static connection, disable Telnet on vtys, allow only SSH based connections, use vtys filters to prevent public routers from getting response from your router, use TACACS (Terminal Access Controller Access Control System) for password verification, set up security labs if not possible set aside at least one spare router and server to try a new service instead of implementing it directly on live network, minimizing the number of transit providers possibly one , team up with other local ISPs for benefits like leasing a scrubbing centre, out of band management and possibly setting up better security labs [22].

4.2 Phishing Countermeasures:

First countermeasures for phishing attack are to educate the end user to recognize phishing and avoid accessing the unauthorized links. Secondly, to prevent the attack at the vulnerability level from materializing at the user's device, and detect the attack once it is launched through the network level. Lastly, use law of enforcement as a deterrent control to overcome attacks [23].

4.3 Malwares Countermeasures:

There are many suggested countermeasures used for mitigating the impacts of the malware on systems. Some countermeasures of malware are Firewall, Security software, manually removing malware and trainings. A firewall is a protection mechanism that control and monitors the network traffic in and out. Based on security rules it allows or blocks such traffic depending on its perceived threat. There are two types of firewall i.e. hardware and software. Several software firewalls are available such as Check Point Next Generation Firewall (NGFWs), SonicWall, official G2 Survey, CiscoNext-Genertion Firewall Virtual (NGFWv), FortiGate NGFW, SophosXG Firewall, Microsoft windows firewall, Macfree, Symantec, TrenMicro, Sygare, and ZoneAlarm.

There are many Security software are available such as antiviruses, internet security software, and removal tools to protect computer systems against malware. Malware removal tools are used to scan and remove malware in computer system. A few removal tools are provided by Microsoft Company, they are Safety scanner, malicious software removal tools, Diagnostics and recovery toolset (DaRT) and Emsisoft Emergency Kit, Avast Free malware scanner and removal tools, malware bytes. The main function of antivirus software includes scanning start-up files, real-time activities (such as downloading files, monitoring application activities). Here are few list of antivirus: McAfee, Symantec, Norton, AVG, Kaspersky, and Quick-heal. Internet security software has additional features compared to antiviruses such as: anti-spyware, family and privacy protection, harmful website blocking, device and platform- independent, and securing online storage. Security awareness training should be given to staff, to know the variety of threats.

4.4 Internal Misuse Countermeasure:

Data breaches are usually the result of humans' psychological weaknesses. To avoid *Internal Misuse*, it is important to educate employees about the warning signs of security breaches, safe practices such as: being careful around opening email attachments, where they are surfing, and what actions to take towards a suspected takeover.

4.5 Ransomware countermeasures:

As stated in an online article by Kaspersky [24], countermeasures for Ransomware are: never click on unsafe links, avoid disclosing personal information on receiving an email, a call or a text message from untrusted source, do not open suspicious email attachments, never use unknown USB sticks, keep programs and OS up to date, use only known download sources, use VPN services on public Wi-Fi networks. Besides these measures, using Anti-ransomware software such as virus scanners, content filters and internet security solutions like Kaspersky Internet Solutions, Bitdefender Total Security, McAfee Anti-virus plus, etc will safeguard from cyber attacks.

4.6 Cloud Risks Countermeasures:

There are various countermeasures for cloud security like firewalls, multi-factor authentication, Virtual Private Networks (VPN), etc. Gray Stevens [25] suggests preventive measures for the five most significant cloud risks. They are: *Access Management* can be avoided by carefully designing access policies and setting authentication and identity verification tools. *Data breaches & leaks* can be managed by establishing secure communication and connections. Frequently backing up data avoids *Data loss*. Careful selection of vendors restricts *Insecure APIs*. Ensuring that the *cloud storage is configured* correctly, check configuration settings.

4.7 AI Countermeasures:

Three countermeasures for AI vulnerabilities are proposed by Mariarosaria Taddeo, et.al.

First, to ensure reliable suppliers design and develop the models In-house as data from system training and testing are collected, validated, and maintained by the system providers directly. Therefore a breach in a cloud system, for instance, may grant the attacker access to the AI model and the training data. Second, a profound method to improve AI system robustness is Adversarial training. Feedback loops enable the AI system to uplifts their performance by adjusting their own variables iteratively. Consequently, adversarial training between AI systems can help to boost their robustness and promote the identification of vulnerabilities of the system. And lastly, parallel and dynamic monitoring helps in assessing the robustness of AI systems, the deceptive nature of attacks, and the learning abilities of the targeted systems.

4.8 IoT Countermeasures:

Countermeasures for IoT proposed by Mohamed Litoussi, et. al [26] at three different layers are as follows:

- At perception layer (PL), hashed based encryption, Public Key Infrastructure (PKI protocol), light weight cryptography can be implemented.
- NL countermeasure includes identity management framework, software-defined networking (SDN) with IoT, cooperation of node communication protocols.
- Similarly, AL countermeasure are special policies and permissions , anti-virus, anti-adware and anti-spyware, risk assessment techniques

4.9 Technical skill gap Countermeasure:

In 2020 when thieves can easily clone the identities for any fraud, hackers can exploit any vulnerability; this will only increase unless there are an equal number of resources with the right skills to tackle this. Companies have to invest in training existing staff to prevent cyberattacks and also have to hire new resources to analyze threats in the network. Otherwise, companies will have to bare huge money loss.

V. CONCLUSION

Cyber security represent a collections of methods, technologies, and processes that help protect the confidentiality, integrity, and availability of computer systems, networks and data, against cyber-attacks or unauthorized access. Cyber security is sometimes referred to as information security.

Cyber threats & security attacks are not new to companies and organizations. Fortunately, in recent years they have reached a level of sophistication. Computer security is a crucial topic as the world is becoming highly interconnected, with networks being used to carry out critical transactions. Cybercrime continues to diverge down different paths with each New Year that passes and so does the security of the information. There are procedures and technology that the companies and organizations need to adopt to prevent any external and internal threats.

The study is done to create awareness regarding the challenges with its solutions to a variety of cyber threats. These kinds of attacks have an impact on the economy too. To alleviate and cope with these threats, end users must involve in educating and training to raise awareness. The complexity of attack requires studying from the past data of users and the way of attacks; reformulating an approach to minimize adverse impact.

REFERENCES

[1] Sushmita chakraborty, Praveen kumar, Dr. Bhawna sinha , “A study on DDoS attacks, danger and its prevention” ,Pg.1. International Journal of Research and Analytical Reviews (IJRAR) E-ISSN 2348-1269, P- ISSN 2349-5138, May 2019, Volume 6, Issue 2.

[2] Anup Bhange, Amber Syad, Satyendra Singh Thakur , “DDoS Attacks Impact on Network Traffic and its Detection Approach”, International Journal of Computer Applications (0975 – 8887) Volume 40– No.11, February 2012.

[3] A. Summer, “Mitigating Phishing Attacks: An overview Computer Science,” pp. 72-77, 2010

[4] Vayansky and S. Kumar, “Phishing- challenges and solutions”, Computer Fraud Security, Vol. no. 1, pp. 15-20, 2018

[5] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf and Imtiaz Khan, “Phishing Attacks: A recent Comprehensive Study and a new Anatomy,” Frontiers in Computer Science, vol. 3 March 2021,Article 563060

[6] Abdullah Fajar and Setiadi Yazid, “The intial socio-technical solution for phishing attack”, Journal of Physics: Conference Series, IOP Publishing, 2020, 1502 012034

[7] Emma Megan, IEEE Computer Society, https://www.computer.org/publications/tech-news/trends/cybersecurity-threats-and-solutions - viewed on 27/06/2021

[8] Chuck Easttom, “Computer Security-Fundamentals”, Third Edition, Pearson Education, Inc., 2016, ISBN-13: 978-0-7897-5746-3

[9] E. Filiol, “Viruses and Malware”, Handbook of information and communication Security, 2010

[10] A. Bettany and M. Halsey, Windows Virus and Malware Troubleshooting, Berkeley, CA:Apress, 2017

[11] Mariwan Ahmed Hama Saeed, “Malware in Computer Systems: Problems and Solutions”, International Journal on Informatics for Development, Vol. 9, No.1, 2020, Pp.1-8, e-ISSN: 2549-7448

[12] Shilpa Pareek, Ashutosh Gautam, Ratul Dey, “Different Type Network Security Threats and Solutions, A Review”, International Journal of Computer Science (IIJCS) ISSN 2321-5992, Volume 5, Issue 4, April 2017

[13] Al-rimy B, Maarof M, Shaid S, “ Ransomware threat success factors, taxonomy, and countermeasures: A survey and research directions”, Computers and Security, 2018 ; 74:144-166.

[14] Popli N, Girdhar A. Verma, Nishchal K, Ghosh A. K, “ Behavioural Analysis of Recent Ransomware and Prediction of Future Attacks by Polymorphic and Metamorphic Ransomware”.. (eds) Computational Intelligence: Theories, Applications, and Future Directions - Volume II ICCI-2017. Springer, Singapore. 2018;799(4):65–80.

[15] Murat Ozer, Said Varlioglu, Bilal Gonen, Mehmet F. Bastug, “ A Prevention and a Traction System for Ransomware Attacks”. 6th Annual Conference on Computational Science & Computational Intelligence (CSCI’19); Dec 05-07, 2019.

[16] I DUNCAN, “’ Discombobulated and upset ’: Baltimore ransomware attack complicates matters for debt payers,” Baltimore, may 2019 [Online]. Available: https://www.baltimoresun.com/politics/ bs-md-20190508-story.html

[17] Bharadwaj D. R., Bhattacharya A., Chakkaravarthy M., “ Cloud Threat Defense – A Threat Protection and Security Compliance Solution”. IEEE International Conference on Cloud Computing in Emerging Markets (CCEM) 2018.

[18] Vishal D. K. Soni, “Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA”. ARTIFICIAL INTELLIGENCE IN CYBERSECURITY OF THE USA [Online], available at: https://ssrn.com/abstract=3624487

[19] Mariarosaria Taddeo, Tom McCutcheon and Luciano Floridi, “Trusting artificial intelligence in cybersecurity is a double-edged sword”, Nature Machine Intellegence, 42256-019-0109-1.

[20] Tasneem Yousuf, Rwan Mahmoud, Fadi Aloul, Imran Zualkernan, “Internet of Things (IoT) Security: Current Status, Challenges and Countermeasures”. International Journal for Information Security Research (IJISR), Volume 5, Issue 4, December 2015

[21] Mouheb, D., Abbas, S., & Merabti, M., “Cybersecurity Curriculum Design: A Survey”. Lecture Notes in Computer Science, 93–107, 2019.

[22] Sushmita chakraborty, Praveen kumar, Dr. Bhawna sinha , “A study on DDoS attacks, danger and its prevention” , pp 2. International Journal of Research and Analytical Reviews (IJRAR) E-ISSN 2348-1269, P- ISSN 2349-5138, May 2019, Volume 6, Issue 2.

[23] B.B. G. Nalin and A. G. A. Kostas, “Defending against phishing attacks: Taxonomy of methods, current issue and future directions”, Telecommunication System, vol. 67, no.2, pp. 247-267, 2018

[24] AN ARTICLE BY KASPERKEY ON RANSOMWARE PROTECTION: HOW TO KEEP YOUR DATA SAFE IN 2021[ONLINE]. AVAILABLE AT: HTTPS://WWW.KASPERSKY.CO.IN/RESOURCE-CENTER/THREATS/HOW-TO-PREVENT-RANSOMWARE

[25] GARY STEVENS, “CLOUD SECURITY: 5 SERIOUS EMERGING CLOUD COMPUTING THREATS TO AVOID”, MAY 26, 2020 [ONLINE]. AVAILABLE AT: HTTPS://WWW.THESSLSTORE.COM/BLOG/CLOUD-SECURITY-5-SERIOUS-EMERGING-CLOUD-COMPUTING-THREATS-TO-AVOID/

[26] Mohamed Litoussi_, Nabil Kannouf, Khalid El Makkaoui, Abdellah Ezzati, Mohamed Fartitchou, “IoT security: challenges and countermeasures”. 7th International Symposium on Emerging Information, Communication and Networks (EICN 2020), November 2-5, 2020, Madeira, Portugal.

[27] Abuagoub, Ali M A, “International Journal of Communication Networks and Information Security”. Kohat Vol. 11, Iss. 3, (Dec 2019): 342-351.

[28] Malatji, M., Von Solms, S., & Marnewick, A., “ Socio-technical systems cybersecurity framework”. Information and Computer Security 2019. doi:10.1108/ics-03-2018-0031