DOI: http://dx.doi.org/10.26483/ijarcs.v13i2.6815

Volume 13, No. 2, March-April 2022

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

ANALYSIS OFMODERN CYBERSECURITY THREAT TECHNIQUES ANDAVAILABLE MITIGATING METHODS

Wumi AJAYI
Software Engineering Department
Babcock University, Ilisanremo
Ogun State Nigeria,

Obi Ibeto, Taiwo Olomola and Mathias Madewa
Computer Science and Information Science Department
Lead city University, Ibadan
Oyo State Nigeria

***Abstract*:** Modern means of communication have improved the way of life of humans around the world. Never has there been a time of unprecedented innovation in the way we humans communicate and share information with one another. Modern Technology has made it conceivable to keep in contact with our family, companions, and colleagues. Modern applications like Zoom, Google Hangout and Microsoft Teams have seen a geometric increase in new users and this growth has reflected the company's share price. However, the use of modern technology has brought with it issues and concerns in terms of cyberthreats. This study helps to identify modern cybersecurity threats and how to effectively mitigate against them.

The methodology used for this study was based on literature search and analysis, we also used model adaptation from generic ones.

Our finding show that Organizations now need to grapple with these unprecedented threats and find effective solutions to protect their data, applications, and people from the risk of cyber-attacks and at the same time ensure they adhere strictly to regulatory requirements. This paper sheds light on the modern cyber security threat and identifies methods of mitigating against these threats. This paper can also be used as a Cyber security survival guide to investigate information and protect against cybersecurity threats in an organization.

In conclusion, the aim of this paper review is to explore the more recent Cybersecurity threats and recommend effective method that can be adopted at an organizational level to guards against these persistent threats.

Keywords: Cybersecurity, Threats, Cyber Attacks, Risk Management, Privacy, Corporate Organizations

I. INTRODUCTION

Cyber security has witnessed increased attention quite recently with the widespread adoption of Information and Communication Technology. Particularly now when most economies are gradually getting out of the recent COVID-19 pandemic and allowing fully vaccinated travelers entry into their respective countries. Significant pressure is being puton organizations and policy makers are gradually coming to terms with the current landscape of information related security threats [2]. From the United States to Japan, Canada to South Africa, China to the United Kingdom, the extreme losses due to cyber security anomalies are well documented. For example, organizations in the United Kingdomlost around $35bn due to cybercrimes in 2016[19]. Cyber-crimesidentified to be the most prevalent are phishing, hacking and viruses [2].

Almost weekly in public media cyber security attacks appear ranging from personal information being compromised from credit card companies, financial institutions and ecommerce businesses to political information being accessed illegally from political parties by individuals, organizations, and strangely foreign governments.[3] Organizations around the world will have to deal with the increasing risk of cyber threats. They must be observant of the challenges created by the need to strike a balance between delicate data and protection issues of individuals who may have been infected by them[17].

Efficient cyber security is quite difficult. Many companies based on proven track record have designed best-practice types of content as well as standards for deploying and evaluating cyber-security [4]. The National Institute of Standards and Technology (NIST) has developed many security publications including over one hundred active Special Publications (SP) and nine Federal Information Processing Standards (FIPS). While bigger organizations have the resources to resolve cybersecurity issues, small-size businesses often do not have such resources [3],

These small companies constitute over 90% of businesses in most countries and account for over 50% of employment but they don't have the resources to make the necessary investments to guard themselves against Cyber security threats hence become vulnerable to all sorts of cyber-attacks from malicious actors.

Just recently the US Department of Defense (DOD) announced a sweeping change to its Cybersecurity Maturity Model Certification (CMMC) program mandating over 350,000 contractors to comply with the new CMMC 2.0 which ushers in additional compliance checks and self - assessment for all contractors providing services to them [22].

This research paper analyzes modern Cybersecurity threats at an operational level and explores methods of mitigating against these threats. The paper is outlined as follows, the next section explains the methodology used in this paper andobjectives therein, the fourth section carefully explains the literature review, and the last section explores the solutions that can be implemented to mitigate these threats.

The immense benefits of Information systems to businesses of all sizes are well archived [22]. We cannot quantify the benefits we all experience from the adoption of Information and Communication Technology. Every technology company seems to be selling "Digital Transformation" like a salesman would go about selling a Laptop Computer, some even go as far as making claims that every company will

eventually be software company [23]. All this marketing tactics have made numerous businesses around the world behave in a herd like manner doing everything within their means to adopt Digital Transformation but on the flip side it has exposed their businesses to digital risk that are dynamic and complex [6]. When an organization decides to automate its processes and transform its practice to unlock efficiency and value for its customers, they are exposed to threats that are unique [6]. Heavy dependency on third party companies have giving cyber criminals access to cause both reputational and monetary damage thereby exposing organisations to all types of digital risk [6]. A typical example is the SolarWinds attack that spread to its clients 'system and went unnoticed for months, Cyber criminals hacked SolarWinds's systems and injected dangerous code into the company's software servers. The server's named "Orion" is widely used by organizations to oversee ICT assets. SolarWinds as at the time of the attack had 33,000 customers that utilize Orion [24]. With the widespread Introduction of more efficient networks through 5G, Artificial Intelligence based applications, Machine Learning based applications, Internet of Things (IoT) devices, you will not need a scientist to tell you the threat landscape is widening, newer attack vectors are emerging that can cause far reaching damage and systemic failure [25]

According to Microsoft, 20% of small organizations in the United States have been hacked in the past while semantics is of the notion that 43% of the Cyber-attacks during 2015 were targeted at small business [3]. Also, according to a cybersecurity report by the administration of the United Kingdom, 43% of organizations and two of every ten foundations (19%) have encountered a network safety breakor hack in the preceding twelve months [7].

This paper seeks to identify these threats and recommend methods of mitigating against them. In tandem, this paper investigates the accompanying inquiries.

II. PROBLEM STATEMENT

The central problem to be researched by the proposed study is the analysis of cybersecurity threats techniques and the available mitigation methods. Two principal questions we seek to answer are:

1) What are the modern Cybersecurity threats and their respective manner of operations?
2) How an organization can guard its data, applications, and people in an operational manner against these threats.

III. OBJECTIVES

The objectives of this paper are:

a) To discover and analyze modern cybersecurity threats

b) To discover most effective methods of mitigating these identified threats from an operational perspective.

V. METHODOLOGY

The methodology used for this study are literature search and analysis and model adaptation (from generic ones).

VI. LITERATURE REVIEW

Digital Transformation and advancement in technology has caused serious challenges with cybersecurity. Hackers, attackers, and cyber-criminals take advantage of these trends and look for loopholes and vulnerabilities in an organizations Information Technology system. A study carried out by Trend micro research [18] during the Covid-19 pandemic concludes there was a sum of more than 910k Spam messages, 737 Malware assaults and 48,000clicks on suspicious links around the globe until the beginning of April 2020. Also, from February 2020 to March 2020 there have been an increase in spam emails by 220% and a 260% increase in malicious URLs. The United States being the leadingtargeted location for detecting spam and malware.[18]. Figure 1 below describes the top 10 cybersecurity threats during COVID-19 pandemic.

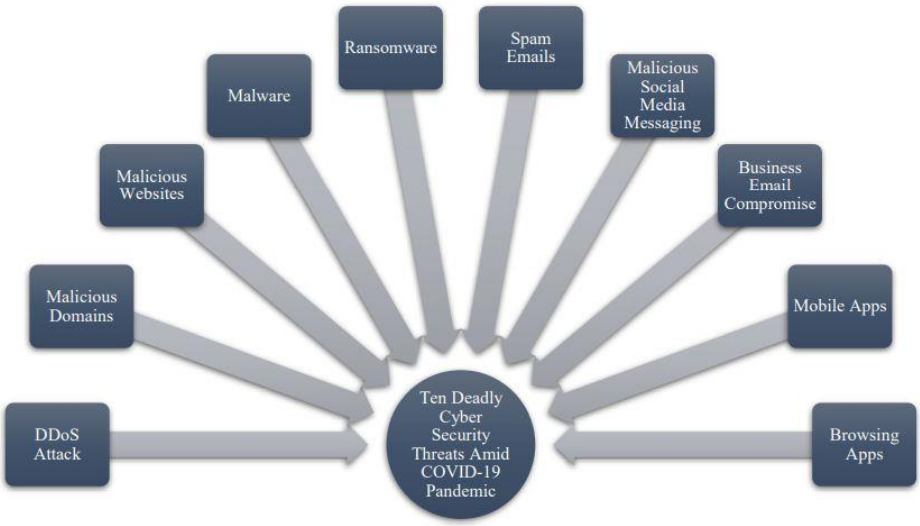

Figure 1: Top 10 Cyber Security Threats Amid COVID-19 Pandemic
Source: [1]Modern Cybersecurity Threats

Initial Compromise (Left of Boom)	Post-Compromise (Right of Boom)
Social Engineering*	Denial of Service (DoS)
Credential or Key Reuse/ Stuffing/Brute Forcing	Theft of Employee or Customer Personally Identifiable Information (PII)
Misusing Open Ports/ Network Shares (Manual or Automated — Worms)	Theft of Proprietary Communications or Information
Web Application Vulnerabilities (Including Web Shells)	Access and Theft of Data from Connected Third Parties
Hardware Vulnerabilities	Blackmail/Extortion
Software Vulnerabilities	Destruction of Data or Systems Availability
Protocol Hijacking (BGP/DNS)	Removal of Confidence in Data Integrity
Physical Tampering	Financial Fraud

Figure 2: Initial Compromise Vs Post-Compromise Source [14]

Threat Types

Phishing: According to the United States Secret Service 91% of all cyber-attacks begin with Phishing [25] and what are phishing attackers trying to accomplish:

1) Pilfer Personally Identifiable Information (PII)
2) Steal Financial Information, account information, payment processes
3) Owed Invoices or outstanding debts
4) Study Company Structure Information, defense posture.
5) Deployment of Malware (keylogger, Remote access trojans (RATs)
6) Install Ransomware

Who is at risk of a Phishing attack? Basically, everybody with an email address is at risk of a phishing attack. Clicking on a link in a phishing email has the tendency to not only compromise your systems but also compromise your corporate network.

According to [19] phishing seems to be the most popular method of attack and Microsoft products topped the list for the most vulnerabilities.

Red Flag to look out for to identify phishing

1) Urgency of request
2) Out of contact and/or lack of contact
3) Language and grammar
4) Multiple instruction emails
5) Links or attachments
6) No prior web presence of footprint
7) Use of chat apps: WhatsApp, Telegram
8) Use of non-traditional payment: money orders, gift cards
9) Use of Irreversible/hard to track payments: wires, virtual currency

Social Engineering Attack: Enterprise organizations that have the resources to deploy state of the art technology to guard against Cybersecurity threat may eventually be at more risk from intruders and attackers who utilize social engineering strategy, techniques, and tactics to achieve their objectives [15] but what exactly is social engineering; [4] clearly defines social engineering as a term designated for attackers who try to defraud people into disclosing sensitive data or perform certain activity, such as downloading and executing files or programs that appear to be benign but are actually dangerous.

DDOS Attack: This can be explained to be a denial-of-service technique (DoS) that uses numerous hosts to perform that attack. Sometimes a dedicated denial of service (DDoS) attack is used to redirect consideration from another, more genuine, assault endeavor [4]

A DoS assault in which numerous frameworks are utilized to flood servers with traffic to overpower avaliable assets (bandwidth, memory, handling power, etc.), making them inaccessible to answer authentic clients [4].

Malware*:* Cybercriminals are exploiting what is happening by spreading Malware, Spyware and Trojans through inserted sites [10] however what precisely is it, Malicious programming (malware) is maybe the main security danger to associations. Public Institute of Standards and Technology (NIST) SP 800-83, Guide to Malware Incident Prevention and Handling for Desktop and Laptops, characterizes malware as follows: A program that is clandestinely embedded into one more program with the expectation to obliterate information, run damaging of meddling projects, or in any case compromise the privacy, respectability or accessibility of the casualty's information, utilization of working framework

Virus: These are vindictive projects that taints PCs and different documents by duplicating itself. It has no ability to work all alone, so it joins with different documents all the more exactly executable records and applications and

because of its increasing capacities, it spreads across documents and even PCs through networks. It brings about PC framework corruption and forswearing of administration (DoS)[11]

Worms: A type of malicious program or piece of code that exists on its own, they propagate through storage devices and emails, also consume network and computer resources which translates to system degradation in performance. Antivirus applications are very effective in identifying this piece of code due to their multiple existence nature [11].

Trojan Horse: Mimics itself as a useful application but its disguise is one of its major characteristics, it is a very destructive program that does not replicate but steals sensitive critical information and had the capability to alter or corrupt file on the computer system or server where it resides.[11].

Rootkit: [4] defines rootkit as "a set of tools used after an attacker has broken into a computer system and gained root-level access".

Ransomware: A classification of malware that endeavors to extricate recover installment as a trade-off for unblocking admittance to an asset that has a place with the person in question or in return for a vow not to unveil the data caught by the ransomware [4].

Spam: Sending unsolicited bulk messages indiscriminately through the abuse of electronic messaging systems [4].

Logic Bomb: Logic bombs usually remains ineffective or idle until a predefined condition is met; the program them initiates an unauthorized action or activity. It is a malicious program inserted into an application by a hacker or an intruded [4].

Backdoor (trapdoor): It can be defined as any mechanism that bypasses a normal security check; it may allow unauthorized access to functionality. [4]

Mobile Code: Software that shipped unchanged to a heterogenous collection of platforms and execute with identical semantics. Examples of Software include scripts, macros, or other portable instruction.

Exploit: Software code specific to a single vulnerability or set of vulnerabilities.

Exploit Kit: Functions to install a malware. Works as a packaged software made avaliable to use by others that uses an arsenal of techniques to infect a system.

Downloader: Usually sent in an electronic email. Downloader is a software program that installs other software on a computer that is under an attach. [4].

Dropper: Often disguised and hidden in a computer's directories, so they appear as valid programs of file types.

Auto-rooter: Used to break into new machines remotely. A tool used by malicious hacker.

Kit (virus generator): Utilized as a bunch of instruments for producing new infections naturally.

Spammer program: A smart intelligent program used to send large volumes of unwanted electronic mails.

Mitigation Methods

We cannot over emphasize the importance of a strategic plan when it comes to mitigating against malicious threats or actors. The first step to guarding against most cybersecurity threats is to carefully draft an Organizational security policy. [15] defines security policies as clear instructions that provide the blueprint for employee behavior in respect to protecting information, they are also basic building blocks in creating effective controls to guard against potential security threats and this can only be implemented by empowering employees with trainings using well-articulated policies and procedures.

Security is about providing answers to a single question: How do you give people access to the correct systems for the correct amount of time, while keeping the wrong people out? [14]. To drastically reduce the potential risk of remote unauthorized access for organizations some key steps need to be taken:

1. Identity and access management
2. Vulnerability management (technology exposure)
3. Third- and fourth-party risk
4. Email Security
5. Web Security

To guard against these threats particularly phishing and web-based attacks a rock-solid strategy will include:

a) Continuous Infrastructure awareness
b) Server Hardening
c) Aggressive threat hunting

Improvements have been made with respect to multi-factor authentication, but passwords are still widely used for authentication. Improvements in Biometric validation – authentication based on retina scan, fingerprint, etc. will go a long way in hardening the process [14].

[12] buttresses the importance of Threat Intelligence and how an organization can actively source this intelligence from open, deep, and dark web to further understand the level of exploitation of vulnerabilities and audit the related risk. Threat Intelligence propels businesses to identify adversary tactics, techniques and methods and ascertain whether these new methods will render existing security controls insufficient [14]. [12] also adds an interesting perspective every organization should undertake and that is overall IT asset management inventory to help understand which one of the assets is exposed or which asset being attacked would be a big impact for the company.

Another valuable mitigation method is to start by hardening basic security controls [14]. Addressing irregularities in password complexity and storage requirements will further strengthen the overall security posture of an organization.

Vulnerability intelligence solutions offers organizations the ability to identify specific vulnerabilities that represent actual risk and visibility into the possibility of an exploitation [12]. A contextual analysis on the powerful utilization of danger insight is giving danger expert preemptive guidance of forthcoming assaults connected with danger vectors. Observing sources like underground

networks, glue locales, discussions can give important knowledge to an association. Then the examiner can work with other security groups to prevent the arranged went after by remediating pertinent weaknesses, expanding checking of focusing on frameworks and fixing security control. [12]. According to [12] Risk Modelling offers a way to critically assess current risks and to estimate clear and financial returns in cybersecurity. Organizations will have to consider the overall security of vendors, partners and other third-party when trying to assess the risk profile of their organization.

FAIR Risk Model

Using the FAIR Risk Model an organization can create a quantitative risk assessment model that contains specific probabilities for loss from specific kinds of threats. The diagram below shows a graphical representation of the FAIR Risk Model.

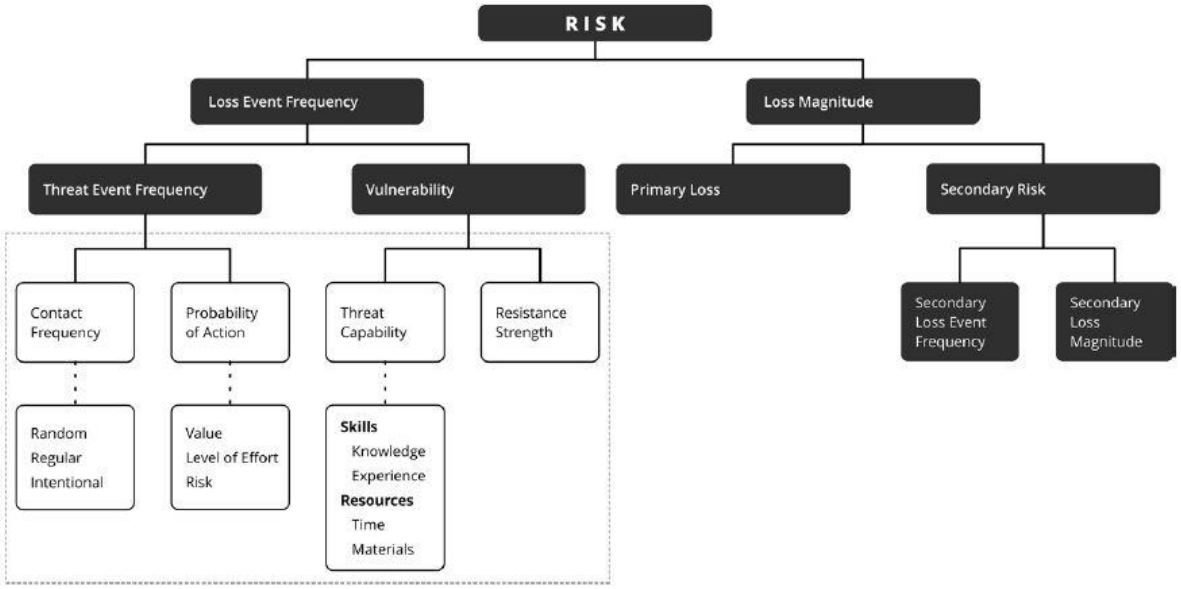

Figure 3: THE FAIR Framework, with elements informed by intelligence highlighted. Source [12]

This quantitative model for information security and functional gamble is fixated on understanding, examining, and measuring data risk in truly monetary terms. The FAIR model enables an association to make risk models that [12]:

a) Show specific loss probabilities in financial terms
b) Are more transparent about assumptions, variables, and outcomes.
c) Make defined measurement of risk.

SMB Protection Starter Pack

But how can an organization protect themselves, what are the basic steps they can take without investing heavily on threat intelligence, vulnerability intelligence and risk modelling? [13] states that each employee should be properly educated to follow basic practices such as:

a) Be cautious about email connection and web joins.
b) Separate Business and PC, cell phones, and record.
c) Pay exceptionally close thoughtfulness regarding individuals you work with and around.
d) Do not interface individual or untrusted stockpiling gadgets or equipment into your PC, Cell phone, or organization.
e) Be cautious downloading programming.
f) Do not give our own or business data.
g) Watch for hurtful pop-ups
h) Use solid secret password; and
i) Conduct online business more safely

Numerous technology solutions exist that can help reduce risk, but Cybersecurity protection is really about humans [14]. Employees represents the greatest assets for any organization and the greatest threat to it. Hiring Talented Security Professionals cannot be overstated but as an organization there are certain principles that must be enshrined in professionals that handle Cybersecurity prevention and remediation. [14] identified them as the three P's (positivity, patience, perseverance) and the three E's (execution, empathy, emotional intelligence) and three C's (curiosity, creativity, and communication).

The United States Small Business Administration (SBA) from time to time publishes a detailed list of top ten techniques for small businesses to protect their information. These includes [20]:

a) Protect against malevolent code, spyware, and infections.
b) Secure networks by embracing firewall as well as encryption
c) Develop a nitty gritty arrangement of safety practices and approaches
d) Provide Education and Training to workers
e) Require all clients to have exceptionally solid passwords
f) Employ best practices for installment cards
g) Have a reinforcement strategy set up that is embraced and stringently stuck to
h) Control actual admittance to data assets

Avoiding Phishing Attacks

Protect all web pages How can you avoid phishing attacks? According to [12]

1) Awareness is key
   (a) Do not click links or attachments,
   (b) Watch for red flags
2) Use a good spam filter, but recognize it will not catch everything
3) Use authentication checking
   (a) Sender Policy Framework (SPF),
   (b) DomainKeys Identified Mail (DKIM),
   (c) Domain-based message authentication, reporting & Conformance (DMARC)
4) Avoid sending personal information.
5) Verify suspicious requests.
6) Use strong passwords, do not reuse passwords.

Dealing with the Command-and-Control Phase

Countermeasures at the command-and-control stage include the following:

a) **Network-based intrusion detection systems (NIDS):**A NIDS can identify and alarm on endeavors to utilize an unapproved or dubious channel.

b) **Firewall:**A firewall blocks correspondence with known or suspected threatening sources and blocks dubious movement or parcel content

c) **Tarpit:**This is an assistance on a PC framework (normally a server) that postpones approaching associations as far as might be feasible. Tarpits were created as a guard against PC worms, in view of the possibility that organization misuses, for example, spamming or expansive checking are less viable assuming they take excessively lengthy. A tarpit is utilized for approaching traffic that isn't on a supported source whitelist.

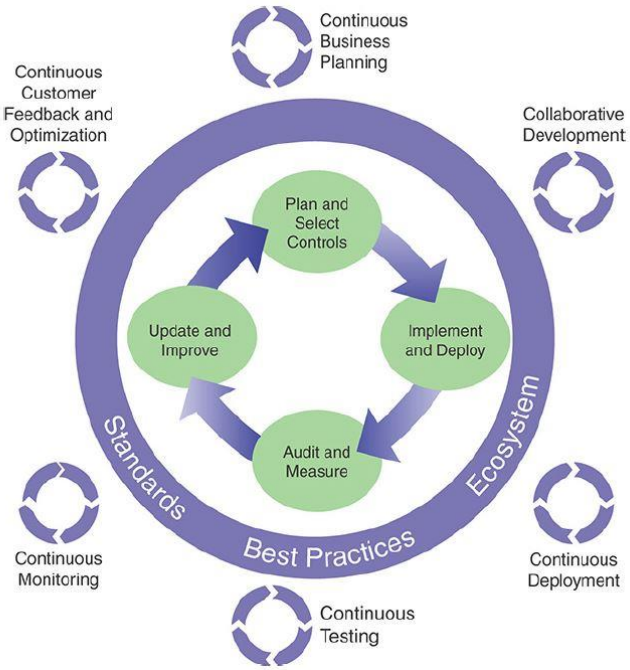

Figure 4: Cybersecurity Management ProcessSource:[6]

VII. RECOMMENDATIONS

Cybersecurity threats are evolving every day, malicious actors are on the prowl seeking for intelligent ways to penetrate an organization's most valuable assets, its data, people, and technology assets. Prevention and detection against cybersecurity threats is a dynamics continuous process that requires constant education and assessments. Organizations must adhere to strict requirements and priorities through a risk-centric model. Cybersecurity Goals must be outlined in the overall security policy and communicated throughout the organization. The goals identified must be specific, measurable, and manageable so results can be easily visible and security engineers and architects should not be hesitant to make changes as needed. It can be very fatal in an industry where threat actor's methods, techniques and procedures are constantly evolving. Risk cannot be eliminated but if the steps in this study are followed judiciously, they can be measured and guarantee valuable benefits to any organization that adopts such practices.

VIII. REFERENCES

[1] Khan, Navid Ali; Brohi, Sarfraz Nawaz; Zaman, Noor (2020): "Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic". TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.12278792.v1. pp 3.

[2] Arun P.C Sukumar, Zimu Xu, Krishna Satyanarayana, Richard Tomlins (2019) "An exploration of cyber-security risk management in small businesses: The case UK Micro and Small firms" ISBE 2019 Conference Proceedings, Institute *for Small Business and Entrepreneurship*, ISBN 978 -1-900862-32-5. pp 1.

[3] Berry, C.T. and Berry, R.L. (2018) 'An initial assessment of small business risk management approaches for cyber security threats', *International Journal of Business Continuity and Risk Management*,Vol. 8, No. 1, pp.1–10.

[4] William Stalling (2019), "Effective Cybersecurity: A Guide to Using Best Practices and Standards". *Pearson Education Inc. Library of Congress Control Number: 2018941168*. pp 39-666.

[5] Pekkola, S. and Päivärinta, T., (2018), Introduction to the Minitrack on Information Systems Success and Benefits Realization. *Proceedings of the 50th Hawaii International Conference on System Sciences*. pp 1.

[6] Eling, M. and Schnell, W., (2016). What do we know about cyber risk and cyber risk insurance? The Journal of Risk Finance, 17(5), pp.474-491

[7] Finnerty, K., Motha, H., Shah, J., White, Y., Button, M. and Wang, V., (2018), Cyber Security Breaches Survey 2018, Department for Digital, Culture, Media and Sports, Cyber Security Breaches Survey 2018: Statistical Release, pp 1.

[8] J. W. Han, O. J. Hoe, J. S. Wing, and S. N. Brohi, "A conceptual security approach with awareness strategy and implementation policy to eliminate ransomware," in Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence, 2017, pp. 222–226

[9]RabiaTahir, (2018)*A study of Malware and Malware Detection Techniques*. Department of Computer science, virtual university of Pakistan. *I.J. Education and Management Engineering,* 2018, 2, 20-30**.** pp. 2-11.

[10]Jeff May, Christopher Ahlberg (2020) The Security Intelligence Handbook Third Edition – How to Disrupt adversaries and reduce risk with security intelligence. Permission Department, CyberEdge Group, 1997 Annapolis Exchange Parkway, Suite 300, Annapolis, MD, 21401, ISBN 978-1-948939-16-4 (eBook). pp 10 - 155

[11] Paulsen, C. , Witte, G. and Feldman, L. (2017), Fundamentals of Small Business Information Security, ITL Bulletin, National Institute of Standards and Technology, Gaithersburg, MD, [online], https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=922990 (Accessed March 21, 2022). pp 1-4.

[12] Levi Gundert (2020) The Risk Business, What CISO Need to Know about Risk-Based Cybersecurity. Permission Department, CyberEdge Group, 1997 Annapolis Exchange Parkway, Suite 300, Annapolis, MD, 21401, ISBN 978-1-948939-16-4 (eBook). pp 3 -93

[13] Kevin D. Mitnick, William L. Simon, (2002) The Art of Deception, forwarded by Steve Wozniak. Wiley Publishing, Inc. 10475 Crosspoint Blvd., Indianapolis, IN 46256. ISBN: 978-0-7645-4280-0, Chapter 12, pp 260.

[14] TM, "Developing Story: COVID-19 Used in Malicious Campaigns," 2020. [Online]. Available: https://www.trendmicro.com/vinfo/us/security/news/cybercrimeand-digital-threats/coronavirus-used-in-pam-malware-file-names- and-malicious-domains. [Accessed: 04-May-2020]

[15] S. P. Berman and J. W. Gately, (2020) "COVID-19 and Its Impact on Data Privacy and Security,". [Online]. Available: https://www.lexology.com/library/detail.aspx?g=dec8ccab-d74a4bc1-9e4a-9b1e5626e936. [Accessed: 04-May-2020]

[16]Course Overview (eccouncil.org)

[17] 7 of the Top 10 Vulnerabilities Target Microsoft (recordedfuture.com)

[18] https://www.sba.gov/managing-business/cybersecurity

[19] Samarati, M, (2017), Cybercrime cost UK businesses £29 billion in 2016, IT Governance Institute, [Online] Accessed 2nd March at https://www.itgovernance.co.uk/blog/2016-cybersecurity-breaches-cost-uk-businesses-almost-30-billion/

[20] US Department of Defense (2021) https://www.defense.gov/News/Releases/Release/Article/2833006/strategic-direction-for-cybersecurity-maturity-m/

[21] Cliff Saran, (2015), https://www.computerweekly.com/news/2240242478/Satya-Nadella-Every-business-will-be-a-software-business

[22] Isabella Jibilian, Katie Canales (2021). https://www.businessinsider.com/solarwinds-hack-explained-government-agencies-cyber-security-2020-12?r=US&IR=T

[23] Aon (2019), Cyber Security Report, what is now and What is next, [Online] Accessed 3rd March at https://www.aon.com/risk-services/cyber.jsp

[24] https://www.educba.com/what-is-ddos-attack (2021)

[25]https://www.educba.com/what-is-malware (2021)

[26]National Institute of Standards and Technology (2021)"https://www.nist.gov/news-events/news/2021/05/nist-releases-tips-and-tactics-dealing-ransomware"

