Applied Mathematics & Information Sciences
An International Journal

http://dx.doi.org/10.18576/amis/180506

Quantifying the Impact of the COVID-19 Pandemic on Quality Assurance Practice

Mahmoud Odeh [1,], Sawsan S. Badrakhan [2], Najlaa Flayyih [3], Mohammad Omar Sabri[4], Zeana Abdijabar[5], Hala Alsabatin[6] and Saleh Hammad[7]*

[1] Department of Cybersecurity, Information Technology School, Zarqa University, Amman, Jordan
[2] Department of Humanities and Social Sciences, Faculty of Arts & Science, Al-Ahliyya Amman University, Amman, Jordan
[3] Department of Private law, College of Law, Ajman University, Ajman, UAE
[4] Department of Business Information Technology, College of Business, Zarqa University, Amman, Jordan
[5] Department of Private law, College of Law, Ajman University, Ajman, UAE
[6] Department of Education Leadership, College of Education, Zarqa University, Zarqa, Jordan
[7] Department of Physical and Health Education, Faculty of Educational Sciences, Al-Ahliyya Amman University, Amman, Jordan

Received: 2 Jun. 2024, Revised: 24 Jun. 2024, Accepted: 7 Jul. 2024.
Published online: 1 Sep. 2024.

Abstract: The aftereffect of the Covid pandemic could be seen as a significant turning point for various reasons. The way of living and working underwent a significant transformation. Several institutions, such as universities, are compelled to adapt their operations. The shift towards remote working has become the new norm in our lives. Ensuring the security of our digital world has become a pressing concern for individuals everywhere. The rise in online applications has attracted the attention of hackers, particularly those targeting users with limited internet experience. This study examines the impact of Covid pandemic on cybersecurity concerns in Jordan. Various methodologies have been used for data collection and analysis process. The data collected by creating 11 interviews, while 312 surveys were collected and analyzed for the quantitative aspect of this research. Furthermore, the process of data collection involves conducting experiments on a variety of devices, including servers, laptops, and desktops. Moreover, several tools were employed for the data analysis, including Nvivo, Microsoft Visio, and visual programming.

Keywords: Cybersecurity, Aftereffect of Covid-19 pandemic, Mathematical model, Hackers.

1 Introduction

The world of cybersecurity is broad and filled with diverse threats. One particular type that raises great alarm isn't so much the overt viruses, but more so those stealthier actions which can infiltrate computers or smart devices without detection by their users. The covid-19 pandemic has significantly affected the lives of almost everyone in several countries around the whole world. For instance, online payments and social media have become essential aspects of our everyday lives, enabling us to fulfill our diverse requirements and maintain connections. In addition, the Covid-19 pandemic has forced students as well as professors to heavily depend on online applications. Nevertheless, the growing reliance on technology has introduced potential vulnerabilities to data security. In today's interconnected world, the vulnerability of internet users has led to an alarming increase in the activities of hackers. Based on a thorough statistical analysis conducted by Rob Sobers, a prominent an information security company named "VARONIS" has discovered a notable increase in data breaches from multiple sources due to the Covid-19 pandemic in 2021[1]. For instance, most data breaches, approximately 95% of them, are a result of human errors [2]. Furthermore, [3] have reported that numerous institutions worldwide have faced spear-phishing attempts. According to a recent study, many business leaders have expressed concerns about the level of preparedness their companies have in terms of cybersecurity [4]). Regrettably, only a small fraction of initiations' data is properly secured. Amidst the chaos of the covid-19 pandemic in the first half of 2020, a staggering 36 billion records were breached worldwide [5]. It is clear that there has been a noticeable increase in cybercrime over the past seven years. It's important to note that there has been an 11% increase in security breaches since 2018 and a remarkable 67% rise since 2014 [6]. In 2020, there were significant instances of Twitter accounts being compromised, affecting notable figures such as Elon Musk, co-founder of Tesla and SpaceX, along with various political figures [7].

Moreover, in 2022, the well-known hotel Marriot encountered a major security breach that affected the information of more than 5.2 million guests. There has been a breach in security where certain individuals have managed to gain unauthorized access to two accounts owned by employees of the Marriot hotel. They efficiently tracked and

*Corresponding author e-mail: Modeh@zu.edu.jo

obtained information from multiple applications related to customers' loyalty cards. An IT project manager would have been vigilant in ensuring that the data breach did not go unnoticed for nearly a month, but unfortunately, it was only detected by the information security team after that time. In October 2016, it was discovered that a significant number of accounts, around 412 million, were compromised [8]

2 Study problems and research questions

This study aims to fill the knowledge gap among Jordanian residents on cybersecurity measures and how to react to cyberattacks, as well as the methods for dealing with cyberattacks after the COVID-19 epidemic. In the field of cybersecurity, there has been a dearth of research that has managed to provide a theoretical and practical framework. A mix of mathematical analysis, factor analysis, and data collected from real-world settings have been used in these investigations. In light of the research challenge, this study aimed to suggest a cybersecurity framework, which may use to evaluate the various degrees of cybersecurity and investigates the variables effecting the influence of the COVID pandemic aftereffects on the quality of information and cybersecurity. This leads us to our following set of study questions: 1. What effect has the COVID-19 epidemic had on cyber threats? 2. How does the degree to which individuals are aware of cybersecurity issues affect these dangers? 3. How much would a cyber-attack's harm be worth? 4. How does the way people behave affect the way cyber-attacks and cybersecurity risks are responded to?

3 Theoretical Framework

Multiple forms of cybersecurity assaults exist. One of the most alarming concerns is clandestine assaults that have the potential to evade detection by users on their personal computers or intelligent gadgets, rather than the viruses themselves. Viruses often induce disturbances on the user's computer, manifesting as file deletions or the establishment of desktop shortcuts [9]. A virus is a little software capable of modifying the functioning of computers. The Trojan horse, a kind of malicious software that masquerades as innocuous, poses a more perilous danger than viruses [10]. The process of generating malicious code that masquerades as innocuous in order to fool and target diverse entities such as E-payment [11]. A (DoS) attack, which entails inundating a targeted website with a substantial volume of requests, resulting in the website being inaccessible or unable to respond to these requests. Based on recent research conducted by [12], it is anticipated that the quantity of Denial-of-Service assaults may escalate to an astonishing 15.4 million by the year 2023. Twitter.com, a widely used social media platform, saw a cyber-attack on December 17, 2009. According to [13], the hackers effectively altered the primary website image and claimed responsibility for the breach, attributing their actions to the Iranian Cyber Army. This research used statistical theories and equations explore the methodology of evaluating the risk associated with Cybersecurity.

The array as (V), where each element represents a specific vulnerability:

To add an array to Equation 1, we can introduce it to represent the different types of vulnerabilities within each risk component. Let's denote the array as \(V \), where each element represents a specific vulnerability:

$$R_v = \sum_{i=1}^{n} V_i \times P_i \quad \text{…………………………..….} \quad 1$$

Here's how we can integrate the array into each risk component:

1. Risk from Remote Work R_w:

$$R_w = \sum_{i=1}^{m} V_{w_i} \times P_{w_i} \quad \text{……………..…………} \quad 2$$

V_{wi} represents the vulnerability level associated with the i^{th} vulnerability related to remote work.

P_{w_i} represents the probability of exploitation of the i^{th} vulnerability related to remote work.

2. Risk from Pandemic-related Phishing R_p:

$$R_p = \sum_{i=1}^{k} V_{p_i} \times P_{p_i} \quad \text{…………………..………} \quad 3$$

V_{p_i} represents the vulnerability level associated with the i^{th} vulnerability related to pandemic-related phishing.

P_{p_i} represents the probability of successful exploitation of the i^{th} vulnerability related to pandemic-related phishing.

3. Risk from Network Vulnerabilities R_n:

$$R_n = \sum_{i=1}^{l} V_{n_i} \times P_{n_i} \quad \text{………………………} \quad 4$$

represents the vulnerability level associated with the i^{th} vulnerability related to network vulnerabilities.

P_{n_i} represents the probability of successful exploitation of the i^{th} vulnerability related to network vulnerabilities.

4. Risk from Supply Chain Vulnerabilities R_s:

$$R_s = \sum_{i=1}^{q} V_{s_i} \times P_{s_i} \quad \text{………………………} \quad 5$$

This formulation allows for a more granular assessment of cybersecurity risks by considering multiple vulnerabilities within each risk component. It acknowledges that each vulnerability may have different probabilities of exploitation and varying impacts on the overall risk. By summing up the

contributions of individual vulnerabilities, organizations can better prioritize their mitigation efforts and allocate resources effectively to manage cybersecurity risks from a managerial perspective.

To add longer and more complex arrays to Equation 1, we can introduce arrays that represent various subcategories or dimensions of vulnerabilities within each risk component. Let's denote these arrays as V_w, V_p, V_n, and V_s where each element of the array represents a specific vulnerability within the corresponding risk component. Additionally, we'll consider arrays for the

probability of exploitation P_w, P_p, P_n, and P_s for each vulnerability. Here's the expanded equation:

$$R_v = \sum_{i=1}^{m} V_{w_i} \times P_{w_i} + \sum_{j=1}^{n} V_{p_j} \times P_{p_j} + \sum_{k=1}^{l} V_{n_k} \times P_{n_k} + \sum_{q=1}^{r} V_{s_q} \times P_{s_q} \quad \ldots 6$$

Now, let's provide more detail for each array:

1. Array for Risk from Remote Work V_w:

$$V_w = [V_{w_1}, V_{w_2}, \ldots, V_{w_m}] \quad \ldots\ldots\ldots 7$$

$$P_w = [P_{w_1}, P_{w_2}, \ldots, P_{w_m}] \quad \ldots\ldots\ldots\ldots\ldots 8$$

V_{wi} represents the vulnerability level associated with the i^{th} vulnerability related to remote work.

P_{wi} represents the probability of exploitation of the i^{th} vulnerability related to remote work.

2. Array for Risk from Pandemic-related Phishing V_p:

$$V_p = [V_{p_1}, V_{p_2}, \ldots, V_{p_n}] \quad \ldots\ldots\ldots\ldots 9$$

$$P_p = [P_{p_1}, P_{p_2}, \ldots, P_{p_n}] \quad \ldots\ldots\ldots\ldots\ldots 10$$

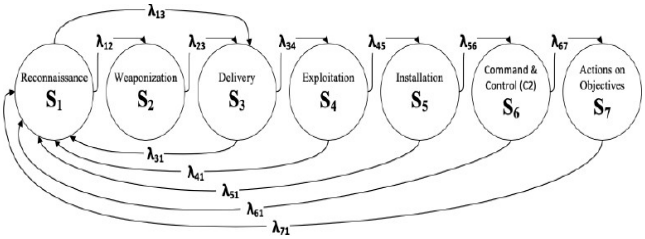
V_{pi} represents the vulnerability level associated with the i^{th} vulnerability related to pandemic-related phishing.

To represent the equation with longer and more complex arrays, we'll introduce multidimensional arrays for vulnerabilities (\(V_{w_i}\), \(V_{p_j}\), \(V_{n_k}\), \(V_{s_q}\)) and their corresponding probabilities of exploitation (\(P_{w_i}\), \(P_{p_j}\), \(P_{n_k}\), \(P_{s_q}\)). Each element of these arrays will represent a specific vulnerability within the corresponding risk component. Here's how we can extend the equation:

$$R_v = \sum_{i=1}^{m}\sum_{j=1}^{n}\sum_{k=1}^{l}\sum_{q=1}^{r} V_{w_{i,j,k,q}} \times P_{w_{i,j,k,q}} + \sum_{j=1}^{n}\sum_{k=1}^{l}\sum_{q=1}^{r} V_{p_{j,k,q}} \times P_{p_{j,k,q}} + \sum_{k=1}^{l}\sum_{q=1}^{r} V_{n_{k,q}} \times P_{n_{k,q}} + \sum_{q=1}^{r} V_{s_q} \times P_{s_q} \quad \ldots\ldots\ldots 11$$

Markov Model

A Markov chain is a probabilistic model that describes a series of events, where the likelihood of each event is determined solely by the state achieved in the preceding event. According to [14], there is a type of sequence that is countable and infinite. In this sequence, the state of the chain changes at specific time intervals. This is known as a discrete-time Markov chain (DTMC). The Markov chain and other relevant literature used in this research to analyze the probability of the cyber killing chain. The findings will be used to assess the risks involved.



Cybersecurity diagram [15].

4 Research Methodology and Main Results

Both quantitative and qualitative sources contributed to the data used in this study. Three hundred and twelve individuals were able to finish the survey that was conducted online. For the qualitative data, eleven cybersecurity experts have also been interviewed using a semi-structured format. The experimental technique has also been used as a fieldwork tactic in testing. The study was completed after the researcher tested sixteen laptops, five servers, and fourteen desktops.

The owner's full consent is necessary to ensure that the test is virus and spam free. We used Nvivo to analyze the qualitative data, and we presented the results of the quantitative data as frequencies. The demographics of the survey takers are shown in Table 2. Interviewee details are coded by the intervals (Px: P1-P16) in Table 2

Table 1: Details About the Online Survey Respondents

Characteristics	Categories	Total (R=312) R (%)
Gender	Male	173(55.44%)
	Female	139 (44.56%)
Governorate	North	97 (31.09%)
	Middle	192(61.54%)
	South	23 (07.37%)
Age (years)	18-30	189 (60.57%)
	31-45	77 (24.68%)
	46-60	29 (9.30%)
	>60	17 (5.45%)
Education	Secondary school	96 (30.77%)
	Diploma/ bachelors	192 (61.54%)
	(Master or Ph.D.)	24 (7.69%)

Table 2: Profiles of Interviewees

S.No	Code	Interviewee profiles
1	P1, P2, and P3.	manager of information technology security, cybersecurity specialist, and adjunct instructor in the field
2	P4, P5, and P6.	Technical engineer, senior technical engineer, and project manager.
3	P7, P8, and	Information Systems and computer

	P9.	science
4	P10, P11, and P12.	Cybersecurity and information knowledge management.
5	P13, P14, P15, and P16.	CEO, CFO, COO, and CTO.

4.1 Cybersecurity threats and breaches are negatively impacted by the COVID-19 pandemic.

Consistent with other studies, these find that the COVID-19 pandemic has greatly increased cybersecurity threats. Almost two-thirds of those who took part in the survey agreed that COVID-19 had a negative effect on cybersecurity because of the extra risks it presents. In contrast, 16% of people think that increasing cybersecurity risks are unavoidable because of the positive association between the two factors. Only 3% of respondents are uncertain about the link between COVID-19 and cybersecurity threats, while 13% hold the opinion that there is no such thing. The results of this investigation are shown in Figure 1, which is structured based on the association between the effects of Pandemic of Covid and cyber intrusions.

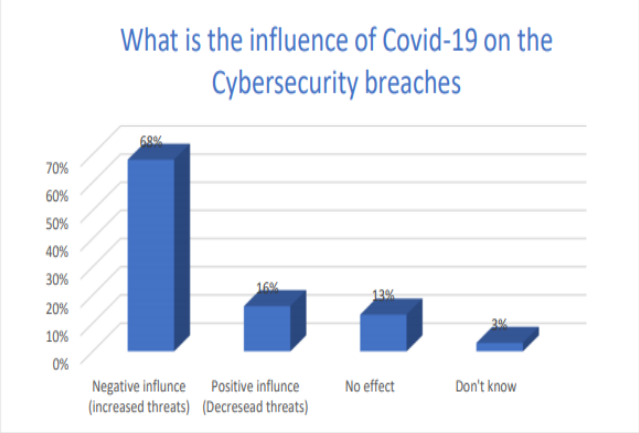


Fig. 1: The effect of the COVID Pandemic on Cybersecurity Incidents

A cybersecurity expert (identified as I3 in this study) from a prominent private institution who took part in the study via mid-term interviews said that, according to the most recent statistics from our company's research department, cybersecurity breaches grew significantly from 2016 to 2020. As far as our IT department is concerned, this is an issue of paramount importance. Some facts supported by data are as follows: With 27% in 2016, 46% in 2018, 52% in 2019, and 66% in 2020, the penetration rate continued to rise. In my opinion, this is a cyber-disaster, and we should be worried about it. A synopsis of the statistical data collected from the semi-structured interviews with participants P3 is shown in Figure 2. According to a technical manager (identified as P4) from the same company in the past. For example, in 2016, our total budget for IT and cybersecurity was 8%; in 2017, it was 11%; in 2018, it was 12%; in 2019, it was 16%; and in 2020, it jumped to 22%. Could you perhaps suggest one for your research? I would be very grateful. In this study, participants I4 were interviewed using semi structured interviews, and the results are summarized in Figure 3.

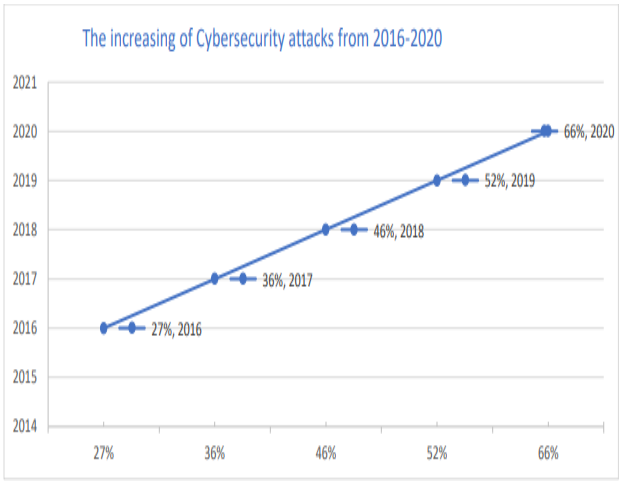


Fig. 2: Cybersecurity attacks have been on the rise from 2016 to 2020

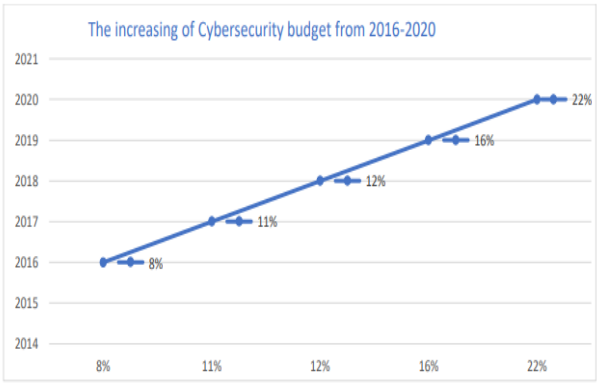


Fig. 3: The Annual Growth of the Cybersecurity Budget, 2016–2020

4.2 The COVID Pandemic Positively Impacting the Cybersecurity Awareness

To protect oneself and one's business from cyberattacks and breaches, cybersecurity expertise is essential. The results of this study show that individuals are more alert now than they were before the COVID-19 outbreak. Improving people's IT competency involves a number of factors, one of which is increasing their level of awareness [16-19]. The results show the survey findings related to this research as can be seen from figure 4. It reveals that while 46% of individuals say COVID-19 makes people more aware of cybersecurity risks, 34% think it goes against the grain since people are already avoiding technology to protect themselves from hackers and cyberattacks. Eleven percent of those who took the survey believed that cybersecurity knowledge had nothing to do with the COVID-19 outbreak. Finally, 9% of poll takers are skeptical about the strength of the relationship between these

factors

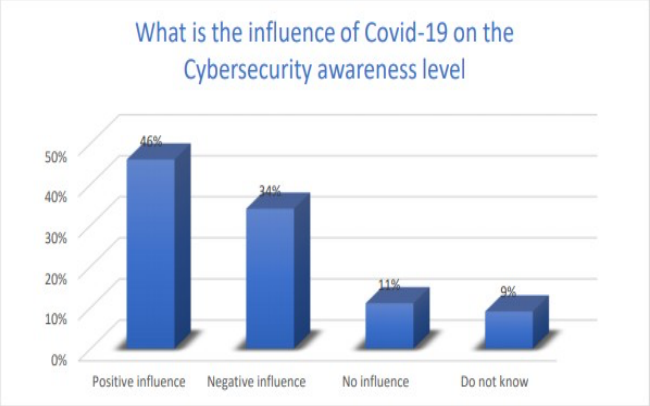


Fig. 4: The Influence of Covid-19 on the Cybersecurity Awareness Level

4.3 There is a positive correlation between the COVID-19 pandemic and awareness of cybersecurity.

To protect oneself and one's business from cyberattacks and breaches, cybersecurity expertise is essential. The results of this study show that individuals are more alert now than they were before the COVID-19 outbreak. Improving people's IT competency involves a number of factors, one of which is increasing their level of awareness [16-19]. The results show the survey findings related to this research from figure 5. It reveals that while 46% of individuals say COVID-19 makes people more aware of cybersecurity risks, 34% think it goes against the grain since people are already avoiding technology to protect themselves from hackers and cyberattacks. Eleven percent of those who took the survey believed that cybersecurity knowledge had nothing to do with the COVID-19 outbreak. Finally, 9% of poll takers are skeptical about the strength of the relationship of these factors.

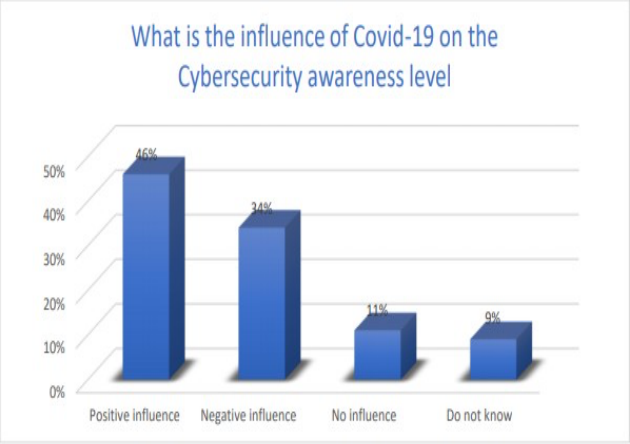


Fig. 5: The Impact of the COVID Pandemic on the awareness of Cybersecurity

4.4 The financial components of cyber security are hit hard by the COVID-19 epidemic.

According to the data gathered in this research, it can be said that the expense of using IT is connected to different issues, such as cybersecurity-attacks and periods of unavailability. Cyberattacks are the primary cause of downtime in the majority of cases. Due to the Covid-19 pandemic, which necessitates remote employment, the majority of individuals and organizations will heavily depend on the internet between 2020 and 2021. Individuals who engaged in remote employment often used computers from their homes. Consequently, the security level is reduced when companies provide internet access to in-house servers over the intranet. This study categorizes the financial perspectives into two groups: expenditures incurred during periods of inactivity and additional budgetary provisions for enhancing cybersecurity. Based on a comprehensive annual report provided by a participant of the research for a renowned firm specializing in airline reservations, it has been shown that the cost of off working time could negatively influence the financial perspectives. According to the research, the total budgetary allocation for the period of 2020-2021 amounted to 3.1 million US dollars, covering almost all of working hours with no exceptions. Periods of inactivity or unavailability that occur at various times throughout the year.

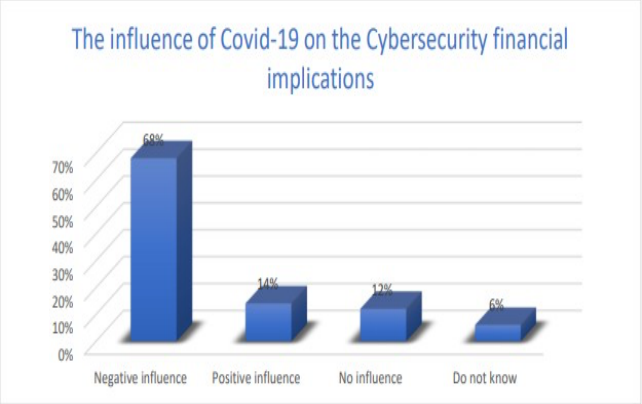


Fig. 6: the financial effects of pandemic on cybersecurity.

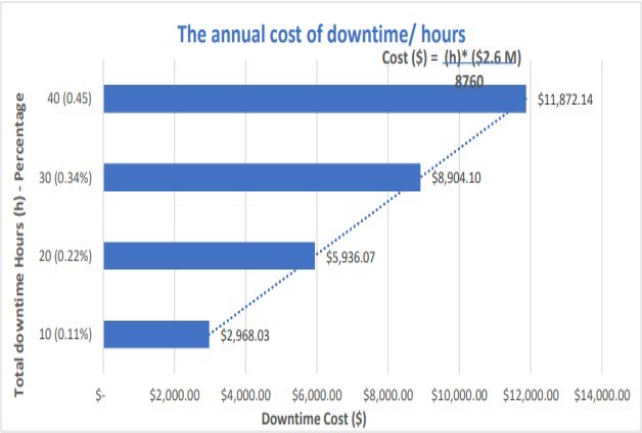


Fig. 7: the periodic cost of delay in operations

5 New Cybersecurity Framework Suggested

This article offers a theoretical and practical Cybersecurity framework based on previous data analysis and collecting. With its theoretical foundations in cyber-kill chain diagram spaces and the Markov chain model, the risk evolution method is the main emphasis of the framework [20]. It can be seen the proposed Cybersecurity Evaluation Model in Figure 8. The cybersecurity level was represented by the risk rating, which went from zero to one on a scale from very low to extreme high. As a result, areas for enhancing cybersecurity, such as surveillance, weaponization, delivery, exploitation, installation, control and command, and achieving objectives, have been associated with cybersecurity levels. There is an ongoing effort to achieve the highest level of security via this form of space-based cybersecurity upgrade.

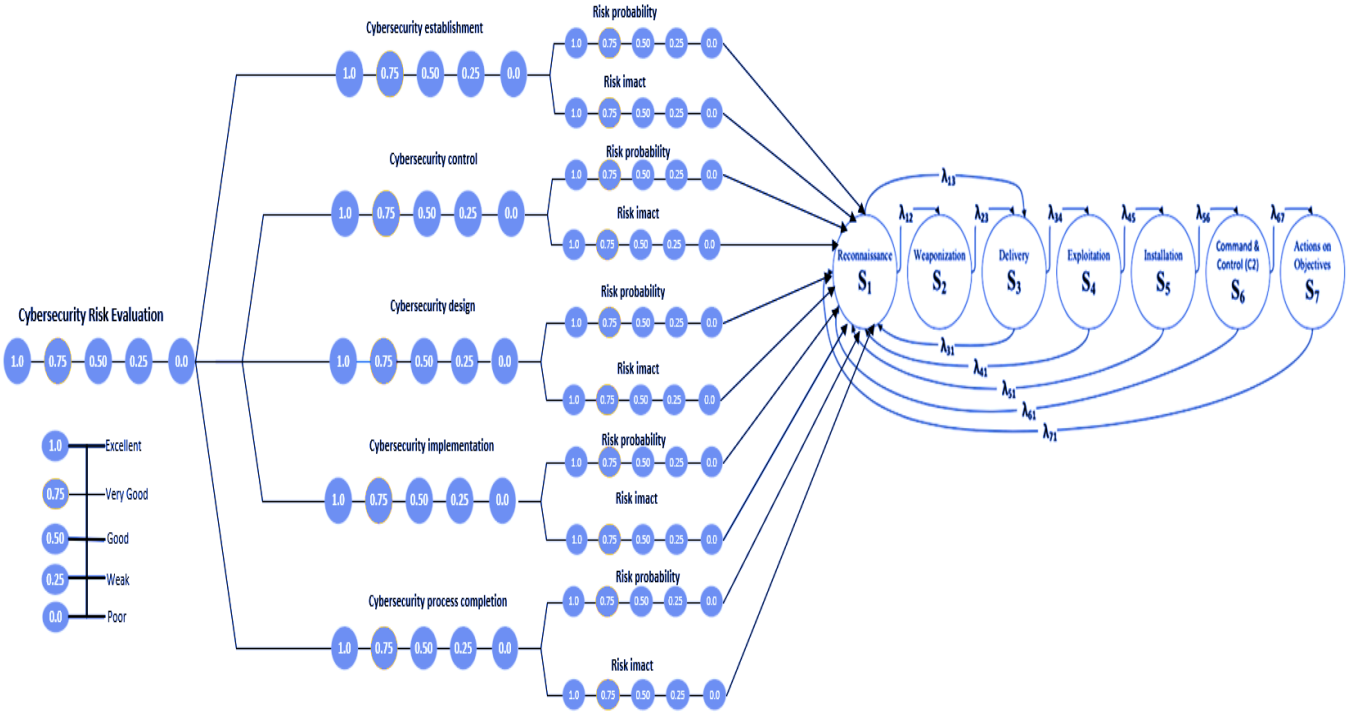


Fig. 8: A suggested framework Based on This Study's Theoretical foundation

6 Conclusion

The effects of COVID-19 on cybersecurity were investigated in this study from both a managerial and a practical perspective. The study relied on the Markov model and evaluation model for its theoretical underpinnings. Concerning the COVID-19 pandemic and cybersecurity awareness, the study did discover some positive news. Cybersecurity risks and costs are significantly impacted by COVID-19, according to the report. Both inductive and deductive reasoning were used by the researchers. Since this was the case, a mixed-methods approach was used in the study. To support the process of improving and evaluating the Cybersecurity, a suggested framework has been developed. All of this rests on top of the theoretical groundwork and the results of the data analysis. With this suggestion, the research comes to a close. From a managerial and pragmatic perspective, the book tackled challenges in its structure. Additional testing of the proposed cybersecurity architecture is necessary prior to any further investigation

References

[1] R. Sobers. (2021, 15/1/2022). 134 Cybersecurity Statistics and trends for 2021. Available: https://www.varonis.com/blog/cybersecurity-statistics/

[2] J. Seaman and J. Seaman, "Developing your human firewall," *Protective Security: Creating Military-Grade Defenses for Your Digital Business,* pp. 487-523, 2021.

[3] K. Evans, A. Abuadbba, T. Wu, K. Moore, M. Ahmed, G. Pogrebna*, et al.*, "RAIDER: Reinforcement-aided spear phishing detector," in *International Conference on Network and System Security*, 2022, pp. 23-50.

[4] S. Kesar, "Smart cities bring new challenges in managing cybersecurity breaches," *ETHICOMP 2020,*

p. 147, 2020.

[5] W. Dicker, "An Examination of the Role of vCISO in SMBs: An Information Security Governance Exploration," 2021.

[6] K. Bissell, R. M. Lasalle, and P. Dal Cin, "The cost of cybercrime—Ninth annual cost of cybercrime study," *Ponemon Institute and Accenture Security,* vol. 50, 2019.

[7] T. Henneman, "Beyond lip-synching: Experimenting with TikTok storytelling," *Teaching journalism & mass communication,* vol. 10, pp. 1-14, 2020.

[8] D. McDaniel, "Data Breaches: Who is Behind Them, Why They Do It, and How to Protect Your Data," *Papers/dmcdaniel_databreaches. pdf,* 2019.

[9] U. Mishra, "An introduction to computer viruses," *Available at SSRN 1916631,* 2010.

[10] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, "Trojan-horse attacks on quantum-key-distribution systems," *Physical Review A,* vol. 73, p. 022320, 2006.

[11] S. A. Schuckers, "Spoofing and anti-spoofing measures," *Information Security technical report,* vol. 7, pp. 56-62, 2002.

[12] S. Scott-Hayward, "Security-focused Networks of the Future," in *Proceedings of the 2021 ACM International Workshop on Software Defined Networks & Network Function Virtualization Security*, 2021, pp. 1-1.

[13] S. Tripathi, B. Gupta, A. Almomani, A. Mishra, and S. Veluru, "Hadoop based defense solution to handle distributed denial of service (ddos) attacks," 2013.

[14] E. Chasioti, "BARC0141: Built Environment Dissertation," 2020.

[15] R. Hoffmann, J. Napiórkowski, T. Protasowicki, and J. Stanik, "Risk based approach in scope of cybersecurity threats and requirements," *Procedia Manufacturing,* vol. 44, pp. 655-662, 2020.

[16] N. Al-Ramahi and M. Odeh, "The impact of innovative technology on the quality assurance at higher education institutions in developing countries: a case study of Jordan," *International Journal of Information and Education Technology,* vol. 10, pp. 826-831, 2020.

[17] M. Odeh and M. Yousef, "The effect of Covid-19 on the electronic payment system: Usage level trust and competence perspectives," *Indonesian Journal of Electrical Engineering and Computer Science,* vol. 22, pp. 1144-1155, 2021.

[18] M. M. Odeh, "A proposed theoretical solution for transferring from physical to virtual machines based on cloud computing," in *2019 5th international conference on information management (ICIM)*, 2019, pp. 221-226.

[19] M. Odeh, "A novel framework for the adoption of cloud computing in the higher education sector in developing countries," *International Journal of Scientific & Technology Research,* vol. 9, pp. 5660-5667, 2020.

[20] S. E. Donaldson, S. G. Siegel, C. K. Williams, and A. Aslam, *Enterprise cybersecurity study guide: How to build a successful cyberdefense program against advanced threats*: Springer, 2018.

Mahmoud Odeh is an associate professor at Zarqa University. He completed his higher education and PhD at Reading and Coventry University, UK. Mahmoud holds more than 15 years' experience in both the practical and academic fields, with 56 international certificates in servers, computer virtualization, smart machine simulation, and cloud computing. The rapid evolution of cloud computing technology inspires his current research, primarily focusing on the implementation of innovative technology.

Sawsan Baderkhan is a professor educational origin in Al-Ahliyya Amman University, Jordan. She received her bachelor's, Master's, and PHD from Jordan University with honorary degree. Her research focuses on educational studies as well as educational methods on the and philosophical spheres. She has many published researches.

Najlaa Flayyih is an Associate Professor of Civil Procedure Law at Ajman University. She has extensive experience teaching at multiple universities and emphasizes linking theoretical knowledge with practical application. Dr. Flayyih believes in the importance of hands-on exercises, moot courts, and analyzing judicial rulings to effectively teach procedural law courses. She has received numerous awards and has multiple published scientific research papers and books to her name. Dr. Flayyih is also actively involved in supervising graduate students. Beyond her academic pursuits, she enjoys listening to classical music as a means of relaxation and maintains an active lifestyle through regular exercise and fitness activities.

Mohammad Omar Sabri is an assistant professor who completed his PhD at the University of the West of England (UWE), UK. Mohammad currently serves as the vice dean of scientific research at Zarqa University. He has a demonstrated history of working in the software development industry and is skilled in various research areas, including Knowledge Management, Business Process Architecture, Business Modelling and Ontologies.

Zeana Abdijabar, professor of Commercial Law and head of the Private Law Department; obtained her doctorate in 2005 from the College of Law - University of Mosul - Iraq, she joined the Faculty of Law at Ajman University in 2013 until now and has many research papers published in prestigious Arab and foreign journals. She supervised a large number of graduate students and also participated as a member of several graduate thesis discussion committees. She is a reviewer for many research and promotion files. She taught all courses related to the specialty of commercial law, such as companies' law, commercial papers, and banking operations, In the Bachelor of Law, Masters, and Ph.D. programs.

Hala Alsabatin's *research interests are deeply rooted in the dynamics of educational leadership, curriculum development, and linguistic studies. Her academic work focuses on exploring innovative leadership strategies within educational institutions, aiming to enhance the efficacy of educational administration and policy-making. She is particularly interested in how effective leadership can influence and improve school environments, teacher performance, and student outcomes. In addition to her work in educational leadership, Dr. Alsabatin is passionate about curriculum development. She investigates how curricula can be designed and implemented to better meet the needs of diverse student populations. Her research often examines the intersection of curriculum and cultural context, seeking to develop educational programs that are both culturally relevant and academically rigorous. Her background in linguistics also informs her research, as she explores the role of language in education. Dr. Alsabatin is interested in how linguistic principles can be applied to teaching methodologies, especially in* multilingual and multicultural classrooms. Her work aims to bridge the gap between linguistic theory and practical teaching strategies, enhancing language acquisition and literacy among students. Overall, Dr. Alsabatin's research is driven by a commitment to improving educational practices and outcomes. By integrating insights from educational leadership, curriculum development, and linguistics, she seeks to create more effective and inclusive educational environments.

Saleh Hammad is a lecturer in physical education at the Faculty of Educational Sciences at Al-Ahliyya Amman University. He holds a master's degree in physical education from the University of Jordan. He has participated in many international conferences and published studies in peer-reviewed global journals. He is a researcher interested in the field of sports and educational management.