

# THE ROLE OF COVID-19 PANDEMIC ON THE CYBERSECURITY: A MANAGERIAL AND PRACTICAL IMPLICATIONS

Mahmoud Odeh, Zarqa University

## ABSTRACT

*The years 2020-2021 were a turning point on several grounds. The way of living and working were dramatically changed. Almost all institutions, in both public and private sectors, are forced to change the way of routine operations. The remote working and social distance have become the new style of life. Cybersecurity is one of the most important aspects that forced citizens to deal with. The focus of using online applications increased the appetite of hackers, especially that the appearance of users with limited experience of using internet applications. This study sheds the light on the role of Covid-19 and its influence on cybersecurity issues in Jordan. Qualitative and quantitative methodologies have been employed for the data collection and analysis process. The qualitative data was collected through conducting 11 semi-structured interviews; where as 312 surveys have been successfully collected and analyzed to cover the quantitative part of this research. In addition, the data collection process includes an experimental method through testing 5 servers, 16 laptops, and 14 desktops using several antispam and antivirus applications. Moreover, several software tools such as Nvivo, Microsoft Visio, Microsoft business intelligence, and visual programming were used for the data analysis process.*

**Keywords:** Cybersecurity, Covid-19, Nvivo, Microsoft Business Inelegant, Jordan, Hackers

## INTRODUCTION

In 2020-2021, the pandemic of covid-19 has dramatically altered the lifestyle of almost all citizens in Jordan. Distance learning, online shopping, online payments, and social media are examples of daily routines to dealing with living requirements. Moreover, the Covid-19 pandemic forced both students and professionals to use online applications. However, such usage came with threats to information. Hackers' appetite has reached the highest level because of gullible internet users. A deep statistical study conducted by Rob Sobers presents professional data security company "VARONIS" stated that one of the greatest side effects of the Covid-19 pandemic in 2021 is the huge increase of hacked data from common sources (SOBERS, 2021). For instance, 95% of data breaches are mainly caused because of human errors (Seaman & Seaman, 2021). Furthermore, 80% of institutions worldwide have experienced spear-phishing attempts (Evans et al., 2021). While 68% of business leader's show that they have a negative expectation about cybersecurity readiness in their companies (Kesar, 2020). However, only 5% of initiations' data is strongly protected. In the first half of 2020 where the covid-19 pandemic was at its peak almost 36 billion recorders around the world have been breached (Dicker, 2021). The increase of cybercrime could be clear in the last seven years, for instance, security breaches have increased by 11% since 2018 and 67% since 2014 (Bissell, LaSalle & Dal Cin, 2019). In 2020, more than one hundred and

thirty famous accounts on Twitter have been breached, such famous accounts include Elon Musk the CEO of Tesla and Space X, and other accounts from the political sector (Henneman, 2020). In addition, in 2020 the famous hotel Marriot has a deep breach that affected data for more than 5.2 million guests. Hackers have login using two accounts of Marriot hotel employees and follow the customers' loyalty cards information from several 2 applications. The breach of data stays for almost one month before it was discovered by the information security team. Another interesting statistical fact in October 2016 shows that around 412 million accounts have been hacked from the FriendFinders.com website (McDaniel, 2019).

## **RESEARCH PROBLEMS, AIM AND QUESTIONS**

The research problem in this study could be summaries into the mechanism of dealing with cybersecurity attacks within the Covid-19 pandemic and the weak awareness between citizens in Jordan about the level of security as well as how to deal with any possible cyber-attack. Very limited studies have developed a practical and theoretical cybersecurity framework based on combinations of mathematics, factors, and data collection from the fieldwork. Therefore, and based on the research problem, this study aimed to develop a novel practical and mathematical cybersecurity framework that helps to investigate the factors influencing the effect of covid-19 on cybersecurity and to find out the levels of cybersecurity. Accordingly, the research questions are as follows: 1. what is the effect of the Covid-19 pandemic on cybersecurity threats? 2. What is the effect of the awareness level of citizens on cybersecurity threats? 3. What is the expected damage cost caused by Cyber-attack? 4. What is the effect of citizen behavior for dealing with Cybersecurity threats in case of cyber-attack?

## **THEORETICAL FRAMEWORK**

Cybersecurity attack has several types. The most dangerousness is not the viruses; it is the hidden attack when the user even does not know that there is a hidden attack inside the computer or any smart device. Viruses usually alter the user that something wrong is happening such as delete files or copy files shortcuts on the computer desktop (Mishra, 2010). A virus, therefore, considers as a small program that changes the way of computers operation. Another threat could be considered more dangerous than viruses such as Trojan horse, which is hidden inside seemingly harmless software (Gisin, Fasel, Kraus, Zbinden & Ribordy, 2006). Whereas, Spoofing refers to users who create a piece of harm code that appears to be something else from other users with a harmless appearance for attack several targets such as credit cards, debit cards, and electronic transactions (Schuckers, 2002). Denial of Service attack or (DoS) as well as Distributed Denial of Service attacks (DDoS) refers to the process of flooding the victim's website with a storm of requests, which makes websites unavailable or even incapable of answering requests (Carl, Kesidis, Brooks & Rai, 2006). It is expected that by 2023, the number of Denial-of-Service attacks could be raised to up to 15.4 million (Scott-Hayward, 2021). On December 17, 2009, the famous social website Twitter.com has been attacked using DDoS, hackers have changed the main website image and announced that this website has been hacked by the Iranian Cyber Army (Tripathi, Gupta, Almomani, Mishra & Veluru, 2013). This study employed theoretical and statistical theories, equations, and frameworks to explain the process of evaluating the threat of Cybersecurity. According to Befekadu, Gupta & Antsaklis (2011), DDoS could be evaluated based on the performance metric, which aims to evaluate the attack detection performance according to three main factors: accuracy of attack and 3 protection, the effectiveness of cybersecurity levels, and speed using process model and cost function as follows:

$$\begin{aligned}
 x_{k+1} &= Ax_k + \beta_{k+1}Bu_k + v_{k+1} \dots\dots\dots 1 \\
 y_{k+1} &= Cx_k + w_{k+1} \dots\dots\dots 2 \\
 k &= 0,1, \dots, T - 1 \dots\dots\dots 3
 \end{aligned}$$

Where  $x_k \in \mathbb{R}^n$  consider as system state, whereas,  $u_k \in \mathbb{R}^m$  consider as the input of control. The observation of output will be in this equation  $\beta_k \in \{0, 1\}$  which represents the DoS attack that works as a sequence of packets.  $N_k$  is the process noise and  $w_k$  are independent based on normal desists  $\varphi \sim N(0, \Sigma)$  and  $\varphi \sim N(0, \Gamma)$  (Befekadu et al., 2011).

The consideration of exponential running cost includes a quadratic function for risk-sensitive based on control problem for DoS would be:

$$J(u) = \left(\frac{1}{\theta}\right) E \left[ \exp \left\{ \left(\frac{\theta}{2}\right) \left\{ \sum_{k=0}^{T-1} (x'_k M x_k + \beta_{k+1} u'_k N u_k) + x'_T M_T x_T \dots\dots\dots (4) \right. \right. \right.$$

As a typical example to find out the optimal control under the attack of DoS it could be as follows:

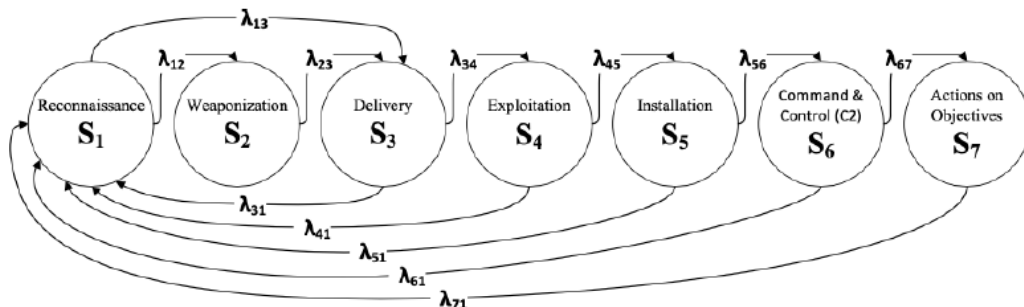
$$F_0 = \inf_{u \in U_{0,T-1}} J(u) = \inf_{u \in U_{0,T-1}} (1/\theta) \left[ \exp \left\{ (\theta/2) \left\{ \sum_{k=0}^{T-1} (x'_k M x_k + \beta_{k+1} u'_k N u_k) + x'_T M_T x_T \right\} \right\} \right]$$

Where to consider the main class of DoS attack as to Bernoulli packet fall because of jams on time  $k$  with probability  $\beta_k$  Within attack model  $ABer(\beta)$ :

$$\begin{aligned}
 A_{Ber(\beta)} = B_k &= \{\beta_0, \beta_1, \dots, \beta_T | P(\beta_k)\} = \bar{\beta} \\
 &k = 0,1 \dots, T\}
 \end{aligned}$$

**MARKOV MODEL**

A Markov chain can be defined as “is a stochastic model describing a sequence of possible events in which the probability of each event depends only on the state attained in the previous event. A countable infinite sequence, in which the chain moves state at discrete time steps, gives a discrete-time Markov chain (DTMC)” P.11 (Chasioti, 2020). This study has employed the Markov chain and other literature to explain the probabilistic of the cyber kill chain, which will be employed in the data analysis that focused on the risk assessment.



**FIGURE 1**  
**CYBER KILL CHAIN DIAGRAM SPACES (HOFFMANN, NAPIÓRKOWSKI, PROTASOWICKI, & STANIK, 2020)**

Figure 1 represents the diagram of the cyber kill chain and its sequential process where S refers to spaces  $S = \{S_1, S_2, \dots, S_7\}$ . The stochastic process in figure 1 is assumed as a behavior of cyber kill process where  $\{X(t), \geq 0\}$ , transaction rate assumed to be unchanged while Q transaction rate matrix is considered to be known:

$$\frac{d}{dt}P(t) = P(t).q$$

Where the equation represents the generation of Q matrix and initial condition:

$$P(0) = [P_1(0), \dots, P_7(0)]$$

$$P_k(t) = P\{X(t) = S_k, t \geq 0\} (k = 1, \dots, 7)$$

As the rate of generating matrix Q with process X(t) moves from space to space. This is defined as:

$$\lambda_{jk} = \lim_{\Delta t \rightarrow 0} \frac{P\{X(t + \Delta t) = k | X(t) = j\}}{\Delta t} \text{ for all } k \neq j, \text{ and } \lambda_{jj} = -\sum_{k \neq j}^7 \lambda_{jk} = -\sum_{k \neq j}^7 \lambda_{jk}$$

Risk (R) can be illustrated based on the below equation if we assume that  $A = \{A_1, A_2, \dots, A_7\}$ , the risk score represented as  $R(t) = P(t).A_T$

The matrix Q for the Markov model in process X(t) for cyber kill chain from S1, S2, to S7. The matrix will be as follows:

$$\begin{bmatrix} -\lambda_{11} & \lambda_{12} & \lambda_{13} & 0 & 0 & 0 & 0 \\ 0 & -\lambda_{22} & \lambda_{23} & 0 & 0 & 0 & 0 \\ \lambda_{31} & 0 & -\lambda_{33} & \lambda_{34} & 0 & 0 & 0 \\ \lambda_{41} & 0 & 0 & -\lambda_{44} & \lambda_{45} & 0 & 0 \\ \lambda_{51} & 0 & 0 & 0 & -\lambda_{55} & \lambda_{56} & 0 \\ \lambda_{61} & 0 & 0 & 0 & 0 & -\lambda_{66} & \lambda_{67} \\ \lambda_{71} & 0 & 0 & 0 & 0 & 0 & -\lambda_{77} \end{bmatrix}$$

Which presents the process of Q for the cyber kill chain process based on the Markov model.

### RESEARCH PROPOSITION

Developing a practical and theoretical framework that considers the effect of Covid-19 on cybersecurity based on the fieldwork and previous literature would help to explainate the relations of hacking with the Covid-19 pandemic as well as improve the security levels.

### RESEARCH METHODOLOGY AND MAIN RESULTS

This study used both qualitative and quantitative methodology for the data collection and analysis process. A total of 312 participants had successfully responded to the online survey. In addition, for qualitative data, 11 semi-structured interviews with experts in Cybersecurity have been conducted. Furthermore, an experimental method as a fieldwork technique has been employed through testing 5 servers, 16 laptops, and 14 desktops have been tested by the researcher after

taking full acceptance from their owner to make an anti-spam and anti-virus free test. The quantitative data results have been presented as frequencies, whereas qualitative data results were analyzed using *Nvivo* software. Table 1 presents the characteristics of participants in the survey, table 2 presents interviewee profiles coded with (Ix: I1-I16), and table 3 presents experimental method machines and testing results for Viruses and Spam after testing.

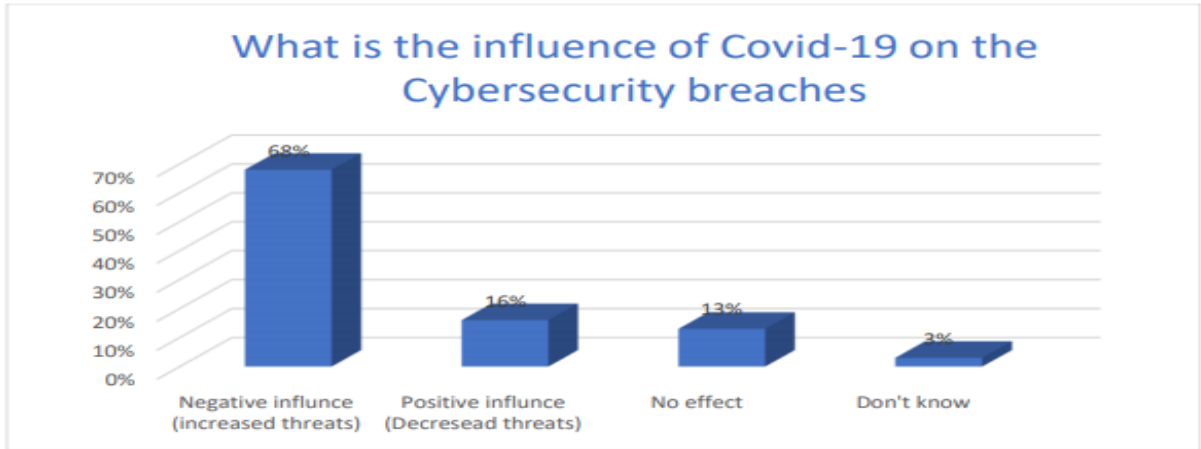
<b>Table 1 CHARACTERISTICS OF PARTICIPANTS IN THE ONLINE SURVEY</b>		
<b>Characteristics</b>	<b>Categories</b>	<b>Total (n=312) N (%)</b>
Gender	Male	173(55.44%)
	Female	139 (44.56%)
Governorate	North	97 (31.09%)
	Middle	192(61.54%)
	South	23 (07.37%)
Age (years)	18-30	189 (60.57%)
	31-45	77 (24.68%)
	46-60	29 (9.30%)
	>60	17 (5.45%)
Educational level	Secondary school or less	96 (30.77%)
	Diploma or bachelors	192 (61.54%)
	High education (Master or Ph.D.)	24 (7.69%)

<b>Table 2 INTERVIEWEE PROFILES</b>		
<b>S.No</b>	<b>Code</b>	<b>Interviewee professional profile</b>
1	I1, I2, and I3.	IT security manager, Professor in Cybersecurity, Assistant professor in Information Systems
2	I4, I5, and I6.	Project manager, senior technical engineer, and technical engineer.
3	I7, I8, and I9.	Assistant professor in Information Systems, Professor in computer science, associate professor in computer science
4	I10, I11, and I12.	Associate professor in digital marketing, professor in information security, assistant professor in management information systems.
5	I13, I14, I15, and I16.	Regional manager, financial manager, senior accountant, accountant.

<b>Machine type</b>	<b>Threat type</b>	<b>Threat level</b>	<b>User awareness</b>	<b>Threat reason</b>
Dell server PowerEdge 200	Malware	Medium risk	Not aware	Web-Mentoring software
Apple MacBook	Malware	Medium risk	Not aware	Free software from an unauthorized website
HP laptop	Trojan	High risk	Aware	Hidden application
HP Desktop	Bad boot sector	Medium risk	Aware	Hardware defect
Dell server	Worm	High risk	Aware	Firewall breach
IBM server	Virus	High risk	Aware	From untrusted website
Lenovo laptop	Trojan	Medium risk	Not aware	Free software installed

### **COVID-19 PANDEMIC HAS A NEGATIVE INFLUENCE ON CYBERSECURITY THREATS AND BREACHES**

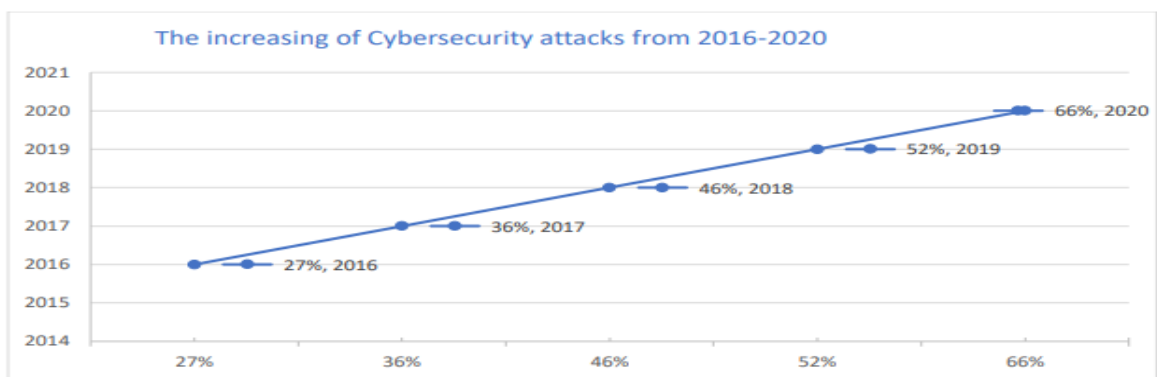
According to the previous literature in this study as well as the results, which support the literature the Covid-19 pandemic has dramatically increased threats of Cybersecurity. 68% of participants in this study strongly believed that Covid-19 has a negative influence on Cybersecurity as it was increased threats. Whereas, 16% of participants argued that the increase of Cybersecurity threats is normal because it already has a positive relationship with time. 13% of participants believed that there is no relation between Covid-19 and Cybersecurity threats and 3% have no answer. Figure 2 presents participants' results from this study according to the relation between the effect of Covid-19 and Cybersecurity breaches.



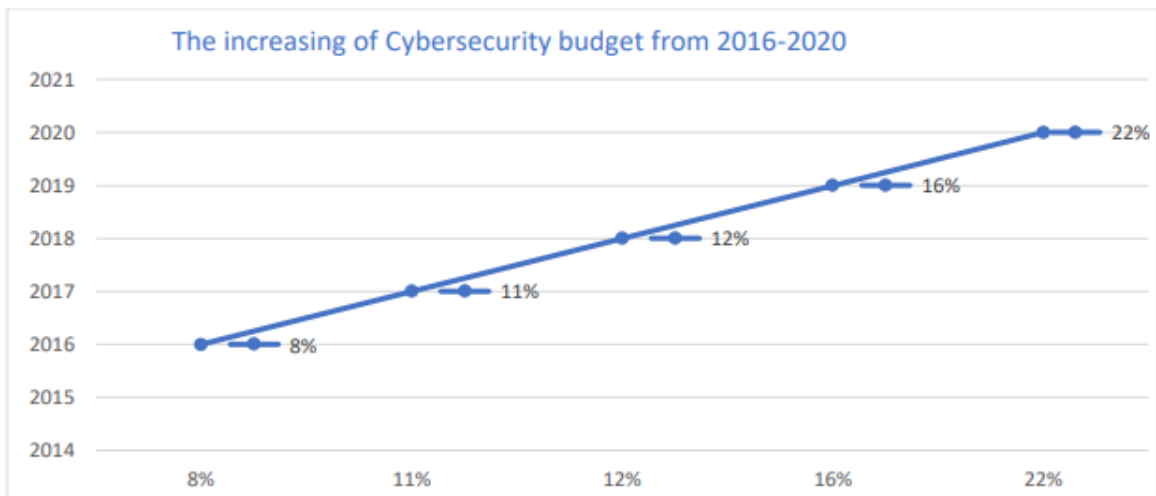
**FIGURE 2**  
**THE INFLUENCE OF COVID-19 ON THE CYBERSECURITY BREACHES**

An expert in Cybersecurity (Coded I3 in this study) from a large and well-known private institution, who participated in this study through semi-structured interview, stated that "According to our last data from our company research department, the Cybersecurity breaches increased dramatically for years 2016-2020. This considers as main concern and priority in our IT department. I will provide some facts with real numbers: in 2016 breaches increased to 27%, 2018 to 46%, 2019 to 52%, and 2020 to 66%. In my opinion, this is a disaster in Cybersecurity and we have to worry about it". Figure 3 summarized the statistical facts provided by participants I3 in the data collection process in this study through the semi-structured interview.

A financial manager (coded I4 in this study) from the same previous private institution added "We always increasing the financial budget for IT and Cybersecurity year after year. For example, we allocate 8% from our total budget in 2016, increased to 11% in 2017, 12% in 2018, and 16% in 2019, and the allocated budget in 2020 for IT and Cybersecurity jumped to 22%, our main problem is that we do not have any mathematical equation to calculate or even estimate the level of Cybersecurity program. It would be great if you could suggest one in your study!". Figure 4 summarized the statistical facts provided by participants I4 for the data collection process in this study through the semi-structured interview.



**FIGURE 3**  
**THE INCREASING OF CYBERSECURITY ATTACKS FROM 2016-2020**



**FIGURE 4**  
**THE INCREASING OF CYBERSECURITY BUDGET FROM 2016-2020**

According to the data provided by interviewees in this study as well as I4 participant suggestions, it could be argued that the Cybersecurity breaches have been increased from 2016-2020. In addition, we may use the following equation based on (Donaldson, Siegel, Williams, & Aslam, 2018) to explain the effectiveness of Cybersecurity systems for protecting against attack as follows:

$$\text{Risk migration index} = \frac{\sqrt{0^2+0^2+0^2+0.5^2+0^2+1^2+0.5^2+0.5^2+0.5^2+1^2}}{\sqrt{10}}$$

$$\frac{1.73}{3.16} = 0.55; \text{ Where number of attack sequence steps measurements}=10$$

$$\text{Functional area index} = \frac{\sqrt{0^2+0^2+0^2+0.5^2+0^2+1^2+0.5^2+0.5^2+0.5^2+1^2}}{\sqrt{10}} = \frac{1.73}{3.16} = 0.55; \text{ Where number of attack sequence steps measurements}=10$$

$$\text{Security index} = \frac{\sqrt{0^2+0^2+0.5^2+0.5^2+1^2+0.5^2+0.5^2+0.5^2+0.5^2+1^2+0.5^2+0.5^2+0.5^2+0.5^2+1^2+0.5^2+0.5^2+0.5^2+0.5^2+1^2+0.5^2}}{\sqrt{34}}$$

$$= \frac{3.32}{5.83} = 0.57; \text{ where the number of security operations elements}=34 \text{ Security index}$$

Cybersecurity systems for protecting weight factor

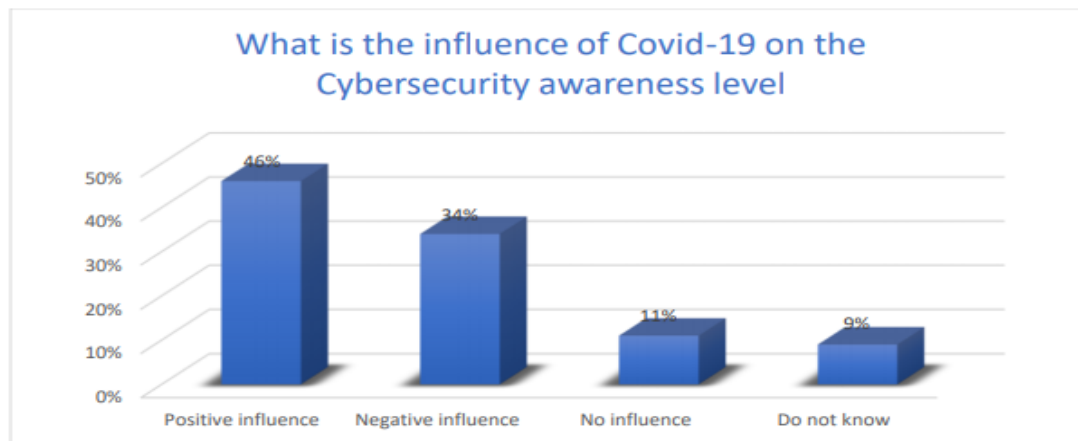
$$= \frac{\sqrt{0.55^2+0.70^2+0.57^2}}{\sqrt{3}} = \frac{1.11}{1.73} = 0.64; \text{ where the number of expert judgment indices}=3; \text{ all weighting factors}=1; \text{ all value scales range from 0 to1.}$$



Were risk migration index= 0.55, functional area index= 0.70, security index= 0.57, and it could be aggregated as a final Cyber security assessment index= 0.64 (value scale 0.0 to 1.0).

### **COVID-19 PANDEMIC HAS A POSITIVE INFLUENCE ON THE CYBERSECURITY AWARENESS**

An awareness of Cybersecurity is one of the most important factors that influence breaches and attacks of both individuals and institutions. According to the results from this study, the pandemic of Covid-19 has a positive influence on the awareness level. Awareness considers as one of the most important factors with other factors that could improve the level of dealing with information technology (Al-Ramahi & Odeh, 2020; Odeh & Yousef, 2021; Odeh, 2020; Odeh, 2019). Based on the survey results from this study Figure 5 shows 46% of participants believed that Covid-19 improves the awareness level in dealing with Cybersecurity issues, while 34% stated that there is a negative influence as users in general preferred to avoid using information technology in general as a solution to avoid hackers and Cyber-attack. 11% of participants cannot find any relation between Cybersecurity awareness and the Covid-19 pandemic. Finally, 9% of participants do not know if there is an exact relation between these factors.



**FIGURE 5**

### **THE INFLUENCE OF COVID-19 ON THE CYBERSECURITY AWARENESS LEVEL**

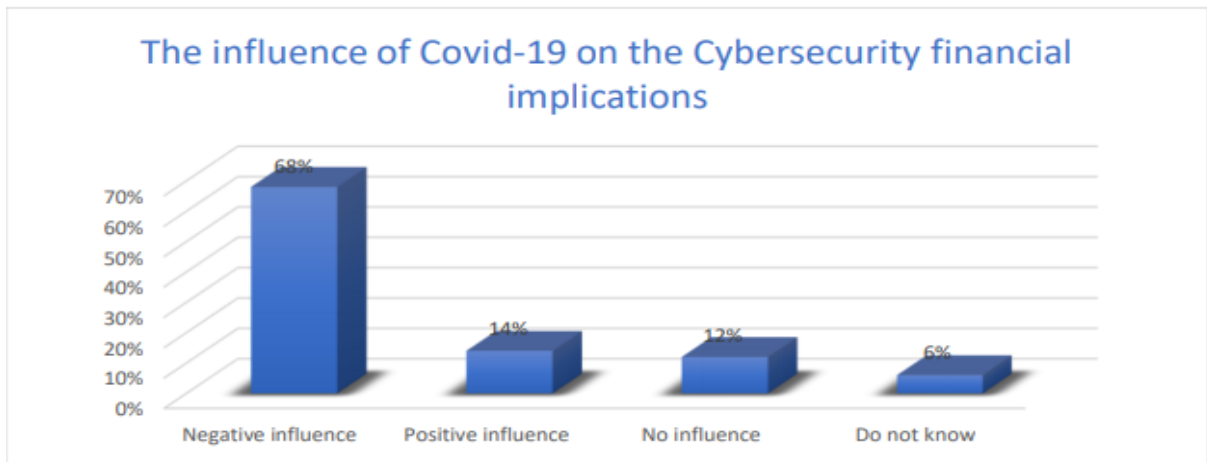
### **COVID-19 PANDEMIC HAS A NEGATIVE INFLUENCE ON THE CYBERSECURITY FINANCIAL IMPLICATIONS**

Based on the data collected from this study it could be argued that the cost of information systems usage is connected with several factors such as cyber-attack and downtime. In most cases, downtime is caused by a cyber-attack. In 2020-2021 most individuals, as well as institutions, have relied heavily on the internet because of Covid-19, which enforce remote working. Individuals who worked remotely from home have in most cases using their computers. Therefore, the level of security is infected, especially when companies enable the access of internal servers and databases through the internet using the intranet. The financial perspectives in this study could be summarized into two parts: the downtime cost and the increase of financial allocations to improve the Cybersecurity level. According to a professional annual report provided by one of the participants in this study for a well-known company working in flying reservations, the cost of downtime could be negatively influencing the financial perspectives. The report stated that the total cost of financial allocation for 2020-2021 was 2.6 million US dollars for the 100% working hours with zero

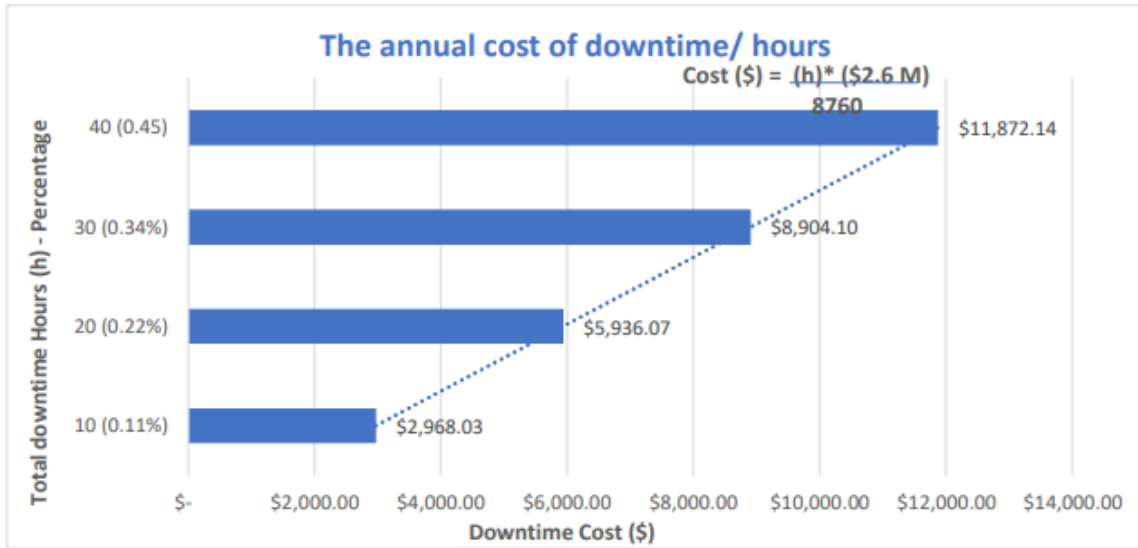
downtime during the year. However, the total downtime in 2020 was 44.06 hours. The following equations could summarize the total losses as follows:

- 100% system W/H → Downtime=0% (where, 365 days)..... (1)
- 365 days=365×24 W/H
- 365 days=8760 Hours (0% W/H, Downtime).
- 100% system W/H → 8760 H..... (2)
- When 33.4 H per year
- 0.38% system W/H → 33.4 H..... (3)
- \$2600000 → 8760 H..... (4)
- Down time cost = (33.4\*2600000\$)/8760
- Down time cost=\$9913.24..... (5)

According to the previous equation provided as a part of this study data reports, it could be argued that downtime may have a negative influence on the financial allocations. However, the survey shows that 68% of participants argued that Covid-19 has a negative influence on the Cybersecurity financial perspectives as it increasing the cost requires for downtime because of Cyber-attack as well as because of any other reasons which may cause a system failure. 14% of participants stated that it may have a positive influence, 12% believe that it has no influence, and 6% do not know. Figure 6 presents the influence of Covid-19 on the Cybersecurity financial implications from this study participants' view of point. Besides, based on the downtime equations, figure 7 shows the cost of downtime for 10 hours, 20 hours, 30 hours, and 40 hours with the percentage of such hours per year/total hours, where the financial allocation equals \$2.6 million.



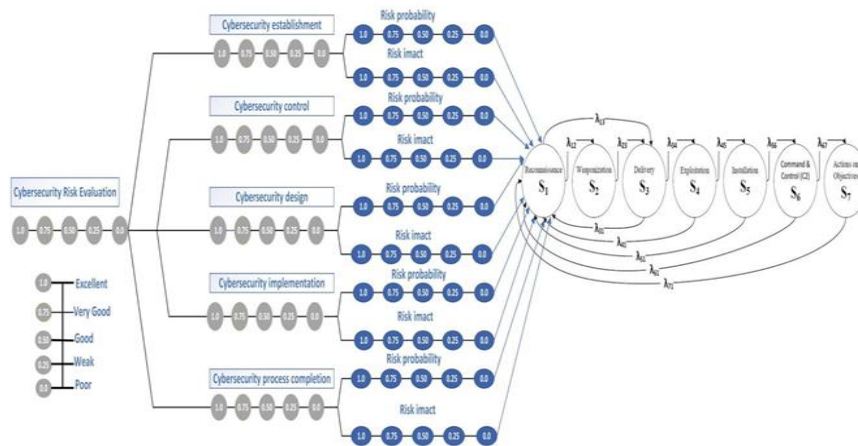
**FIGURE 6**  
**THE INFLUENCE OF COVID-19 ON THE CYBERSECURITY FINANCIAL IMPLICATIONS**



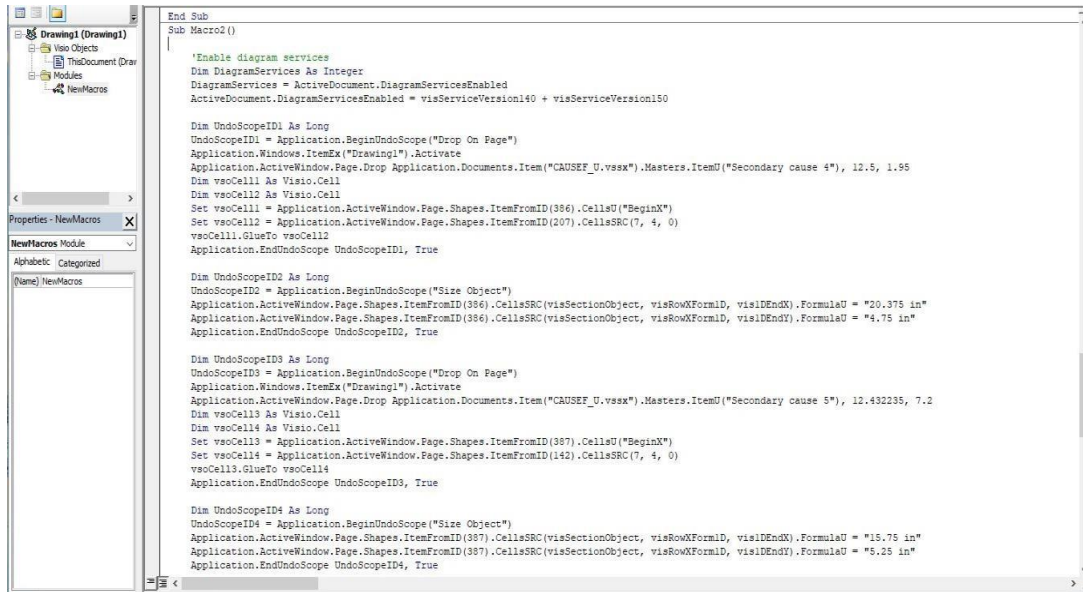
**FIGURE 7**  
**THE ANNUAL COST OF DOWNTIME/ HOURS**

**PROPOSED NOVEL CYBERSECURITY FRAMEWORK**

According to the previous data collection and analysis, and based on the theoretical foundation, this study proposes a practical and theoretical Cybersecurity framework. The framework focus on the risk evolution technique using the Markov chain model as a theoretical foundation as well as cyber-kill chain diagram spaces (Donaldson et al., 2018). Figure 8 represents the proposed Cybersecurity evaluation model. The risk level started from 0-1 to present the cybersecurity level from a poor-excellent level. The level of Cybersecurity then has connected with spaces to improve the Cybersecurity level, which: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objectives. Such improvement of Cybersecurity through spaces considers as a repetitive process to achieve an excellent level of protection. Figures 9 and 10 present a sample of the practical draw application for the framework.



**FIGURE 8**  
**CYBERSECURITY EVALUATION FRAMEWORK BASED ON THE THEORETICAL FOUNDATION OF THIS STUDY**



```
End Sub
Sub Macro2 ()

'Enable diagram services
Dim DiagramServices As Integer
DiagramServices = ActiveDocument.DiagramServicesEnabled
ActiveDocument.DiagramServicesEnabled = visServiceVersion140 + visServiceVersion150

Dim UndoScopeID1 As Long
UndoScopeID1 = Application.BeginUndoScope("Drop On Page")
Application.Windows.ItemEx("Drawing1").Activate
Application.ActiveWindow.Page.Drop Application.Documents.Item("CAUSEF_U_vssx").Masters.ItemU("Secondary cause 4"), 12.5, 1.95
Dim vsoCell1 As Visio.Cell
Set vsoCell1 = Application.ActiveWindow.Page.Shapes.ItemFromID(386).CellsU("BeginX")
Set vsoCell2 = Application.ActiveWindow.Page.Shapes.ItemFromID(207).CellsSRC(7, 4, 0)
vsoCell1.GlueTo vsoCell2
Application.EndUndoScope UndoScopeID1, True

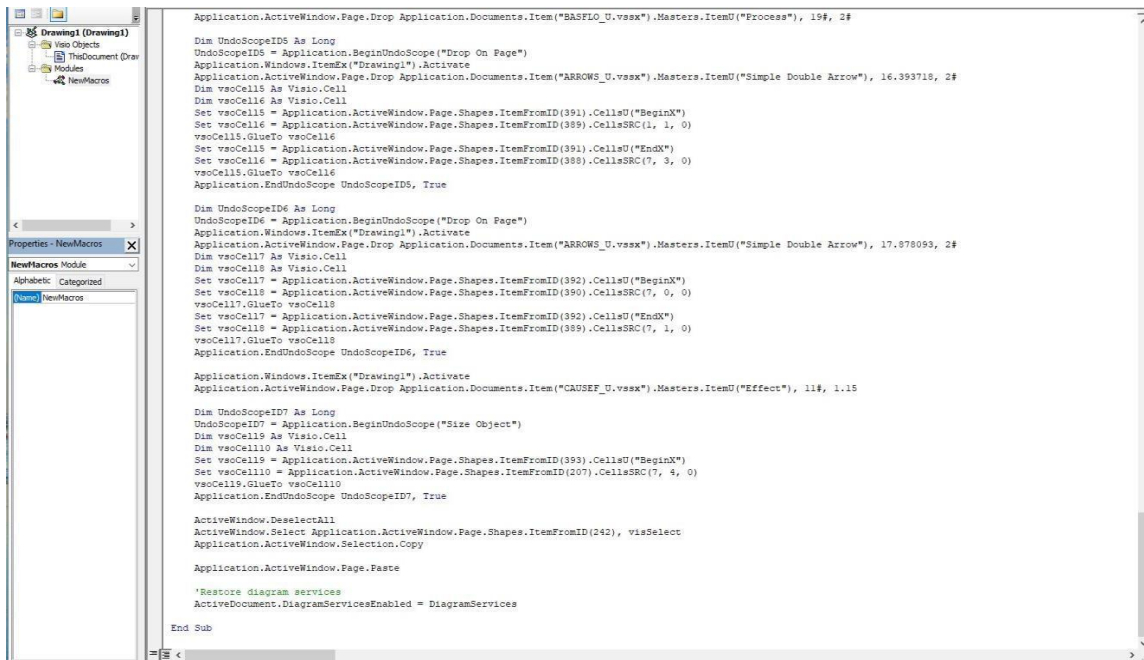
Dim UndoScopeID2 As Long
UndoScopeID2 = Application.BeginUndoScope("Size Object")
Application.ActiveWindow.Page.Shapes.ItemFromID(386).CellsSRC(visSectionObject, visRowFormID, visIDEndX).FormulaU = "20.375 in"
Application.ActiveWindow.Page.Shapes.ItemFromID(386).CellsSRC(visSectionObject, visRowFormID, visIDEndY).FormulaU = "4.75 in"
Application.EndUndoScope UndoScopeID2, True

Dim UndoScopeID3 As Long
UndoScopeID3 = Application.BeginUndoScope("Drop On Page")
Application.Windows.ItemEx("Drawing1").Activate
Application.ActiveWindow.Page.Drop Application.Documents.Item("CAUSEF_U_vssx").Masters.ItemU("Secondary cause 5"), 12.432235, 7.2
Dim vsoCell3 As Visio.Cell
Dim vsoCell4 As Visio.Cell
Set vsoCell3 = Application.ActiveWindow.Page.Shapes.ItemFromID(387).CellsU("BeginX")
Set vsoCell4 = Application.ActiveWindow.Page.Shapes.ItemFromID(142).CellsSRC(7, 4, 0)
vsoCell3.GlueTo vsoCell4
Application.EndUndoScope UndoScopeID3, True

Dim UndoScopeID4 As Long
UndoScopeID4 = Application.BeginUndoScope("Size Object")
Application.ActiveWindow.Page.Shapes.ItemFromID(387).CellsSRC(visSectionObject, visRowFormID, visIDEndX).FormulaU = "15.75 in"
Application.ActiveWindow.Page.Shapes.ItemFromID(387).CellsSRC(visSectionObject, visRowFormID, visIDEndY).FormulaU = "5.25 in"
Application.EndUndoScope UndoScopeID4, True

End Sub
```

**FIGURE 9**  
**CYBERSECURITY EVALUATION FRAMEWORK PRACTICAL CODING SAMPLE 1**



```
Application.ActiveWindow.Page.Drop Application.Documents.Item("BASFLIO_U_vssx").Masters.ItemU("Process"), 19#, 2#

Dim UndoScopeID5 As Long
UndoScopeID5 = Application.BeginUndoScope("Drop On Page")
Application.Windows.ItemEx("Drawing1").Activate
Application.ActiveWindow.Page.Drop Application.Documents.Item("ARROWS_U_vssx").Masters.ItemU("Simple Double Arrow"), 16.393718, 2#
Dim vsoCell5 As Visio.Cell
Dim vsoCell6 As Visio.Cell
Set vsoCell5 = Application.ActiveWindow.Page.Shapes.ItemFromID(391).CellsU("BeginX")
Set vsoCell6 = Application.ActiveWindow.Page.Shapes.ItemFromID(389).CellsSRC(1, 1, 0)
vsoCell5.GlueTo vsoCell6
Set vsoCell5 = Application.ActiveWindow.Page.Shapes.ItemFromID(391).CellsU("EndX")
Set vsoCell6 = Application.ActiveWindow.Page.Shapes.ItemFromID(389).CellsSRC(7, 3, 0)
vsoCell5.GlueTo vsoCell6
Application.EndUndoScope UndoScopeID5, True

Dim UndoScopeID6 As Long
UndoScopeID6 = Application.BeginUndoScope("Drop On Page")
Application.Windows.ItemEx("Drawing1").Activate
Application.ActiveWindow.Page.Drop Application.Documents.Item("ARROWS_U_vssx").Masters.ItemU("Simple Double Arrow"), 17.878093, 2#
Dim vsoCell7 As Visio.Cell
Dim vsoCell8 As Visio.Cell
Set vsoCell7 = Application.ActiveWindow.Page.Shapes.ItemFromID(392).CellsU("BeginX")
Set vsoCell8 = Application.ActiveWindow.Page.Shapes.ItemFromID(390).CellsSRC(7, 0, 0)
vsoCell7.GlueTo vsoCell8
Set vsoCell7 = Application.ActiveWindow.Page.Shapes.ItemFromID(392).CellsU("EndX")
Set vsoCell8 = Application.ActiveWindow.Page.Shapes.ItemFromID(389).CellsSRC(7, 1, 0)
vsoCell7.GlueTo vsoCell8
Application.EndUndoScope UndoScopeID6, True

Application.Windows.ItemEx("Drawing1").Activate
Application.ActiveWindow.Page.Drop Application.Documents.Item("CAUSEF_U_vssx").Masters.ItemU("Effect"), 11#, 1.15

Dim UndoScopeID7 As Long
UndoScopeID7 = Application.BeginUndoScope("Size Object")
Dim vsoCell9 As Visio.Cell
Dim vsoCell10 As Visio.Cell
Set vsoCell9 = Application.ActiveWindow.Page.Shapes.ItemFromID(393).CellsU("BeginX")
Set vsoCell10 = Application.ActiveWindow.Page.Shapes.ItemFromID(207).CellsSRC(7, 4, 0)
vsoCell9.GlueTo vsoCell10
Application.EndUndoScope UndoScopeID7, True

ActiveWindow.DeselectAll
ActiveWindow.Select Application.ActiveWindow.Page.Shapes.ItemFromID(242), visSelect
Application.ActiveWindow.Selection.Copy

Application.ActiveWindow.Page.Paste

'Restore diagram services
ActiveDocument.DiagramServicesEnabled = DiagramServices

End Sub
```

**FIGURE 10**  
**CYBERSECURITY EVALUATION FRAMEWORK PRACTICAL CODING SAMPLE 2**

**ACKNOWLEDGMENT**

This research is funded by the Deanship of Research at Zarqa University, Jordan.

## CONCLUSION

This study investigated the role of Covid-19 on Cybersecurity from a managerial and practical view of point. The study employed the Markov model and evaluation model as a theoretical foundation. On one hand, the study argued that the pandemic of Covid-19 has a positive influence on cybersecurity awareness. On the other hand, the study shows that Covid-19 has a negative influence on both Cybersecurity threats and financial implications. Both inductive deductive research approaches have been employed. Therefore, the study used mixed-mode qualitative and quantitative methodological approaches. At the end of the study, and based on the theoretical foundation as well as the data collection and analysis results, a proposed Cybersecurity framework has been developed to help in improving and evaluating the Cybersecurity level. The Novel framework covered both managerial and practical perspectives. Further testing of the proposed Cybersecurity framework is required for future research.

## REFERENCES

- Al-Ramahi, N., & Odeh, M. (2020). 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*, 10(11).
- Befekadu, G.K., Gupta, V., & Antsaklis, P.J. (2011). *Risk-sensitive control under a class of denial-of-service attack models*. Paper presented at the Proceedings of the 2011 American Control Conference, 643-648.
- Bissell, K., LaSalle, R., & Dal Cin, P. (2019). The cost of cybercrime: Ninth annual cost of cybercrime study unlocking the value of improved cybersecurity protection. *Accenture Security*.
- Carl, G., Kesidis, G., Brooks, R.R., & Rai, S. (2006). Denial-of-service attack-detection techniques. *IEEE Internet Computing*, 10(1), 82-89.
- Chasioti, E. (2020). *BARC0141: Built environment dissertation*.
- Dicker, W. (2021). *An examination of the role of vCISO in SMBs: An information security governance exploration*.
- Donaldson, S.E., Siegel, S.G., Williams, C.K., & Aslam, A. (2018). *Enterprise cybersecurity study guide: How to build a successful cyberdefense program against advanced threats*. Apress.
- Evans, K., Abuadba, A., Ahmed, M., Wu, T., Johnstone, M., & Nepal, S. (2021). *RAIDER: Reinforcement-aided spear phishing detector*. arXiv Preprint arXiv:2105.07582.
- Gisin, N., Fasel, S., Kraus, B., Zbinden, H., & Ribordy, G. (2006). Trojan-horse attacks on quantum-key-distribution systems. *Physical Review A*, 73(2), 022320.
- Hakan, A. (2018). A tool within the scope of security and process efficiency in Web applications: DEBSA. *Ataturk University Journal of Economics and Administrative Sciences*, 34(4), 1407-1430.
- Henneman, T. (2020). Beyond lip-synching: Experimenting with TikTok storytelling. *Teaching Journalism & Mass Communication*, 10(2), 1-14.
- Hoffmann, R., Napiórkowski, J., Protasowicki, T., & Stanik, J. (2020). Risk based approach in scope of cybersecurity threats and requirements. *Procedia Manufacturing*, 44, 655-662.
- Kesar, S. (2020). Smart cities bring new challenges in managing cybersecurity breaches. *Ethicomp 2020*, 147.
- McDaniel, D. (2019). *Data breaches: Who is behind them, why they do it, and how to protect your data david McDaniel East Carolina University*.
- Mishra, U. (2010). *An introduction to computer viruses*. Available at SSRN 1916631.
- Odeh, M., & Yousef, M. (2021). The effect of covid-19 on the electronic payment system: Usage level trust and competence perspectives. *Indonesian Journal of Electrical Engineering and Computer Science*, 1144-1155.
- Odeh, M. (2020). *A novel framework for the adoption of cloud computing in the higher education sector in developing countries*, 9(02), 5660-5667.
- Odeh, M.M. (2019). *A proposed theoretical solution for transferring from physical to virtual machines based on cloud computing*. Paper presented at the 2019 5th International Conference on Information Management (ICIM), 221-226.
- Schuckers, S.A. (2002). Spoofing and anti-spoofing measures. *Information Security Technical Report*, 7(4), 56-62.
- Scott-Hayward, S. (2021). Security-focused networks of the future. *Paper presented at the Proceedings of the 2021 ACM International Workshop on Software Defined Networks & Network Function Virtualization Security*, 1.

- Seaman, J., & Seaman, J. (2021). Developing your human firewall. *Protective Security: Creating Military-Grade Defenses for Your Digital Business*, 487-523.
- Sobers, R. (2021). 134 cybersecurity statistics and trends for 2021.
- Tripathi, S., Gupta, B., Almomani, A., Mishra, A., & Veluru, S. (2013). Hadoop based defense solution to handle Distributed Denial of Service (DDoS) attacks.