Cyber Security Attacks and Challenges in Saudi Arabia during COVID-19

Nourah Almrezeq[1†], Mamoona Humayun[1†], Madallah Alruwaili[2††], Saad Alanazi[2††], NZ Jhanjhi[3†††]
[1]Department of Information systems, College of Computer and Information Sciences, Jouf University
[2]College of Computer and Information Sciences, Jouf University, Saudi Arabia
[3]School of Computer Science and Engineering (SCE), Taylor's University, Malaysia
Corresponding author: Nourah Almerzeq (401205949@ju.edu.sa)

Abstract
The outbreak of COVID-19 had affected almost every part of the world and caused disastrous results, the number of reported COVID-19 cases in past few months have reached to more than 29 million patients in the world globally. This pandemic has adversely affected all the activities of life, ranging from personal life to overall economic development. Due to the current situation, routine***ly*** turned to online resources, and people have relied on technology more than they have been before. Since cybercriminals are an opportunist and they utilized this entirely, by targeting the online services for all sectors of life. This fortnight online dependency of the community over the internet opened several easy doors for the cybercriminals. This causes exponential attacks over internet traffic during this epidemic situation. The current Covid-19 pandemic situation appeared at once, and no one was ready to prevail this. However, there is an urgent need to address the current problem in all means. . KSA is among one of the countries most affected by these CA and is a key victim for most cyber-crimes. Therefore, this paper will review the effects of COVID-19 on the cyber-world of KSA in various sectors. We will also shed light on the Saudi efforts to confront these attacks during COVID -19. As a contribution, we have provided a comprehensive framework for mitigating cybersecurity challenges.

Keywords:
COVID- 19, Cybersecurity, Saudi Arabia, Cyber-Attacks. Pandemic Situation.

1. Introduction

COVID-19 is a pandemic that has surprised the world. The epidemic has succeeded in striking fears across countries and individuals across the globe [1]. Even though the epidemic started in China, other countries throughout the world, such as the KSA is having severe challenges in controlling the epidemic and its harmful impacts. Figure 1 presents the situations of COVID-19 in KSA; its statistics is taken from Worldometer [2]. In March 2020, the WHO stated it as a global pandemic due to its widespread around the world. Coronavirus pandemic has brought a change in perspective from the conventional workplace towards online mode. The vast majority of the services and different divisions of economy moved quickly towards online administrations and web networks because of the lock-down, social-separating and the conclusion of all administrations, for example, schools, legislative workplaces, privately owned businesses, parks, films, coffeehouses eateries and so forth [3]. The spread of the COVID-19 pandemic has affected many life activities around the world and restricted the world from performing their activities comfortably ranging from religious activities to entertainment, education, economy, travel, healthcare, tourism, business and social interactions [4].

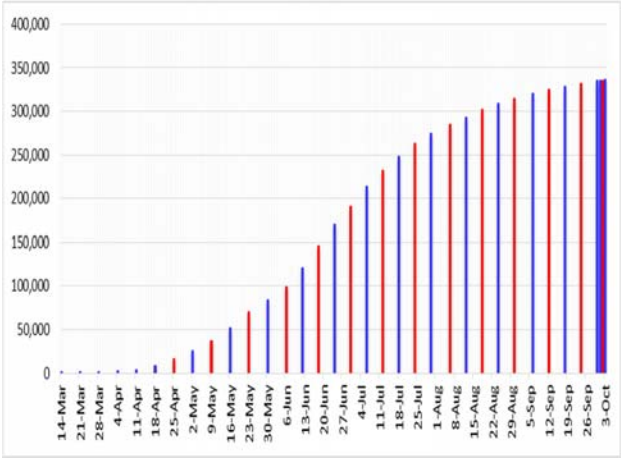

Fig. 1: COVID-19 cases in KSA during the last few months

COVID-19 emergency was stunning for the entire world, and it was hard to hold up under and adjust, as none of the nations was intellectually ready for it. Notwithstanding, an antagonistic impact of COVID-19 looked by KSA was quickly expanding cyber-crimes during COVID-19 period. Figure 2 provides a broad picture of cyberattacks during COVID-19. The insights which is distributed by Hackmageddon Information Security Timelines and Statistics [5] show that the crime percentage is high in 2020 when contrasted with earlier years.
COVID-19 continues spreading wherever all through the world, and cybercrime levels have been expanding with it [6][7]. Cybercriminals are misusing the COVID-19 pandemic and trying to delude individuals as well as organizations to acquire delicate information such as passwords, messages, and details of bank accounts[7][8].

Manuscript received October 5, 2023
Manuscript revised October 20, 2023
https://doi.org/10.22937/IJCSNS.2023.23.10.22

Subsequently, we have decided to explore key CA targeting KSA during COVID-19 along with its policies to confront these attacks. Based on analysis of existing data, we provide a framework that will guide IT users' in better understanding of the phenomenon and will be able to keep themselves safe from security breaches[4][9]

The reason of choosing KSA are manifold: First, during literature survey, it was analyzed that the KSA is one of the highest impacted counties in the Middle East due to the number of reported CA in most governmental agencies of the kingdom [3]. As per The Symantec's Internet Security threat report, KSA is the most elevated affected region in the Middle East and Africa in the field of information security[10][11]. Subsequently, COVID-19 pandemic is the most noticeably terrible time in the history of the KSA and the entire world also. CA, during this period, have caused significant financial loses for Saudi organizations and government agencies [12]. Cybercriminals had also launched Cyber-attack on ARAMCO (one of the well-known industry of KSA) in the past. They have also launched CA on Saudi entertainment authority as well [14] [15] there is a need to educate the people of the kingdom and provide them with awareness about security breaches [13]. To fill this gap and as a contribution to research, we will explore all cyber-crimes and challenges faced by the people of KSA. In this exploration, we examine the key potential difficulties that are faced by the Saudi public and private segment concerning Cybersecurity attacks during COVID-19. We shed light on the Saudi endeavours to face these assaults during and will sum-up our work by providing a comprehensive framework for detecting and mitigating these CA attacks

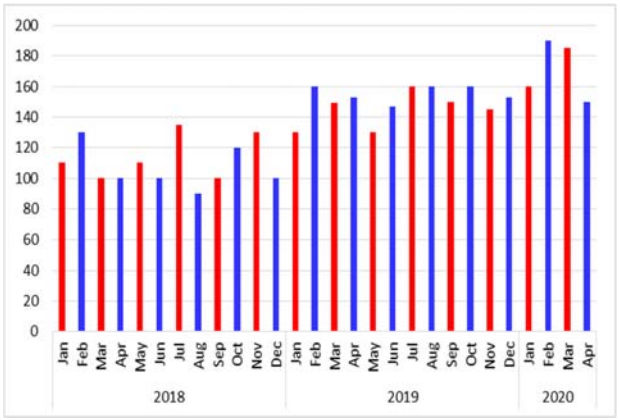

Fig. 2: Cyber-attacks during COVID-19 worldwide

The organization of the remaining paper is as follows: Section 2 review and discuss related works and challenges of Cybersecurity during COVID19 followed by security issues faced by KSA during COVID-19. The third section provides an overview of the current situation and an analysis of existing data. Section 4 discusses the results. Finally, Section 5 concludes our work by providing directions for future work.

Table 1: Acronym and specifications

Acronym	***Abbreviations***
COVID-19	Coronavirus 2019
WHO	World health organization
CA	Cyber-attacks
KSA	Kingdom of Saudi Arabia
CS	Cybersecurity
SOC	Security Operations Center
ITC	Information Technology and Computing
KPMG	Klynveld Peat Marwick Goerdeler

2. Literature Review

The spread of the COVID-19 radically influencing everything and is considered as an extraordinary move for everybody. Therefore, numerous organizations, foundations, and government sectors have been affected, and it will also keep on influencing the public activities and distinctive segments unless the problems is fully resolved. Due to the rapid spread of COVID-19 in the KSA, the kingdom has taken bold steps and implemented strong restrictions. There have been many challenges such as religious, political, economic, social, and educational etc. The government and health authorities imposed many measures to confront this pandemic. These procedures include Social distancing, lock-down, closure of two holy mosques for performing Umrah etc. A lot of important events were also shifted to online mode [15]. From last couple of months, work from the home strategy is adopted by various organizations, educational sector, especially at the primary level is shifted to the online mode of learning [16].

Toward the start of 2020, it was the pinnacle of the spread of the COVID-19. During this period, there was a developing enthusiasm of cybercriminals in abusing the worldwide frenzy of this pestilence by spreading their malware. ITC's SOC uncovered the security dangers that are abusing the distraction of the medical care segment to spread digital assaults. Cybersecurity or Network safety is a significant worry for each country. Subsequently part of exploration is going on in this field. In most countries, the novel COVID-19 spread so rapidly that people's fear and anxiety led them to search the internet engines for online information related to the term "COVID-19" and thereby to capture the attention of internet and website users. As a consequence, cybercriminals manipulate the fear and anxiety of the outbreak of COVID-19 to fraud people. Kenneth and Olajide [17] show the effects of COVID-19 on user privacy and security, along with useful recommendations.

During the COVID-19 crisis, the transition of employees to work remotely around the world needs a high level of knowledge of CA and ignorance of fake websites that mislead users when searching for COVID-19 information. Therefore, this study emphasizes that institutions and companies must protect their employees and educate them about the current CA that is expected to get double by the end of 2020 [18]. Most of the persons who use the internet are not aware of the risk and threats related to cybercrime and cybersecurity. The majority of the participants in the study preferred to have an application to provide them with the required information on security awareness. The results of the research show that the cybercrime index is on the rise [19].

During the COVID-19 pandemic, this paper [20] also focuses on researching cybersecurity threats and how these CA have evolved through different epidemics. It also guides cyber-attack defense. The growth of COVID-19 on cybersecurity in the public sector, the economy and the business sector is highlighted. This paper also focused on the cybersecurity education aspect, since the main reason for it is lack of learning and knowledge, so education is often the best approach to reduce these attacks.

Owing to the lockdown and closing of schools and colleges, there has been a need for e-learning. The critical problems hindered by e-learning systems were addressed in this study [4]. It discusses the key factors helping and promoting the use of the e-learning system during the COVID-19 pandemic by conducting data from Saudi society interviews. The findings of this study include valuable guidance for categories such as designers, policy-makers, developers and researchers, which will enable them to gain deeper knowledge and experience of the fundamentals of the use of the e-learning system effectively during the COVID-19 pandemic.

In the Corona era, technology and digital transformation were used in many sectors, such as education, commerce, governance, and health. Further, this pandemic had a positive effect on technology, as many IT solutions were created during this time for different sectors of life. On the other hand, there is a negative effect as a result of this growth that has increased cybersecurity threats. In this article, it explained that through the NIST System, which is commonly used to handle cybersecurity threats, organizations can respond to CA and threats. [21].

During the COVID-19 period, CA are on the rise, as 3 to 4 attacks daily are recorded. This paper presents a series of common attacks during COVID-19. The population of the United Kingdom was used to research the cases and to classify the CA during the COVID-19. Several CA were addressed in this study which includes Phishing, fake emails, DOS, etc. The research statistics also showed that 14% of the attacks target the United Kingdom, while 66% of the attacks targeted other countries [22].

KSA is one of the fastest and most developed countries in terms of communications and information technology; therefore, it is the country that is most targeted by cybercriminals. This paper discussed cybersecurity challenges in the Middle East, with a focus on explaining some cases of attacks in KSA as well [23].

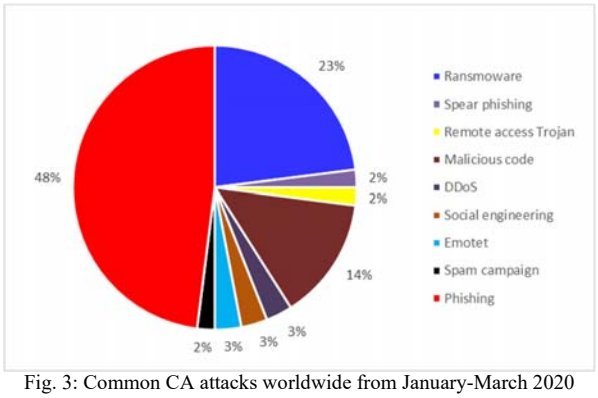

Fig. 3: Common CA attacks worldwide from January-March 2020

The above discussion demonstrates that CA, particularly during the COVID-19 era, are a key challenge facing the world as a whole. In addition, the literature indicates that KSA is a primary target of CA. Therefore, before proceeding towards a solution, there is a need to study the impact of COVID-19 on Saudi cyberspace by providing the details of security issues and challenges faced during this period by providing CA overview on targeting key sectors of the economy along with some mitigation and prevention strategies. Figure 3 shows an overview of common attacks that occurred from January to March in the world during COVID-19[24] to provide an overview of cybersecurity threats to readers.

3. Cyber-Security challenges

By leveraging the world's concern with this pandemic and the dependency of different industries on online working methods, this poses a great risk, which gives cybercriminals an incentive to increase CA and improve their technologies. CA during COVID-19 can be said to be one of the greatest cybersecurity threats ever [25]. In the long run, data loss and cybercrime can have a negative effect on the economies of countries. It is therefore important to pay attention to cybersecurity as well as other issues affecting the economy and growth of countries. Since the first cases of COVID-19 emerged, by deceiving users and sending preventative instructions against COVID-19, there has been a significant rise in attacks such as malware. Sites pretending to be sites for COVID-19 details, which are fake data-stealing sites, have also increased. From the beginning of January 2020 to March [17] [26], more than 136,000 new domains linked to COVID-19 have emerged.

Table 2: Summary of literature Review

Date	paper	Target	Cyber-attacks	Ways to protect against attacks
January 2020	Harjinder et Al..2020	CA challenges in UK during covid-19	Hacking , malware , Dos, financial fraud, phishing, pharming, extortion	Not mentioned
February 20202	Kenneth and Olajide 2020)	CA challenges during COVID-19.	Malicious software, social engineering, Phishing and spam, Fake websites and online portals.	1. Test websites before payments. 2. Vigilance with the use of spam mail. 3. Fine-tune digital readiness. 4. Install anti-malware software. 5. Cyber awareness. 6. Avoid questionable web and URLs. 7. backup 6. Verify information source. 9. Avoid suspicious attachments.
March 2020	Yezli and Khan 2020	Political, economic, social and religious challenges in Saudi during covid-19.	Not mentioned	Not mentioned
March 2020	Francois and Coning 2020	CA threat during COVID-19	Phishing , Fake URLs , Physical Attacks , Preying on the good of people , Spreading Personal Agendas , Spreading Misinformation , Malicious Websites , Upcoming Attacks.	1. Use the right map to COVID-19. 2. Check before downloading anything. 3. Before donate make sure the right place. 4. Test any URL or email address. 5-Make sure before open shortened links. 6-Be aware of fake emails asking for confidential information. 7-Download program and files from trusted websites.
April 2020	Tabrez 2020	Home-working people Institutions security challenges	ransomware attacks, insecure remote access to corporate networks, unauthorized user, banking trojan malware, phishing	1.Enable multi-factor authentication 2.use VPN 3.update CA policy 4. Use IT equipment 5.provided by employers. 5. Don't use personal devices to access the work network.
May 2020	Almaiah and et Al..2020	E-learning systems challenges.	Not mentioned	Not mentioned
May 2020	Tim and San 2020	mitigation and response CA during COVID-19	ZOOM bombing , Spyware and phishing , Malware, Health check—ISPs, cloud providers, UCaaS during pandemic	1. Securing remote access. 2. Mitigating from fraud and malware threats. 3. Assessing new suppliers. 4.protecting core information system 5. Rebuild security program priorities, architectures, and budgets. 5. Managing work force morale.
May 2020	A. AlZain et Al..2020	the challenges of cybercrime in the Middle East	Spam , Worms , Sniffer , Phishing , Denial of service attack , Virus Dissemination , Cyber Stalking , Password Attacks	Not mentioned

Cybersecurity Ventures' annual report says that the world's fear of this pandemic causes them to continuously visit questionable websites that have a connection with COVID-19 without knowledge. Many web-sites claim to be the WHO have also increased [18]. Data from 'Arab News' shows that, despite KSA's prosperity in remote work during this time, 73 percent of employees did not receive cybersecurity-related instructions [27]. KSA is a primary target and is of high importance to cybercriminals. According to a cybersecurity expert, there are two explanations for KSA's increase in CA: one is KSA's growth in digital transformation, and the other reason is the role of KSA in the oil and energy sectors [28]. Among these attacks, KSA reported 344 attacks during COVID-19. 266 were spam, 17 were fake URLs, and 59 were malware threats. KSA is the country most affected by the number of phishing attacks among the Gulf Cooperation Council countries in 2020[29], according to a Kaspersky survey, with millions of CAs appearing in KSA. Criminals use the actual situation and circumstances to construct e-mail phishing messages, such as: an e-mail containing the shipment's warehouse that was delayed due to these circumstances. Another type of Phishing, which is bank phishing, has also spread at this time, it is for deceiving people by offering various amounts and incentives due to the epidemic to credit institution customers. Below we discuss those sectors of the economy which were mainly affected by CA during COVID-19.

Business Sector

The 2020 Ministry of Communications and Information Technology report clarified that 96 percent of Saudi businesses are threatened by CA and could not deal with it on time [30]. The reason for the increase in CA is the lack of commitment to daily backups, as about 30 percent of KSA businesses do not perform backups through which data can be restored. Tenable also announced that over 95 percent of companies in KSA had been subjected to CA in recent months. Their companies have been adversely impacted by this attack [46]. One of the proposals under Vision 2030 is the defense of KSA from CA. In the background of the COVID-19 crisis, the Saudis also demonstrated their efforts by offering remote workshops and competitions such as Cyber Night in May [32]. By highlighting the risks faced by government and cyberspace firms, the CEO of Saudi Aramco calls for more participation and cooperation in the field of cybersecurity [27]. Many staff in businesses and organizations use insecure networks outside the company, which raises the risk of electronic attacks due to the incompetence of their employees. The KPMG website warns businesses that cybercriminals are using COVID-19 to increase CA. As KPMG noticed a rise in malware, and as a result, it reported that businesses need to make strict decisions regarding CA and informed people about online security work. [33]. Figure 4 shows the most recent CA that pose a threat to the businesses sector in KSA Among Saudi businesses and organizations, 59% were exposed to a cyber-attack that could have a negative effect on business[34]. Ransomware has the highest level of occurrence among the main CA, and this poses a danger to the integrity of large and small businesses and threatens their continuity of business [47].

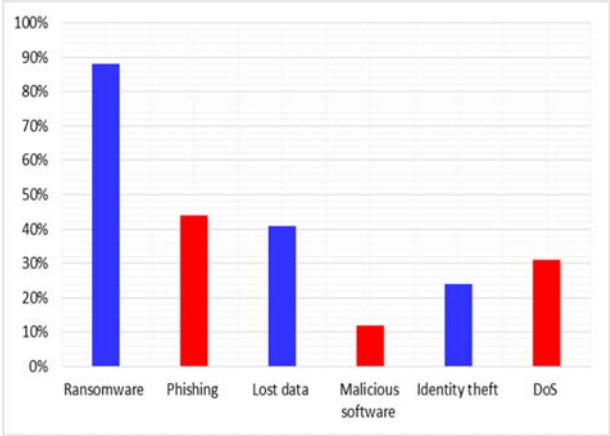

Fig. 4: Common security attacks targeting business sector during COVID-19

Education sector

It was shown during the literature survey that electronic attacks endanger students significantly who research online. KSA focuses on providing awareness regarding CA to pupils, teachers, and university students. Educational leaflets to guard against CA in online education were also released by the Saudi CA Authority [32]. Students 'reliance on electronic devices and e-learning systems make them more vulnerable to CA. Access to the Madrasati public education website has been blocked for two days, suggesting that this sort of website is still vulnerable to denial of service attacks. KSA online education concentrate on e-learning platforms which can be accessed via the Internet and internet is full of cyber threats, so education and knowledge face the threats of social engineering and phishing, should be avoided by students and educators. [31]. For example, Publishing links that pretend to be e-learning links or exchanging student ratings, or text messages that appear from ministries of education, while the attachments have fake links. This report notes that the success of education protection depends to a large extent on teachers' cooperation in educating their students against these attacks. The most recent CA that poses a threat to the education sector in KSA is shown in figure 5. Popular attacks targeting government agencies and the education sector over the past 12 months are provided in Figure 5[32], according to a study by the Saudi Authorities for CA. Paloalto Network Report [36], reported data on malicious

sessions, and it can be inferred that malicious software is a widespread attack affecting the education sector.

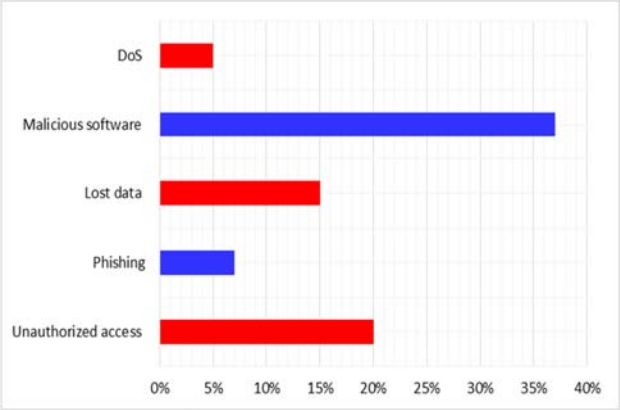

Fig. 5: Common CA attacks on education sector during COVID-19

Health sector

A group of malicious threats is directed at health care facilities and workers. The WHO reported that due to the concern of employees in the current situation, the CA of health sector employees will increase 5 times than before. In April 2020, a cyber-attack led to the company leaking 250 million email addresses and passwords. In addition, for fundraising, fake e-mails were also sent. An online agreement between the Council of Cooperative Health Insurance and the Saudi Authority for CA, Programming and Drones was signed in May to increase the capabilities of platforms in the health sector and protect them from CA [37] by creating a strategy to tackle these attacks and educate staff against these attacks since the losses occurred. Leakage of this patient-specific data may lead to heavy losses. According to the Panda Protection Survey, CA's health and financial sectors are among the most affected sectors in 2020 due to COVID-19[25]. In the health sector, the expense of security breaches has reached more than 7 million [38]. Like education, malicious software is the sector with the most attacks on the healthcare sector [36].

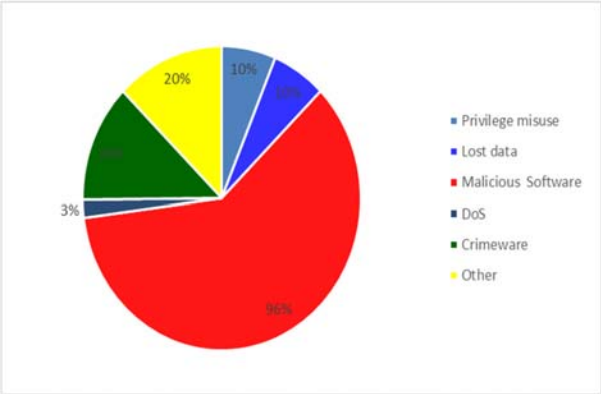

Fig. 6: Common CA attacks on health sector during COVID-19

Financial sector

The financial sector is considered one of the most critical sectors in which, due to its significance for the continuity of services such as banking services and the integrity of banks, protection needs to be accomplished in an optimal manner. The financial sector is one of the industries most impacted by CA [25] [39] due to financial rewards. In addition to the health sector and the oil sector, the financial sector is a targeted sector in Arab countries. According to a study published by the Arab Monetary Fund, Phishing and social engineering attacks, manipulating individuals working in financial institutions, identity theft, denial of service attacks and malware are the most common attacks in the financial sector [40]. Many of the breaches of security come from web apps. Internal errors and misuse of employees equally lead to cyber threats as well as external attacks. Figure 7 shows that malicious software is the biggest attack that affects the financial sector [36]. Kaspersky also reported that bank phishing attacks were mainly populated by e-mail, by deceiving the client or offering rewards and financial benefits, as these attacks increased significantly in the second quarter of 2020[41]. Kaspersky also added in its report that KSA users are more affected by phishing attacks than any other Arab country.

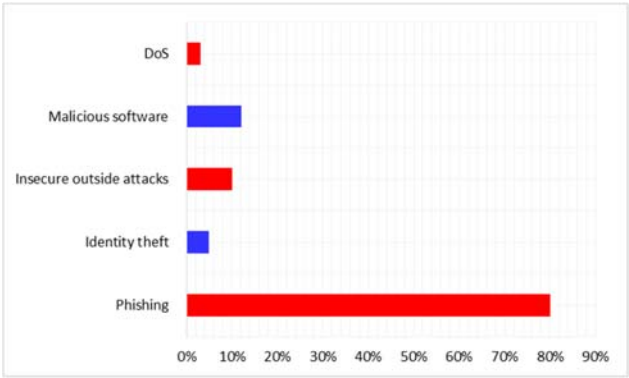

Fig. 7: Common CA attacks on financial sector during COVID-19

4. Analysis and Results

According to Saudi Gazette[42], as shown in Figure 6, the number of CAs has risen in the past few months. This indicates that offenders have taken advantage of the current pandemic situation and have used internet web portals and resources to conduct regular work activities excessively. Its good financial position and favorable world ranking are one of the main reasons for rising CA in KSA. KSA is one of the countries that has handled this pandemic in the best way and rapidly adapted the online mode to reduce delays in daily work activities [43]. KSA's high income made it a good and an ideal target for all cybercriminals, besides financial ranking is another main factor [44].

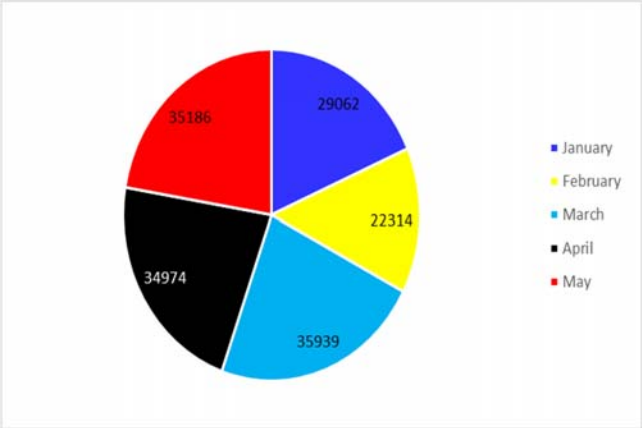

Fig.8. Common CA attacks on KSA during COVID-19

CA continues to develop, and KSA's key and ongoing challenge is how to protect both its public and private sectors from these attacks, especially during the COVID-19 pandemic, as most of these sectors are currently relying on online operations. The current data related to CA during COVID-19 was gathered and analyzed during this research to study the magnitude of the effect of these attacks on different Saudi sectors and to explore the most significant factors that triggered the rise in these attacks during this period . The key explanation for the increased attacks is the vulnerability of the infrastructure of the systems, according to previous studies that list the security challenges in KSA, Verification of system infrastructure in various sectors, such as hospitals, communication networks, petroleum terminals and institutions, is inevitable. Any fault in the infrastructure of these systems will, therefore, cause unforeseen severe damage and severe losses to the state. In addition to several attacks on the ministries of labor, social progress, media, information technology and transport, the Shamoun assault on Aramco is one of the most recent examples of these attacks [45]. It is a noble objective to achieve the protection of these infrastructures, which may restrict and decrease CA. Further efforts are needed after the COVID-19 pandemic to increase cyber resilience and enhance infrastructure security [35]. The use of different security methods in addition to the infrastructure helps to safeguard devices on a personal and functional level, and the most important of these methods are as follows.

- Install anti-virus programs to protect computers and mobile devices.
- Downloads programs from trusted resources
- Make sure of the links before opening that they are from reliable resources
- Don't open suspicious e-mail attachments, until you know the source of sender.
- Update mobile devices and computer programs
- Ensure that the Firewall is activated
- Do not connect to open networks
- Use complicated passwords that are difficult to predict
- Activate the two-factor authentication

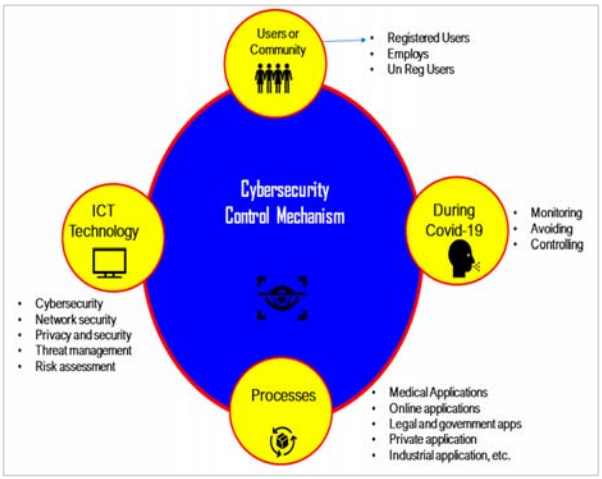

Fig.7. Cybersecurity Framework for COVID-19 pandemic

Many workers of organizations and businesses do not know the magnitude of the value of these security ways and what damages are incurred by non-compliance with these ways. Therefore, organizations in the private and public sector must develop a set of policies that employees must obey to protect devices and data relevant to the institution. Finally, without a person's security knowledge of CA, all of these security factors do not achieve maximum protection, so all of these factors are complementary to each other in order to minimize and eradicate these attacks, and ignoring one factor may allow criminals to spread their CA.

5. Conclusion

Technology has advanced, and the internet revolution has been coupled with an increase in CA, especially with the COVID-19 pandemic, and with all sectors relying on personal or work-level technology. Cybercriminals use the fear of people to trick them and fulfill their malicious intentions. There has been a noticeable increase in these attacks following a comprehensive study of CA in KSA during COVID-19, so if these CA are not controlled and with the best measures, they will adversely affect the state economy, because the weakness of the services provided and the loss of public confidence. There is an urgent need to research the effect, especially in KSA, of the increase in CA during COVID-19. The CA challenges faced by KSA during COVID-19 in the public and private sectors were analyzed in this paper and explained the Saudi attempts to confront these attacks. This paper recommends the most significant interrelated factors to be followed in order to increase the level of protection and to react to limit

the rise in these attacks. Finally, we end with a structure for the avoidance and elimination of CA from different industries.

References

[1] Khan, N. A., Brohi, S. N., & Zaman, N. (2020). Ten Deadly Cyber Security Threats Amid COVID-19 Pandemic.

[2] Saudi Arabia Coronavirus: 337,243 Cases and 4,923 Deaths - Worldometer. (2020). Retrieved 2 October 2020, from https://www.worldometers.info/coronavirus/country/saudi-arabia/

[3] Alkhamees, A. A., Alrashed, S. A., Alzunaydi, A. A., Almohimeed, A. S., & Aljohani, M. S. (2020). The psychological impact of COVID-19 pandemic on the general population of Saudi Arabia. Comprehensive psychiatry, 102, 152192.

[4] Mamoona Humayun. "Blockchain-Based secure framework for e-learning during COVID-19." Indian journal of science and technology 13, no. 12 (2020): 1328-1341.

[5] Lallie, Harjinder Singh, Lynsay A. Shepherd, Jason RC Nurse, Arnau Erola, Gregory Epiphaniou, Carsten Maple, and Xavier Bellekens. "Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic." arXiv preprint arXiv: 2006.11929 (2020).

[6] Alqurashi, R., 2020. Cyber Attacks and Impacts: A Case Study in Saudi Arabia. International Journal of Advanced Trends in Computer Science and Engineering, 9(1), pp.217-224.

[7] Computer Fraud & Security, 2020. Attacks on hospitals increase as criminals exploit pandemic. 2020(4), pp.1-3.

[8] Humayun, M., Niazi, M., Jhanjhi, N. Z., Alshayeb, M., & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study. Arabian Journal for Science and Engineering, 1-19.

[9] Alarifi, A., Tootell, H. and Hyland, P., 2012. A study of information security awareness and practices in Saudi Arabia. International Conference on Communications and Information Technology.

[10] Al Amro, S., 2017. Cybercrime in Saudi Arabia: fact or fiction?. International Journal of Computer Science Issues (IJCSI), 14(2), p.36.

[11] Ebrahim, S., Ahmed, Q., Gozzer, E., Schlagenhauf, P. and Memish, Z., 2020. Covid-19 and community mitigation strategies in a pandemic. BMJ, p.m1066.

[12] Onyema, E., Eucheria, N., Obafemi, a., Sen, S., Atonye, F., Sharma, A. and Omar Alsayed, A., 2020. Impact of Coronavirus Pandemic on Education. International knowledge sharing platform,.

[13] Sabillon, R., Serra-Ruiz, J., & Cavaller, V. (2019). An effective cybersecurity training model to support an organizational awareness program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. Journal of Cases on Information Technology (JCIT), 21(3), 26-39.

[14] Bronk, C. and Tikk-Ringas, E., 2013. The Cyber Attack on Saudi Aramco. Survival, 55(2), pp.81-96.

[15] Elnaim, B. M. E. (2013, December). Cybercrime in Kingdom of Saudi Arabia: The threat today and the expected future. In Information and Knowledge Management (Vol. 3, No. 12, pp. 14-19).

[16] Brohi, Sarfraz Nawaz; Jhanjhi, NZ; Brohi, Nida Nawaz; Brohi, Muhammad Nawaz (2020): Key Applications of State-of-the-Art Technologies to Mitigate and Eliminate COVID-19. TechRxiv. Preprint. https://doi.org/10.36227/techrxiv.12115596.v2

[17] Okereafor, K. and Adebola, O., 2020. Tackling the cybersecurity impacts of the coronavirus outbreak as a challenge to internet safety. International journal in IT & Engineering, 8(2).

[18] Ahmad, T., 2020. Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. SSRN Electronic Journal.

[19] Alotaibi, F., FurnellIngo, S., Stengel, I. and Papadaki, M., 2020. A survey of cyber-security awareness in Saudi Arabia. 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST).

[20] Mouton, F. and Coning, A., 2020. COVID-19: Impact on the Cyber Security Threat Landscape. : Social Engineering: Defining the field from both an Attack and Defence Perspective.

[21] Weil, T. and Murugesan, S., 2020. IT Risk and Resilience—Cybersecurity Response to COVID-19. IT Professional, 22(3), pp.4-10.

[22] Singh Lallie, H., A. Shepherd, L., R. C. Nurse, J., Erola, A., Epiphaniou, G., Maple, C. and Bellekens, X., 2020. Cyber Security in the Age of COVID-19: A Timeline and Analysis of Cyber-Crime and Cyber-Attacks during the Pandemic.

[23] Alqurashi, R. K., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. (2020). Cyber Attacks and Impacts: A Case Study in Saudi Arabia. International Journal, 9(1).

[24] Mc Ewan, K. A. (2020). Cyber-threats as Political Risk: Increased Risk for the Oil and Gas Industry.

[25] Panda Security Mediacenter. 2020. 43 COVID-19 Cybersecurity Statistics - Panda Security Mediacenter. [Online] Available at: <https://www.pandasecurity.com/mediacenter/news/covid-cybersecurity-statistics/#covid> [Accessed 21 September 2020].

[26] Alzahrani, A. A. The Extent to which Individuals in Saudi Arabia are subjected to Cyber-Attacks and Countermeasures.

[27] Arab News. 2020. Employees Lack Cyber Protection Amid Working From Home Boom. [online] Available at: <https://arab.news/w6nja> [Accessed 3 August 2020].

[28] Alriyadhdaily.com. 2020. Riyadh Daily. [online] Available at: <http://alriyadhdaily.com/article/a7f7ccd7390344aaaac5c5e2b04d82f3> [Accessed 23 September 2020].

[29] Ndichu, D., 2020. Saudi Arabia Led GCC In Number Of Phishing Attacks In Q2: Kaspersky Report. [Online] Gulf Business. Available at: <https://gulfbusiness.com/saudi-arabia-led-gcc-in-number-of-phishing-attacks-in-q2-kaspersky-report> [Accessed 17 September 2020].

[30] Mcit.gov.sa. 2020. Cyber-Attacks Threaten 69% Of Saudi Firms, Symantec. [Online] Available at: <https://www.mcit.gov.sa/en/media-center/news/92474> [Accessed 7 September 2020].

[31] Arabnews.jp. 2020. Saudi Students Working Remotely At Risk from Cyberattacks: Experts Arab News Japan. [Online] Available at: <https://www.arabnews.jp/en/saudi-arabia/article_25141/> [Accessed 12 September 2020].

[32] Alshuaibi, A., 2017. Technology as an important role in the implementation of Saudi Arabia's vision 2030. International Journal of Business, Humanities and Technology, 7(2), pp.52-62.

[33] Ebrahim, S.H. and Memish, Z.A., 2020. COVID-19: preparing for superspreader potential among Umrah pilgrims to Saudi Arabia. Lancet (London, England), 395(10227), p.e48.

[34 Hakak, S., Khan, W.Z., Imran, M., Choo, K.K.R. and Shoaib, M., 2020. Have You Been a Victim of COVID-19-Related Cyber Incidents? Survey, Taxonomy, and Mitigation Strategies. IEEE Access, 8, pp.124134-124144.

[35] Abukari, A. M., & Bankas, E. K. (2020). Some cyber security hygienic protocols for teleworkers in COVID-19 pandemic period and beyond. International Journal of Scientific & Engineering Research, 11(4), 1401-1407.

[36] Lallie, H. S., Shepherd, L. A., Nurse, J. R., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2020). Cyber security in the age of covid-19: a timeline and analysis of cyber-crime and cyber-attacks during the pandemic. arXiv preprint arXiv:2006.11929.

[37] Rahman, A., Hossain, M. S., Alrajeh, N. A., & Alsolami, F. (2020). Adversarial Examples–Security Threats to COVID-19 Deep Learning Systems in Medical IoT Devices. IEEE Internet of Things Journal.

[38] Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019). Security Vulnerabilities, Attacks, Countermeasures, and Regulations of Networked Medical Devices—A Review. IEEE Communications Surveys & Tutorials, 21(4), 3723-3768.

[39] Alelyani, S., & Kumar, H. (2018). Overview of cyberattack on saudi organizations.

[40] Nicola, M., Alsafi, Z., Sohrabi, C., Kerwan, A., Al-Jabir, A., Iosifidis, C., & Agha, R. (2020). The socio-economic implications of the coronavirus pandemic (COVID-19): A review. International journal of surgery (London, England), 78, 185.

[41] AlMindeel, R., & Martins, J. T. (2020). Information security awareness in a developing country context: insights from the government sector in Saudi Arabia. Information Technology & People.

[42] Saudigazette. 2020. Saudi Arabia Saw Almost 160,000 Cyberattacks On Smartphones. [online] Available at: <https://www.saudigazette.com.sa/article/594321> [Accessed 17 September 2020].

[43] Alshahrani, H., 2016. A Brief History of the Internet in Saudi Arabia. TechTrends, 60(1), pp.19-20.

[44] Ebrahim, S. and Memish, Z., 2020. Saudi Arabia's drastic measures to curb the COVID-19 outbreak: temporary suspension of the Umrah pilgrimage. Journal of Travel Medicine, 27(3).

[45] Alshathry, S. (2016). Cyber-attack on Saudi Aramco. International Journal of Management, 11(5).

[46] Perlroth, N., & Krauss, C. (2018). A cyberattack in Saudi Arabia had a deadly goal. Experts fear another try. New York Times, 15.

[47] Aldosari, S. R. A Review of Cybersecurity in the Saudi Arabian Context. Journal of Contemporary Scientific Research (ISSN (Online) 2209-0142), 2(8).