CYBERCRIMES IN THE COVID-19 PANDEMIC ERA: A MIX OF SOCIAL PSYCHOLOGY AND SOCIAL ENGINEERING CONCEPTS

[*1]Odule, Tola John;[1]Adesina, Ademola Olusola; Usman, Mustapha Adewale; Odunewu, Abiodun Olusegun .

[1]Mathematical Sciences Department, Olabisi Onabanjo University
[2]The Central Library, Olabisi Onabanjo University, Ago-Iwoye, Nigeria.
[*]tola.odule@oouagoiwoye.edu.ng

ABSTRACT

COVID-19 pandemic has placed more emphasis on digital telecommunications in the conduct of the individual, corporate and government businesses. However, cybercriminals are exploiting the obscurity offered by web-based communications to commit crimes and lure youngsters into illicit carnal activities. This paper established a pattern of online crimes perpetration, induced by the situational factors of the pandemic that may assist corporate governance in tackling cybercrimes in future crises. The study used deductive and inductive coding with a themed analysis of the datasets that cut across various sectors of the global economy. An R-based qualitative data analysis (RQDA) tool was used for the storage and analysis of the datasets. 152 text-based documents were analysed for the research. 45 random samples of the input documents were coded, aggregated and abstracted by an independent arbiter, and the result compared with the researchers' output, to improve analytical triangulation and enhance validity and reliability of the experimental outcomes. Content analysis was performed using the statistical functions of the RQDA. Results showed a 226% rise in cybercrime activities sequel to the outbreak of the pandemic just as three of the several organisations targeted by cyber fraudsters made up over 70% of the total number of occurrences. These results revealed the use of a mix of social engineering and other psychosocial techniques by cybercriminals in their exploits. Further studies may, therefore, consider the contributory effects of each of these techniques on cybersecurity as a means of broadening empirical knowledge on this subject.

Keywords: Pandemic, COVID-19, Cybercrime, Cybersecurity, Social engineering

***Accepted Date:** 10 Oct., 2020*

Introduction

Between late 2002 and middle of 2003, a form of Severe Acute Respiratory Syndrome—SARS, called coronavirus, broke out in Beijing, China, in which twenty-nine (29) nations were affected. An estimated eight thousand and ninety-six (8,096l) infections were recorded with about seven hundred and seventy-four (774) casualties or 9.6% death rate. Though mainland China finally recorded five thousand two hundred and thirty-seven (5, 237) infections of SARS, the new coronavirus of Wuhan, China was more widespread than SARS with a record of five thousand nine hundred and seventy-four (5,974) instances of the new coronavirus—2019-n Cov—confirmed as of January 29, 2020, by the Chinese government. The novel 2019-nCov cases, as at the end of January 2020, exceeded eight thousand and ninety-six (8,096l), the total number of global SARS infections in 2003. Consequently, the 2019-nCov was pronounced as a "global health emergency of international concern" by the World Health Organisation (WHO). 2019-nCov was later named as COVID-19 and declared a pandemic by the WHO on March 11, 2020.

Following the episode of the COVID-19 pandemic,

many nations implemented wide-ranging confinement measures, including travel limitations, restrictions to civic life and lockdowns bringing about numerous companies and their workers having to telecommute from home. COVID-19 pandemic is as severe a medical problem as a digital security hazard. Cybercriminals quickly exploited the rate of infection and are manipulating the interest individuals have for data and supplies. Cybercriminals have utilised the COVID-19 emergency for impersonation assaults such as phishing messages through spam promotions and more directed efforts towards, for example, unauthorised business email disclosure. For example, Zscaler announced seeing an expansion of 30,000% in phishing, mischievous sites, and malware focusing on remote clients—all identified with COVID-19 since January 2020. Analysts discovered that phishing assaults based around COVID-19 were directed at organisations and clients (Kona & Shanker, 2020).

COVID-19-induced mass cutbacks actually fuelled a mass leakage of business information. A company dealing in insider risks, Code42, reported seeing a substantial increase in "ex-filtrated" information in this pandemic period. Joe Payne, the company's chief executive, claimed that the organization witnessed an avalanche of information leaked after the cutbacks that it needed to adjust its innovation to feature especially terrible conduct from increasingly copious and harmless information moves (Miller, 2020). Similarly, cybercriminals using ransomware requested 33% more from their prey in quarter one (Q1) of 2020 than in the past quarter, going by the report of BleepingComputer. The typical rescue payment from bigger business outfits in Q1 of 2020 was $111,605. Lesser companies were likewise focused for inherently lower ransoms, with a mean ransom of $44,021 (Abrams, 2020).

General civic outcry and disarray related to the COVID-19 pandemic gave a variety of chances for cybercriminals.The malware, EventBot, first identified in March 2020, has focused on Android portable clients above two hundred (200) distinctive banking, cash movement administrations, and typical cryptographic money pouch applications. As indicated by ThreatPost report, analysts caution that it is quickly developing with different varieties being distributed periodically (O'Donnell, 2020).An contemporary investigation done by old people's care organisation, Provision Living, revealed that almost one-fourth of Americans have encountered a spike in robocalls as at the outbreak of COVID-19 just as 1 in every 5 people have got a robocall concerning COVID-19 (Provision Living, 2020). A different study by the legal aid, Citizens Advice, found that about 33% of Britons have been reached by fraudsters as at the outbreak of the global health emergency. The outcomes similarly showed that specific sets are prone to a higher threat of focus by COVID-19-induced frauds. Fifty-four percent (54%) of individuals are confronted with revenue loss because of the global health emergency and forty-five percent (45%) of individuals having long-term ailments or incapacities reported having been the focus of organised fraud lately (Citizens Advice, 2020). BleepingComputer reports a hacker making an offer of a database with over ninety-one (91) million accounts belonging to Tokopedia via a shady site online for a mere five thousand dollars ($5,000). With over ninety million dynamic clients and four thousand seven hundred (4,700) workers, Tokopedia ranks as the biggest virtual retailer in Indonesia (Abrams, 2020). Even with the present predicament being over, cybercrimes may be reworked by fraudsters to take advantage of situations after the pandemic.

These days, everything concerns "now", given the instantaneousness, as well as the undeniable benefits, provided by virtual communication made up of electronic mail, short message service, social networking and teleconferencing. This development is especially made more relevant as our everyday life, as well as enterprises, have been radically influenced, including an upset in the global economy and supplies, by COVID-19. More emphasis has thus been placed on teleworking and digital communication as the "new normal" in the conduct of corporate and government businesses. A major threat imparting on the web is the obscurity that Internet offers (Leukfeldt and Yar, 2016). Although it may be a sort of freedom to establish an existence on the web while concealing one's genuine personality, this equivalent capability gives fraudsters and cybercriminals the audacity to take on the appearance of nearly anybody to deceive their targets. The related monetary rewards induce quite a few of these pillagers; some shroud their personalities to control individuals for

inextricable delight. Based on this same anonymity, erotic marauders are known for utilising the Internet to approach and nurture susceptible, young-at-heart individuals for illicit carnal activities and, kids and ladies are often their focus and bait. While email is fascinating for correspondence, it is nonetheless a very potent route for distributing infectious applications. Cybercriminals exploit clients' trust in communications that appear to originate from collaborators or companions. Unique malware risks are even directed at portable gadgets, permitting malevolent programmers to pry into the priceless electronic information that numerous individuals haul about in their versatile portable life-saver.It is, therefore, of scientific importance to have an understanding of the methods and tools deployed by these cybercriminals to lure victims and gain unauthorised access. This knowledge is a first step in designing robust cybersecurity frameworks by information security professionals.

This study used an amalgam of theories from the realm of social psychology, in consonance with popular social engineering techniques, to establish a pattern of online crimes perpetration induced by situational factors such as COVID-19 pandemic. Such patterns may thus assist governments and corporate organisations in formulating policies to thwart, resist or mitigate the impacts of similar threats on their corporate activities in future-pandemics.

This study is significant in three respects. One, within the available evidence in the open literature, it is one of the very few theoretical documentations on the influence of theories outside the domain of pure and computational sciences on a global pandemic of the magnitude and strength of COVID-19 on computational security. Two, unlike the works of Mathew(2020); Brohi et al. (2020)that address mainly the technological components of cybercrimes, and Abukari & Bankas (2020) whose themes focus on prescribing countermeasures in the event of a cyber-attack, this work examines the *modus operandi* of cybercriminals to expose the human vulnerabilities exploited by cyber offenders. Three, and most importantly, this work and its findings like those of Naidoo (2020) and Hawdon et al. (2020) is targeted at all the three hierarchies of management, in varying degrees, at policy conceptualisation, implementation and evaluation levels.

A discussion of cybercrimes, including various techniques used for its perpetration by cybercriminals, with emphases on the non-technological ones, dominates section 2. Section 3 introduces the materials and methods used for the study. Results and discussion of findings from the study constitute the main focus of section 4, while section 5 concludes the report of the study with an appropriate recommendation for future work.

Materials and Method

The method of data collection used for this study is secondary. The data were garnered from a variety of sources such as RiskIQ, Global Initiative, Europol and Nuspire. They were mostly in the form of daily and weekly updates of events as they unfold in the pandemic crises around the globe. The convoluted nature informed the choice of secondary source of data for the problem under investigation as dictated by the novel coronavirus pandemic. Due to the exploratory nature of the research, a hybrid approach has been taken in the treatment of data collected. Precisely, the study used both the deductive and inductive coding with a thematic analysis of the datasets. This approach enables the data to be more representative and reflective of the nuances and realities of cybercrimes. It also affords policymakers and implementers of cybersecurity protocols a clear insight into the cloaked world of cybercriminals, within the ambits of the induced situational factors (Azungah, 2018).

This study used a dataset that cuts across various sectors of the economy, including financial, health, telecommunication and social services as well as government agencies. Even though the COVID-19 pandemic peaked between March and April, the data collected spanned the months of January and July. The reason for this is to show a clear picture of the trends of cybercrime activities as events unfold in the pandemic era for comparative analysis.

In the treatment of the datasets, the first thing was to highlight sections of the text forming the data to come up with suitable 'codes' that describe the contents of interest, as informed by the review of the literature (Maguire & Delahunt, 2017). The datasets were later assembled into clustersclosely mirrored by the codes. This procedure affords the investigators to acquire anabridgedimpressionof the main points that informed the objectives of the study. The next phase was to find patterns amid the

codes and formed the themes. Codes that do not appear often were discarded while some others were refined to more appropriately reflect items under investigation. Finally, the identified and refined themes were then defined and named to reflect the items in Fig. 1.

RQDA, an open-source R-based computer-assisted qualitative data analysis software (CAQDAS) tool, was utilised for the storage and analysis of the source documents from which the data were collated. RQDA, unlike ATLAS.ti and NVivo, supports only text-based (.txt) documents, meaning that it cannot process audio and video files. However, this is not a disadvantage from the perspectives of this study since cybercriminals mostly impersonate through phishing, vishing, smishing and other non-video notes in order to hide their identity and cover their tracks. The choice of RQDA was reinforced by its open-source (free) nature, simplicity and the ease with which coding output (HTML) files can be shared during the research process. These qualities afford replication of the experiments by gatekeepers (co-researchers, journal reviewers, editors) and, therefore, increases the credibility and transparency of the investigation.

A total of 152 text-based documents were analysed for the research. Coding was done based on the textual revelations in the input documents, where the first-level categories were identified. Code abstraction was later carried out to aggregate the first-level codes into higher-level code categories that better summarise the underlying data. While one of the researchers undertook the coding, the other three researchers worked independently on the review of the categorisation and coding abstractions, as a check on the validity of the coding and code aggregation outcomes. To further improve the analytical triangulation, 45 arbitrarily-chosen samples, representing about 30%, from the input documents, were given to an independent party for coding and aggregation. The party, acting as an arbiter, returned a result that was 79.3% in agreement with those of the researchers. This outcome acts as a further confirmation of the validity and reliability of the experimental process (Nowell*et al.*, 2017).

The statistical functions of the RQDA, combined with the deductive and inductive features of the package, were used to perform content analysis to confirm the strength and applicability of the proposed conceptual model with facts that emerged from the records of the source documents.

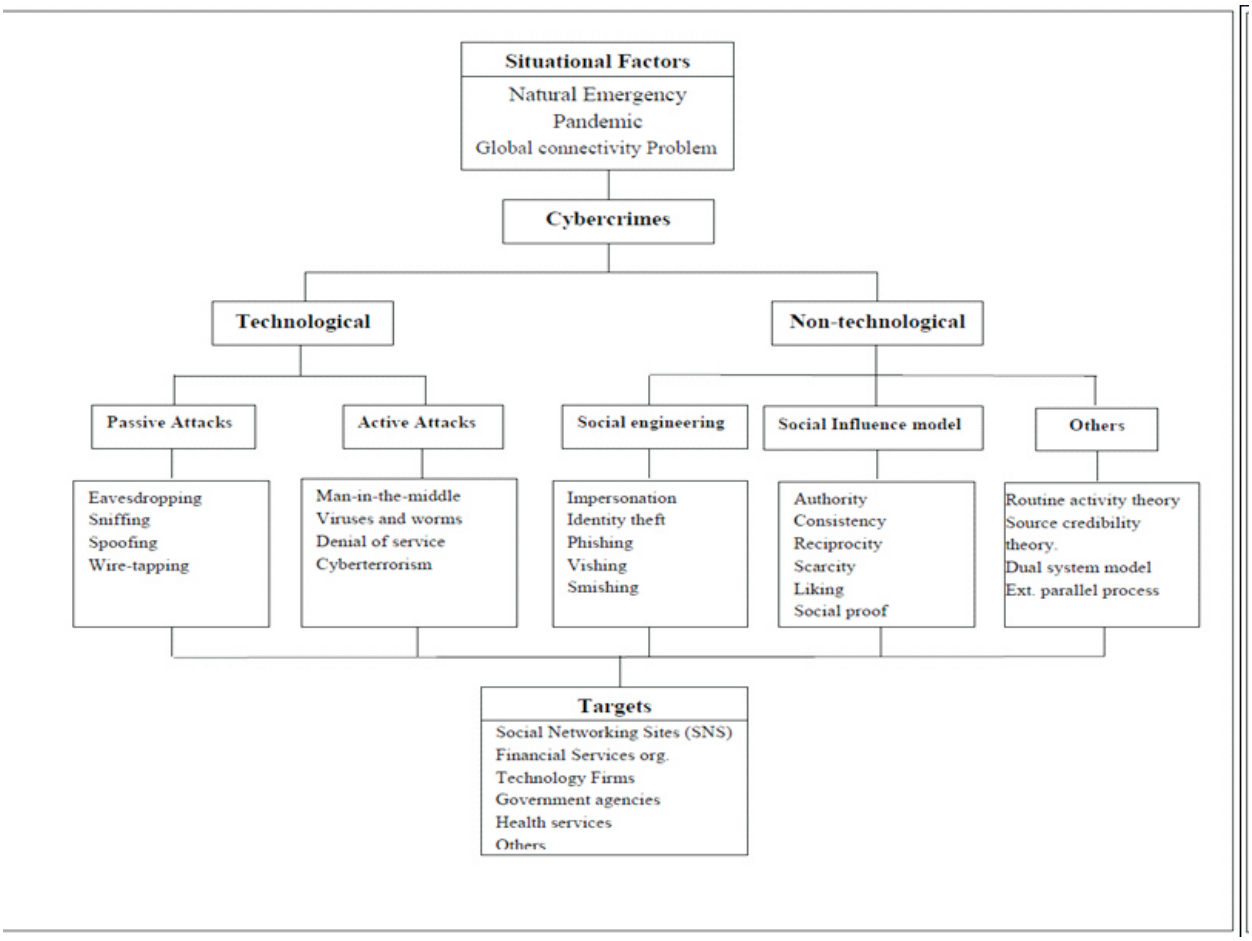

Figure 1: Conceptual Framework

Results

A chart of COVID-19 related cybercrimes is shown in Fig. 2. A critical study of the graph reveals that sequel to the global outbreak of coronavirus in February, the number of cybercrimes induced by the declaration rose by 226% compared to January. This trend continued until it climaxed in April. However, starting from May, the 'curve' started declining up to July. Breaking it further down, analysis of the type of cyber-attacks showed phishing as the most prevalent within the period under consideration (Fig. 3); followed by identity fraud. Since identity fraud is a form of impersonation often committed through vishing and smishing, the value reported for it should be taken as a combination of these two techniques. Similarly,Fig. 4shows that the top four attack types: phishing, identity fraud, hacking and spamming constitute about 51% of the total number of cybercrimesrecorded within the period under investigation. More instructive, however, is that most of these attack types employ social engineering techniques. Table 1 provides detailed statistics for COVID-19 induced cybercrimes from January to July 2020.

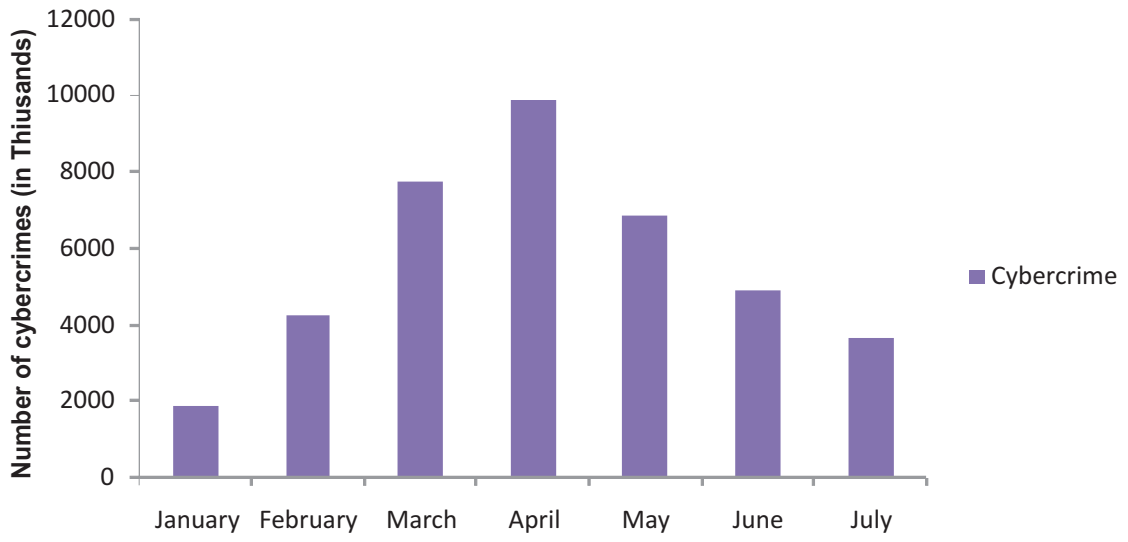

Figure 2: Cybercrime statistics between January and July, 2020.

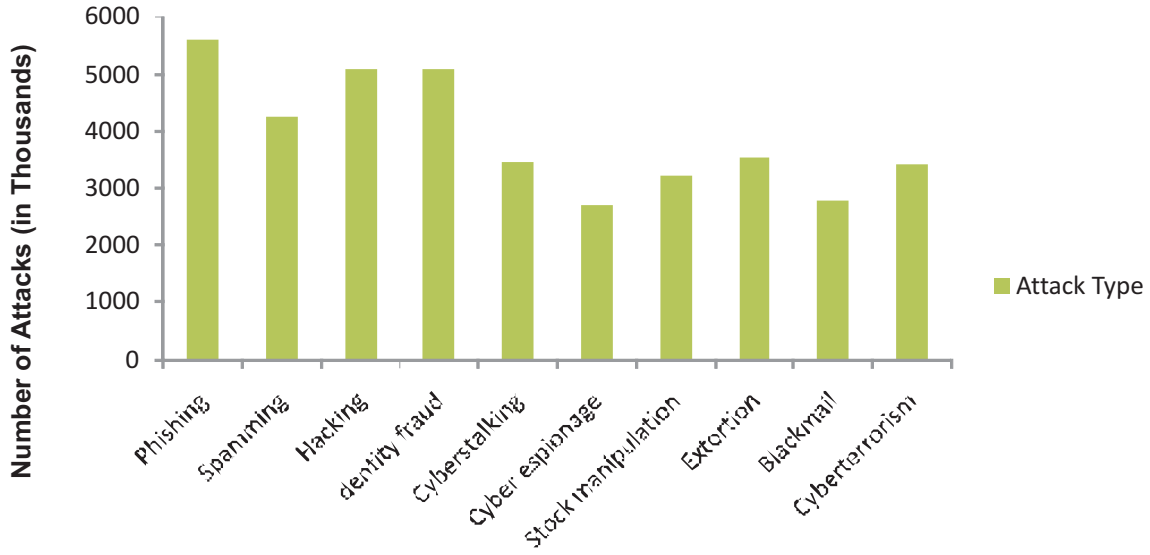

Figure 3: Statistics of cyber-attacks used by cybercriminals in the COVID-19 period

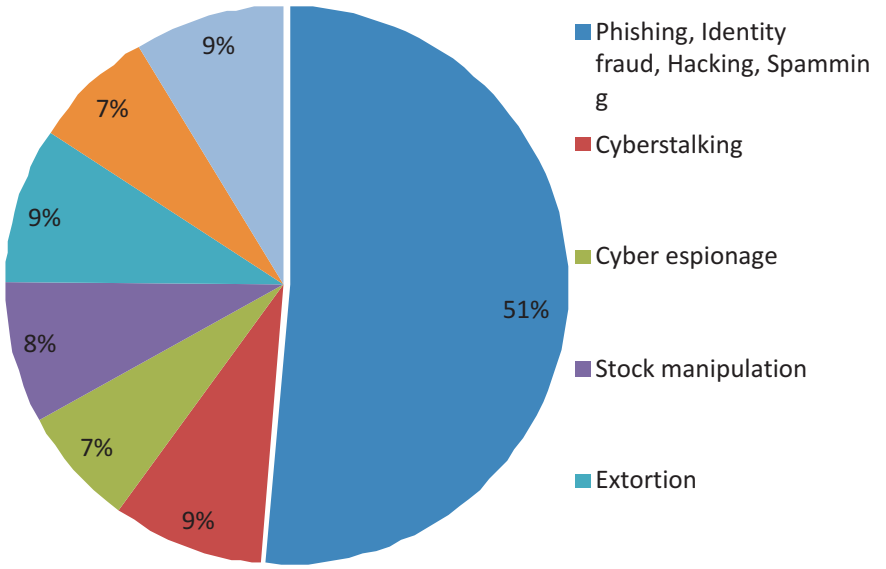

Figure 4: Percentage of the top four cyber-attack types used by cybercriminals

Table 1: COVID-19 Induced Cybercrimes from January to July, 2020 [Figure]

Month / Crime Type	Jan	Feb	Mar	Apr	May	Jun	Jul	
	No of Occurrence (in thousands)							
Phishing	275	780	955	1160	1035	830	560	5595
Spamming	185	330	870	965	890	540	480	4260
Hacking	200	550	965	1200	895	735	540	5085
Identity Fraud	215	635	980	1450	870	520	430	5100
Cyberstalking	145	320	680	910	600	425	380	3460
Cyber espionage	110	215	625	845	420	300	185	2700
Stock manipulation	225	370	665	750	585	365	270	3230
Extortion	195	330	745	995	640	430	215	3550
Blackmail;	105	220	535	850	420	360	290	2780
Cyberterrorism	230	510	720	750	510	420	280	3420
Total	1885	4260	7740	9875	6865	4925	3630	

Table 2: Spam Email Statistics (January – July, 2020)

Month	No of Spam Emails	COVID-19 Unique Subj.	% Spam	% of Total
January	1,732,568	143,857	8.30	8.74
February	2,183,712	205,421	9.41	12.48
March	3,537,849	383,154	10.83	23.27
April	3,816,451	527,383	13.82	32.03
May	1,906,152	171,234	8.98	10.40
June	1,479,211	121,035	8.22	7.35
July	1,182,105	94,321	7.98	5.73

Table 2 gives the spam email statistics recorded between January and July 2020. While the numbers seem to be high, a numerate critique of the data showed that less than 10% of the spam mails carried COVID-19 subjects. Not surprisingly, almost 6% of this figure happened between March and April. The immediate and direct implication of Table 2 is the popularity and use of impersonation as a veritable and potent tool by cybercriminals. Two factors account for this observed development: one, the anonymity and two, the immediacy of Internet communication. These two give a somewhat sense of short-term safety to cyber fraudsters and have even made apprehension of the culprits difficult and sometimes impossible due to technical vulnerabilities occasionally manifested by computing platforms.

Activities of the cybercriminals and hence, their impacts reverberate throughout the sectors of the global economy. As shown in Table 3, SNS accounted for almost 34% in terms of frequency of targets and has the highest prevalence among the organisations. SNS recorded this value due to its popularity with people. A major takeaway from Table 3 is that the top three organisations in the list: SNS, Health and Financial services are relatedly used by cyber fraudsters to perpetrate cyber frauds in the pandemic era, thus accounting for over 70% of the total frequency of occurrence.

Table 3: Cybercrime Targets by Orga nisations

Organisation	No of Occurrence	% Frequency
Government Agencies	12	7.9
Health Facilities	29	19.0
Financial Services	27	17.8
Social Networking Sites (SNS)	51	33.6
Technology Firms	23	15.1
Others	10	6.6

Fig. 5 echoes the impact of COVID-19 induced cybercrimes on the Health service facilities. The industry has been made attractive to cybercriminals by the infodemics engendered by the pandemic. The financial losses caused by the infodemics are captured in Fig. 6. A point of note, however, is the period between March and April.

Finally, Table 4 gives an insight into the modus operandi of the cybercriminals. Cyber fraudsters take advantage of the physical and social distancing protocols of COVID-19 to hack into related platforms like Zoom, GoogleMeet (21.0%) as well as Facebook, Twitter, Instagram, and the likes (19.7%). Cyber fraudsters are also using the social influence principles to extort money from victims through email (17.7%) and online payments (14.5%) under the pretext of donations, charity and payments for fake merchandise. Cloud-based services, telecommunication and video sharing respectively attract 13.2%, 7.2% and 6.5%. Most of the factors exploited are based on social engineering and other psychosocial models.

Table 4: Cybercrime Te chnology and Factors Exploited

Technology	Factors Exploited	No of Occurrence
Telecommunications	Free data/web surfing	11
Cloud-based services	Remote work and virtual	20
Teleconferencing	meetings	32
Social Networking Sites	Social distancing	30
Video s haring websites	Entertainment	10
Email	Donations & charity	27
Online payments	Drugs-related purchases	22

Discussion

Every crime—cyber-based or otherwise—occurs within a context. A proper grasp of this context will, therefore, assist criminologists and other experts in detecting as well as forestalling possible further similar occurrences. The context within the framework of this study is occasioned by the COVID-19 pandemic and its associated situational factors.

Findings from this study concerning the 226% rise noticed in the number of cybercrimes sequel to the outbreak of coronavirus in February 2020 confirm that cybercriminals exploit context and the associated situational factors to launch their various crimes as reported in Holt *et al*. (2020). The relatively high number of spam emails recorded between March and April in Table 2 confirms the submission of Naidoo (2020) regarding the high number of COVID-19 related websites registered in the wake of the pandemic. Furthermore, that some of these sites might be genuine—as posited by the author—perhaps accounted for a less than 10% of the total spam mails being purely targeted at COVID-19 extortions, as revealed in the Table. Similarly, the 34% value observed for SNS in Table 3—in terms of organisational targets—is in agreement with Algarni *et al.* (2017). The authors posit that an average barely literate person will own at least one social media account, even without being computer savvy, since it is considered a social trend these days; thus making it a suitable target.

That cybercriminals readily make use of social engineering techniques is apparent in the dominance of phishing, identity fraud, hacking and spamming attacks, as shown in Fig. 4. This fact is also confirmed by Aiken *et al*. (2016). A critical analysis of the modus operandi of cybercriminals reveals that they always make use of a variety of outlets in the commission of crimes. This approach makes the socioeconomic effects of their actions propagate across the major sectors of the economy with notable impacts (Ibrahim, 2016). This fact is evident from Table 3, where the top three organisations targeted accounted for over 70% of the total number. The use of emotional factors by cybercriminals is also noted—either in the form of fear of reprisals or relief from a reward—combined with social credibility theory Hawdon et al., 2020). This claim is confirmed by the impact of COVID-19 induced cybercrimes on the Health services as shown by the results in Figs. 5 and 6.

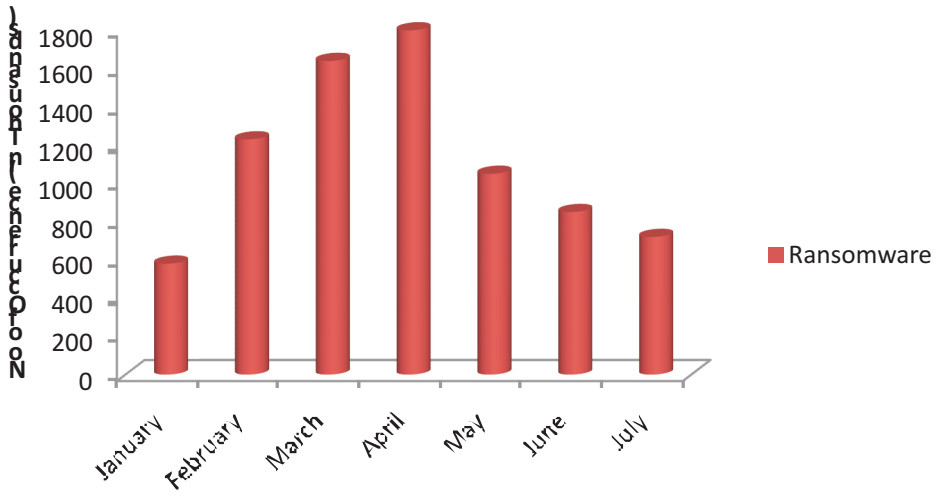

Figure 5: Statistics of the COVID-19 induced cybercrimes on the health services

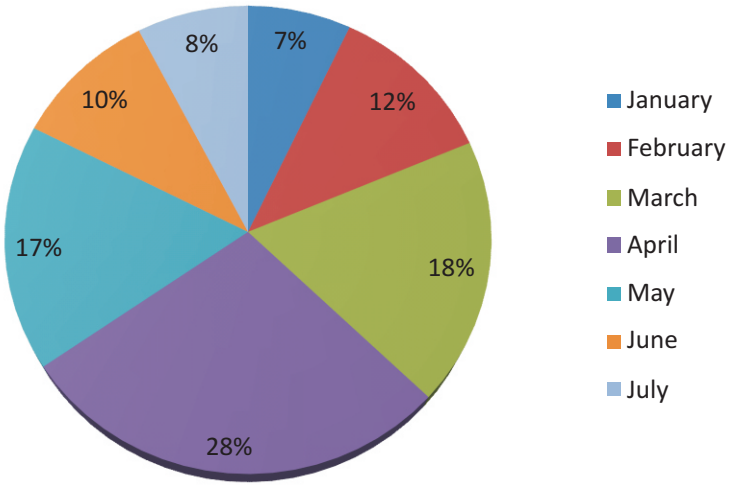

Figure 6: Percentage financial losses by health services in the COVID -19 pandemic period

-Results from this study, however, showed that cybercriminals employ a mix of social engineering and other psychosocial theories to exploit the social vulnerabilities inherent in human nature.

Conclusion

This study investigates the impacts of cybercrime activities on the global economy—as contextualised within the situational factors induced by the global COVID-19 pandemic—from the perspectives of computational criminology. Assessment of such impacts may thus form the bedrock of computational security policies to guide in future global emergencies. The modus operandi of cybercriminals is continuously changing in scope, variety of attack types and depth. Similarly, investigations showed that cybercriminals are continually aligning their activities to contexts and the situational factors engendered by such contexts. It is, therefore, very crucial to understand the activities of these fraudsters from this perspective. This study contributes to the body of knowledge in computational security with a tinge on the psychosocial influences underpinning criminology. It is thus one of the very few studies in this area to focus on the use of a combination of technological and social influence principles by cybercriminals, within the situational context of a pandemic, as a decoy. The completeness of the data used for the study is noted as a limitation. While the emphasis of the study is on the use of a combination of techniques, the impacts of a particular technique are yet to be investigated and, could thus have some latent, isolated effects on the overall outcome of the study. Further studies in this area may, therefore, examine the contributory effects of each of these techniques on cybersecurity as a means of broadening empirical knowledge on this subject.

References

Abrams, L. (2020). Companies start reporting Ransomware Attacks as Data Breaches. Accessed July 7, 2020, from https://bleepingcomputer.com/news/security/companies-start-reporting-ransomware-attacks-as-data-breaches/

Abrams, L. (2020). Hacker sells 91 million Tokopedia accounts, cracked passwords shared. Accessed June 30, 2020, from https://bleepingcomputer.com/news/security/hacker-sells-91-million-tokopedia-accounts-creacked-passwords-shared/

Abukari, A.M & Bankas, EK (2020). Some cybersecurity hygienic protocols for Teleworkers in Covid-19 pandemic period and beyond, *International Journal of Scientific & Engineering Research*, 11(4): 1401-1407.

Aiken, M., Mc Mahon, C., Haughton, C., O'Neill, L. & O'Carroll, E.(2016).A consideration of the social impact of cybercrime: examples from hacking, piracy, and child abuse material online,*Contemporary Social Science*,11:4,373-391, DOI: 10.1080/21582041.2015.1117648

Akbar, N. (2014) Analysing Persuasion principles in phishing emails. Masters Thesis. The University of Twente.

Algarni, A., XU, Y., & Chan, T. (2017). An empirical study on the susceptibility to social engineering in social networking sites: The case of Facebook. *European Journal of Information Systems*, 26(6), 661–687. https://doi.org/10.1057/s41303-017-0057-y

Azungah, T. (2018). Qualitative research: deductive and inductive approaches to data analysis, *Quantitative Research Journal*, 18(4): 383-400. https://doi.org/10.1108/QRJ-D-18-00035

Boney, Joe (2020) Vishing and Cybercriminals During COVID-19. Accessed July 7, 2020, from https://www.securitymagazine.com/articles/92277-vishing-and-cybercriminals-during-covid-19

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., & Polak, P. (2015).What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviours. *MIS Quarterly*, 39(4), 837–864. https://doi.org/10.25300/MISQ/2015/39.4.5

Brohi, S.N., Jhanjhi, N.Z. & Brohi, N.N. (2020). Key Applications of State-of-the-Art Technologies to Mitigate and Eliminate COVID-19,

Cialdini, R. B. (2001). Influence: Science and practice (4th ed.). Allyn and Bacon.

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, 44(4), 588–608. https://doi.org/10.2307/2094589

Corman, S.R. (2006). Using activity focus networks to pressure terrorist organisations. *Comput Math Organiz Theor***12,** 35–49. https://doi.org/10.1007/s10588-006-7082-z

Dillard, J., & Peck, E. (2006). Persuasion and the structure of affect. *Human Communication Research*, 27(1), 38–68. https://doi.org/10.1111 /j.1468-2958.2001.tb00775.x

Ferreira, A., Coventry, L., & Lenzini, G. (2015). Principles of Persuasion in social engineering and their use in phishing. In T. Tryfonas & I. Askoxylakis (Eds.), Human aspects of information security, privacy, and trust. (pp. 36–47). Springer International Publishing.

Gartner. (2020). Gartner HR survey reveals 88% of organisations have encouraged or required employees to work from home due to coronavirus, Gartner (March 19, 2020) https://www.gartner.com/en/newsroom/press-releases/2020-03-19-gartner-hr-survey-reveals-88%2D%2Dof-organizationshave-e. Accessed July 3, 2020.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. *Journal in Computer Virology*, 2 (1), 13–20. https://doi.org/10.1007/s11416-006-0015-z

Hawdon, J., Parti, K. & Dearden, T.E. (2020). Cybercrime in America amid COVID-19: the Initial Results from a Natural Experiment, *American Journal of Criminal Justice* (Online). https://doi.org/10.1007/s12103-020-09534-4

Hayward, K. (2007). Situational crime prevention and its discontents: rational choice theory versus the 'culture of now'. *Soc. Policy & Adm.* 41 (3): 232-250.

Holt, T. J., VanWilsem, J., Van DeWeijer, S., & Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimisation. *Social Science Computer Review*, 38(2), 187–206. https://doi. org/10.1177/0894439318805067

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice* 47: 44-57

Jagatic, T. N., Johnson, N. A., Jakobsson, M., & Menczer, F. (2007). Social phishing. *Communications of the ACM*, 50(10), 94–100. https://doi.org/10.1145/1290958.1290968

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems*, 28(1), 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

Kona, K. & Shanker, D. (2020). The Emergence of Coronavirus and Olympics Scams. Accessed July 4, 2020from https://zscaler.com/blogs/research/emergence-coronavirus-and-olympics-scams/

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2015). Advanced social engineering attacks. *Journal of Information Security and Applications*, 22, 113–122.

https://doi.org/10.1016/j.jisa.2014.09.005

Kumaran, N., & Lugani, S. (2020). Identity and security. Protecting businesses against cyber threats during COVID-19 and beyond. Accessed April 20, 2020, from https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-andbeyond

Leukfeldt, E.R. & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis *Deviant Behavior*, 37 (3): 263-280, https://doi:10.1080/01639625.2015.1012409

Maguire, M. & Delahunt, B. (2017). Doing a Thematic Analysis: A Practical, Step-by-Step Guide for Learning and Teaching Scholars, *All Ireland Journal of Teaching and Learning in Higher Education (AISHE-J)*, 9(3):3351-33514.

Mathew, A. R. (2020). Cybersecurity Pros Warn – COVID-19 Pandemic as a Tool, *International Journal of Engineering and Advanced Technology (IJEAT)*, 9(4): 2441-2443.

Miller, C. (2020). Salary cuts, layoffs and furloughs at COVID-19. Accessed June 28, 2020, from https://google.com/amp/s/www.bizjournals.com/twincities/news/2020/04/09/salary-cuts-layoffs-and-furloughs-at-code42.amp.html

Moneva, A., Miró-Llinares, F., & Hart, T. C. (2020). Hunter or prey? Exploring the situational profiles that define repeated online harassment victims and offenders. *Deviant Behavior*, 1–16. https://doi.org/10.1080/01639625.2020.1746135

Naidoo, R. (2020): A multi-level influence model of COVID-19 themed cybercrime, *European Journal of Information Systems*, (Online). https://doi.org/10.1080/0960085X.2020.1771222

Nowell, L.S., Norris, J.M., White, D.E., &Moules, N.J. (2017);Thematic Analysis: Striving to Meetthe Trustworthiness Criteria, *International Journal of Qualitative Methods*, **16**:: 1–13 https://doi:10.1177/1609406917733847

O'Donnell, L. (2020). New Android Malware Targets Paypal, CapitalOne App Users. Accessed June 28, 2020, from https://threatpost.com/android-malware-paypal-capitalone-app/155341/

Omodunbi B.A., Odiase P.O., Olaniyan O.M. and Esan AO (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. *FUOYE Journal of Engineering and Technology,* 1(1):37-42.

Orbach, B. (2018). Con men and their enablers: The anatomy of confidence games. *Social Research: An International Quarterly*, 85(4), 795–822. https://muse.jhu.edu/article/716115

Osborne, A. & Sphinx, Z. (2020) Malware resurrects to abuse COVID-19 fears, ZDNet, Accessed June 30, 2020, from https://www.zdnet.com/article/zeus-sphinxmalware-resurrects-to-abuse-covid-19-fears-andsteal-banking-data/

Petty, R. E., & Cacioppo, J. T. (1986). The elaboration likelihood model of persuasion. In L. Berkowitz (Ed.), Advances in experimental social psychology (pp.123–205). Academic Press.

Provision Living (2020). Survey Reveals how often Americans Receive Robocalls. Accessed June 28, 2020, from https://provisionliving.com/news/

RiskBased Security, (2020). Year-end Data Breach Report. Accessed July 2, 2020, from https://pages.riskbasedsecurity.com/2019-year-end-data-breac-quickview-report/

Rohrlich, J. (2020)/ Concern for coronavirus victims evident even among cybercriminals in dark web forums, Accessed June 21, 2020, from https://qz.com/1822744/coronavirus-brings-outsofter-side-of-dark-web-cybercriminals/

Schatz, D., Bashroush, R. & Wall, J. (2017). Towards a more representative definition of Cybersecurity, Journal of Digital Forensics, Security and Law, ***12****(2): 23-27.*

*Sillitoe, P. (2006). Why Spheres of exchange. Ethnology.****45*** *(1): 16.* https://doi:10.2307/4617561

Stajano, F., & Wilson, P. (2011). Understanding scam victims: seven principles for systems security. *Communications of the ACM*, 54(3), 70–75. https://doi.org/10.1145/1897852.1897872

Westerman, D., Spence, P. R., & Van Der Heide, B.

(2014). Social media as information source: Recency of updates and credibility of information. *Journal of Computer-Mediated Communication*, 19(2), 171–183. https://doi.org/10.1111/jcc4.12041

Williams, M. (2010). The Virtual Neighbourhood Watch: Netizens in Action. In Handbook of Internet Crime, by Jewkes, Y. and Yar, M. (eds.), Cullompton Willan, pp. 562–581.

Yar, M. (2005). The Novelty of Cybercrime: An Assessment in Light of Routine Activity Theory. *European Journal of Criminology* 2(4):407–427.

Yue, W. T., Wang, Q.-H., & Hui, K.-L. (2019). See no evil, hear no evil? Dissecting the impact of online hacker forums. *MIS Quarterly*, 43(1), 73–95.https://doi.org/10.25300/MISQ/2019/13042