Turkish Online Journal of Qualitative Inquiry (TOJQI)
Volume 12, Issue 10, October 2021: 1839-1851

Theorising Corruption with a 'Click': Adopting Gioia Methodology

Assoc. Prof. Dr. Zaleha Othman[a], Assoc. Prof. Dr. Saliza Abd Aziz[b,] Assoc. Prof. Dr. Subramaniam A/L Sri Ramalu[c]

[a] Principal Research, Othman Yeop Abdullah Graduate School of Business, Universiti Utara Malaysia, 50300 Kuala Lumpur, Malaysia

[b] Tunku Puteri Intan Safinaz School of Accountancy, Universiti Utara Malaysia, Sintok, 06010, Kedah, Malaysia

[c] School of Business Management, Universiti Utara Malaysia, Sintok, 06010, Kedah, Malaysia

Abstract

Understanding corruption in the cyber space warranted greater attention. What more, there are relatively limited studies in the literature that provide understanding of the phenomenon. The objective of the study is to provide understanding of corruption in the cyber space and how corruption risk management could assist in mitigating corruption in the cyber space. This study employed a Gioia methodology. Using Gioia methodology process of data collection, i.e. interviews as primary data collection, fourteen experts were interviewed to gain in-depth understanding of the phenomenon. Gioia data analysis process was used to provide understanding on the concept. This study found several important findings. First, cyber corruption is escalating in Malaysia. Second, Corruption Risk Management (CRM) is significant in curbing corruption activities in the cyber space. Third, there are three stages of CRM: 1) recognising corruption by a 'click,' 2) analysing the system, and 3) evaluation. The findings advance the knowledge on cybercrime, where it extended previous work on mitigating measures. As this is the first study that developed a CRM model using Gioia methodology, the findings contribute to giving novelty to fraud study, indicating a pathway to mitigate corruption in the digital environment.

Keywords: Corruption, cyber-corruption, qualitative, Gioia methodology, risk management

1. Introduction (Times New Roman 10 Bold)

Corruption is a topic of unabated relevance to the government and society of developing countries like Malaysia. However, despite various efforts to combat corruption (Kapeli, N. & Mohamed, N. 2019; Siddique. N. 2011; Yusoff, A.Y. et.al., 2013; Leppanen, A. et al., 2020) corruption problem is becoming quite alarming. This is an issue that shows no signs of slowing down in the near future (Drapeau, D. 2020). According to Caroll, P. & Windell,J. (2018, p.287), 'cyber has provided a "virtual bridge" across borders, allowing criminality to be conducted on a larger scale, at greater pace and with potential for greater return.' The so-called 'virtual bridge' creates sophistication in cyber space, resulting in an exponential growth in the number of cyber victimization over the years. As it is, corruption was reported to cost the global economy about 5% of the world's gross domestic product (Djekic. M.D. 2020).

Scholars also view that the ineffective anti-corruption initiatives contributed to the escalating of corruption in Malaysia. For instance, Yusoff, A.Y. et al., (2013) in their study contended that the government's anti-corruption initiatives to curb corruption are ineffective and failed to mitigate the corruption problem. This paper argues that one of the factors contributing to the increase in the severity of corruption is the limitation of existing anti-corruption measures in preventing corruption. The United Nations Development Programme (UNDP) also shared similar concerns, claiming that among all its efforts to achieve Sustainable Development Goals (SDGs), the anti-corruption initiatives as part of the anti-corruption reforms are still considered limited and need to be strengthened. The UNDP believes that tackling corruption is essential to good governance, equitability, and socially inclusive development. Thus, organisations need to develop effective model to mitigate cyber-crime (Leppanen, A. et al., 2020), indicating the existing CRM is somewhat inadequate to cope with the advancement of cyber technology.

This paper concurs with the above view in regard to the limitations of the existing approach in addressing the issue. The basis of our argument is that the efforts to strengthen the fight against corruption will be unsuccessful without taking into consideration the possible impact of advancement of technology. The paper aims to narrow the gap by theorising the concept and develop a mitigating model from the perspective of preventing cyber corruption. This paper asserts that an effective preventive tool is needed now more than ever. A mitigating measure is necessary to monitor and provide security to corporations to curb corrupt schemes. Strong detection prevention systems with the adoption of technologies to assist in combatting corruption in the cyber era is crucial. Using a Gioia methodology, this study aims to develop a model to counter cyber corruption. This study postulates that a corruption risk management framework adaptable to cyber security measures would be timely as it will act as a monitoring mechanism to prevent corruption in cyber digital environments. The study contributes to previous work on preventing criminal, in particular corruption activities.

2.Significance of The Study

Mitigating corruption is important, particularly in the digital age. Literature indicates that risk management is a tool useful to mitigate corruption conducted in the cyber space, thus, support the significant of the study. Considering corruption is a serious problem in Malaysia and that the present study is significant as the findings are useful to provide enforcement agencies, government, and industry players to design CRM that are not based on cohesive approaches rather more practical approach adaptable to digital age. Most significant is that unlike other study, the present study forward the proposition that corruption risk management is an important preventive measure for combating corruption, which enlighten the government, enforcement agencies, corporations about the importance of preventing corruption.

3.Review of Related Studies

To date, there have been few studies conducted to investigate cyber frauds. To our surprise, little efforts have been taken to explore the phenomenon in detail despite its complexity and severity, with most of the available studies merely treating it as a general understanding of corruption in the digital environment. For instance, in a study conducted by Price Waterhouse Cooper found that 35% of the participating organizations experienced corruption in the last two years (PWC, 2018). The survey found that cyber security (i.e. cyber risk) is the least concern among Malaysian companies. This finding

further revealed that only 36% of the companies surveyed have cyber-attack vulnerability assessment tools. More shocking is that as many as 45% of the companies surveyed admitted that they do not use technology at all to monitor corruption, although 75% admitted that they agree that technology enables monitoring of cyber-attacks more effectively. The findings imply that Malaysian companies are vulnerable, yet unprepared for new forms of cyber-crimes, such as cyber corruption. Although the survey helped to shed some light in regard to cyber-crimes in the country, we find that the survey was too general and lacks scientific evidence on corruption risk management. We believe studies focusing on corruption activities in the cyber era need to consider conducting in-depth, exploratory studies as the knowledge and understanding of the phenomenon is still limited and unclear. In addition, there is also a lack of information regarding the underlying process of how risk management assists in combatting cyber corruption. Little is even known on what mechanisms and measures are available to prevent cyber corruption.

Corruption Risk Management

There are several defining international standards that deal with the CRM, including the following: Australian and New Zealand risk management standard: AS/NZS ISO 31000: 2009; Australian standard AS 8001-2008 - Fraud and Corruption Control; COSO standard; United Nation's Convention against Corruption (UNCAC); OECD Public Sector Integrity – A framework for assessment; USAID Anti-corruption Assessment Handbook; United Nations Global Compact Management; UNDP (United Nations Development Programme); INTOSAI (2004); and Self-Assessment Integrity (Saint Model). Despite these standards using different methodologies across various countries and international organizations, all these approaches have the same goal: to reach, promote, and to maintain integrity within institution(s) through eliminating risks and vulnerabilities. Empirical studies have proven that the CRM is an effective preventive tool that could minimize corruption (Skrbec, 2016). The U4 Anti-Corruption Resource Centre (2018) stated that the CRM process has a minimum of three stages: risk identification, risk assessment, and risk mitigation. However, the U4 Anti-Corruption Resource Centre (2018) claims that the failure of the CRM is that organizations are often stuck at the risk identification stage.

CRM as a Preventive Measure: Conventional

Reading the literature on corruption, there appears to be little research given to risk management perspectives. Albeit limited, the available studies have focused on the conventional risk management approach as a prevention measure. There are several possible factors that could contribute to this gap. First, it is obvious to us that there are inconsistencies found in the literature in terms of defining the concept of the CRM itself. Some research used the term ‘corruption risk indicator’ when referring to the CRM (Fazekas, M. et al., 2016), while others used the term ‘corruption risk management.’

Literature also highlights that the existing empirical studies have proven the significance of the CRM to organizations as a measure to fight corruption (Fazekas, M. et al., 2016; Hauser, C. & Hogenacker, J. 2014). Hauser, C. & Hogenacker, J. (2014). For example, in their empirical study among internationally active firms on their response to the increased requirements of their organization regarding corruption prevention, found that firms do not anticipate the risk of potentially being confronted with corruption when operating in foreign countries (the level of corruption is perceived to be high). The above findings suggest that implementing risk management to prevent corruption is

essential for all organization. Fazekas, M. et al. (2016) found the CRM, or corruption indicator, is an important measure for organizations in measuring their risk associated with potential corrupt acts.

Previous studies have found that there is a causal effect between the CRM and corruption. For instance, Fazekas, M. et al. (2016) created a corruption indicator at the contract level that can be aggregated to other levels such as individual organizations, sectors, regions, and countries. Their study was conducted in Hungary and they found that firms with higher corruption risk scores had relatively higher profitability, a higher ratio of contract value to initial estimated price, a greater likelihood of politicians managing or owning them, and a greater likelihood of registration in tax havens than firms with lower scores on the index. Prior to that study, Dorn, Levi and White (2008), in their study on procurement processes, found that risks are summarized in terms of insider-driven specifications, low visibility of procurement processes, and ample opportunities for renegotiation of terms. Risks may be increased by innovative procurement practices, which may have an effect in terms of extending the manoeuvring between tenderers and public bodies, such as competitive dialogue. Particular risks that may not have been sufficiently addressed will arise at the procedural preparation of specifications, selection of tenderers, and the execution of contracts. Healy, P.M. and Serafeim,G. (2016) provide an analysis of firms' self-reported anticorruption efforts and found that firms with lower residual ratings have higher subsequent citations in corruption news events. Charron, N. et al. (2017), in their comprehensive empirical test on the relation between meritocracy and corruption, found that corruption risks are lower when bureaucrats' careers do not depend on political connections, but rather on their peers. This suggests corruption risks are indeed significantly low when bureaucrats' career incentives exclusively follow professional criteria.

There are several important studies on the CRM that were conducted in China worth noting. For example, Shan, Chan, Le, Xia and Hu (2015) developed a fuzzy measurement model to assess potential corruption in public construction projects in China. They used Fuzzy Set Theory and found that the corruption model can facilitate in evaluating, revealing, and monitoring corruption in public construction projects. Zou (2006) on the other hand, focused on prevention strategies in a study among Chinese construction companies. He found that corruption happens in different forms during various stages of construction project procurement, and the current anti-corrupt practices are found to be reactive rather than proactive. Reforms in terms of improvements on the legal system, inspection strategies and processes, and promotion of ethical culture is required. He also suggests that the institution of random and regular checks, severe punishment and prosecution of corrupt personnel, and promotion of a healthy and clean construction culture are necessary to mitigate the scourge. In a nutshell, we find the CRM is an important topic to study to establish measures to prevent corruption from happening. However, there are gaps in the literature indicating that the topic of CRM is understudied. The pattern of previous studies pointed to CRM as a diagnostic tool rather than a prevention process. There is also a gap in understanding the role of CRM as prevention measures. Most importantly, we noted that all of the studies focused on conventional CRM and none sought understanding the CRM from the perspective of a digital environment, leaving an important gap in the research.

4.Objectives of The Study

- To provide understanding of corruption in the digital environment

- To develop a cyber-corruption risk management model as mitigating tool to curb corruption using cyber space.

5. Methodology

This study employed a Gioia methodology. Gioia methodology was established by Gioia, D., Corley, K.G. & Hamilton, A.L. (2012) and aims at developing a theory or model. It articulates a grounded theory, making it suitable for a topic that is unexplored or new. We employed interview as our primary data collection. Thus, fourteen (14) face-to-face interviews were conducted using semi-structured interview questions. The main aim of the interviews is to gain in depth exploration of the concept in order to develop a CRM model that suits the digital environment.

Choice of Respondents- Purposive Sampling

Specifically, we designed our interviews to obtain perceptions on corruption in the digital environment. A heterogeneous sampling was used as basis of sample selection. To be more specific, the respondents that were interviewed were selected using purposive sampling. The criteria of selecting the respondents was based on their experience, skills and knowledge. Hence, each one of sample in the present study had dealt with corruption cases or at least have knowledge about corruption. According to Campbell, L.J. & Goritz, S.A. (2014), similarities across different organizations point to general mechanisms in corrupt organizations.

To be exact, there are three groups of interviewees: i) those with direct contact to corruption cases and CRM; ii) those with indirect contact to corruption cases but not CRM; and iii) those with knowledge about corruption through research. Through this array of professional views on corruption, we were able to elicit information about corruption and CRM. Thus, a total of 14 interviews involving experts holding various positions were conducted. The interviewees were from various backgrounds, ranging from enforcement agencies to Non-Governmental Organizations, including experts in forensic accounting, integrity officers, and academia. Several of the respondents were involved in the Anti-Bribery Management System (ABMS) project at the national level, under the Centre for Governance, Integrity and Anti-Corruption, Malaysia, an establishment under the National Anti-Corruption Plan (NACP). Table 1 depicts the profile of the respondents.

Table 1: Profile of the respondents

Respondent	Position	Gender	Comment
R1	Officer from Enforcement Agency	Female	In charge of CRM at one of the statutory bodies
R2	Director, Cybercrime – Federal Investigation Agency (FIA).	Male	He has more than thirty years of experience
R3	Associate Professor/ Criminologist	Male	He has years of experience as a criminologist in the USA
R4-8	Officers from Corruption Agency, Indonesia	Group Interviews	Officers from Corruption Department in Indonesia

R9	CRM consultant, Kuala Lumpur, Malaysia	Male	He has nine years of experience as an officer at MACC and years of experience as a CRM consultant
R10	Director, Integrity Institute Malaysia	Male	He initiated several projects of integrity for the public sector
R11	Lawyer, Kuala Lumpur, Malaysia	Male	He is a member of TI- Malaysia and has been a lawyer for many years
R12	Retired Deputy Commissioner, MACC, Kuala Lumpur, Malaysia	Female	She has more than thirty years of experience with MACC
R12	Transparency International, Kuala Lumpur, Malaysia	Male	He is the president of TI and an advocate for fighting against corruption
R14	CRM researcher	Male	He is attached with government agency. He did his doctoral thesis in CRM

There were two stages for the interview process: the preliminary and the fieldwork. Two respondents were interviewed at the initial stage of the project. The aim of this process is to undertake exploratory interviews and develop appropriate questions to be asked during the field work. This empirical experience guided the research to identify a set of interview questions fit for the field work. At the preliminary stage, several basic themes were developed. However, during the actual fieldwork, the basic themes appeared to be the same, hence there was no issue with developing the conceptual framework for the study. The interviews were tape-recorded and transcribed for subsequent analysis. Several of the interviews were not tape-recorded due to requests from the respondents. For the non-recorded interviews, the researcher conducted reflexivity notes and recalled the conversation soon after the interviews. In total, there were about over 25 hours of interviews. The interviews covered the following questions: What are your views on the cyber corruption? How to mitigate corruption using CRM?

In regard to the analysis, the researchers have conducted several levels of abstractions using Gioia, D., Corley, K.G., & Hamilton, A.L. (2012) proposed method of data analysis. First, the data developed a comprehensive compendium of 1st order themes. Second, the numerous themes were organized further into 2nd order level of abstractions. The final stage of data analysis involved seeking patterns of meaning developed from the 2nd order level themes, which is known as the aggregate dimension stage. At this stage, the study makes predictions to obtain a developed understanding, leading to the creation of the ethics story board and ethics content. This stage is termed as building a data structure which will be later interpreted into a sensible meaning. The researchers used manual coding since the researchers found the process of interacting with the data to be more feasible.

Themes across Data Analysis

Theme 1: Corruption with a 'Click'

Our data indicates that there is a paradigm shift of corruption activities in Malaysia. The data delineates that a trend of digital corruption is appearing. As one of the respondents described, corruptors used digital means as a mechanism. The respondents acknowledge that there is a shift from 'traditional' to 'digital,' and corruption is becoming sophisticated. Procurement is one high-risk area that corruptors use digital mechanisms to abuse. KPK officials shared their experiences about offenders using hackers as a means to get in the system of e-procurement. The respondents of the study perceived that although the corruption schemes are similar with conventional means, their mode of the schemes changed. Table 2 summarises the voice of the respondents.

Table 2: Corruption with a 'Click'

Respondent	Quote
R6	'The type of corruption will be the same, but the means of corruption will be different. I called it the corruption scheme. So, the scheme will be different. So those we are talking about exchange of money, carry money in the big cases and those things disappear already. The medium could be digitalized'
R5	'They use electronic tools as a mechanism. I used to say 'corruption by click,' because they corrupt in the digital world. '
R5	'Corruption mechanisms are shifting from traditional to sophisticated/digital and are getting sophisticated. There are cases in Indonesia about procurement. They are offenders, register for a bid in a public sector institution where you win a bid, then you hire a hacker who enters into the system where the e-procurement system works. I don't know whether he got into the other bidders' documents to know the prices they quoted…they can do it through their hackers…that's being done so…if they learn faster than us, then we lose in this digital world.'

Our respondents stated that since the digital transformation is already here to stay, CRM has to be transformed. Our data indicates that if perpetrators use digital means, then the opposing CRM Model has to be similarly advanced. The respondents believed that advanced technology is required as a part of risk management. In contrast, there is also a perspective that the mechanism of preventing corruption, regardless of whether it is technology-based or conventional-based, is primarily defined by the issue of the human factor. Humans that lack integrity may cause corruption, regardless of the means of technology. As one of the respondents said 'there is no direct impact between technology and integrity. "Human" is the factor of concern, as the level of integrity relates with the human factor.' The excerpts in Table 3 support the evidence behind this statement.

Table 3: Human Factor

Respondent	Quote
R3	'I am not excited about the advancement of technology at the workplace ...but in regards to ethics, integrity has no technology that is going to make any human being less sound…take hacking for example...hacking is not done by the robot…meaning whoever is putting the virus or whatever…who controls

	this?…[T]his is a human behind these things… yes, technology is a wonderful advancement for higher efficiency and productivity. But I don't think it will have the direct impact on integrity or whether it is going to assist with integrity…because I think even they use the technology still managed by humans, so the human factor is a major component.'

According to our respondent (R14), political influence, which is human related, is one of the fundamental causes of corruption. High rates of nepotism caused the land office in Malaysia to become of the most active sites of corruptions, regardless of whether the means of doing business was conventional or digital.

Theme 2: Cyber Corruption

Our data indicates that cyber corruption is defined as perpetrators using cyber space to conduct cyber corruption. We identified two themes across our respondents' responses relating to cyber corruption. Both themes are sample attributes that described cyber corruption. The two themes appeared as the modus operandi of cyber corruption, they are: 1) Digital corruption activities, and 2) Digital technology as an enabler of cyber corruption. Our findings also explained that perpetrators are very advanced in respect to corruption in cyber space, thus cyber corruption will be more complex.

Digital Corruption Activities

Our data defined digital corruption activities as corruption activities that are conducted using technology. We also identified that there are various ways that perpetrators use to conduct digital corruption activities, including money laundering, corrupting systems through viruses, data corruption, cryptocurrency, and extortion. The most common activity is using digital technology to extort victims. Extortion is a forceful act or the threatened use of force to gain the property of another. One respondent claimed that perpetrators may corrupt a system through computer viruses and later extort the victims for ransom money.

Table 4: Digital Cyber Corruption Activities

Respondent	Quotes
R5	'They corrupt the system through viruses such as a computer virus etc.'
R5	'Procurement is one of our areas where we use our sophisticated measurements because I heard from our previous meeting that some US/UK experts are visiting us to get us prepared for our system. Although it will not be up to the AI but a bit below than that. But this is not a traditional one, it's quite sophisticated. So, the system could see the pattern of fraud in procurement.
R5	'[T]hey launder money in cryptocurrency etc. We need to just track it. We just need to learn how to seize it. On the one hand it's a trap, but on the other hand it's an opportunity to be more transparent.
R5	'Yes, that's exactly how it happens in organized crime and corruptions. Such as electronic ID…through it they gain a lot…the intention was basically to

	cause corruption through it. Yes, one of the officials asked me whether KPK can handle such sophisticated corruption…I said, we are still learning the digital world, like cryptocurrency.'

Digital Technology as an Enabler Associated with Cyber Corruption

Digital technology as an enabler means using technology to conduct corruption activities. One of the respondents shared his experience, where he described how the perpetrators used hackers to hack the e-procurement system to gain information illegally to bid for projects. Alarmingly, the respondents explained that this corrupt scheme is becoming common.

Our data also found that cyber corruption is becoming worrisome. This is because of the influence of crypto currency. We found that cryptocurrency, such as bitcoin and other cryptocurrencies, have given perpetrators yet another way to conduct corrupt activities, and this is a form of cyber corruption. One of the respondents shared his story of a similar case. The respondents who are the enforcement officers said that the perpetrator used cyber mechanisms to transfer bitcoins to his account using a password. The perpetrator is an investigation officer who was investigating the case. He gained the password and digitally transferred the amount to his account. Table 5 depicts this information from one of our respondents.

Table 5: Digital Technology as an Enabler

Respondent	Quote
R5	'The corruption mechanism is shifting from "traditional" to "digital" and is getting sophisticated. There are cases about procurement. There are offenders, registered for bid in a public sector institution where to win the bid the offender hired the hacker who entered the system where the e-procurement system works. They can do this through their hackers.'
R2	'[d]igital corruption will rise, such as cryptocurrency…recently we got a complaint: A person had 2-3 million rupees' worth of bitcoins in his account…someone got his password and through that he transferred the amount into his account. It is a sort of fraud/corruption. Corruption in the sense that the person who got the password…was actually the investigator, he was investigating him for some other issues…during the investigation he got the password and…transferred the bitcoins…through a misuse of authority,…fraud,…and digital corruption.'
R1	'CRM is one of the mechanisms in managing corruption risk effectively. It emphasizes processes that identify and assess corruption risk and also determine the level of risk. Through CRM, appropriate control measures are taken to prevent or fight corruption.'
R2	'[h]owever, to me, these high-tech gadgets provide checks on the tendencies of corrupt elements…for example, many times it has been observed that you approach an official regarding some task. . . finally, you enter into a deal that

the official will perform a certain task for you and you pay a certain amount, etc.'

Turning now to the challenges, our data indicates that because of hidden identities, the traceability of perpetrators has become complex. This is because personal identity is hidden, thus tracking down criminal activity is limited. Similar with laundering money, there are limited chances for enforcement to detect the perpetrators. In the present study, we found the increasing use of internet has advanced the means of committing corruption even further. The complexity of the internet enables perpetrators to conduct untraceable activities, which fits well with the characteristics of corrupt actors.

In contrast, our data discovered that the lack of expertise among enforcement agencies (e.g. MACC) in cyber security and an over-dependence on conventional modes to tackle corruption are the two themes that appear as obstacles in catching perpetrators. According to the data, human capacity and capabilities are the two themes that appear to explain the increase in cyber corruption. Factors such as lack of expertise, skills, knowledge, and a lack of technological capabilities due to reliance on conventional detection and investigation means by enforcement agencies are the challenges that could escalate cyber corruption even further.

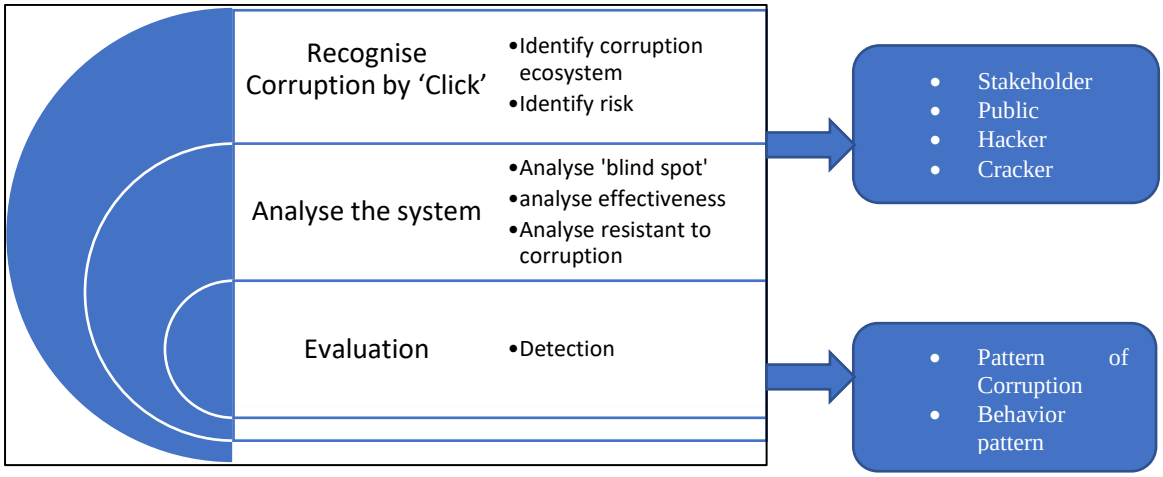
Theme 3: CRM as a Mitigating Measure in the Digital Age

We also identified that CRM is a good mitigating measure in the digital age. Our data indicates that CRM can manage risk and potential risk effectively. The processes in identifying and assessing corruption risk and determining the level of risk through appropriate control measures are the two significant preventive processes. When asked whether digital means can cater for a digital environment, our respondents perceived that there are three justifications that it could cater for the digital environment: 1) an online corruption risk register can be assessed by the public to report corruption, 2) control measures by agencies are reported and can be accessed by the public, and 3) promotion of anti-corruption materials through social media. However, there are challenges in implementing CRM, including the following: 1) understanding the risk management process, 2) commitment of leadership in an organization, 3) culture of anti-corruption across all levels of organisations, 4) continuous anti-corruption promotions, and 5) enforcement.

Theme 4: Stages of Corruption Risk Management

The data described CRM as a diagnostic tool. Our data indicates that CRM is indeed an assessment tool that prevents and manages corruption in an organization. Based on the analysis, all of the respondents perceived that CRM is a preventive mechanism. It is a tool that organizations use to diagnose corrupt activities. CRM assists organizations in identifying corruption risks, misuses of power, and mismanagement as it provides a systematic risk management plan that creates good governance and minimizes corrupt opportunities. Our findings on the association between cyber corruption risk management in Diagram 1. We found the process of CRM has three stages, there are: 1) recognize corruption by click, 2) analyse the system, and 3) evaluation.

Diagram 1: Cyber Corruption Risk Management



Source: Research Findings

Stage 1: Recognising Corruption by 'Click'

Multiple categories, as shown in column two (see Diagram 1), identified corruption ecosystems and risk loopholes, which are termed as recognizing the risk of cyber corruption or corruption by 'click.' These are the two processes that organizations could adopt to recognize corruption by 'click,' which means detecting any corrupt activities conducted via internet. Column three is the list of categories of actors (stakeholders: white hat and hackers: black hat) which emerged from the analysis.

Stage 2: Analyse the System

The second stage of CRM, from the perspective of cyber corruption, is analysing the system. This theme emerged as the second layer after identification of risk in the organizations. There are three steps in analysing the system: 1) analyse any blind spot, 2) analyse the effectiveness of the system, and 3) analyse resistance to corruption. The aim of these three steps is to achieve transparency and accountability. The three steps mitigate the measures of any crypto activities (e.g. hackers and crackers) from penetrating the system.

Stage 3: Evaluation

The last stage is the evaluation stage. At this stage, the organization will be able to detect patterns of corruption, learn about the behaviour of the perpetrators, and conduct asset tracking. Information gathered in the evaluation stage will allow the organizations to revisit the existing processes and take necessary counter measures to close the loop if the model did not yield expected results. This stage can only be achieved when the other two earlier stages of CRM have been implemented.

6. Discussion

The fraud triangle model builds on the scholarly work of Albretch W. S., et al., (2012) and is the most well-received conceptual model to explain how individuals are able to overcome fraudulent activities such as corruption. The fraud triangle depicts three core factors, which are pressure, opportunity, and the rationalization of the individual to conduct fraudulent acts. This study's theoretical basis is related to the fraud triangle model. Available evidence indicates that regardless of the medium, individuals

will act upon corrupt actions if there is pressure, opportunity, and/ or rationalization. In connection with using cyber space (i.e. using technology to commit cyber corruption), our data indicates that technology and the use of cyber space as a platform opens up greater opportunity for individuals to engage in corrupt acts. This finding is congruent with studies carried out by Caroll, P. and Windell, J. (2018) who found that cyber space has provided a virtual bridge across borders, allowing criminality to be conducted on a larger scale, at greater pace, and with the potential for greater returns.' The researchers further stated that the virtual bridge has created sophistication in cyber space and resulted in a greater number of cyber frauds. Cyber activities such as money laundering, extortion, and exploitation of criminal activities have escalated in recent years due to this virtual bridge. Interestingly, there are views that the advancement of digital technology has created opportunities for corruption to happen instead of helping to curb the corruption. Nonetheless, some believe that digital technology is the best tool to reduce corruption.

Our study infers that CRM is a mitigation measure to fight corruption. Available empirical evidence also suggested that CRM is an effective preventive measure of corruption (Fazekas, M. et al., 2016; Hauser, C., & Hogenacker, J. 2014). Consistent with previous studies, our findings indicate that the risk for corruption is even higher in cyber space, thus, a cyber-security-based CRM model is highly needed to combat cyber corruption or corruption by 'click.'

We also found three core components of CRM: 1) recognize corruption by 'click,' 2) analyse the system, and 3) evaluate. All three components should work effectively to fight cyber corruption. The evaluation component is crucial since it provides relevant feedback to earlier processes in order to close any gap that arises in the model. This finding is also congruent with the previous studies. For example, the U4 Anti-Corruption Resource Centre (2015) also suggested a three stage corruption management model: risk identification, risk assessment, and risk mitigation. Our study found that regardless of the medium, all three stages are crucial to combat cyber corruption. Selim, M.A., Yousef, H.P. & Hagag, M. (2019) also found 'identification of risk' and the 'analytical process' to be crucial stages of risk management. However, CRM has to be technology or cyber space friendly. It is important to note that the process of recognizing corruption by 'click' involves the structure and people. The structure includes identification of corruption ecosystems and the identification of risk loopholes. On the other hand, the people aspect involves all relevant individuals connected with the ecosystem.

7. Conclusion

Of late, it appears that corruption is becoming aggressive and unstoppable. The impact is tremendous to the extent that corruption increases poverty and bankrupts a nation. Thus, government initiatives are established to increase the society' s expectations and status of living. In the context of Malaysia in particular, the government has pledged to reduce corruption and transform the country into a high-income nation. Thus, any preventive measures and initiatives to combat corruption would benefit the nation and the people. Therefore, the Corruption Risk Management model adapted as a preventive measure against cybercrime is a step forward to deter corruption in the country. This initiative is in tandem with the country's aspiration to build the nation so that it can generate higher income and provide better lives to the people of the country. In this study, we proposed an appropriate model, which we termed as a 'cyber corruption risk management model,' to direct corporations as a cyber-

security tool in combating cyber corruption. Our findings imply that businesses have fiduciary duties to various stakeholders, meaning they have to invest in cyber security measures in order to safeguard their organizations from hackers and crackers. The findings contribute to giving novelty to the literature on corruption. In addition, providing insightful knowledge on how to mitigate cyber corruption, a new wave of cyber-criminal.

Acknowledgement: We would like to thank the funder of this study i.e. Ministry of Higher Education Malaysia under the Fundamental Research Grant Scheme (FRGS) SO Code: 13807

References (APA)

[1]. Albrecht, W. Steve, Conan C. Albrecht, Chad O. Albrecht, & Mark F. Zimbelman. (2009). Fraud Examination, 3rd Edition. Mason, OH: South-Western.
[2]. Campbell, L.J. & Goriz, S.A. (2014). Culture corrupt! A qualitative study of organisation Culture in corrupt organisations. Journal of Business Ethics, 120, 3, 291 – 311
[3]. Carroll, P. and Windle, J. (2018). Cyber as an enabler of terrorism financing, now and in the future. Journal of Policing, Intelligence and Counter Terrorism, 13 (3), 285 – 300
[4]. Charron, N., Dahlstrom, C., Fazekas, M., & Lapuente, V. (2017). Careers, Connections, and Corruption Risks: Investigating The Impact of Bureaucratic Meritocracy On Public Procurement Processes. Journal of Politics, 79 (1), 89-104.
[5]. Djekic, M.D. (2020). The link between corruption and cyber defense. https://www.cyberdefensemagazine.com/the-link-between-corruption/ via @cyberdefensemag (Accessed 06 June 2020).
[6]. Dorn, N., Levi, M., & White, S. (2008). Do European procurement rules generate or prevent crime? Journal of Financial Crime, 15 (3), 243 – 260.
[7]. Drapeau, D. (2020) The state of cybersecurity and cybercrime in 2020 and beyond. Retrieved from https://shar.es/aHlMb1. Accessed 06 June 2020.
[8]. Fazekas, M., Toth, I.J, & King, L.P. (2016). An objective corruption risk index using public procurement data. European Journal on Criminal Policy and Research, 22 369-397.
[9]. Gioia, D. Corley, K.G, Hamilton, A. L. (2012). In seeking qualitative rigor in inductive research: Notes on the Gioia methodology. Organizational Research Methods, 16 (1), 15 – 31.
[10]. Hauser, C. & Hogenacker, J. (2014). Do firms proactively take measures to prevent corruption in their international operations? European Management Review, 11(3), 223 - 237
[11]. Healy, P. M. & Serafeim, G. (2016). An analysis of firms' self-reported anticorruption efforts. Accounting Review, 91(2), 489 – 51
[12]. Kapeli, N. & Mohamed, N. (2019). Battling corruption in Malaysia: What can be learned? Journal of Financial Crime, 26 (2), 549 – 555
[13]. Leppanen, A., Toiviainen, T., & Kankaanranta, T. (2020). International Journal of Cyber Criminology, 14 (1), 63-80.
[14]. PWC (2018). Global Economic Crime Survey 2018. Retrieved from https://www.pwc.com/my/en/publications/2018-gecfs-malaysia.html.
[15]. Selim, M.A., Yousef, H.P. & Hagag, M. (2019). Risk allocation for infrastructure projects by PPPs-under environmental management and risk assessment mechanisms', International Journal Risk Assessment and Management, 22(1), 89 – 108.
[16]. Shan, M., Chan, A. P. C., Le, Y., Xia, B., & Hu, Y. (2015). Measuring Corruption in Public Construction Projects in China. Journal of Professional Issues in Engineering Education and Practice, 141(4).
[17]. Siddique, N.A. (2011). Approaces to fighting corruption and managing integrity in Malaysia: A Critical perspective. Journal of Administrative Science, 8(1), 47-74.
[18]. U4 Anti Corruption Resource Centre (2015). The basic of corruption risk managmenet: A framework for decision making and integration into the project cycles. U4, 18.
[19]. Yusoff, A.Y., Murniati, S. & Gryzelius, J. (2013). Combatting Corruption: Understanding Anti-Corruption Initiative in Malaysia. Kuala Lumpur: Institute for Democracy and Economic Affairs, 183. ISBN: 978-967-10094-7-5.
[20]. Zou, X.W.P. (2006). Strategies for Minimizing Corruption in the Construction Industry in China. Journal of Construction in Developing Countries, 11(2), 15-29.