Global Scientific JOURNALS

GSJ: Volume 8, Issue 11, November 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

UCD DUBLIN

Submission Deadline	Received Date

Assignment Submission Form

- **Please complete and attach this form to your assignment. All assignments must be submitted on the stipulated submission date.**
- **Please add a "✓" into appropriate box to indicate your assignment type.**

✓ Assignment 1* / ☐ Assignment 2*

***If your module only has one assignment submission, please tick the 'Assignment 2' box above.**

Program / Intake : MSc42

Pathway: RP2

Student Name:	Lim Jun Wen, Jawn	**Student Number:**	12258146
Module:	Research Paper 2 BMGT4023S (Part 2)		
Lecturer/Tutor:	Dr Ajit K Prasad	**Grade:**	

DECLARATION: I hereby declare that the attached assignment is my own work. I understand that if I am suspected of plagiarism or another form of cheating, my work will be referred to the Academic Registrar/ or the Board of Examiners, which may result in me being expelled from the program.

Signed: _____ **Date Submitted:** **18th Oct 2020**

National University of Ireland, Dublin

Masters of Science (BMGT4023S)

Intake MSc42

Module: Research Paper 2 (Part 2)

Essay Title: How employees perceive the adoption of cybersecurity in job performance within Company XYZ?

Submitted by: Lim Jun Wen, Jawn

Student Number: 12258146

Lecturer: Dr Ajit K Prasad

Submission Date: 18h Oct 2020

Word Count: 13,000

Acknowledgements

I would like to thank my thesis supervisor, Dr Ajit Prasad for his wholeheartedly support and guidance throughout my entire research study.

I would also like to extend my appreciation to the staff of all the 8 different industries that have agreed to assist my in this research. I am privileged for their luxury time spent during the interviews as well as for their most genuine inputs without hiding any facts.

I greatly too appreciate all my friends, colleagues and relatives for their support and encouragement as it is a tedious journey.

Finally, I would like to thank my family especially my wife who takes the initiative to take good care of our son has thus given me ample time to collect findings and complete this research successfully.

Abstract

The purpose of this study is to explore the factors that could result in the adoption of cybersecurity behaviour in Singapore. The research will be leveraging on Organizational Behaviour by gathering empirically literature review globally and locally to proceed with further findings in Singapore's SME.

Following an extensive range of literature view, a more reliable research methodology has been carried out that is closely related to the research question. A case study of Organization XXX, consisting 8 different industries was done. All the participants were either senior executive or higher. Data was done via semi-structured interviews. After which, it was transcribed with Nvivo to pick up the main common themes which will be explained further in this paper.

The research is not without its limitation as it is based only in 8 different industries particularly in SME which limits its generalizability to other unchosen industries. Furthermore, this case is based in Singapore private companies which may not be fully contribute to the entirety of Singapore's organizational behaviour. However, it is hoped that this study, can add to the limited literature from Organizational Behaviour context and especially it is based solely in Singapore.

Key words: Cybersecurity Practises, Organizational Behaviour, Singapore's SME, Leadership, Change Management, Communication.

.

Table of Contents

Chapter 1: Introduction

1.1 Background

Modern technology has been evolving exponentially that more people are seeking for convenience and efficiency. This also indirectly influenced the increase of Cyber-attack rate **(Vanitha and Padmavathi, 2018)**. As a result, adoption of cybersecurity gradually became a hot topic with some organization investing tremendously in Cybersecurity with the help of government incentives as a means of sustain their asset **(Gordon, Loeb, Lucyshyn and Zhou, 2015)**. However, in reality, despite organization investing the right tools to mitigate Cyber-attack incident rate, many organization continue to face challenges **(Reddy, Nikhita G., and Reddy, Ugander G.J. (2014)** such as convincing employees to adopt cybersecurity practices which could be due to a myriad of reasons such as sharing password **(Whitty, Doodson, Creese and Hodges, 2015, Szumski, 2018)**. **(Marble et al., 2015)** also agreed that human factor is the first line of defence to build a successful cybersecurity practice. Thus, with all these challenges in placed, a constant update of solution is always required which will be discussed in the later part.

One of the key factor contributing to the effectiveness of adopting Cybersecurity is "Organizational Behaviour" (OB). Organizational Behaviour has been empirically researched in a very wide range of explanation such as the human behaviour and attitude constantly changing within and outside of an organization (**Kaifi, Belal & Noori, Selaiman. 2011 & Foerster-Metz et al., 2018).** Positive Organization Behaviour (POB) aspects for instance self-efficacy, optimism, hope and resilience to contribute the well-being of an individual **(Heinitz, Lorenz, Schulze and Schorlemmer, 2018)**. **(Pan, Chen, Hao and Bi, 2018)** also further implemented POB on the effectiveness in the context of Human Resource Management. Thus, by leveraging on the right OB, it gives organization an opportunity to mitigate Cyber-attack which could do severe damage.

Cyber-attack is ubiquitous that it can happen any time, any place and to any organization **(Sibi Chakkaravarthy et al., 2018)** such as supply chain, human resource, manufacturing, retail and many more which many organization have started to focus a lot on corporate security **(Mukherjee, Sourav, 2019)**. Although many researchers have greatly utilized the theory of OB such as TRA/TRB to improve the adoption of cybersecurity and awareness, some researchers emphasized that company contribution to cybersecurity skills or awareness

might be a reverse effect to increase cybersecurity vulnerability due to the self-efficacy on misuse intention when one has mastered it **(Choi et al, 2013)**.

Many of the reports were seen researched towards a global perspective **(Leccisotti, Chiesa and De Nicolo, 2016 & Dreyer et al., 2018)** which did not concentrate much on a specific country, even to the level of the business sectors. Thus, with the above mentioned, it is thus necessary to address the gap in the field of how OB theory can be effectively adopted in cybersecurity within Singapore as well as how it can be modified or conceptualized to contribute on further research.

Hence, the research topic for this study; "Technology innovation towards employees perception in cybersecurity?

1.2 Purpose of Research – Research Question and Objectives

The purpose of this research is stated on the above mentioned topic where it relates to this question for further research, "How employees perceive the adoption of cybersecurity in job performance within Company XYZ?"

The objective of this research is to identify and pin point what exactly is the underlying and potential issues on employees' perception towards the practice of cybersecurity despite receiving multiple training on cybersecurity awareness as well as investment on IT expenditures **(Wang, 2019)**. Could it be lack of motivation or the efforts employees contributed are not paid off? If the theory of Organizational Behaviour has been adopted for so many years, what would be the research gap that is lacking to be applied to further contribute in the future literature especially in the context of Company XXX in Singapore?

1.3 General Approach of this Study

This study mainly encompasses of literature review from many researchers on the adoption of cybersecurity, information security as well as in the area of technology innovation aspect. In order to have the upper hand to the research objective, empirical research methodology and theoretical framework particularly in OB context will be used. Additionally, the study will also re-iterate the necessity of involving different sub-topics and how it can be integrated and influence individual towards cybersecurity practice. On top of that, a portion of non-empirical research will be also included as part of the study based on the personal observation and interview from the participant to better align with the author experiences as an IT Consultant.

The literature review emphasises on some of the advantages and disadvantages of how different industries adopt cybersecurity leveraging on a myriad of OB theories from motivation, leadership, group dynamic, and culture to a wide range of possibilities.

The data will be collected from interview with a certain criteria such as executive and managers who have worked for more than 10 years or encountered cyber-attack experiences.

At the end of the report, the results will be collected and analysed to see how effective is the existing empirical framework from researchers and cover necessary gap on the theory or framework for a better approach.

1.4 Main Results of Study

The research was concluded that despite multiple stringent enforcement of cybersecurity practices using within organization, there is still a percentage of employees not able to abide to it due to their individual behaviour. This will be further discussed in Chapter 4 on why participants are behaving a different way towards their respective organization.

1.5 Limitations of the Study

The study of this report is limited to two aspects.

a. A Single Country with multiple Industries within SMEs
b. Conceptualizing Framework from a Combination of OB Theories

Firstly, the author has chosen Singapore based company within different industries, particularly in the SME field. Another hindrance faced along the journey was the limited amount of study in Singapore despite majority of research being studied in leading countries (**Khlaponin et al., 2019).** Thus, as the research continues, it progressively increases the difficulties. Although only a few industries were being selected, the study can however be applied to other industries due to the fact that many of the participants were from cross-industry experiences.

Secondly, many of the journal articles are mainly discussed on either one or sub-topics in OB perspective such as "*Leadership*" **(Rodosek, G. & Koch, R, 2016)**, "*Decision Making*" **(Gratian et al., 2018)**, "*Organizational Structure*" **(Dorosh, M. 2015).** Thus, the limitation of building the conceptualized framework would be to rigorously select relevant topics from researchers and merge it into one model.

In terms of the limitation of data collection, focus group will be opted out due to the time constraint and thus it will be solely interview session. A minimum sample size of 8 participants will also be kept to uphold the quality of the research objective **(van Rijnsoever FJ (2017)**

1.6 Overview of this Report

This report will be organized and below is the structure of the chapters;

Chapter 1: Background of Research

This chapter basically give the reader an overview of the entire purpose of the research. It explains how and why the research topic and questions were derived and thus being selected based on the author's experience in the IT field. It will discuss on the research methodology and mitigation approach to deal with the matter based on result found.

Chapter 2: Literature Review

This chapter explains the literature on Cybersecurity adoption and discusses on various themes such as the importance of Cybersecurity practices, SME's way of handling individual and organization behaviour, the advantages and disadvantages of certain theories that can be supported to give an appropriate approach based on case by case situation. Argument will also be factored in to compare the right theories in OB Context particularly in Singapore SMEs.

Chapter 3: Research Methodology

This chapter will always be reviewed from time to time and ensure that it is aligned to the research question and objectives. After which, it will give the reviewer a clear direction why this research methodology is selected.

Chapter 4: Findings and Analysis

This chapter will be derived after gathering all the researched responses which detailed findings and analysis will be presented further.

Chapter 5: Conclusion and Recommendations

Lastly, the chapter will be discussing on some of the mitigation or recommendation that can be useful for future research.

Chapter 2: Literature Review

2.1 Introduction

This chapter provides a deep insight of literature on the topic of Cybersecurity with the support of empirical data from journal articles. As the technology advances and becomes prominence and phenomenon, more internet users begin to access data externally freely without any security mind-set which **Dutton, W. H. (2017)** mentioned that people should focus on fostering "security mindset" rather than identifying the preventive or safe measures. **(Zimmermann and Renaud, 2019)** further reiterated that cybersecurity should have a changed in mindset on enhancing factors that contribute to positive outcomes and resilience rather than "the problem". **(Kremer, 2014)** supported that different "security mindsets" will have distinct approaches to influence the organization in a right manner.

Given the exposure of open data, it has provided an extensive chance for the attackers to exploit endless attacks regardless of individual or organization **(A. Bendovschi, A. Al-Nemrat and B. Ionescu (2016)** also mentioned that the success rate of attack usually comes along with an individual who is not doing their due diligence in upgrading their technology infrastructure as well as not being initiative to keep up with the awareness level. In most cases, it is always the situation where internal security system is not well equipped, **(Shan et al., 2018)** further proposed an internal network security metric method with a flow chart to minimize the probability of being attacked.

With the myriad of recommendations on the internet, relationship between Cybersecurity and Organizational Behaviour are becoming inextricably interwoven which is a truism that many researchers have always been leveraging between them in many areas especially when dealing with all kinds of cyber related factors such as cyber resilience **(Weems et al., 2018)**, cyber threats **(Maalem Lahcen, Caulkins, Mohapatra and Kumar, 2020)** , cyber-crimes **(Arora, 2016)**, cyber influence **(Michel and King, 2019)**, cyber risks **(Ben-Asher and Meyer, 2018)**, cyber warfare **(Faga, 2017)**, cyber hygiene **(van der Kleij and Leukfeldt, 2019)** and finally cyber terrorism and espionage **(Katzan, K. 2016)**. After understanding and analysing some of the key important factors, researcher such as **Lebek, B., Uffen, J., Neumann, M., Hohler, B. and H. Breitner, M. (2014)** further integrated it into Theory of Planned Behaviour (TPB), General Deterrence Theory (GDT), Protection Motivation Theory (PMT) and Technology Acceptance Model (TAM). Majority of researchers have essentially proven that behavioural is the always the main key underlying factor that is able to control

the intensity, sophistication, severity, magnitude and frequency of cyberattack (**Levy, Ramim and Hackney, 2013, Hadlington, 2017)**

With the above extensive review, it gives the author a deep understanding on various factor that contributes to the relationship between Cybersecurity and Organizational Behaviour, which also brings into the research questions and objective as to address the issue or the gap of how these factors can be associated to Singapore's SME adoption in Cybersecurity.

2.2 Definition of Cybersecurity & Cyberattack

Over the past few decades **(Dunn Cavelty and Wenger, 2019)**, it was known that cyberattack and cybersecurity have been emerged and prevailed as the most common and popular literature review adapted by many researchers. However, some might not able to fully comprehend the meaning of it and it is extremely important to educate one in order to apply the right strategy wisely in any research approach.

2.2.1 What is Cyber Attack?

According to most of the researchers **(Kim Y., Kim I., Park N. 2014)**, cyberattack is deliberate exploitation of computer systems, technology-dependent enterprises and networks. **(Miranda Silgado, David, 2018)** further supported the deliberate exploitation of computer systems using malicious code to disturb computers and data. **(Jay P. Kesan & Carol M. Hayes, 2012)** argued that cyberattack is being generalized in a broad manner which should be rather perceived as cyber intrusion deriving from the merger of "cyberattack" and "cyber exploitation".

2.2.2 What is Cyber Security?

(P.S, S and M, 2018, Pardini, Heinisch and Parreiras, 2017) defined cybersecurity as it's being protected by internet-connected systems, including hardware, software and data, from deliberate and accidental attacks. **(Katzan, K. 2016)** supported by emphasizing the need to protect one's privacy such as identity and personal data from intrusion. On the other hand, **Diakun-Thibault, Nadia, 2014** argued that Cybersecurity has been broadly defined as highly variable, subjective, informative and lack of concise information which should be rephrased in a more pragmatic way shown below.

> *"Cybersecurity is the organization and collection of resources, processes, and structures used to protect cyberspace and cyberspace-enabled systems from*

occurrences that misalign de jure from de facto property rights." **(Diakun-Thibault, Nadia, 2014)**

In general, cyberattack can be an impetus to drive the topic of cybersecurity which allows cybersecurity to take the precedence over everything else in an organization due to the importance of safeguarding data. Thus, it is essential for organization to always keep up with their cybersecurity awareness and knowledge. However, **(Willard, Gerald, 2015)** mentioned that by implementing new cybersecurity capabilities, it can actually have a reverse effect of accelerating the attack evolution and innovation.

2.3 Relationship between Cybersecurity and Information Security

As mentioned in the previous section, Cybersecurity can be generalized as a tool to protect against any kind of information from cyberattack. However, **Reddy, Nikhita G., and Reddy, Ugander G.J. (2014)** argued that cyber security is not just about securing the data in IT industry but also contributing to a vast and substantial amount of impact in various other fields like cyber space which is mostly defined as a virtual environment that interconnect almost everything that is internet enabled **(Azmi, Kautsarina, Apriany and Tibben, 2020).**

On the other hand, Information Security was also described in a very broad approach such as 'Information Systems Security', 'IT Security', 'Information Security', 'Cyber Security' and 'Cyber Resilience **(Diesch, Pfaff and Krcmar, 2018).**

While in general, both of them can be conceptualized to meet the same ultimate objective, it does have a clear-cut differentiator to identify each roles. **Howard, David J., 2018** mentioned that it is important to demarcate between information security and cybersecurity. With that being said, it is equally important to understand the relationship to conjunction both to form into a single piece of solution which will be discussed in the next sub section.

2.3.1 Main role of Cybersecurity and Information Security

(Paulsen and Toth, 2016 & Box D, Pottas D. 2014) described the role of "Information Security" as to protecting the information an organization creates, uses, or stores from wide range of attacks. To protect these stored information, Cyber security thereafter comes into place to manage the risk **(Kure, Islam and Razzaque, 2018)** in all organization level especially protecting the IT infrastructure such as devices, equipment, endpoints and system of the stored data. **(Maple, 2017 & Omar Y. Sharkasi, 2015).** Below is an example of the

main relationship between Cybersecurity and Information Security which is summarized in Figure 1

Figure 1 *– Relationship of Cybersecurity and Information Security* ***(Self-Developed, 2020)***

Author	Cybersecurity	Information Security	Keywords
Roles *(What does it do?)*	The techniques of protecting computers, networks, programs and data from unauthorized access **(Aye Mya Sandar, Ya Min, Khin Myat Nwe Win, 2019)**	To protect and preserve the confidentiality, integrity, and availability of information **(Fazlida & Said, 2015)**	- Protect System - Preserve Privacy - Prevent exploits
Problem faced *(What's the issue?)*	Highly socialized in an increasingly connected world with all the information maintained in a digital or a cyber form **(Reddy, Nikhita G., and Reddy, Ugander G.J. (2014)** The world is becoming highly interconnected, with networks being used to carry out critical transactions. **(Aye Mya Sandar, Ya Min, Khin Myat Nwe Win, 2019)**	Lack of knowledge in this important field of information security will be more likely to develop applications that are not secure easier for attackers to penetrate **(Alhassan, Mohammed & Adjei-Quaye, Alexander, 2017)** Adopting a process to rigorously assess the risk associated with information security threats is essential to developing a coherent information security risk management strategy **(Yildirim, 2016)**	- Globally connected - Digitalization - Incompetency skillset - High Risk Taker
Objective *(What's the desired outcome?)*	To protect information system and data from unauthorized access by hacker and also prevent illegal activities on the internet. **(Akintaro, Mojolaoluwa, Teddy Pare, and Akalanka Mailewa Dissanayaka, 2019)**	To identify, protect, detect, respond, and recover from cyberattacks. **(Gutta, Ramamohan, 2019)**	- Defend Data - Mitigate Risk - Preventive measures for future threats
Target Audience *(Who is responsible?)*	Cybersecurity is essential for individuals, for public and non-public organizations **(de Bruijn and Janssen, 2017)** Cybersecurity is critical for all business such as Government agencies, corprations, hospitals, financial instituion, military **(Khari, Shrivastava, Gupta and Gupta, 2018)**	Every organisation should secure data from illegal access, unwanted interruption, unauthorised alteration or data annihilation **(Alqahtani, 2017)** Information security (IS) remains one of the critical concerns for modern and many organisations **(Alghananeem, Altaee and Jida, 2014)**	-All Business -All Organization -All Individual

As reference from Figure 1.1, it was seen that in a high level perspective, the relationship between Cybersecurity and Information Security were very much similar in terms of sharing the same ultimate goal. However, how can this goal be achieved and to what level of extend one needs to perform to become cyber literacy?

This leads to the next topic of best practices which organization should be wary about especially cybercrime is no longer just limited to targeting at developed or developing countries **(Świątkowska, J. 2020)**

2.4 Cybersecurity best practices and principle

Best practices and principle of Cybersecurity have been revolving extensively and informatively on the internet with many researchers such as **(Hutchins et al., 2015, Rabai, Jouini, Aissa and Mili, 2013, Maqbool, Makhijani, Pammi and Dutt, 2016, N. Gupta Gourisetti, M. Mylrea and H. Patangia, 2019)** benchmarking many plethora of theoretical framework from the world renowned Cybersecurity companies such as NIST's Cybersecurity Framework **(NIST, 2020)**, CIS's Controls **(CIS, 2020)** and Cyberark's Mitigation of Security vulnerabilities **(Cyberark, 2020).**

2.4.1 Elements of Principles

(E. Luiijf et al. 2013) emphasized at a National angle of perspective the emerging cyber principles should be as such; global interoperability, network stability, reliable access, multi-stakeholder governance and cyber security due diligence. **(D. Kriz, 2011)** also further supported six effective principles shown in Figure 2. It is indeed, principles are the foundation of forming the right motives and directions towards the sense of achievement, however to attain a constructive solution, a right practice must be instilled which will be discussed later.

> *"We seek principles that can be shared as principles regulating our practices, these principles need to be ones that address the types of decisions that we actually tend to take,"* **(Brännmark, 2019)**

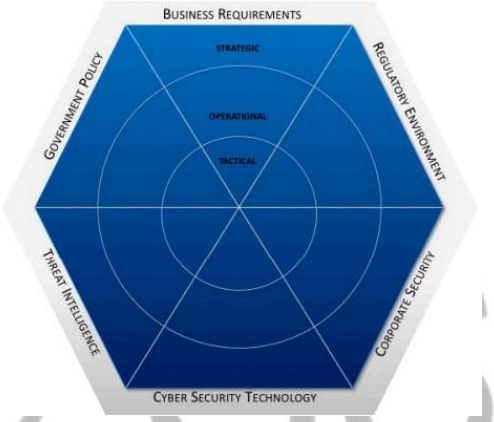
Figure 2 - *The Six Principles and Their Importance to enhance Cybersecurity* ***(D. Kriz, 2011)***

- Leverage public-private partnerships and build upon existing initiatives and resource commitments;
- Reflect the borderless, interconnected, and global nature of today's cyber environment;
- Be able to adapt rapidly to emerging threats, technologies, and business models;
- Be based on effective risk management;
- Focus on raising public awareness; and
- More directly focus on bad actors and their threats.

2.4.2 Elements of Best Practices

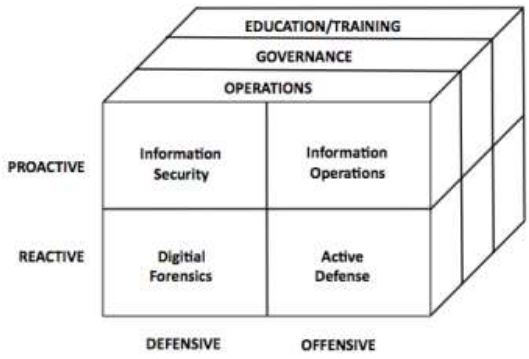
The statement of "Cybersecurity best practices" might vary depending on the area of focus. **(Szumski, 2018).** (**IIROC, 2020)** mentioned that Cybersecurity is not just an IT problem but an interdisciplinary approach and a comprehensive governance commitment which later conceptualized six elements of best practices approach shown in Figure 3. **(David J. Oberly , 2017)** also supported by adding more contributing factors such as providing more education and training, patches and updating, robust policies and cybersecurity-oriented work culture.

Figure 3: *Six Elements of Cybersecurity Best Practice of Conceptual Framework (**IIROC, 2020)***



To distil a substantial amount of essential aspects towards the Cybersecurity best practices and principle. **Kessler, G. C., & Ramsay, J. (2013)** has summarized into a paradigm of cybersecurity in terms of Cybersecurity Education in Homeland Security Program (Figure 4). Basically, it comprises of 3 planes of study; operations, governance and education/training which then explains how cybersecurity actions can be taken place in two-pair of dimensional space such as reactive and proactive, defensive and offensive.

Figure 4: *Paradigms in information assurance/cybersecurity (**Kessler, G. C., & Ramsay, J. (2013)***



With the above pointers, it is clearly shown that one's action and behaviour can lead to the efficiency and effectiveness of adoption of Cybersecurity practices **(Lynne Coventry, Pamela Briggs, John Blythe, and Minh Tran. 2014)** This brings the focus to the next topic of "Organizational Behaviour".

2.5 Advantages and limitation of applying OB theory in Cybersecurity practices

Human behaviour is one of the most risky elements of cyber security **(Szumski, 2018)**. **(Pfleeger and Caputo, 2012)** also acknowledged the importance of human behaviour when designing, building and using cyber security technology. Surely, it is important to apply OB theories in resolving things but individual role must be played well to serve the purpose. **Thakur, G. R. (2014)** emphasized that successful Organizational Behaviour audits set the foundation for the success of future organizational functions.

Despite the advantages of applying Organizational behaviour, on the other hand, at times it can also create reverse effect in terms of the limitation and constraints of the effectiveness of adopting it. **(Ramzy, Bedawy and Maher, 2018)** rebutted that Dysfunctional behavior such as lack of fairness and lack of transparency can force the employees to feel humiliation and lack of equity thus revealing the negative part of it. (**Bada et al, M. Bada, A. Sasse, J.R.C. Nurse, 2015)** also supported that the lack of individual's psychological theories of awareness and behaviour is the reason why security-awareness campaigns often fail.

Next, in order to understand how effective OB can ameliorate the adoption of cybersecurity practices in tough time especially in the current global pandemic situation where Covid-19 **(Ahmad, Tabrez, 2020)** has led people to take things lightly which indirectly allows the cybercriminals to leverage on this opportunity **(Mouton, Francois & de Coning, Arno, 2020)**, theories, concepts and framework will be discussed in depth to identify the mitigation plans case by case.

2.6 Identification of potential factors contributing to Cybersecurity adoption in OB Context

Certainly, adoption of Cybersecurity practices has been deeply researched in the multitude of Behavioural theory context such as Perceived Behaviour Control, Protection Motivation Theory, General Deterrence Theory, Rational Choice Theory **(Pham, Brennan and Richardson, 2017)**. **(Enisa, 2019)** has also identified that the top investigated behaviour is

Theory of Planned Behaviour (TPB), followed by Compliance and Intention. **(Blythe, J.M., 2013)** mentioned that many security behavior studies were done primarily on the surface of applying theories and conceptualizations which lack of in depth researched in the context of how security behavior was influenced.

However, there is a distinct lack of information in combining other range of OB discipline such as "*Leadership*" (**M. Hathaway, 2012**), "*Organization Culture*" (**Huang and Pearlson, 2019**), and other factors that can be essentially important in contributing a wise decision to tackle the transboundary harm of cybercrime. Thus, on top of those popular behaviour theories, an additional of eight factors have been taken in consideration and will be discussed in the latter section.

2.6.1 Leadership

Leadership often relates to how one can actually influence the others to follow their successful path **(Ganta, and Manukonda, 2014, Hao, M. J., & Yazdanifard, R. (2015**) contributes to a great impact in Cybersecurity practices. **(Rodosek, G. & Koch, R, 2016)** proposed a leadership matrix model consisting of "*Governance*", "*Leadership*", "*Managing*" and "*Administration*" to support the cybersecurity strategy and activities (Figure 5). Latter, it was addressed that all of these four concepts are implemented at all activities (Figure 6) and neither one should be not concerned or overemphasized to balance the effectiveness of cybersecurity strategy from the leadership point of aspect.

Figure 5 – *The leadership Matrix Model* ***(Rodosek, G. & Koch, R, 2016)***

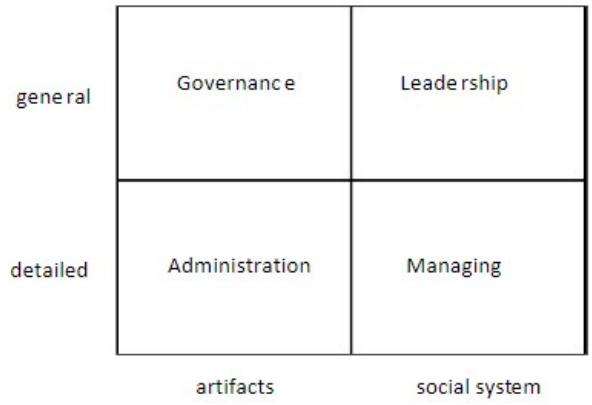
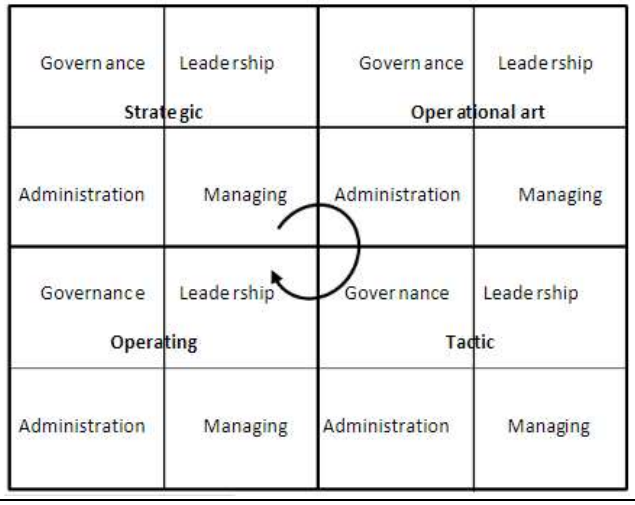


Figure 6 – *Four Concepts revolving at strategic, operational art, tactics and operating level* ***(Rodosek, G. & Koch, R, 2016)***



(Adams, M., & Makramalla, M. 2015) further supported by applying a gamification approach to build cybersecurity skills in leadership so to reduce the financial burden from cyberattacks. On the other hand, **Cleveland, Simon & Cleveland, Marisa. (2018)** argued that Leadership Theory and Style (Figure 7) should however be identified to see which type of leadership such as "*Inspiration*", "*Mentorship*", "*Transformational*" perspective should be applied in the various cybersecurity preparation and response stages in order to educate cybersecurity leaders. **(Porter, Jason, Sr. 2019)** latter claimed to further research on whether Transformational leadership style can really empower employees to mitigate cyber risks.

Figure 7 – *Cybersecurity leadership framework* ***(Cleveland, Simon & Cleveland, Marisa, 2018)***

Function Area	Leadership Theory and Style	Sources
Identify	Adaptive; Authentic; Theory Y; Servant; Inspirational; Mentorship	Albright (2016) ; Bass (1988); Heifetz, Grashow & Linsky (2009); Hewitt (2015); Hult & Sivanesan (2013); Knapp (2015); Morareschu (2009); Northhouse (2017);
Protect	Adaptive; Theory X; Inspirational; Transformational; Mentorship	Avolio & Bass (2002); Bass (1988); De Pree (2002) ;Galloway (2016);Heifetz, Grashow & Linsky (2009); Hult & Sivanesan (2013); Knapp (2015); Morareschu (2009);
Detect	Adaptive; Inspirational; Transformational; Mentorship	Avolio & Bass (2002); Bass (1988);De Pree (2002); Galloway (2016);Heifetz, Grashow & Linsky (2009);Hult & Sivanesan (2013);Knapp (2015); Morareschu (2009);
Respond	Adaptive; Authentic; Inspirational; Resilient; Stackllberg equilibrium; Mentorship	Bass (1988); Hewitt (2015); Heifetz, Grashow & Linsky (2009);Hult & Sivanesan (2013); Morareschu (2009); Karaman, Çatalkaya & Aybar (2016); Knapp (2015); Leitmann (1978); Singha et al. (2015)
Recover	Adaptive; Authentic; Inspirational; Servant; Transitional; Mentorship	Albright (2016) ; Bass (1988);Heifetz, Grashow & Linsky (2009); Hewitt (2015); Hult & Sivanesan (2013);Knapp (2015); Morareschu (2009);

Based on the above facts, it is empirically proven that leadership seems to be the frontline against cyberattacks **(Y. Connolly and Wall, 2019)** and has been essentially influencing the effectiveness of cybersecurity practice. At times, Leadership can also affect the employees' acceptance of change based on the culture set in an organization **(Tayal et al., 2018 & Hao, M. J., & Yazdanifard, R. 2015 & (Tran, 2017)** which will be discussed later.

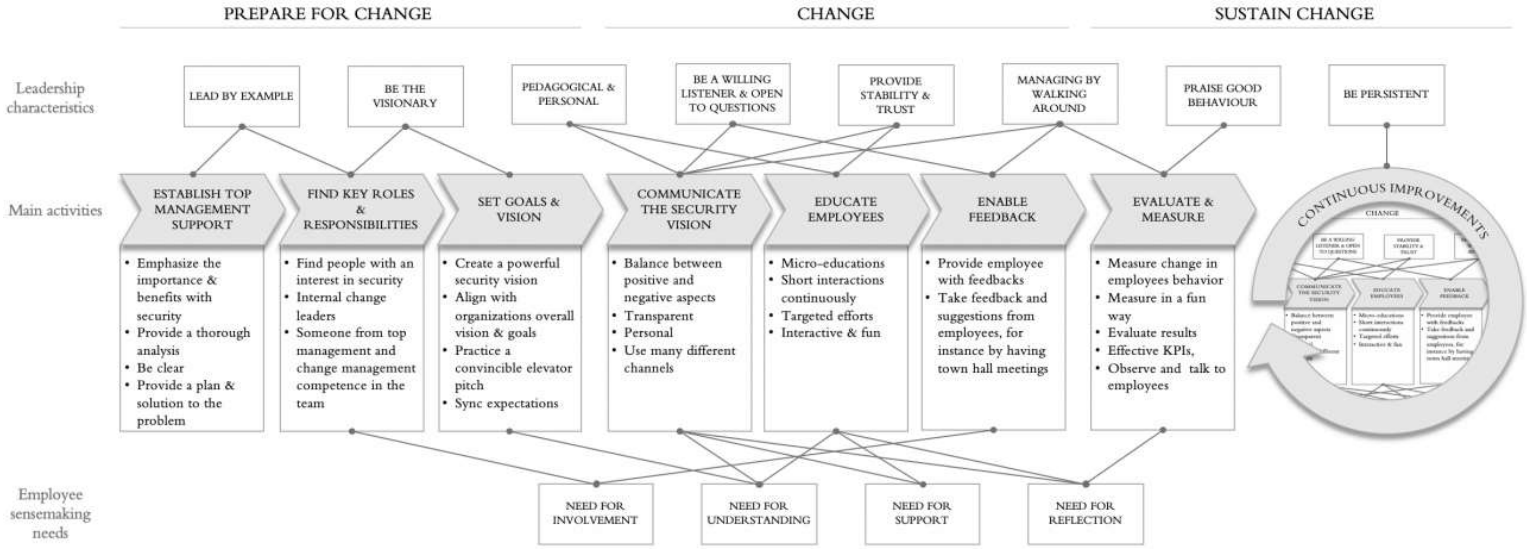
2.6.2 Organization Culture & Change Management

Organizational culture is collectively referred as notion of shared belief, values, perception of employees in an organizational **(Tsai, 2011 & Taylor et al., 2018 & Yahya, Yean, Johari and Saad, 2015)**. To simplify it, (**Ceauşu, Ioana & Murswieck, R. & Kurth, Bastian & Ionescu, Razvan. 2017)** has defined it as the "*Lifestyle of an organization*". Certainly, Organization Culture can shape employees' attitude and behaviour. Organizational culture is often embedded to change process driving towards organization success **(Johnson et al., 2016).**

> *"Change has always been an issue for organization, just as it has always been a common characteristic of human life"* **(Hao, M. J., & Yazdanifard, R. 2015)**

In order to develop and maintain cybersecurity organizational culture, there is a need to adopt new mind-sets and behavioural change **(van 't Wout, Carien. 2019)**. **(Ryttare, E. 2019)** has also conceptualized how culture and change can be co-related extensively in improving cyber security by providing a framework shown in Figure 8.

Figure 8 *– A framework for successful cyber security culture change* ***(Ryttare, E. (2019)***



Besides understanding how culture and change can affect cybersecurity, **(Salaheddine Bendak, Amir Moued Shikhli & Refaat H. Abdel-Razek 2020)** has brought in the study that the focus of organizational culture have been shifted to more intangible qualities which help in the decision-making processes. (**Yoel, S. 2015 & Jalal, 2017)** also agreed that

Organizational culture can influence the many aspects in an organization such as leadership decision making process which will be discussed in depth later.

2.6.3 Decision Making

Decision making is an act of processing information related to problems and situation in order to come to a rational economic model. **(Glazer, Sharon & Karpati, T. 2014).** Decision making is a one of the key salient element to identify individuals' perception towards their security behaviour **(Gratian et al., 2018)**

(Jalali, Siegel and Madnick, 2019) developed a simulation game and identified that managers who can make proactive decisions making are able to develop a successful cybersecurity capability which **(Bashir, Wee, Memon and Guo, 2017)** also supported that cybersecurity participants who displayed rational decision making style tends to show more interest in cybersecurity context. Furthermore, **(Akhmetov, Lakhno, Akhmetov and Alimseitova, 2018)** exemplified it by developing a decision making support system can help in information protection such as password protection.

Figure 9** - Risk Rationalisation Flow **(M'manga et al., 2019)

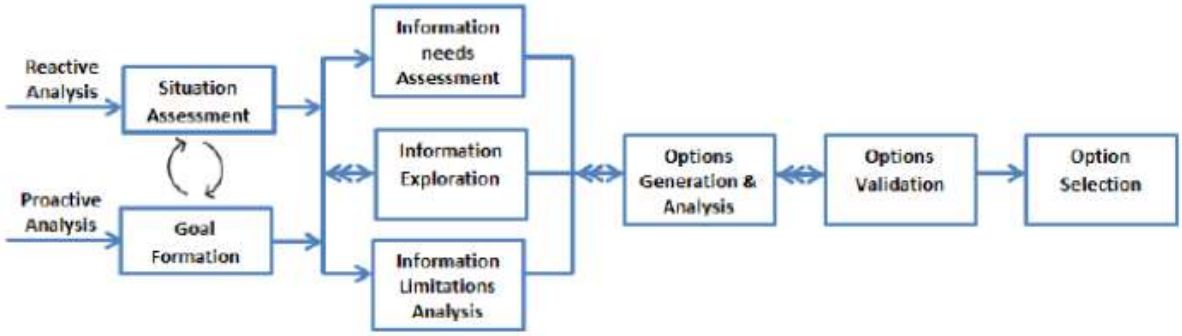


Figure 9 shows an eight steps approach of how a normative model influence the risk of security decision and providing a systematic approach to rationale behind security decision making. **(M'manga et al., 2019).** Having a successful decision making requires a proper formation of group, **(Benjamin Dean and Rose McDermott, 2017)** discussed that cybersecurity policy decision making can be segregated in four different level of group such as International, National, Organizational and individual.

2.6.4 Group motivation

Based on the above section, in order to produce an effective decision making process, the formation of the group is certainly important to cybersecurity practices. Researchers such as **(Kumar, Deshmukh and Adhish, 2014 & Dr. Alex Jones, 2019)** even till now are still using the most influential Tuckman's model of "*Forming*", "*Storming*", "*Norming*" and "*Performing*" **(Tuckman., B, 1965)** as it has been effectively related to the modern organization environment even till today. While, to create an effective group, motivation comes into place.

Motivation often covers a wide topic of many historical empirical theories such as motives and needs, expectancy theory, equity theory, intrinsic, extrinsic and many more **(Lee and Raschke, 2016)**. In general, it can be summarized as a constellation of beliefs, perceptions, values, interests, and actions that are all closely related **(Lai, E.R. 2011)**. **(Kumar, Deshmukh and Adhish, 2014)** further defined in a group effort perspective that "Motivation is accomplishing things through the efforts of others".

(**Julie M. Haney and Wayne G. Lutters. 2019)** stated that Cybersecurity advocates are a subset of security professionals who promote, educate about, and motivate adoption of security best practices and technologies. While there can be multiple of groups in an organization, it is often important to look into how an organization structure their business units or even groups within department.

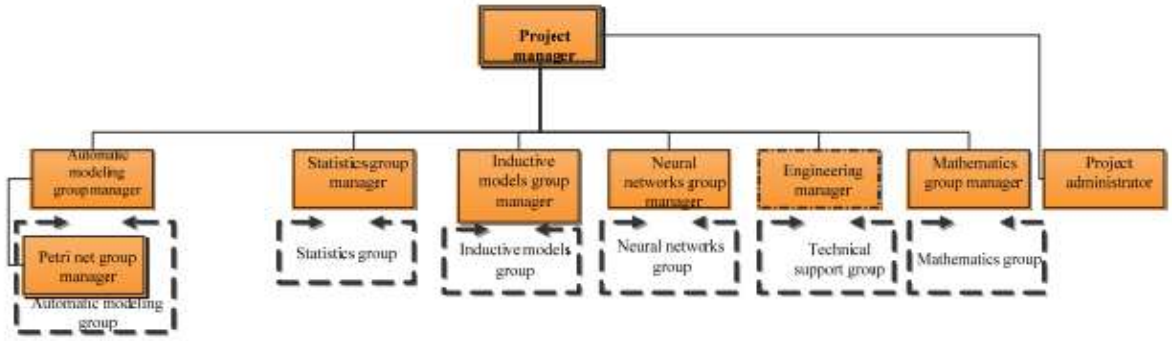
2.6.5 Organization Structure and Design

Organization structure can be seen as the most important criteria of all the other theories in the context of Organization Behavior **(Colquitt, J., LePine, J., Wesson, M. 2014)**. **(Ahmady, Mehrpour and Nikooravesh, 2016)** described Organizational structure as the framework of the relations on jobs, systems, operating process, people and groups making efforts to achieve the goals. (**Ceausu et al. 2017)** further added managers who implement and monitor the management of innovation that are organized.

Cybersecurity measures and the practices would also influence on how the structure of an organization is built. **(Quigg et al., 2016)** stated that if security and resilience in cyberspace are goals, then an analysis of structure should be an initial primary consideration. Certainly, a well-organized structure is the skeleton to begin with especially developing a cybersecurity

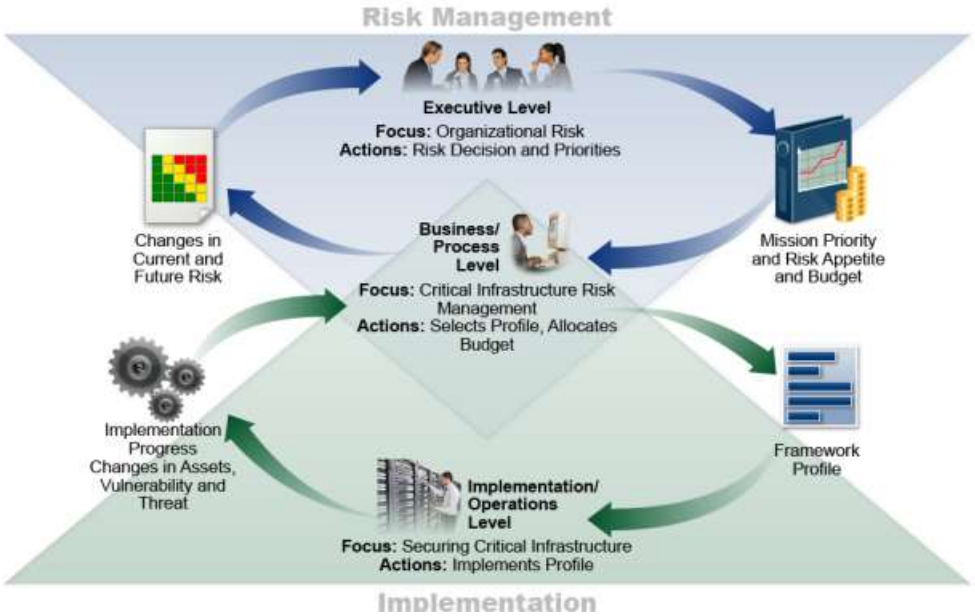
model to protect against attack. **(Dorosh, M 2015)** emphasized on the importance and developed an organization structure to prepare for the cybersecurity execution in Ukraine as shown in Figure 10.

Figure 10**: Organizational Structure of Project Preparation for Project Cyber Security Execution **(Dorosh, M. 2015)



(C. I. Cybersecurity, 2014) has also presented another perfect example on the best practices of cybersecurity by coming up with a systematic organization structure to process for identifying, assessing and managing risk shown in figure 11.

Figure 11** - Notional Information and Decision Flows within an Organization **(C. I. Cybersecurity 2014)



Having said that, to build a successful hierarchy of organization structure, communication comes into place **(H. Widhiastuti, 2013)** which will be discussed in the next section.

2.6.6 Communication, Conflict and Negotiation

(van Ruler, 2018) posits that communication is a process that is associated in all levels regardless if it's negotiation, presentation or any other form of omnidirectional communicating method. Communication is an important key and indispensable to influence individual or group actions. **Cacciattolo, K. (2015)** stated that people who don't know how to communicate, among other things may be incapable of motivating their associates.

> *"Communications and collaboration applications are most vulnerable to insider attack*" **(Evans, Maglaras, He and Janicke, 2016)**

Modern communication systems and infrastructure are increasingly reliant on advances in cybersecurity **(Guariniello and DeLaurentis, 2014).** In the modern days, especially when technology advances exponentially, everyone needs internet to communicate. (**Quigley, K., Burns, C., & Stallard, K. 2013** mentioned that everyone can't avoid communicating via email, texting and social media **(Ewing, M., Men, L. R., & O'Neil, J. (2019)** and thus it indirectly affects the security behaviour and perception of risks. In figure 12, **(J. R. Nurse, 2013)** re-iterate the importance of effective communication to build a best practices dealing with cybersecurity risk.

Figure 11 *– Ten Recommendations for Effective Communication of Cybersecurity Risks* ***(J. R. Nurse, 2013)***

1) Plan how cybersecurity risks will be communicated
2) Design with the understanding that humans possess a limited processing capacity
3) The meaning of information presented in security-risk messages should be clear
4) Users should be presented with clear and consistent directions for action
5) Limit use of technical and security-specific terms and jargon
6) Be mindful when communicating cybersecurity risks numerically
7) Be mindful when communicating cybersecurity risks visually
8) Be mindful when communicating cybersecurity risks verbally
9) Provide help, advice and documentation for security
10) Make security functionality visible and accessible

Next, to approach an effective communication, it is known that everyone has a limitation to have the rights to say. **(Wasserman, 2018)** argues that the field of communications studies covers power and political issues relations.

2.6.7 Power and Politics

(Soares, Laura Porter 2018) described the literature of organization politics within workplace can be actually termed as negative, neutral and positive. Having said that, organization power must come into place to be part of the combined phenomenon. **(Peyton, Zigarmi and Fowler, 2019)** entails power as a condition in which some individuals have control over resources and some do not. Certainly, when these two combined together, it gives one an authority to decide things without much negotiation.

Myriam Dunn Cavelty and Florian J. Egloff, 2019 describes cybersecurity is notoriously hard to pin down and is contested politically in both national and international arenas. In additional, due to the evolution of environment change, many things are subjected to political scrutiny and shifts of power. **(Dunn Cavelty and Wenger, 2019)** further supported that cybersecurity politics can be segregated into 2 areas;

a) Conflictual negotiation processes – formal and informal settings involving government, society, private sectors and more
b) Digital technology – misuse and use of technology in economic, social and political context

Later, it was outlined into 6 factors with two drivers in each sphere showing the interplay between them revolving within each other (Figure 12) with a slight difference in organizational trust, design and view as one of the factor **Koch, Robert. (2017)** shown in Figure 13.

Figure 12 *- Six factors driving cyber security politics.*
(Dunn Cavelty and Wenger, 2019)

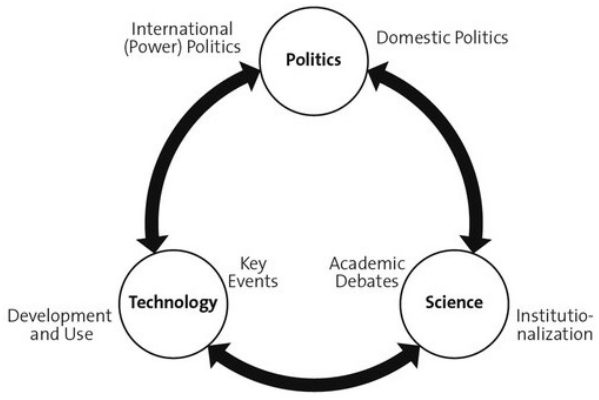


Figure 13 *- Multifold security dilemma arising from the technical, organizational and political*
Robert. (2017)

It is seen that the trajectory of cybersecurity can be shaped by multiple theories such as dealing with the complexity and opaqueness of possibilities that can shed lights to identify how perception of cybersecurity practices can be adopted.

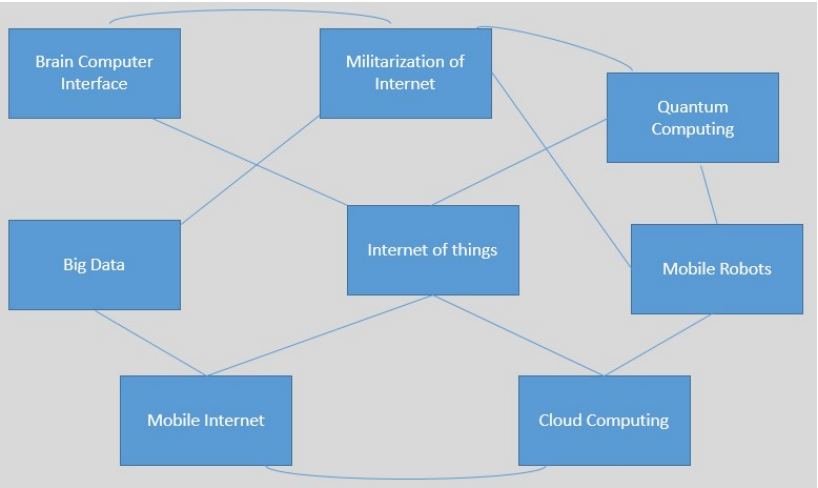
2.7 The future of cybersecurity threat and precaution to overcome it

With hindsight of the evolution of cyberattacks, precaution can be implemented early to dissolve or minimize cyberattacks.

> *"In the near future within cyberwarfare context, Russia and China will continue to pose the largest cybersecurity threats to the United States and other democracies"* ***(Adam Segal et al., 2020)***

In 2011, **(Sacha Tessier Stall, 2011)** predicted that the future cybersecurity threats will be deriving from the non-state actors which includes terrorists, 'hacktivist' groups, organized crime and lone individuals. To overcome this problematic issue, the involvement of the states, private sectors and other international level should improving situational awareness as the key priority. A few years later, **Al-Qahtani, H.S. (2016)** addressed eight major disciplines that can be threatening to cybersecurity as shown in Figure 14 and supported improving situational awareness to avoid conflict of interest and politics that can do harm to cybersecurity.

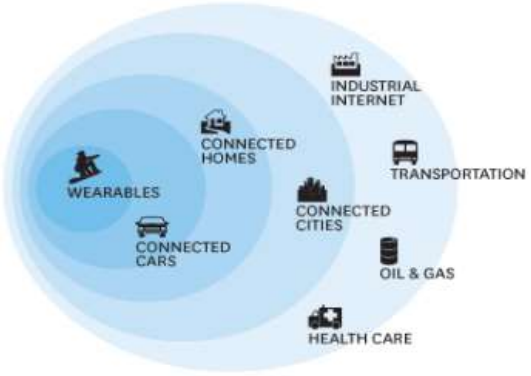
Figure 14 *– Eight major disciplines threatening future cybersecurity (****Al-Qahtani, H.S. 2016)***



Adharsh Krishnan, M. Deva Priya (2019) emphasized that most of the connected devices are vulnerable to attacks which Internet of things (IOT) will be the next 10 years in time to come for insecurities and flaws. Some of the flaws include weak in mobile security,

authentication, authorization, framework, software, data transmission and encryption. Thus, the precaution would be to strengthen the defence and public awareness

***Figure 15** – IoT Landscape* **(Adharsh Krishnan, M. Deva Priya, 2019)**



2.8 Research Gap

While there is a myriad of empirical theories proven to be a key concern to cybersecurity awareness and practices in OB context, most of the reports were designed solely on a single topic such as one of the seven sub-topics as explained in the previous section. There is however a distinct lack of research gap on 2 aspects.

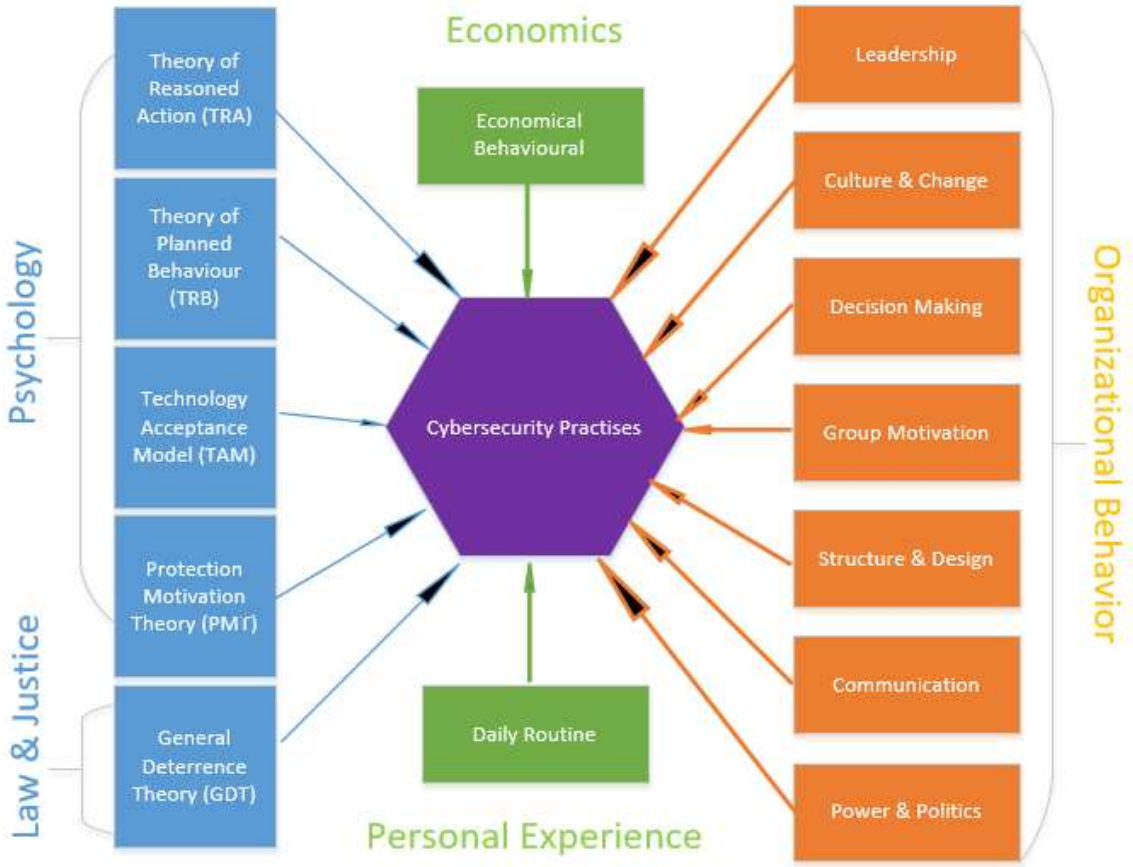
Firstly, most of the target audience were based either in 4 perspectives such as country/regions, market/industry, sectors and organization size (Figure 16). It can been seen that the organization size is relatively low compared to others. Thus, it would be interesting to research in depth on SMEs especially in Singapore.

***Figure 16** – Researchers' Target Audiences* **(Self-Developed, 2020)**

Country/Region	Market/Industry	Sectors	Organization Size
Ukarine *Dorosh, M., (2015)*	**Healthcare** *Box D, Pottas D., (2014)*	**Public** *Yahya, Yean, Johari and Saad, (2015)*	**SME** *van der Kleij, R. and Leukfeldt, R., (2019)*
Sweden *Ryttare, E., (2019)*	**Manufacturing** *Hutchins et al., (2015)*	**Public & Private** *A.Bendovschi, A. Al-Nemrat and B. Ionescu, (2016)*	
Singapore *Jhee Jiow, (2013)*	**Shipping** *Miranda Silgado, David, (2018)*	**Private** *Gordon, L., Loeb, M., Lucyshyn, W. and Zhou, L., (2015)*	
Taiwan *Chuang, L., Chen, P. and Chen, Y., (2016)*	**Electric/Communications/Transportation/Healthcare** *Kure, H., Islam, S. and Razzaque, M., (2018)*	**Private & Public** *Dreyer et al., (2018)*	
India *Tayal et al., (2018)*	**Education** *Thakur, G. R. (2014)*	**Public** *Kremer, J., (2014)*	
Europe *Carrapico and Barrinha, (2018)*	**Financial** *Huang, K. and Pearlson, K., (2019)*	**Private & Public** *Arora, B., (2016)*	
United Kingdom *Hadlington, L., (2017)*	**Gaming** *Adams, M., & Makramalla, M. (2015)*	**Public** *Michel, M. and King, M., (2019)*	
South East Asia *Adam Segal et al., (2020)*		**Private & Public** *D. Kriz, (2011)*	

Secondly, close to none of the researchers elaborated in-depth on a wide range of the possibilities covering majority of the sub-topics of Organizational Behaviour. Although some were able to overlap a few sub-topics with a good delineation of frameworks and elucidated profoundly, many were seen to be reliant on the replication of ideas from others with a slight improvised and manifested version. Thus, there is a limited research on all the possible outcomes as well as "*Economical Behaviour*" **(Moore, 2010)** and "*Personal Experience*" **(Haselhuhn, Michael P., et al, 2012).** Therefore, it would be interesting to combine all into a conceptual framework and research on which sub-topics mean the most to the modern society from the interviewed participants.

Figure 17 – *Conceptual Framework – Singapore's SME Employees' Adoption to Cybersecurity practices* ***(Self-Developed, 2020)***



2.9 Conclusion

To summarise, this literature review covers most of the topics that is related to OB coupled with some of the other popular theories in psychology, law and justice, economics and personal experience aspects. All of these covered topics are in line with the author's research objective. While one might say that there is an ambivalence of choices from the pool of theories which is rather tedious to determine the right theory, the author felt otherwise. The author felt that in order to effectively and rigorously select a relevant topic, all possible internal and external factors should be considered thoroughly with empirical proven figures, theories, and framework. After which, researched methodology will come in to place for final findings and results.

Thus, the literature review will be intended to use closely during the interview and findings to address the research question: *"How employees perceive the adoption of cybersecurity in job performance within Company XYZ?"*

Chapter 3: Research Methodology

3.1 Introduction - Research Questions and Objectives

(Kumar, 2019) explained that to constitute an answer in research methodology begins with what an individual wants to find out through the research questions. Later, a specific statements of goals to achieve at the end of research journey is often called Research Objective. **(Majid, 2017)** further emphasized that a research question should by identifying the research problem that is compelling and important to stakeholder for a successful implementation.

The aim of this research is to identify how employees actually adopt cybersecurity practices in the discipline of Organizational Behaviour. In order to address the research question, the below research objectives will be carried out to seek for a better answer.

Research Question:

- How employees perceive the adoption of cybersecurity practices in their job performance within company XYZ?

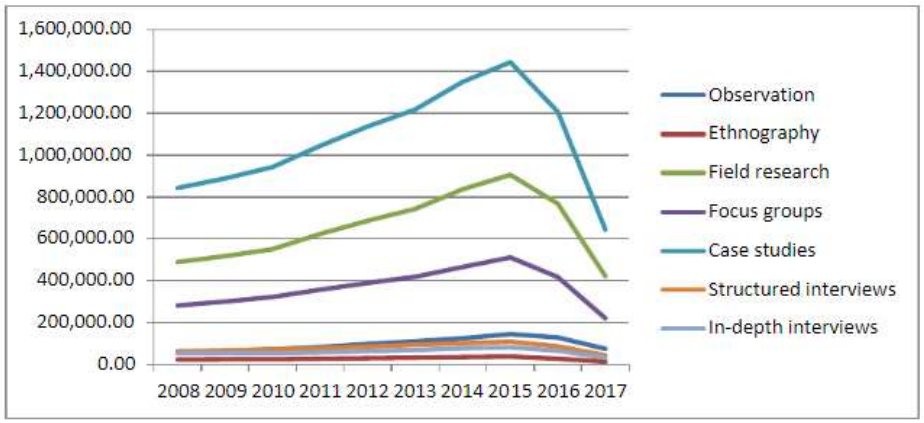
Research Objectives:

- To understand the importance of cybersecurity awareness in any aspect of business
- To identify the relationship between cybersecurity and information security
- To identify the advantages and disadvantages of applying OB theory in Cybersecurity
- To determine cybersecurity best practices and ascertain mitigation method for future approach

3.2 Research Design

In this study, due to the time constraint on quantitative research such as gathering numerical data which requires an extensive amount of time, qualitative research will be carried out instead. Qualitative research focuses on the events that transpire and on outcomes of those events from the perspectives of those involved **(Teherani et al., 2015).** The author has decided to use a qualitative research as it gives a more accurate and effective way of understanding individual behaviour, attitude and experience in real life situation **(Aspers and Corte, 2019),** such as **(D. Eyisi., 2017)** who provided an overview of 10 years evolution of qualitative studies such as observation being the highest, followed by open-ended questions, in-depth interview, focus group and field notes as shown in Figure 18. On the other hand, **(Daniel, 2016)** argued that as qualitative research is more structured in "*dynamic*" rather than "*static*", it is very unlikely to replicate the same result at any time or place as opposed to quantitative research.

Figure 18 - *Evolution of studies that adopt qualitative research methods* **(D. Eyisi., 2017)**



Next, in order to propose a good qualitative research, a research design is a necessary mandate to begin with. Over the years, researchers such as **(Sutton and Austin, 2015, Moore, FahmeenaOdetta., 2017 & Aspers, P. and Corte, U., 2019)** described some of the

popular options such as "*Grounded Theory*", "*Phenomenological*", "*Case study*", "*Ethnographic*", **(Bengtsson, 2016)** further added "*Hermeneutics*" & "*Content analysis*". **(Bruce et al., 2016 & Butina, M., 2015)** also considered "*Narrative Research*" as an important role towards the notion of emergent design. An overall overview of research design is therefore extracted for a clearer understanding (Figure 19).

Figure 19 – *7 different methodologies towards a qualitative research design* **(Self Developed, 2020)**

The author thought it would be extremely important first to understand the respective roles of each theories and analyse the advantages and disadvantages before deciding the methodologies. Figure 20 shows a holistic view of various types of research design.

Figure 20 – *Understanding various types of research design* **(Self Developed, 2020)**

Type of Design	Definition	Pros/Strength/Advantages	Cons/Limitation/Disadvantages
Grounded Theory	To discover or construct theory from data, systematically obtained and analysed using comparative analysis	a. Fosters Creativity b. Provides for Data Depth & Richness c. Potential to conceptualize	a. Exhaustive Process b. Potential for Methodological Errors c. Limited Generalizability
	Chun Tie, Birks and Francis, 2019	Hussein, M. E., Hirst, S., Salyers, V., & Osuji, J. (2014)	
Hermenutics /Phenomenological	Exploring how the informants make sense of experience and transform experiences into consciousness	a. Usefulness in understanding experience b. Subjective and lived-experience	a. Validty, Time and quantity of data b. Small Sample Size (lack of generalizability) c. Large Sample Size (Inconsistent to answer RQ)
	Bengtsson, M., 2016	*(Barrow, 2017)*	
Case Study	An investigation and analysis of a single or collective case, intended to capture the complexity of the object of study	a. grounded in, and applicable to, real-life b. Contemporary human situations c. Provide in-depth relevant data	a. limited generalizability and its rigor b. Bias the finding on desired case study c. offer no basis for reliability of result
	(Ebneyamini and Sadeghi Moghadam, 2018)	Krusenvik, L. (2016)	
Ethnographic	Observing a situation and conducting interviews and interpret the situation from perspective of participants	a. In-depth knowledge about the situation in analysis	a. Huge investment in the researcher's time b. Results can be diversed c. Results can be difficult to extract precise and targeted
	Queirós, Faria, & Almeida, (2017)		
Content Analysis	Systematically transform a large amount of text into a highly organised and concise summary of key results.	a. Useful for analyzing archival material b. Establishing reliability is easy and straightforward c. Can be applied to examine any written document, as well as pictures, videos, and situations	a. Purely descriptive method b. May not reveal the underlying motives for the observed pattern c. Analysis is limited by availability of material
	(Erlingsson and Brysiewicz, 2017)	(Vitouladiti, 2014)	
Narrative Study	Understanding about individual life stories and personal/collective experience	a. Acknowledges the constant change that occurs in learning b. Allow to examine how the different components of a person's context interact with one another c. Explore the personal and the social aspects of learning	a. Building a quality narrative analysis b. Critique centers on the relationship between the researcher and the participants
	Cowger, T., Tritz, J. (2019).		

Given that the goal is to understand the life experience of the participant such as how an individual adopts cybersecurity practices, the author has decided to choose a mixture of "*Hermeneutics Phenomenological*" and "*Ethnography*" study for this research design.

Hermeneutics Phenomenological is often known as attempt to learn and understand human experience through their life stories and experiences which is subjective experience of individuals and groups **(Neubauer, Witkop and Varpio, 2019). Bynum, T. (2016)** has also leverage on the Hermeneutics Phenomenological to discuss about the homeland security in the U.S and described on the management style in government sectors to raise the cybersecurity awareness.

To complement Hermeneutics Phenomenological, Ethnographic study will also be necessary as it helps to accumulate observations, interviews and documentary data to produce detailed results **(Reeves, Peller, Goldman and Kitto, 2013). (Ching, Chang, H., Ya, Wang., and Squires, S., 2016)** has also supported Ethnographic to understand how security is perceived by IT and Non-IT professionals.

3.3 Research Site

A total of 8 organization (XXX) particular in the Small Medium Enterprises (SME) field were chosen for this research site in this study. Let's named it as C1, C2, C3, C4, C5, C6, C7 and C8.

Figure 21 – *8 Organization (XXX) in different SME's industries* **(Self Developed, 2020)**

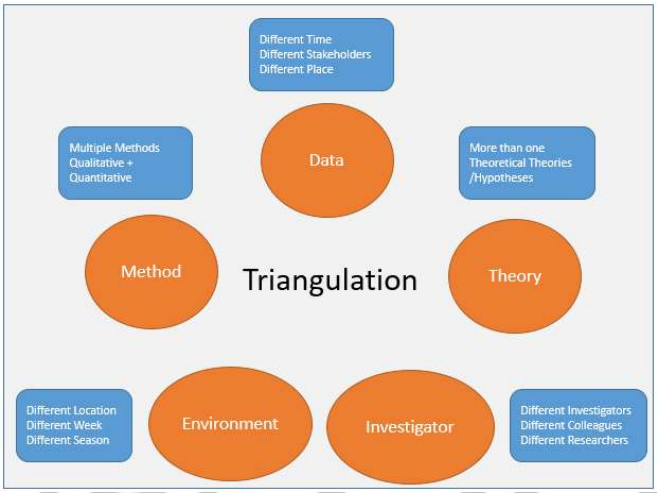
Candidate	Founded (Year)	Industry	Presence	Customer	Employees	Profession
C1	2007	Audit & Compliance	Singapore, Malaysia, Brunei, Indonesia	South East Asia	300	IT Audit, Security & Compliance
C2	1997	Exhibition, Events, Interior Architecture	Singapore, Malaysia, China, Thailand, Vietnam, UAE	South East Asia	200	creative talents, communications experts, brand architects, marketing practitioners, project managers and craftsmen
C3	2011	Law and Legal	Singapore, Malaysia, Cambodia, Thailand, Vietnam, Taiwan, China, Seoul	South East Asia		Lawyers, litigation, Corporate Consultant, Financial services
C4	1991	LED Lighting	Singappore, Indonesia, Philipines	South East Asia	38	Developers, Engineers, Project Manager
C5	2000	Shipping, Marine, Fuel	Asia Pacific	South East Asia	50	Vessels, Marine Fuel, Cargo Trading
C6	2002	CRM, Loyalty & Digital Agency	Singapore	South East Asia	50	creative, digital services and technology, CRM
C7	1968	IT Distributor	Singapore	South East Asia	200	IT Distributor
C8	1950	IT Service Provider	Singapore, Malaysia, Hong Kong, China	South East Asia	60	Enterprise IT Solutions, Cloud, Big Data, AI

Figure 21 shows a detailed summary of various chosen research site. Industries include LED, Law and Legal, Exhibition and Events, CRM & Digital Agency, Fashion, IT, Shipping and Marine Fuel and last but not least Logistic. Employees typically range from 38 to 200 and most organizations have presence in local as well as globally. 8 Organization XXX were also founded for at least 10 years and above.

3.4 Method

A triangulation method will be utilized in this study. Different type of sites, methods and observations will be conducted to increase the quality of the research. **(Santos et al., 2020)** mentioned there are 5 types of triangulation method to establish validity of research, mainly the 1) "*Data*", 2) "*Investigator*", 3) "*Theory*", 4) "*Methodological*", and lastly 5) "*Environmental*" as shown in Figure 22.

Figure 22 – *5 different types of triangulation* **(Self Developed, 2020)**



(Vogl, Schmidt and Zartler, 2019) discussed that "Data Triangulation" targets on different sources of data to study the same phenomenon at different times, places, and populations. As the author is targeting 8 different industries which will be targeted with different stakeholders such as managers, directors and employees' role for interview, data triangulation method will be used.

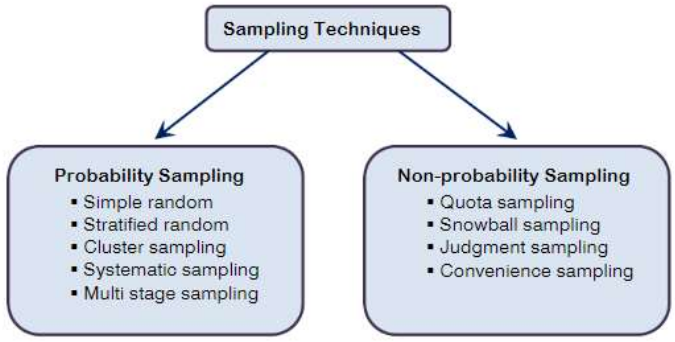
Next, in order to practice the Data Triangulation method effectively, 3 different techniques will be carried out; "*Sampling*", "*Data Collection*" and "*Data Analysis*" which will be discussed further.

3.4.1 Sampling

(Taherdoost, 2016) presented 2 major differences of sampling methods shown in Figure 23. Firstly, it is the "*Probability Sampling*" encompasses of 5 different sub-components as shown below. **(Etikan, 2017)** further added that "*Probability Sampling*" is more appropriate to quantitative research and on the other hand, "*Non-Probability Sampling*" is associated to

qualitative research. Thus, leading the author to choose the second option which **(Taherdoost, 2016)** has also covered with 4 different sub-components mainly the "*Quota*", "*Snowball*", "*Judgement/Purposive*" and lastly "*Convenience*".

Figure 23 – *Various types of Sampling Techniques* **(Taherdoost, 2016)**



In terms of the non-probability sampling, the author has decided to use "*Convenience Sampling*" in conjunction with "*Judgement/Purposive Sampling*" as part of the techniques.

Showkat, Nayeem & Parveen, Huma. (2017) discussed that a "*Non-Probability Sampling*" uses non randomized methods and it's usually selective in terms of the participants thus being judgemental in a way.

Sampling Techniques	Definition
Convenience	Researcher accommodate participants at their own convenience (Readily accessible or available)
Purposive	Researcher chooses the participants that benefits him/her to address the study (Exploratory approach)

Source: *Showkat, Nayeem & Parveen, Huma. (2017)*

Based on the above table, a "*Convenience Sampling*" gives the researcher a free and easy way to collect the data possibly in a convenient manner in terms of the environment, time and place. Due to the current global pandemic (Covid-19) **(Pung et al., 2020)**, the author understood that a certain percentage of people will be working from home or on-site. Time and place did not permit on all the 8 participants for any reason, thus, the author did not limit or restrict the place and time as flexibility is one of the way to achieve a quality result **(Moser and Korstjens, 2017)**. Sampling could also be in a form of video conference method if participants are convenient.

Next, "*Purposive Sampling*" allows the researcher to ensure selective participants are more advantage to be qualified for the study. Based on the author's experience, 8 selective participants have met the criteria such as;

i) Employees who has worked for the company for more than 10 years
ii) Employees who experienced cyberattacks for at least once
iii) Management roles and above

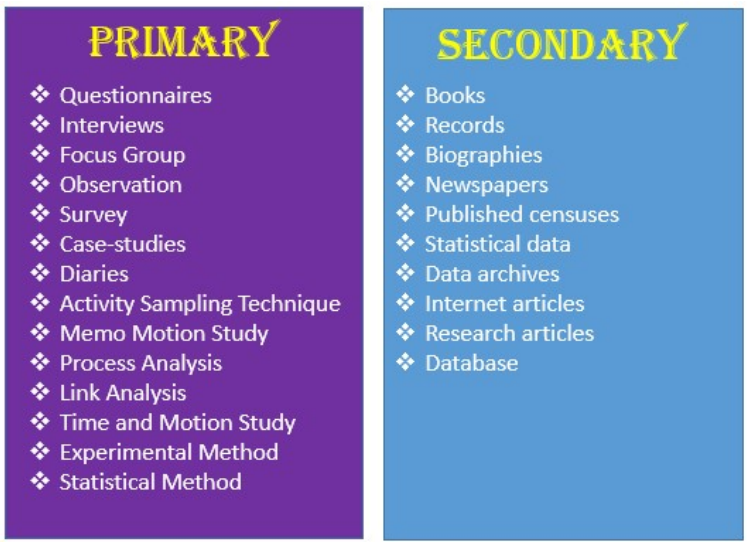
On the other hand, to ensure questions were answered in a convenient and transparent manner, the author has intentionally chosen the participants who are either business partners, distributor or vendors with at least 3 years of relationship.

3.4.2 Data Collection

In this study, both primary and secondary data will be used to increase the reliability of the data. **Ajayi, Victor. (2017)** simplified the definition of "*Primary Data*" as first hand data gathered by the researcher and "*Secondary Data*" as data collected by someone else earlier. On the other hand, **Kabir, Syed Muhammad. (2016)** has also gave a high overview of options to choose between the 2 different data collections (Figure 24)

> *"A research can be conducted without secondary data but a research based on only secondary data is least reliable and may have biases because secondary data has already been manipulated by human beings"* **Kabir, Syed Muhammad. (2016)**

Figure 24 – *Summary of Primary and Secondary Data Collection Methods* ***(Self-Developed, 2020)*** ***(****Points derived from* Kabir, Syed Muhammad, 2016)



In terms of the primary research, the author has chosen interview. The interview will be conducted with 8 different participants in different industries, comprising of Management and Non-Management staff depending on their respective criteria met. "*Semi-Structured*" interview was chosen instead of "*Structured*" and "*Unstructured*" as it was proven to be more effective for collecting qualitative, open-ended data, exploring participant thoughts and feelings, and last but not least delve into personal issue **(DeJonckheere and Vaughn, 2020)** which is in the interest of the author. Through the interview session, a fair bit of "*Participant Observation*" will also be engaged to share the author's ideas and perspective with the participant so to delve both parties into a natural and comfortable conversation **Qaddo, Myasar. (2019).**

In terms of the secondary research, the author will be presenting with some past example of cyberattacks from journal and newspaper to give a hindsight to both parties before embarking on the interview session which will be co-related and beneficial to the research question. **(Unachukwu, Kalu and Ibiam, 2018).**

To standardize and reduce the biasness of the interview questions across the stakeholders such as managers, executive, or directors, only one set of interview questions (Appendix 1) was prepared. Open-ended questions will be engaged as well to eliminate "yes" and "no" response. **(Bolderston, 2012)**

An official email (Appendix 2) was sent to individual head of organization (XXX) for approval. A total of 8 organization received the email indicating on the intended research questions. Approval was given after a few days and the author started to arrange an appointment with participants. Participants were very co-operative and none of them rejected the appointment.

Consent form (Appendix 3) was printed out one day prior the interview. The author explained thoroughly on every rows such as recorded interview session will encrypted and completely wiped out after author's graduation before the participant officially signed and agreed with it.

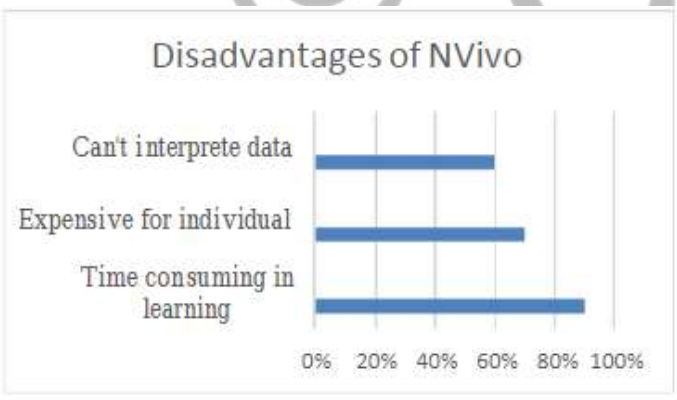
3.4.3 Data Analysis

After gathering all the data, it is finally time for the next most crucial aspect of analysing the data. **(Sutton and Austin, 2015)** discussed that the most important for this area is to be honest and true to participants' response as that is what should be meant to be heard by researchers, participants and future readers.

As this research is solely on a qualitative study, inductive approach will be used instead of deductive approach. **(I. Jebreen, 2012)** define inductive as taking the raw data from participants and transform it into concepts, theories and framework through author's interpretation. On the other hand, deductive approach involves the hypothesis in the hope of the author's desired outcome. Thus, the author will be gathering participants' information from the above mentioned primary research typically the interview and observation, Inductive approach will be deemed to be the best approach.

Next, audio-recorded information will be transcribed into PDF and subsequently coded to break down the list of themes for future research to reference. Due to the time constraint and time consuming to manually code the themes, the author will be using coding software such as NVivo for coding. **(Dollah, Abduh and Rosmaladewi, 2017)** mentioned that it can be very time consuming in learning new software and despite the benefit of identifying the themes, at times the software may not accurately interpret the data in the researchers' point of view. (Figure 25) However, in this case, Nvivo is in favour of the author as there is only 8 participants in total. On top of that, the coding can be completed within 2 weeks by using the trial version to access the adoption of cybersecurity in Organization (XXX).

Figure 25 –Disadvantages of NVivo ***(Dollah, Abduh and Rosmaladewi, 2017)***

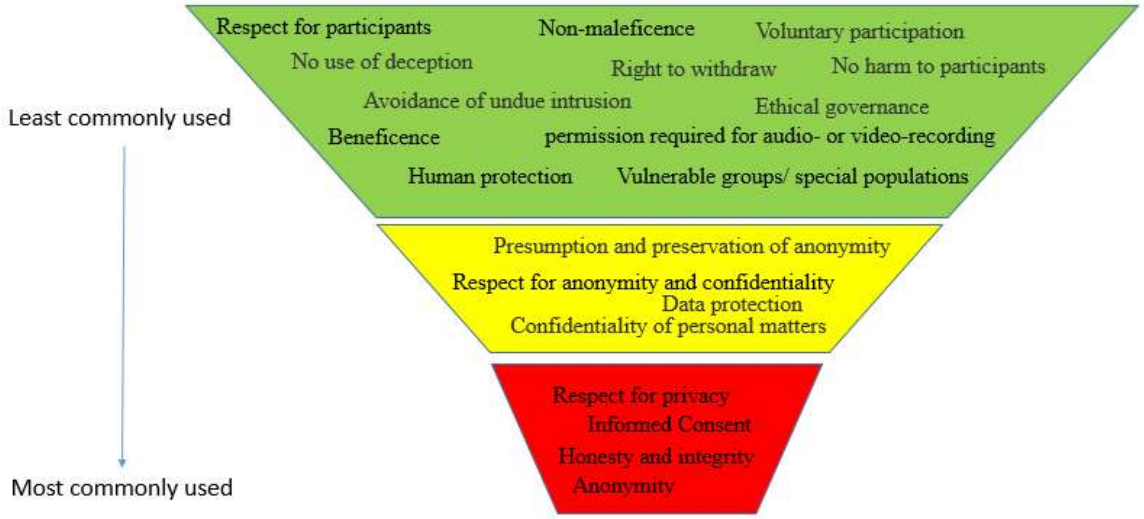


,

3.5 Ethics of Research

Ethics is considered one of the most important aspect to achieve quality outcome. Figure 26 shows an overview of ethics' principles advocates from many researchers **(Vilma, 2018, Marianna, M, 2011, Akaranga SI, Makau BK, 2016 & Vanclay, Baines and Taylor, 2013).** The top down approach funnel cascading down from green to yellow, and yellow to red shows the popularity of factors. The author has later chosen 3 principles which will be considered as the most important aspects shown below.

Figure 26 –An overview of possible ethics factors ***(Self-Developed, 2020)***



3.5.1 Privacy, Confidentiality, Anonymity

Vilma, 2018 defined confidentiality as the respect of anything that is presented as confidential such as sensitive information which can be part of cultural background, names and company (**Akaranga SI, Makau BK, 2016).**

The author has informed the 8 participants beforehand that, due to the respect of individual's dignity (**Wathuta J., Mnisi M.F. 2019),** privacy or sensitive information will never be revealed as it is for research purpose. In order to conceal the identity, the author has disguised the participants' name to a simple indication such as P1, P2, and so forth for reference.

3.5.2 Honesty and Integrity

(Akaranga SI, Makau BK, 2016) emphasized the need to be honest in front of the participants such as the researched methods, framework, information and data collected **(Vilma, 2018)** must be cited appropriately as that is part of the researchers' responsibility.

For every rows, phrases and figures, the author has did the necessary due diligence by cross-checking multiple times to ensure that this no form of plagiarism so not to violate the university rules and regulation.

3.5.3 Informed Consent

(Vilma, 2018) argued that an Informed Consent is required to have 5 components such as "*Disclosure*", "*Understanding*", "*Voluntariness*", "*Competence*" and lastly "*Consent*". Each

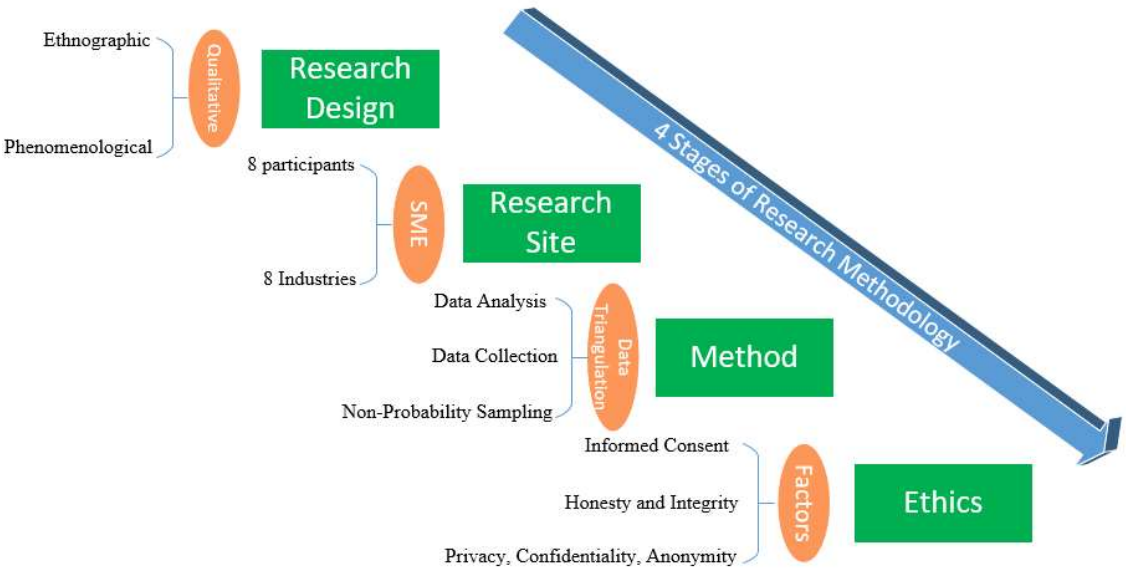
of these components are very co-related and seeks to incorporate individual rights and protecting their autonomy (**Akaranga SI, Makau BK, 2016).**

Before the commencement of the interview, the author has made a call to respective participants that a thesis research is to be carried out in August and September based on voluntary approach. During the interview day, the author has handed over the consent form as per discussed over the phone and re-emphasize on every rows to re-confirm the mutual agreement.

3.6 Summary

This study approaches on the findings of how employees actually adopt on cybersecurity practices. An overall summary of the entire research methodology comprises of the research design with 8 different industries particularly in Singapore's SME field. Later, the "*Data Triangulation*" method was implemented to collect "*Non-Probability Sampling*" in the areas of *"Convenience" and "Judgement"* approach. Data was collected was conducted via "*Semi-Structured*" interview coupled with observation method. Audio-recording session was transcribed and coded manually into different key themes. Finally, ethics was also practiced accordingly to meet the "*Confidentiality*", "*Integrity*" and "*Consent*" along with the participants for quality purpose. Last but not least, an overview of the entire mind-map can be seen it Figure 27.

Figure 27 –4 Stages of Research Methodology ***(Self-Developed, 2020)***



Chapter 4: Findings and Analysis

4.1 Introduction

The main purpose of this study is to identify how Organizational Behaviour can affect individuals' attitude and behaviour towards adopting Cybersecurity practices. A total of 8 senior and management staff from organizational were interviewed with either using video meeting such as Microsoft Teams or some via face to face meet up.

The main reason for this chapter is that it gives a whole new idea of how different aspects of Organizational Behaviour can affect the adoption of cybersecurity practices from the semi-structured interviews.

4.2 Research Question

This study began with the understanding of how Singapore SME's employees tend to behave and in terms of adopting any existing or new cybersecurity practices flowing down from the management. It is mainly pertaining to various themes within Organizational Behaviour context. Thus, it seeks to answer the research question, "How employees adopt cybersecurity practices in job performance within Singapore SME?"

4.3 Interview Questions

With regards to the interview questions, only one set of interview questions are presented across to all the participants. A detailed interview questions can be found in **(Appendix 2)**. Some participants did request for some examples of the interview questions to see if there is sensitive questions. Fortunately, all the participants did not find any difficulties understand the questions and were very passionate to give quality and professional response.

4.4 Participant Demography

A total of 8 participants from different industries were interviewed for this study. All of them were given a short 10 minutes call to confirm their comfortability before sending an official email to their Head of Organizational via email shown in **(Appendix 1)**. After getting approval from their management, the interviewer gave them a consent form to agree upon the meet up via Teams or face to face in their office.

4.4.1 Designation and Divisions

All the 8 participants hold the roles of either senior or management positions. Participants are very well aware of the organizational as they hold a very big responsibility to contribute to the organization. The participants are also from different SME's industries which cover IT, Exhibition, Design, Shipping, Audit, Law, Fashion and Lighting firm. 2 of them hold director positions such as CFO and COO. The rest of them are mostly managers such as IT infrastructure manager, security manager, senior IT system engineer, operation manager. Hence, in terms of technical, there is sufficient information and the level of understanding in terms of Cybersecurity practices is represented with professionalism.

4.4.2 Years of working experience in Organization

2 of the participants (Director) started ever since the start of the organization which the company is around for about 30 years. The rest of them worked at least more than 8 years with a very strong and solid background in IT terms as well as the operational and administration of how the organization has been running.

4.4.3 Management and Technical Experience

All the 8 participants started from the ground work and slowly climbed up the ladder to be manager. Although at some point of time, they leave the ground work for the juniors to work on it, they still hold a very strong concept of whether a solution is workable or require some form of improvement. This is due to their constant learning and passion towards their expertise.

4.5 Findings from the Interviews

All the participants were given the same set of questions and most of them are in the senior to managerial positions. There is not difficulties understanding the questions and the participants were able to answer the questions almost immediately and professionally.

Below is the summarized findings of all the 8 participants as follows:

Questions	Participants' Designation	Summary of Analysis
Working Environment / Culture		
Can you give us a brief overview of your job at company XYZ? How long have you been in your company?	All participants (2 Seniors Executive, 6 Managers and above)	2 of the senior executive works for about 4 years. Another senior executive and the 5 managers work for close to 10 years. The other 2 directors have been there for almost up to 30 years. Basically, all the participants hold a responsibility in taking care of a team of people from 5 to over 200 employees.
Can you describe team working culture in your company when undertaking projects?	All participants (2 Seniors Executive, 6 Managers and above)	The responses were quite positive as most of them have a well-organized and structured team to handle projects. 7 out of 8 respondents have a dedicated project manager/director designation. While 1 of them is holding primary role of senior IT manager as well as occasionally acting as the Project Manager.
Communication		
What is the biggest challenges you faced in handling cyberattack? How do you manage and communicate it?	All participants (2 Seniors Executive, 6 Managers and above)	6 out of 8 respondents mentioned that they have been attacked by cyberattack such as ransomware previously. Majority of them were targeted at one of the endpoint (computer) which was either left unattended with a remote session turned on or not shut down after employees left the premises. One of the main reason was due to the ***human awareness issue***. Many said that employees tend to take things too lightly when it comes to protecting their assets against cyberattack or even adopting the cybersecurity practises. Most of them would also have an **external IT service provider** to assist them on handling cyberattacks when there is any incident. The IT service provider will also recommend the company to buy or upgrade software that is vulnerable to cyberattacks, which most actually followed the right direction so as to protect their company assets.

How effective is the vertical communication within organization in considering adopting and implementing cybersecurity practices?	All participants (2 Seniors Executive, 6 Managers and above)	All the participants hesitated for a moment to answer this questions as they were thinking of the vertical communication across their departments. Only about 4 out of 8 respondents work closely with other departments to disseminate any latest cybersecurity update to the team. The other 4 respondents seem neutral in the way that they did not show much concern of sharing cybersecurity practises.
What are your challenges when convincing your peers or management level to adopt your perspective towards cybersecurity adoption? How do you overcome it?	All participants (2 Seniors Executive, 6 Managers and above)	7 out of 8 respondents felt that convincing the peers may not seem to be as tedious as the management level. In terms of persuading the management, most said that there will be 2 criteria to be met in order to attract the management attention. Firstly, "**The time must be right**", in short, there must be some case studies or references to prove why the solution such as buying cybersecurity software is required. Secondary, "**depending on needs**", for instance, upgrading the IT hardware or software will not only mitigate attacks, it will also speed up the efficiency of work for the employees as there is higher disk performance.
Decision Making and Power		
Is the management's advice been rationale all the time? Why? Could it be better?	All participants (2 Seniors Executive, 6 Managers and above)	5 out of 8 respondents gave a relatively positive feedbacks about their management decision. Most of them are quite supportive and always did a thorough study beforehand. However, the other 3 respondents felt that many times, the management only knows the surface but not the ground work. Thus, some of the decision making does not make sense at all. For instance, Candidate 1 mentioned that the management did not understand the employees' tight schedule as well as the project scale size. With only information on the surface, the management requested to perform most the project after office hours which caused many

		to be extremely fatigue in long run. Candidate 7 also emphasized that the management sometimes heed advices from their friends more than their employees who are more familiar with the internal products.
Does your team have any influencer that is able to influence the management decision making process? What are their roles? And how do they influence them?	All participants (2 Seniors Executive, 6 Managers and above)	6 out of 8 respondents are the influencer themselves. Most of influencers are either involved in the technical roles or holding the director level position. The other 2 respondents have a more open concept or rather flexible way of giving suggestion so long it is rationale and in favour to the organization. Price will also be another concern, the influencer needs to do some read up and source for a cost effective solution. In terms of the influence method, majority mentioned that a test cases and plan will be required to show the management that the solution works before purchasing the idea.
Individual and Group Motivation		
How often do you use Cybersecurity practices when instructed by management?	All participants (2 Seniors Executive, 6 Managers and above)	6 out of 8 respondents practice cybersecurity from daily to bi-monthly basis. In most cases, it was due to previous attack that motivated them to be more vigilant in adopting cybersecurity practices. Whenever, there is a suspicious or malicious activities, most will immediately communicate via email or WhatsApp group chat to ask if the file or data is from a trustworthy source. On the other hand, the other 2 respondents rely much on the IT service provider to monitor any cyber threats as they would rather put the focus on their core business.
Change Management		
How often does your company prioritize and constantly update on	All participants (2 Seniors Executive, 6	Almost 7 out of 8 respondents depend on their IT service provider to give them the latest cybersecurity updates. Whenever, they received the updates, they will be told to buy certain products to protect their

Cybersecurity latest trend?	Managers and above)	businesses. Most of the time, management will act on it if the investment is still within the budget. Otherwise, other alternative solutions will be considered such that unnecessary features can be opted out to save cost. The other respondent depends solely on himself by attending online courses regularly as he is a very passionate in learning new cybersecurity updates.
What is the biggest challenge in convincing the management that resist change in your view?	All participants (2 Seniors Executive, 6 Managers and above)	2 out of 8 respondents mentioned that everything is quite smooth when convincing the management to act on their suggestion. On the other hand, the other 6 respondents felt that the management is always very resistance to change especially when it comes to exceeding their budget. Also, even with the best solution such as investing a higher end firewall to protect the company network would be tough to convince the management if it is not the right time or from the right person to initiate this.
Leadership		
How does the management bring across Cybersecurity practices to everyone? If there is anyone refuse to accommodate to such instructions, what would be the consequences?	All participants (2 Seniors Executive, 6 Managers and above)	All the 8 respondents mentioned that most of the cybersecurity practices are delivered via various methods such as email, team gathering or via WhatsApp group chat. Majority of the employees will abide to the instructions given by the management. However minority of them are stubborn sometimes, thus warning letter or immediate termination will be carried out depending on situation.
Are there any incentives for employees to adopt cybersecurity practices in order to show its value for better work commitment?	All participants (2 Seniors Executive, 6 Managers and above)	Only 1 out of 8 respondents receives incentives such as cash voucher and a letter of commendation if the employee manages to spot and report a suspicious activities before any unforeseen and avoidable attack happen to the company. While the other 7 respondents shared the same thought that it should be the

		employees' responsibility to take care of their own data like how they take care of their personal phone.
Due to the current global pandemic (covid-19) that has affected many organizations, how did your company sustain?	All participants (2 Seniors Executive, 6 Managers and above)	2 out of 8 respondents are willing to invest to enhance cybersecurity even during pandemic period. Their main reason was that security is highly linked to a company reputation and success. Thus, they would not hesitate to invest if there is a need. All the 8 respondents were slightly affected due to the pandemic, many are working from home and projects only started just these few months when entering phase 2 of the circuit breaker (CB).
Economical Behaviour		
Was there any personal bias seen in the management when spending more money to invest in their employees?	All participants (2 Seniors Executive, 6 Managers and above)	5 out of 8 respondents mentioned that as much as possible, the management will send all the employees for training such as cybersecurity awareness course to raise employees' awareness level. Some of the employees would also be sent for other courses if the company requires employees to develop new skill set. On the hand other, the other 3 respondents felt that training or courses should only be given to the management level or those who have performed extremely well in bringing benefits to the company.

Based on the findings, the author has transcribed the audio to PDF and later did a coding using Nvivo software. The result shows 3 of the most influential themes that are "Culture & Change Management", "Decision Making & Communication", and "Leadership" as shown in Figure 28 and 30. Thus, 3 of the themes will be discussed later to show the relevance and relatedness of how different themes' theoretical framework can be used based on the responds from 8 participants.

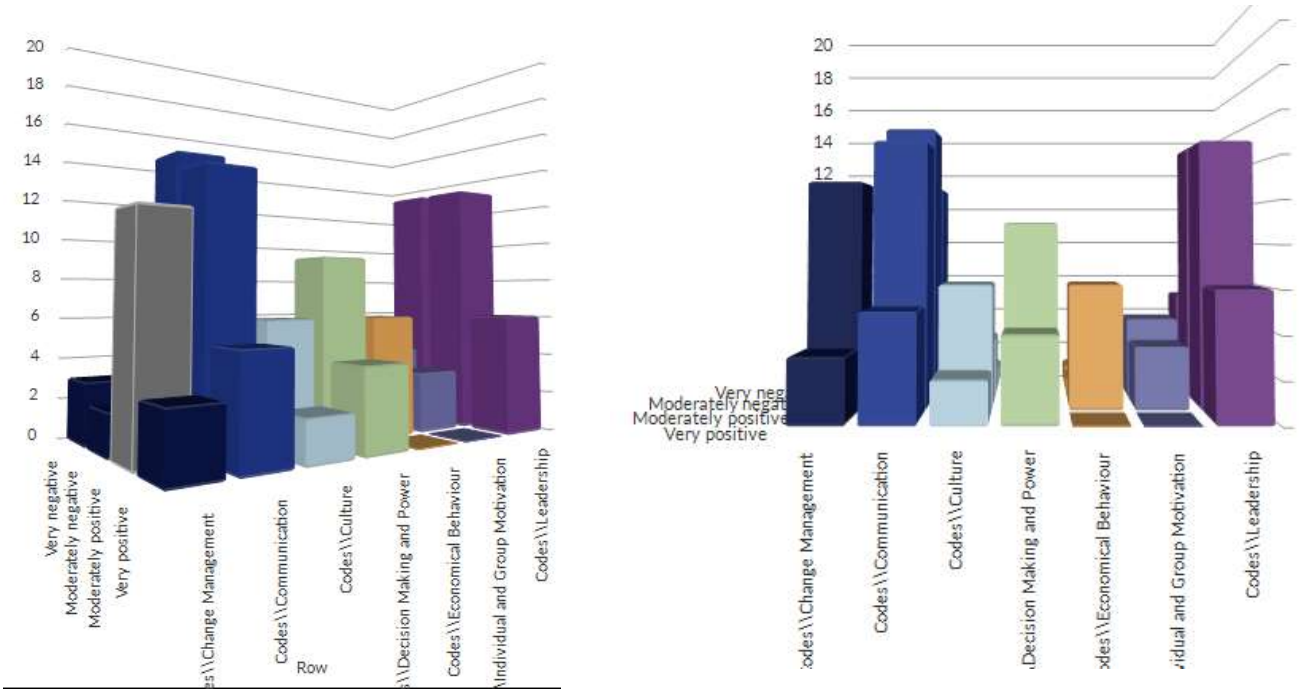
Figure 28 –3 Top Themes That Greatly Impact Employees' Behaviour (***Self-Developed, 2020)***

	A : Very negative	B : Moderately negative	C : Moderately positive	D : Very positive
1 : Codes\\Change Management	3	2	11	3
2 : Codes\\Communication	11	14	13	5
3 : Codes\\Culture	1	3	6	2
4 : Codes\\Decision Making and Power	2	5	9	4
5 : Codes\\Economical Behaviour	1	1	5	0
6 : Codes\\Individual and Group Motivation	3	4	3	0
7 : Codes\\Leadership	5	13	13	6

Based on the number of word counts (Figure 29), it also proved that the key words are closely related to the above top 3 influential themes. For instance, "Management" is linked to Decision Making as well as Leadership. "Employees" and "Team" are linked to "Culture"

Figure 29 –Top key words used by the 8 participants (***Self-Developed, 2020)***

Figure 30 –Front and Side view of Sentiment Chart Results (***Self-Developed, 2020)***



4.6 Rodosek, G. & Koch, R, (2016) – Leadership

Rodosek, G. & Koch, R, (2016) mentioned that leadership usually incorporates with a smooth "*Managing*", "*Administration*" and "*Governance*" to achieve the leadership matrix model. Based on the overall leadership summary of the 8 participants, 3 components are closely related to the leadership matrix model.

Managing is about controlling employees and external parties in favour to the company's direction and also making the right decision as a management **Rodosek, G. & Koch, R, (2016)**. 7 out of 8 respondents were seen to be able to control well in terms of setting the right expectation from the beginning towards their employees. For instance, their employees know that adopting cybersecurity practises should be individual responsibility and not something that should be asked for in return if anyone practices it diligently. One of the candidate (C5 and C8) mentioned in a very aggressive tone when asked if the incentives should be given if employees adopt cybersecurity practises to show its value for better work commitment.

C8: *"It is a responsibility and obligation to adopt the practises, and rewards should not be provided for complying!"*

C5*: The company felt that it should be employees' responsibility to take care of their data. Like how they take care of phone.*

Rodosek, G. & Koch, R, (2016) also indicated that administration is about backend support which enables an organization to execute an implementation according to the regulations. It is clear that many of the respondents gave positive feedbacks that their management give them all the best in terms of supporting them. For instance, due to the current global pandemic (covid-19), most of the employees are working from home. 5 out of 8 respondents gave feedback that their management purchased many laptops and standby their IT service provider to support them as and when if the employees face any technical issue. Thus, administration is part of the process that will impact employees' behaviour. Both candidate 1 and 4 also expressed the support given from their management.

C1: *"Due to the pandemic and as per our local authority regulation, we were being placed to work from home. Communication and remote support were still possible over the past few couple of months."*

C4: *"Yes, during this lock down period, we definitely spend more money to buy hardware such as laptops for our employees working from home."*

Lastly, it will be the governance which includes many aspects such as guidelines, procedures and high-level structure in terms of how the organization should plan the governing process **Rodosek, G. & Koch, R, (2016).** Governance is as important as without a proper governance process, the entire organization will be put to risk or even threaten by internal employees due to politics. All the 8 respondents mentioned that they were given a proper instruction and guidelines to follow before joining the company. As and when if there is any new instruction such as following a standard set of cybersecurity practises, majority will abide to it. A warning or termination letter will also be issued if one tends to break the regulation too often. Candidate 6 set a very good example of how the organization governs the entire process which is put across everyone regardless of their status.

C6: *"New hirers will be provided a copy of all IT policies, including Acceptable usage, security and VPN policies. Which then they will sign accordingly on all pages to acknowledged. When there is a breach on conduct it will start by a warning letter depending on the severity at worst, termination."*

4.7 Ryttare, E. (2019) - Organization Culture & Change Management

Ryttare, E. (2019) is a perfect model to be discussed in terms of how the change evolves over the time. It kicks off with the preparation stage which the organization should prepare the

pre-requisite for the change. Next, the change will be executed after the preparation and lastly to sustain the change, organization will need to evaluate the results and observe the employees' behaviour for continuous improvement.

Preparation stage comprises of key activities such as establishing top management support and finding the right key roles and responsibility. Candidate 1 stated that having the right people with the right roles and responsibility to support any new proposed solution or idea will increase the chances of management agreement.

C1: *"Sometimes, when I have my own opinion, I will require second and third perspectives who are mainly my direct supervisor or senior colleague who is experienced in the particular field to support me and convince my management"*

Implementation stage comprises of educating the employees and enable feedback to prepare for the post stage. Candidate enjoyed working with his team whenever there is any new projects as it is always an opportunity to learn new things.

C7: *"We have a team of excellent engineers who are very friendly and always share their knowledge within the team. Whenever, there is any project, the project head will take the lead and manage the team accordingly"*

Post stage comprises of sustaining the change by constantly collecting feedbacks and monitor the employees' behaviour for any area of improvement. For instance, candidate 1 mentioned that at any point of time, if any employee is interested in any course such as cybersecurity, management will not hesitate to send them so nurture and groom their skillset and knowledge.

4.8 M'manga et al., (2019) - Decision Making & Communication

M'manga et al., (2019) discussed that a proper decision making process requires a correct formation to come up with a rationale conclusion. 5 out of 8 respondents felt that the management decision is one of the most important aspect that will influence their behaviour towards cybersecurity practises.

Two of the key components of **M'manga et al., (2019)** model would be "Situation assessment" and "Goal Formation". Situation awareness targets at the level of understanding the situation before acting on the real scenario. **R. Nurse, (2013)** also supported that communication and understanding of the design is extremely important as it will affect the

decision making process. Most of the candidates gave positive feedbacks that the management decision is mostly practical and make sense to the majority. Most of the candidate gave similar comments like what Candidate 3 has stated as shown below.

C3: *"Most of the time, he is very practical as he has done his homework and cross check with the respective cybersecurity vendors to ensure any proposed solution is workable"*

On the other hand, goal formation discussed on a few factors such as "what is the goal?" and "what is the obstacles that will hinder the goal to success". Majority of the candidates were able to influence the management to make certain decision that is related to cybersecurity. The ultimate goal is to achieve a strong position in strengthening the security of their IT infrastructure. However, 2 of the candidates faced many obstacles when trying to convince or influence the management. There are many reasons such as the high investment that exceeded the organization budget, the confidence level of new products as well as the necessity of the product to invest on. Candidate 3, 6 and 8 mentioned that a proof of concept (POC) is necessary every time if there is a new product or upgrade requirement. Once the evaluation has been completed successfully, most management will be able to proceed with the acknowledgement of buying the solution.

Chapter 5: Conclusion and Recommendations

5.1 Summary of Research Paper

This paper had set out to examine the adoption of Cybersecurity practises from an employee point of view by reviewing existing literature. Some of common themes such as "Psychology" and "Law & Justice" were identified but later it was found that there was a research gap that could be a factor of an individual behaviour and attitude towards Cybersecurity practises. Organizational behaviour, Economics and Personal Experience were brought into the picture with about to 8 different themes. These themes were broadly studied in the aspect of analysing employees' behaviour especially towards the adoption of Cybersecurity globally in the recent years. However, to leverage on these themes in Singapore, a more in-depth research was carried out to discern which themes will impact the organization most. Thus, it leads to warranting this study in attempt to answer the Research Question:

"How employees perceive the adoption of cybersecurity in job performance within Company XYZ?"

This study involves the empirical research which is mainly on qualitative rather than quantitative. The qualitative research consists of semi-structured, video meeting and face to face interview. As the study is based within Singapore SMEs, a total of 8 participants from all different industries were interviewed. Of all the 8 participants, 2 are Seniors Executive and the rest are managers and above. Interview session was recorded and transcribed with NVivo to capture the themes and the key words.

8 of the participants were interviewed for about 30minutes each and the interviews aimed to answer the following questions:

1) Are there any incentives for employees to adopt cybersecurity practices in order to show its value for better work commitment?
2) What are your challenges when convincing your peers or management level to adopt your perspective towards cybersecurity adoption?
3) What is the biggest challenge in convincing the management that resist change in your view?

4) How effective is the vertical communication within organization in considering adopting and implementing cybersecurity practices?

The interview findings revealed that majority of the employees in their respective Organization XXX are more likely to be affected from the perspective of Organizational Behaviour. Popular themes such as Theory of Reasoned Action (TRA), Theory of Planned Behaviour (TRB) and Technology Acceptance Model (TAM) are proven to be gradually fading away as the time passed. In the modern days, Organizational Behaviour tends to be changing the way employees think and act on certain rules and regulation.

Even though all the themes in Organizational Behaviour are relatively important with some overlapping with one another, the findings of the research were dived down to three models;

- M'manga et al., (2019) - Decision Making & Communication
- Ryttare, E. (2019) - Organization Culture & Change Management
- Rodosek, G. & Koch, R, (2016) – Leadership

Rodosek, G. & Koch, R, (2016) focused on how a leadership matrix model such as "*Managing*", "*Administration*" and "*Governance" would affect Organization XXX which was proven from some of the participants. While* M'manga et al., (2019) shed light that a leader needs to also make practical and rationale decision in order to influence the employees' behaviour which some of the participants completely agreed with it. Lastly, with Ryttare, E. (2019) model, organization culture and change management are the toughest themes for any organization to adopt successfully as culture could not be replicated identically from one place to another, thus change management would be necessary to influence the employees' behaviour in the correct direction.

In sum, all these factors guided the researcher to answer the Research Question, "*How employees perceive the adoption of cybersecurity in job performance within Company XYZ?"* In conclusion, Organizational Behaviour should be applied more frequent in the study of adoption of Cybersecurity practises.

5.2 Research Limitation

This research study was supported with many in-depth empirical researches over the past few years. As the findings were drawn from 8 different industries in Singapore's SME, it can however be applied to a majority of businesses in Singapore since Singapore's SME

constitutes about 99% in total (Singstat, 2019). Thus, it dictates how Singapore can be affected by cyberattack or a potential risk could arise if most of the SMEs are not in favour to adopt cybersecurity practises diligently.

However, there could be a lot more factors to be discovered as this research is purely based on the adoption of cybersecurity in the OB Context. Furthermore, this exploratory is only focused on a qualitative aspect which could however be expanded to quantitative for a comparison and see if the result is the same in terms of picking up the most influential OB's theme. Thus, there is still limitation for further research.

5.3 Recommendations for Future Research

As mentioned above, a further research can be carried out with a quantitative study or even a hybrid of qualitative and quantitative approach to understand and validate the contradictions of the results. **(Wisdom J and Creswell JW, 2013)** mentioned that a mixed method of integrating qualitative and quantitative can provide a rich and comprehensive data and even augment the outcomes to for a more in-depth research. On the other hand, this paper examined only the SME's field, future researcher can however focus on MNC or even other industries apart from the authors' findings to increase the reliability of findings.

5.4 Contributions

This study has been researched in the field of Organizational Behaviour that is proven theoretically or even empirically that it is applicable to understanding an individual behaviour adopting cybersecurity. Also, this paper has demonstrated that more studies can be carried out to identify other factors contributing to adoption of cybersecurity practises regardless of the size and industries of Singapore's organization.

Bibliography

A.Bendovschi, A. Al-Nemrat and B. Ionescu. (2016). Statistical Investigation into the Relationship between Cyber-Attacks and the Type of Business Sectors. International Journal of Business Humanities and Technology, vol. 6, no. 1, pp. 49-61.

Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. Technology Innovation Management Review, 5(1): 5-14.

Adam Segal, Valeriy Akimenko, Keir Giles, Daniel A. Pinkston, James A. Lewis, Benjamin Bartlett, Hsini Huang, and Elina Noor. (2020). Asia policy, volume 15, number 2 (April 2020), 57–114 https://www.nbr.org/publication/asia-policy-15-2-april-2020/

Adharsh Krishnan, M. Deva Priya. (2019). The Future of Cyber Security. International Journal of Advance Research, Ideas and Innovations in Technology, 5(2) www.IJARIIT.com.

Ahmad, Tabrez. (2020). Corona Virus (COVID-19) Pandemic and Work from Home: Challenges of Cybercrimes and Cybersecurity. Available at SSRN: http://dx.doi.org/10.2139/ssrn.3568830

Ahmady, G., Mehrpour, M. and Nikooravesh, A. (2016). Organizational Structure. *Procedia - Social and Behavioral Sciences*, 230, pp.455-462.

Ajayi, Victor. (2017). Primary Sources of Data and Secondary Sources of Data. 10.13140/RG.2.2.24292.68481.

Akintaro, Mojolaoluwa, Teddy Pare, and Akalanka Mailewa Dissanayaka. (2019). "Darknet and black market activities against the cybersecurity: A survey", In The Midwest Instruction and Computing Symposium. (MICS), North Dakota State University, Fargo, ND, April 5-6

Akaranga SI, Makau BK. (2016) "Ethical considerations and their applications to Research: A case of the University of Nairobi." Journal of Educational Policy and Entrepreneurial Research. 2016;3(12):1-9.

Alghananeem, K., Altaee, M. and Jida, B. (2014). The Impact of the Goals of Information Security Standards to Ensure Information Security. *Journal of Management Research*, 6(2), p.74.

Alhassan, Mohammed & Adjei-Quaye, Alexander. (2017). Information Security in an Organization. International Journal of Computer (IJC). pp 100-116.

Almeida, Fernando & Faria, Daniel & Queirós, André. (2017). Strengths and Limitations of Qualitative and Quantitative Research Methods. European Journal of Education Studies. 3. 369-387. 10.5281/zenodo.887089.

Alqahtani, F. (2017). Developing an Information Security Policy: A Case Study Approach. *Procedia Computer Science*, 124, pp.691-697.

Al-Qahtani, H.S. (2016). Latest Trends and Future Directions of Cyber Security Information Systems. Journal of Information Engineering and Applications, 6, 9-14.

Arora, B. (2016). Exploring and analyzing Internet crimes and their behaviours. *Perspectives in Science*, 8, pp.540-542.

Aspers, P. and Corte, U. (2019). What is Qualitative in Qualitative Research. *Qualitative Sociology*, 42(2), pp.139-160.

Aye Mya Sandar, Ya Min, Khin Myat Nwe Win. (2019). Fundamental Areas of Cyber Security on Latest Technology. Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456- 6470, Volume-3, Issue-5, August 2019, pp.981-983

Azmi, R., Kautsarina, K., Apriany, I. and Tibben, W. (2020). Revisiting "Cyber" Definition. Modern Theories and Practices for Cyber Ethics and Security Compliance, pp.1-17.

Bada et al, M. Bada, A. Sasse, J.R.C. Nurse. (2015). Cyber security awareness campaigns: Why do they fail to change behaviour? International Conference on Cyber Security for Sustainable Society 2015 Conference paper (2015), 118–31

Barrow, Donna Marie. (2017). A Phenomenological Study of the Lived Experiences of Parents of Young Children with Autism Receiving Special Education Services. Dissertations and Theses. Paper 4035.

Bashir, M., Wee, C., Memon, N. and Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. Computers & Security, 65, pp.153-165.

Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, 2, pp.8-14.

Benjamin Dean and Rose McDermott. (2017). A Research Agenda to Improve Decision Making in Cyber Security Policy, 5 PENN. ST. J.L. & INT'L AFF. 29.

Blythe, J.M. (2013). Cyber security in the workplace: Understanding and promoting behavior change. In: Proceedings of CHI Italy Doctoral Symposium, Trento, September 1-10

Bolderston, A. (2012). Conducting a Research Interview. Journal of Medical Imaging and Radiation Sciences, 43(1), pp.66-76.

Box D, Pottas D. (2014). A model for information security compliant behaviour in the healthcare context. Procedia Technol.16:1462–70.

Bruce, A., Beuthin, R., Sheilds, L., Molzahn, A. and Schick-Makaroff, K. (2016). Narrative Research Evolving. *International Journal of Qualitative Methods*, 15(1), p.160940691665929.

Butina, M. (2015). A narrative approach to qualitative inquiry. Clinical Laboratory Science, 28(3), 190-196.

Bynum, T. (2016). The evolution of homeland security: A hermeneutic phenomenological exploration toward defining the term.

Cacciattolo, K. (2015). Defining organisational communication. European Scientific Journal, 11(20), 79-87.

Carrapico, H. and Barrinha, A. (2018). European Union cyber security as an emerging research and policy field. European Politics and Society, 19(3), pp.299-303.

Ceauşu, Ioana & Murswieck, R. & Kurth, Bastian & Ionescu, Razvan. (2017). The organization culture as a support of innovation processes. International Journal of Advanced Engineering and Management Research. 2. 2392.

Choi, Min & Levy, Yair & Hovav, Anat & Choi. (2013). The Role of User Computer Self-Efficacy, Cybersecurity Countermeasures Awareness, and Cybersecurity Skills Influence on Computer Misuse.

Chuang, L., Chen, P. and Chen, Y. (2016). The Determinant Factors of Employees' Behavioural Intention in Green Building Restaurants - Integration TRA and TAM. Universal Journal of Management, 4(12), pp.704-713.

Chun Tie, Y., Birks, M. and Francis, K. (2019). Grounded theory research: A design framework for novice researchers. *SAGE Open Medicine*, 7, p.205031211882292.

Ching, Chang, H., Ya, Wang., and Squires, S. (2016). Using Trace Ethnography to Compare Perceived Cyber-Threats of IT to Non-IT Professionals. Twenty-second Americas Conference on Information Systems, San Diego.

CIS. (2020). *Cybersecurity Best Practices - CIS*. [online] Available at: <https://www.cisecurity.org/cybersecurity-best-practices/> [Accessed 3 July 2020].

Cleveland, Simon & Cleveland, Marisa. (2018). Toward Cybersecurity Leadership Framework.

Colquitt, J., LePine, J., Wesson, M. (2014). Organizational Behavior: ImprovingPerformance and Commitment in the Workplace, McGraw-Hill, New York.

Cowger, T., Tritz, J. (2019). Narrative Analysis Research: A Tool for Extension Educators Extension conferences. Journal of Extension, 57(6), Article 6TOT5

Cyberark. (2020). *5 IT Best Practices That Also Mitigate Cyber Security Vulnerabilities In OT*. [online] Available at: https://www.cyberark.com/resources/blog/5-it-best-practices-that-also-mitigate-cyber-security-vulnerabilities-in-ot [Accessed 3 July 2020].

C. I. Cybersecurity. (2014). Framework for Improving Critical Infrastructure Cybersecurity, Framework, vol. 1, pp. 11.

D. Kriz. (2011). Cybersecurity principles for industry and government: A useful framework for efforts globally to improve cybersecurity, *2011 Second Worldwide Cybersecurity Summit (WCS)*, London, pp. 1-3.

David J. Oberly. (2019). Best Practices for Effectively Defending against Ransomware Cyber Attacks. The Intellectual Property & Technology Law Journal (Vol. 31, No. 7), a Wolters Kluwer publication. Reprinted with permission.

de Bruijn, H. and Janssen, M. (2017). Building Cybersecurity Awareness: The need for evidence-based framing strategies. *Government Information Quarterly*, 34(1), pp.1-7.

DeJonckheere, M. and Vaughn, L. (2020). *Semistructured Interviewing In Primary Care Research: A Balance Of Relationship And Rigour*.

Diakun-Thibault, Nadia. (2014). Defining Cybersecurity. Technology Innovation Management Review. 2014.

Diesch, R., Pfaff, M. and Krcmar, H. (2018). Prerequisite to Measure Information Security - A State of the Art Literature Review. *Proceedings of the 4th International Conference on Information Systems Security and Privacy*.

Dollah, S., Abduh, A. and Rosmaladewi, M. (2017). Benefits and Drawbacks of NVivo QSR Application. Proceedings of the 2nd International Conference on Education, Science, and Technology (ICEST 2017).

Dorosh, M., Lytvynov, V., Saveliev, M. (2015). Project management in cybersecurity research in Ukraine. Information models & analyses. Volume 4, 324-335.

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, J. W., & Winkelman, Z. (2018). Estimating the Global Cost of Cyber Risk. Research Reports RR-2299-WFHF, Rand Corporation.

Dunn Cavelty, M. and Wenger, A., 2019. Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy*, 41(1), pp.5-32.

Dutton, W. H. (2017). Fostering a cyber security mindset. Internet Policy Review, 6(1). DOI: 10.14763/2017.1.443.

E. Luiijf et al. (2013). Nineteen national cyber security strategies. Int. J. Crit. Infrastructure, vol. 9, no. 1.2, pp. 3-31.

Ebneyamini, S. and Sadeghi Moghadam, M. (2018). Toward Developing a Framework for Conducting Case Study Research. International Journal of Qualitative Methods, 17(1), p.160940691881795.

Enisa. (2019). Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity. European Union Agency for Network and Information Security (ENISA) ISBN: 978-92-9204-267-7.

Erlingsson, C. and Brysiewicz, P. (2017). A hands-on guide to doing content analysis. *African Journal of Emergency Medicine*, 7(3), pp.93-99.

Etikan, I. (2017). Combination of Probability Random Sampling Method with Non Probability Random Sampling Method (Sampling Versus Sampling Methods). *Biometrics & Biostatistics International Journal*, 5(6).

Evans, M., Maglaras, L., He, Y. and Janicke, H. (2016). Human behaviour as an aspect of cybersecurity assurance. Security and Communication Networks, 9(17), pp.4667-4679.

Ewing, M., Men, L. R., & O'Neil, J. (2019). Using social media to engage employees: Insights from internal communication managers. International Journal of Strategic Communication, 13(2), 110-132.

Faga, H. (2017). The Implications of Transnational Cyber Threats in International Humanitarian Law: Analysing the Distinction Between Cybercrime, Cyber Attack, and Cyber Warfare in the 21st Century. Baltic Journal of Law & Politics, 10(1), pp.1-34.

Fazlida, M. and Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. *Procedia Economics and Finance*, 28, pp.243-248.

Foerster-Metz, U., Marquardt, K., Golowko, N., Kompalla, A. and Hell, C. (2018). Digital Transformation and its Implications on Organizational Behavior. *Journal of EU Research in Business*, pp.1-14.

Ganta, V. C. and Manukonda, J. K. (2014). Leadership During Change And Uncertainty In Organizations. International Journal of Organizational Behaviour & Management Perspectives, 3(3), 1183.

Glazer, Sharon & Karpati, T. (2014). The role of culture in decision making. 27. 23-29.

Gordon, L., Loeb, M., Lucyshyn, W. and Zhou, L. (2015). Increasing cybersecurity investments in private sector firms. *Journal of Cybersecurity*, p.tyv011.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J. and Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security*, 73, pp.345-358.

Guariniello, C. and DeLaurentis, D. (2014). Communications, Information, and Cyber Security in Systems-of-Systems: Assessing the Impact of Attacks through Interdependency Analysis. *Procedia Computer Science*, 28, pp.720-727.

Gutta, Ramamohan. (2019). Managing Security Objectives for Effective Organizational Performance Information Security Management. Walden Dissertations and Doctoral Studies. 7147. https://scholarworks.waldenu.edu/dissertations/7147.

H. Widhiastuti. (2013). The Effectiveness of Communications in Hierarchical Organizational Structure, *International Journal of Social Science and Humanity*, vol. 2, no. 3, pp. 185-190.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), p.e00346.

Hao, M. J., & Yazdanifard, R. (2015). How Effective Leadership can Facilitate Change in Organizations through Improvement and Innovation. Global Journal of Management and Business Research: Administration and Management, 15(9), 1-5.

Haselhuhn, Michael P., et al. (2012). The Impact of Personal Experience on Behavior: Evidence from Video-Rental Fines. Management Science, vol. 58, no. 1, 2012, pp. 52–61.

Howard, David J. (2018). Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents. Graduate Theses and Dissertations. https://scholarcommons.usf.edu/etd/7306.

Huang, K. and Pearlson, K. (2019). For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. Proceedings of the 52nd Hawaii International Conference on System Sciences.

Hussein, M. E., Hirst, S., Salyers, V., & Osuji, J. (2014). Using Grounded Theory as a Method of Inquiry: Advantages and Disadvantages. The Qualitative Report, 19(27), 1-15. Retrieved from https://nsuworks.nova.edu/tqr/vol19/iss27/3.

Hutchins, M., Bhinge, R., Micali, M., Robinson, S., Sutherland, J. and Dornfeld, D. (2015). Framework for Identifying Cybersecurity Risks in Manufacturing. *Procedia Manufacturing*, 1, pp.47-63.

I. Jebreen. (2012). Using inductive approach as research strategy in requirements engineering, International Journal of Computer and Information Technology, vol. 01, no. 02, pp. 162-173.

Iiroc.ca. 2020. [online] Available at: <https://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf> [Accessed 3 July 2020].

J. R. Nurse. (2013). Effective communication of cyber security risks. *7th International Scientific Conference on Security and Protection of Information (SPI 2013)*.

Jalal, A. (2017). Impacts of Organizational Culture on Leadership's Decision- Making. Journal of Advances in Management Sciences & Information Systems, 3, pp.1-8.

Jalali, M., Siegel, M. and 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), pp.66-82.

Jhee Jiow, H. (2013). Cyber Crime in Singapore: An Analysis of Regulation based on Lessig's four Modalities of Constraint. Singapore.

Julie M. Haney and Wayne G. Lutters. (2019). Motivating Cybersecurity Advocates: Implications for Recruitment and Retention. In SIGMIS-CPR '19: ACM SIGMIS Computers and Personnel Research, June 20–22, 2019, Nashville, TN . ACM, New York, NY, USA, 9 pages. https://doi.org/10.1145/3322385. 3322388.

Kabir, Syed Muhammad. (2016). METHODS OF DATA COLLECTION.

Kaifi, Belal & Noori, Selaiman. (2011). Organizational Behavior: A Study on Managers, Employees, and Teams. Journal of Management Policy and Practice. 12.

Katzan, K. (2016). Contemporary Issues in Cybersecurity. Retrieved from http://southeastinforms.org/Proceedings/2012/proc/p120604001.pdf.

Kessler, G. C., & Ramsay, J. (2013). Paradigms for Cybersecurity Education in a Homeland Security Program. Journal of Homeland Security Education, 2(). Retrieved from https://commons.erau.edu/dbsecurity-studies/7.

Khari, M., Shrivastava, G., Gupta, S. and Gupta, R. (2018). Role of Cyber Security in Today's Scenario. *Cyber Security and Threats*, pp.1-15.

Khlaponin, Y., Kondakova, S., Shabala, Y., Yurchuk, L. and Demianchuk, P. (2019). ANALYSIS OF THE STATE OF CYBER SECURITY IN THE LEADING COUNTRIES OF THE WORLD. *Cybersecurity: Education Science Technique*, (4), pp.6-13.

Kim Y., Kim I., Park N. (2014). Analysis of Cyber Attacks and Security Intelligence. In: Park J., Adeli H., Park N., Woungang I. (eds) Mobile, Ubiquitous, and Intelligent Computing. Lecture Notes in Electrical Engineering, vol 274. Springer, Berlin, Heidelberg.

Koch, Robert. (2017). On the Future of Cybersecurity.

Kremer, J. (2014). Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information & Communications Technology Law*, 23(3), pp.220-237.

Krusenvik, L. (2016). Using case studies as a scientific method: Advantages and disadvantages. Retrieved March 14, 2018.

Kumar, S., Deshmukh, V. and Adhish, V. (2014). Building and leading teams. *Indian Journal of Community Medicine*, 39(4), p.208.

Kumar. (2019). Research methodology: A step-by-step guide for beginner Sage Publications Limited.

Kure, H., Islam, S. and Razzaque, M. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences*, 8(6), p.898.

Lai, E.R. (2011). Motivation: A Literature Review. Pearson Research Report.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. Management Research Review, Vol. 37 No. 12, pp. 1049-1092. https://doi.org/10.1108/MRR-04-2013-0085.

Levy, Y., Ramim, M. and Hackney, R. (2013). Assessing Ethical Severity of e-Learning Systems Security Attacks. Journal of Computer Information Systems, 53(3), pp.75-84.

Lynne Coventry, Pamela Briggs, John Blythe, and Minh Tran. (2014). Using behavioural insights to improve the public's use of cyber security best practices. Technical Report. Northumbria University.

M. Hathaway. (2012). Leadership and Responsibility for Cybersecurity, *Georg. J. Int. Aff.*, pp. 71-80.

M'manga, A., Faily, S., McAlaney, J., Williams, C., Kadobayashi, Y. and Miyamoto, D. (2019). A normative decision-making model for cyber security. Information & Computer Security, 27(5), pp.636-646.

Maalem Lahcen, R., Caulkins, B., Mohapatra, R. and Kumar, M. (2020). Review and insight on the behavioral aspects of cybersecurity. *Cybersecurity*, 3(1).

Majid, U. (2017). Research Fundamentals: The Research Question, Outcomes, and Background. The Undergraduate Research in Natural and Clinical Science and Technology (URNCST) Journal, 1(2), pp.1-7.

Maple, C. (2017). Security and privacy in the internet of things. *Journal of Cyber Policy*, 2(2), pp.155-184.

Maqbool, Z., Makhijani, N., Pammi, V. and Dutt, V. (2016). Effects of Motivation: Rewarding Hackers for Undetected Attacks Cause Analysts to Perform Poorly. *Human Factors: The Journal of the Human Factors and Ergonomics Society*, 59(3), pp.420-431.

Marianna, M. (2011). What are the major ethical issues in conducting research? Is there a conflict between the research ethics and the nature of nursing? Health science journal, 5.

Michel, M. and King, M. (2019). Cyber Influence of Human Behavior: Personal and National Security, Privacy, and Fraud Awareness to Prevent Harm. *2019 IEEE International Symposium on Technology and Society (ISTAS)*.

Miranda Silgado, David. (2018). Cyber-attacks: a digital threat reality affecting the maritime industry. World Maritime University Dissertations. 663.

Moore, FahmeenaOdetta. (2017). Qualitative Design Options for a Study. 10.13140/RG.2.2.21925.29925.

Mouton, Francois & de Coning, Arno. (2020). COVID-19: Impact on the Cyber Security Threat Landscape.

Moser, A. and Korstjens, I. (2017). Series: Practical guidance to qualitative research. Part 3: Sampling, data collection and analysis. *European Journal of General Practice*, 24(1), pp.9-18.

Mukherjee, Sourav. (2019). Overview of the Importance of Corporate Security in business. 10.15680/IJIRSET.2019.0804002.

Myriam Dunn Cavelty and Florian J. Egloff. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. St Antony's International Review 15 no.1:37-57.

N. Gupta Gourisetti, M. Mylrea and H. Patangia. (2019). Application of Rank-Weight Methods to Blockchain Cybersecurity Vulnerability Assessment Framework," 2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, NV, USA, pp. 0206-0213, doi: 10.1109/CCWC.2019.8666518.

Neubauer, B., Witkop, C. and Varpio, L. (2019). How phenomenology can help us learn from the experiences of others. *Perspectives on Medical Education*, 8(2), pp.90-97.

NIST. (2020). *Cybersecurity Framework*. [online] Available at: https://www.nist.gov/cyberframework [Accessed 3 July 2020].

Omar Y. Sharkasi. (2015). Addressing Cybersecurity Vulnerabilities, ISACA Journal., vol 5, pp. 19-29.

P.S, S., S, N. and M, S. (2018). Overview of Cyber Security. IJARCCE, 7(11), pp.125-128.

Pan, X., Chen, M., Hao, Z. and Bi, W. (2018). The Effects of Organizational Justice on Positive Organizational Behavior: Evidence from a Large-Sample Survey and a Situational Experiment. *Frontiers in Psychology*, 8.

Peyton, T., Zigarmi, D. and Fowler, S. (2019). Examining the Relationship Between Leaders' Power Use, Followers' Motivational Outlooks, and Followers' Work Intentions. *Frontiers in Psychology*, 9.

Pfleeger, S. and Caputo, D. (2012). Leveraging behavioral science to mitigate cyber security risk. Computers & Security, 31(4), pp.597-611.

Porter, Jason, Sr. (2019). Capitol Technology University, ProQuest Dissertations Publishing, 2019. 27668373.

Pung, R., Chiew, C., Young, B., Chin, S., Chen, M., Clapham, H., Cook, A., Maurer-Stroh, S., Toh, M., Poh, C., Low, M., Lum, J., Koh, V., Mak, T., Cui, L., Lin, R., Heng, D., Leo, Y., Lye, D., Lee, V., Kam, K., Kalimuddin, S., Tan, S., Loh, J., Thoon, K., Vasoo, S., Khong, W., Suhaimi, N., Chan, S., Zhang, E., Oh, O., Ty, A., Tow, C., Chua, Y., Chaw, W., Ng, Y., Abdul-Rahman, F., Sahib, S., Zhao, Z., Tang, C., Low, C., Goh, E., Lim, G., Hou, Y., Roshan, I., Tan, J., Foo, K., Nandar, K., Kurupatham, L., Chan, P., Raj, P., Lin, Y., Said, Z., Lee, A., See, C., Markose, J., Tan, J., Chan, G., See, W., Peh, X., Cai, V., Chen, W., Li, Z., Soo, R., Chow, A., Wei, W., Farwin, A. and Ang, L. (2020). Investigation of three clusters of

COVID-19 in Singapore: implications for surveillance and response measures. *The Lancet*, 395(10229), pp.1039-1046.

Qaddo, Myasar. (2019). Participant Observation as Research Methodology: Assessing the Validity of Qualitative Observational Data as Research Tools.

Quigley, K., Burns, C., & Stallard, K. (2013). Communicating Effectively about Cyber-Security Risks: Probabilities, Peer Networks and a Longer Term Education Program. Halifax, Canada: Dalhousie University.

Quigg, M., Lopez, J., Rice, M., Grimaila, M. and Ramsey, B. (2016). Cyberspace and Organizational Structure: An Analysis of the Critical Infrastructure Environment. Critical Infrastructure Protection X, pp.3-25.

Reddy, Nikhita G., and Reddy, Ugander G.J. (2014) A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies.

Reeves, S., Peller, J., Goldman, J. and Kitto, S. (2013). Ethnography in qualitative educational research: AMEE Guide No. 80. *Medical Teacher*, 35(8), pp.e1365-e1379.

Rodosek, G. & Koch, R. (2016). Proc. of the 15th European Conference on Cyber Warfare and Security ECCWS-2016, Munchen, Germany, 6.-7.7.2016, pp. 173-181, Academic Conferences and Publishing International Limited.

Ryttare, E. (2019). Change Management: A Key in Achieving Successful Cyber Security: A Multiple Case Study of Organizations in Sweden.

Sacha Tessier Stall. (2011). The Future of Cybersecurity, The Hague Centre for Strategic Studies and TNO, Paper No. 2011-4, 3 February 2011, http://www.hcss.nl/reports/the-future-of-cybersecurity/19/ (11 December 2013), p.7.

Salaheddine Bendak, Amir Moued Shikhli & Refaat H. Abdel-Razek. (2020). How changing organizational culture can enhance innovation: Development of the innovative culture enhancement framework, Cogent Business & Management, 7:1, DOI: 10.1080/23311975.2020.1712125.

Santos, K., Ribeiro, M., Queiroga, D., Silva, I. and Ferreira, S. (2020). O uso de triangulação múltipla como estratégia de validação em um estudo qualitativo. *Ciência & Saúde Coletiva*, 25(2), pp.655-664.

Shan, C., Jiang, B., Xue, J., Guan, F. and Xiao, N. (2018). An Approach for Internal Network Security Metric Based on Attack Probability. *Security and Communication Networks*, 2018, pp.1-11.

Showkat, Nayeem & Parveen, Huma. (2017). Non-Probability and Probability Sampling.

Sibi Chakkaravarthy, S., Sangeetha, D., Venkata Rathnam, M., Srinithi, K. and Vaidehi, V. (2018). Futuristic cyber-attacks. *International Journal of Knowledge-based and Intelligent Engineering Systems*, 22(3), pp.195-204.

Soares, Laura Porter. (2018). Organizational Politics: Harmful or Helpful?. Instructional Design Capstones Collection. 44.

Sutton, J. and Austin, Z. (2015). Qualitative Research: Data Collection, Analysis, and Management. The Canadian Journal of Hospital Pharmacy, 68(3).

Świątkowska, J. (2020) Tackling cybercrime to unleash developing countries' digital potential. Pathways for Prosperity Commission Background Paper Series; no. 33. Oxford, United Kingdom.

Szumski, O. (2018). Cybersecurity best practices among Polish students. *Procedia Computer Science*, 126, pp.1271-1280.

Taherdoost, H. (2016). Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *SSRN Electronic Journal*.

Tayal, R., Kumar Upadhya, R., Yadav, M., Rangnekar, S. and Singh, R. (2018). The impact of transformational leadership on employees' acceptance to change. VINE Journal of Information and Knowledge Management Systems, 48(4), pp.559-578.

Teherani, A., Martimianakis, T., Stenfors-Hayes, T., Wadhwa, A. and Varpio, L. (2015). Choosing a Qualitative Research Approach. Journal of Graduate Medical Education, 7(4), pp.669-670.

Thakur, G. R. (2014). A study of organizational behavior of college of education of Maharashtra state. India: North Maharashtra University.

Tran, S. (2017). GOOGLE: a reflection of culture, leader, and management. International Journal of Corporate Social Responsibility, 2(1).

Tsai, Y. (2011). Relationship between Organizational Culture, Leadership Behavior and Job Satisfaction. BMC Health Services Research, 11(1).

Tuckman B. (1965). Development sequences in small groups. Psychol Bulletin. 63:384–399.

van der Kleij, R. and Leukfeldt, R. (2019). Cyber Resilient Behavior: Integrating Human Behavioral Models and Resilience Engineering Capabilities into Cyber Security. *Advances in Intelligent Systems and Computing*, pp.16-27.

van Rijnsoever FJ. (2017). (I Can't Get No) Saturation: A simulation and guidelines for sample sizes in qualitative research. PLoS ONE 12(7): e0181689. https://doi.org/10.1371/journal.pone.0181689.

van Ruler, B. (2018). Communication Theory: An Underrated Pillar on Which Strategic Communication Rests. *International Journal of Strategic Communication*, 12(4), pp.367-381.

van 't Wout, Carien. (2019). Develop and Maintain a Cybersecurity Organisational Culture.

Vilma, Ž. (2018). Implementing Ethical Principles in Social Research: Challenges, Possibilities and Limitations. Vocational Training: Research And Realities, 29(1), pp.19-43.

Vitouladiti, O. (2014). Content Analysis as a Research Tool for Marketing, Management and Development Strategies in Tourism. *Procedia Economics and Finance*, 9, pp.278-287.

Vogl, S., Schmidt, E. and Zartler, U. (2019). Triangulating perspectives: ontology and epistemology in the analysis of qualitative multiple perspective interviews. *International Journal of Social Research Methodology*, 22(6), pp.611-624.

Unachukwu, L., Kalu, A. and Ibiam, O. (2018). Accessing Secondary Data : A Literature Review. Singaporean Journal of Business Economics and Management Studies, 6(6), pp.53-63.

Wang, S. (2019). Integrated framework for information security investment and cyber insurance. Pacific-Basin Finance Journal, 57, p.101173.

Wathuta J., Mnisi M.F. (2019). Human Dignity Protection in Social Science Research: Perspectives from Selected African Countries. In: Nortjé N., Visagie R., Wessels J. (eds) Social Science Research Ethics in Africa. Research Ethics Forum, vol 7. Springer, Cham. https://doi.org/10.1007/978-3-030-15402-8_14.

Weems, C., Ahmed, I., Richard, G., Russell, J. and Neill, E. (2018). Susceptibility and resilience to cyber threat: Findings from a scenario decision program to measure secure and insecure computing behavior. *PLOS ONE*, 13(12), p.e0207408.

Willard, Gerald. (2015). Understanding the Co-Evolution of Cyber Defenses and Attacks to Achieve Enhanced Cybersecurity. Journal of Information Warfare. Volume 14. Pages 17-31.

Wisdom J and Creswell JW. (2013). Mixed Methods: Integrating Quantitative and Qualitative Data Collection and Analysis While Studying Patient-Centered Medical Home Models. Rockville, MD: Agency for Healthcare Research and Quality. AHRQ Publication No. 13-0028-EF.

Y. Connolly, L. and Wall, D. (2019). The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. Computers & Security, 87, p.101568.

Yahya, K., Yean, T., Johari, J. and Saad, N. (2015). The Perception of Gen Y on Organizational Culture, Religiosity and Corruption in Malaysian Public Organizations. Procedia Economics and Finance, 31, pp.251-261.

Yoel, S. (2015). Cultivating Organizational Culture within Globalized Companies Using the Wellness Kickoff Tool. Procedia - Social and Behavioral Sciences 209: 533-539.

Zimmermann, V. and Renaud, K. (2019). Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, 131, pp.169-187.

.

Appendix 1

Email to Executives and Senior Executives

Dear _____

I am Jawn Lim, a candidate of Master of Science in IT of University College Dublin. I am writing to you to introduce the purpose of my Masters Thesis and to seek your consent so to collect information that for my research project.

About the Masters Thesis

The topic of my thesis is, "How Organizational Behaviour influences Cybersecurity Practices in Company XYZ?". Given that Cybersecurity is becoming vital to every organization regardless of their industries, I have taken up the role to research on this area specifically in the context of Organizational Behaviour. During the preliminary research stage, it was found that there is a research gap of understanding the behaviour of individual particularly in the Singapore's SMEs.

As such, the primary objective of this study is to explore variable options of applying Organizational Behaviour throughout the entire thesis and analyse which theories would be the most appropriate model to be implemented and the research question of this study is, 'How employees perceive the adoption of cybersecurity in job performance within Company XYZ?'.

About the Interview

To standardize the questions across different level of every employees' rank, tile and job designation, there will be only one set of questions for the selected participants and for the researcher to understand adoption behaviour of Cybersecurity in Company XYZ.

The interview will take approximately less than 30 minutes.

In terms of the interview session and procedures, the below pointers will be considered:

- Interview will be conducted either via video conferencing or on-site face to face.
- Interviews will only be carried out after consent has been obtained from the company head.
- Interviews will be based on voluntary thus, at any point of time, participants interviewees may have the rights to stop or refuse any question.

To protect the participants' privacy, the data will be kept confidential. Interviews will also be audio-recorded to allow the researcher to transcribe. Thesis will also be shared to the participants to ensure no manipulation and ethics will be kept.

Benefits of participating in this study

This study is intended to understand the current adoption methodology and the importance of how new theories can be applied to help organization achieve better cybersecurity practices. I will be more than happy to share my research report at the end of October 2020.

Thank you for allocating your precious time and I hope to arrange the meeting with you and the interview will be in September of 2020. Feel free to contact me at 9235-5858 should you have any enquiries.

Appendix 2

Master MSc42 - Interview Questions

Working Environment/Culture

1. Can you give us a brief overview of your job at company XYZ? How long have you been in your company?
2. Can you describe team working culture in your company when undertaking projects? (lead them with e.g. Teamwork)

Communication

1. What is the biggest challenges you faced in handling cyberattack? How do you manage and communicate it?

2. How effective is the vertical communication within organization in considering adopting and implementing cybersecurity practices?

3. What are your challenges when convincing your peers or management level to adopt your perspective towards cybersecurity adoption? How do you overcome it?

Decision Making & Power

1. Is the management's advice been rationale all the time? Why? Could it be better?
2. Does your team have any influencer that is able to influence the management decision making process? What are their roles? And how do they influence them?

Individual & Group Motivation

1. How often do you use Cybersecurity practices when instructed by management?
    a. How would you motivate others? (optional)

Change Management

1. How often does your company prioritize and constantly update on Cybersecurity latest trend?

2. What is the biggest challenge in convincing the management that resist change in your view?

Leadership

1. How does the management bring across Cybersecurity practices to everyone? If there is anyone refuse to accommodate to such instructions, what would be the consequences?

2. Are there any incentives for employees to adopt cybersecurity practices in order to show its value for better work commitment?

   a. Due to the current global pandemic (covid-19) that has affected many organizations, how did your company sustain? Do they spend more money and enhance cybersecurity?

Economical Behaviour

1. Was there any personal bias seen in the management when spending more money to invest in their employees?

Appendix 3

CONSENT FORM

The Adoption of Cybersecurity in Company XYZ

You are invited to be in a research study of the Adoption of Cybersecurity in Company XYZ. You were selected as a possible participant because of your many year of working experience in XYZ and thus data collected will be most valid to this research. We seek your full collaboration to read and consent this form and ask any questions before we continue to further.

This study is being conducted by: Lim Jun Wen, Jawn, MSc 42, University College Dublin

Background Info

The purpose of this study is to investigate which Organizational Behaviour theory would be most influential that can be used to improve employees' cybersecurity adoption in Company XYZ.

Procedures

If you agree to be in this study, we will ask you to:

i) Take part in a semi-structured either video conferencing or face-to-face interview that will last for about 30 minutes. The interview will be audio-recorded and transcribed thereafter.

Risks and Benefits of being in the Study

The study does not entail any risks.

The benefits to participation are: The findings and conclusions drawn from the study will be made available to you upon request.

Compensation:

You will not receive any forms of remuneration payment for your participation.

Confidentiality:

The records of this study will be kept private. In any sort of report we might publish, we will not include any information that will make it possible to identify a subject. Research records will be stored securely and only researchers will have access to the records. Study data will

be encrypted according to current University policy for protection of confidentiality. The tape recordings will be accessed by the researcher, name of student and/or his supervisor, Dr Ajit Prasad. The recordings will be erased upon the conclusion of the study and the compilation of the report. The expected time of completion is end of October 2020.

Voluntary Nature of the Study:

Participation in this study is voluntary. Your decision whether or not to participate will not affect your current or future relations with the researcher or the University College of Dublin. If you decide to participate, you are free to not answer any question or withdraw at any time without affecting those relationships.

Contacts and Questions:

The researcher conducting this study: Lim Jun Wen, Jawn. You may ask any questions you have now. If you have questions later, you are encouraged to contact him at +65 9235-5858 or email him at junwen89@hotmail.com.

You will be given a copy of this information to keep for your records.

Statement of Consent:

I have read the above information. I have asked questions and have received answers. I consent to participate in the study.

Signature:_____ Date: _____

Signature of parent or guardian:_____ Date: _____

(If minors are involved)

Signature of Investigator:_____ Date: _____

Appendix 4

Interview Transcript: Interviewee C1

The interview was conducted on 9th Sept 2020 at 3.30pm.

Interviewee C1 was invited to be part of the interview at a café in town. Some of the questions were given beforehand as C1 would like to know if questions are confidential to be revealed. The interviewer took him through the Consent Form and proceed with the interview.

Interviewee C1 is working as a senior system engineer which is accountable for many clients. It was a fruitful experience having him to providing informative responses towards cybersecurity practises.

Working Environment/Culture

1. Can you give us a brief overview of your job at company XYZ? How long have you been in your company?

I work as a senior system engineer under a business unit of an Audit Company. Our company primarily hire engineers to be outsourced or out stationed for SME's clients. Personally, I hold about 20 accounts, managing mostly entire IT Infrastructure of client data such as and I have been working for close to 3 years.

2. **Can you describe team working culture in your company when undertaking projects?**

During projects, our team acts as an IT manager representing our clients, we ought to be very familiar with the infrastructure before proposing solution that suits clients' requirement. For instance, I will sometime approach my Technical Manager to work out for proposal related to upgrading of our system, network and security requirement such as firewall and anti-virus. After coming up with proposal, we will have to work closely with our sales team. Normally, we meet up during operating hours or over a call. Sometimes, we do need to return to office after office hours to get things settled due to tight deadlines.

Communication

1. What is the biggest challenges you faced in handling cyberattack? How do you manage and communicate it?

Cyberattack comes in many forms where social engineering is the most frequent attack if humans are not vigilant. Sometime we see customers being asked on some personal questions and that could be part of reason of being attacked as personal details and credentials were either accidently leaked or recorded.

One of the biggest challenges that we faced was a customer of mine in the manufacturing industry selling stationary. They overlooked on closing the remote session program leaving the application running at the background which everyone was able to access as the username and password were too easy to guess. It happened that the endpoint was one of the CORE system in the logistic platform that had CRM system installed. Data was compromised and encrypted. A fee to decrypt was later shown on the screen. Customer quickly contacted me and I told them to disconnect the Internet cable to prevent any further damage. This was eventually brought up to my Technical Manager. We did a thorough diagnostic on the server and managed to restore the data from backup.

3. How effective is the vertical communication within organization in considering adopting and implementing cybersecurity practices?

As an IT system administrator, for all my clients, we either communicate face to face or through email about the latest trend of cyberattacks. In terms of internal colleagues, most of the time, our management always update us regularly such as the notorious ransomware attack “WannaCry”. In my experience, majority of the times, our office departments and colleagues are very vigilant towards adopting and implementing any new cybersecurity practices.

4. What are your challenges when convincing your peers or management level to adopt your perspective towards cybersecurity adoption? How do you overcome it?

Firstly, our company will always look at the cost to see if it is justifiable when investing on any new proposed software or hardware. There was one instance when I proposed using a new automation tool that will alert our colleagues once awhile to remind them on importance of cybersecurity. Our management always ask questions like “who is going to manage it?”, “Do we outsource or internally manage?” There has been many factors to be able to convince them as the decision making always comes from management community. We have to do a

lot of show case to prove the effectiveness and a lot of cost comparison study to see which best fits our organization.

Decision Making & Power

1. Is the management's advice been rationale all the time? Why? Could it be better?

No. There was one scenario we were being awarded on a Cybersecurity project. Our management requested us to perform the deployment after office hours so to reduce downtime for our customers. However, at times, we were so busy during the day to support the customer, projects have to always push over the weekends. I felt that it depends on the project scale size. If it's small scale project, we should do it during office hour if it doesn't impact much on operational. If its big scale, I am totally fine to implement after office hours or weekend, however compensation of time off should be given for employee welfare.

2. Does your team have any influencer that is able to influence the management decision making process? What are their roles? And how do they influence them?

Yes, as our company also sell CRM solution, at times our clients may face an outdated software version that could be vulnerable to cyberattacks. We have to work with together with the CRM departments to propose a solution which might require hardware replacement and verify if new updates would have any compatibility issues. We have to work out the pros and cons for a final solution. Later, my technical manager will be the representative to escalate the proposal to the management team. My technical manager mainly use the reason of an outdated software might not be supported by the principle vendors and thus could be a loophole to our clients as well if they do not upgrade.

Individual & Group Motivation

1. How often do you use Cybersecurity practices when instructed by management?

The most fundamental practice was to have our servers updated by bi-monthly basis, not only common products like Microsoft, all products related to IT hardware and software will be something that we cannot overlook. Sometimes, I will ask my team or even clients for a gathering such as a catch up for lunch and share some real life cyberattack news or hindsight that impacted organization so they will be able to absorb the importance of cybersecurity awareness.

Change Management

1. How often does your company prioritize and constantly update on Cybersecurity latest trend?

As our company is golden partner with many top cybersecurity companies, we always have newsletters from our vendors though emails whenever there's a major attack taken placed. As soon as we received the news, our company will set aside budget to send engineers to relevant courses to keep them competent in the industry. After the completion of the course, they are required to share knowledge between the team and client on the current trend of the cybersecurity of the best practices.

2. **What is the biggest challenge in convincing the management that resist change in your view?**

Sometimes, when I have my own opinion, I will require second and third perspectives who are mainly my direct supervisor or senior colleague who is experienced in the particular field to support me and convince my management. For instance, I would always request to hire more competent or high skillset engineers as there are more projects coming in which requires certain expertise.

Leadership

1. How does the management bring across Cybersecurity practices to everyone? If there is anyone who refuses to accommodate to such instructions, what would be the consequences?

Our company always provides a mandatory security awareness training internally on a quarterly basis that could take up to 4 weeks. Any point of time, if our engineers are absence or did not complete the training, email will be sent to supervisor to inform them. There are cases where our company wanted to see how our engineers are performing by sending some "legit" phishing email on alternate basis and monitor the behaviour and responds of our employees. Generally, there won't be any penalty but our company tries to enforce the employees through many methods.

2. **Are there any incentives for employees to adopt cybersecurity practices in order to show its value for better work commitment?**

Yes, there will be attractive cash vouchers as an incentive provided with a letter of commendation which will be published to our intranet dashboard. It's kind of like a point

system which anyone can complement you. However, in order to earn that points, it has to go through 3 levels of approval from 2 different supervisors. And lastly, would be the compensation department to decide the amount of voucher to be given. There was one instance that I was being awarded with a voucher because I was the fastest person to report a phishing email that was spreading across our department. That email was seen as per normal but I was able to identify that the one of the alphabet in the email domain was supposed to be letter "O" rather than numerical "0".

a. Due to the current global pandemic (covid-19) that has affected many organizations, how did your company sustain?

In terms of leadership, our CEO and management always put staff health as their first priority. Due to the pandemic and as per our local authority regulation, we were being placed to work from home. Communication and remote support were still possible over the past few couple of months. Even working from home, revenue stream was still generating as we are considered the essential service company. However, as and when, we will be needed to go office.

Economical Behaviour

1. Was there any personal bias seen in the management when spending more money to invest in employees?

Not really. As per mentioned above, we always have set aside budget to prepare for employees to increase their competency. If the employee is very interested in the course and it is relevant to his/her job of scope, the supervisor and management will be more than willing to invest in them as they see the new skillset is recognized in the industry. Moreover, after employees get certified, those knowledge can be eventually converted to revenue such as upselling to clients.

Appendix 5

Interview Transcript: Interviewee C2

The interview was conducted on 10th Sept 2020 at 1.00pm.

Interviewee C2 was invited to be part of the interview at a local coffee shop (Kopitiam). Some of the questions were given beforehand as C2 would like to know if questions are confidential to be revealed. The interviewer took him through the Consent Form and proceed with the interview.

Interviewee C2 is working as a Chief Finance Officer (CFO) which is accountable for many clients in a few regions. It was a fruitful experience having him to providing some of the experiences that he faced and how he actually dealt with the past cyberattack incident.

Working Environment/Culture

1. Can you give us a brief overview of your job at company XYZ? How long have you been in your company?

I work in an exhibition, events and designing firm. I am the Chief Finance Officer (CFO) for almost 20 years in the company. As a Finance Officer, I oversee regional offices and always ensure that the overall saving is always achieved. Sometimes it can be quite painful to lay off my employees especially this pandemic period. However, for the sake of sustaining company, certain sacrifice is required.

2. Can you describe team working culture in your company when undertaking projects?

Basically, my project director will take the lead. My salesman will be in charge of understanding clients' requirement and brainstorming with our designers. They will have to go many phases of budget plan, product quality, traffic flow, design and layout, corporate identity and our clients' history. All these information must be collected and compiled in order for our designers to do the necessary architect design. Our sales will also need to understand the environment or location best fit for exhibition so to attract more customers.

For instance, we should try to avoid any obstacles along the left and right aisle of walking passage.

Communication

1. What is the biggest challenge you faced in handling cyberattack? How do you manage and communicate it?

We ever encountered an incident of ransomware attack about 3 years ago on one of our employees' laptop. It was quite bad as our operation has been affected for nearly consecutive 3 days due to all our servers were shut down to restore backup data. After the incident, we decided to engage our IT Service provider for some ransomware prevention software to protect our asset. We did an investigation and realized that it was due to human awareness issue. This is something that I personally felt that if our employees are not interested in practising cybersecurity, regardless of "N" number of enforcement, it is pointless. We even try to control some website access via firewall but a human mistake could easily bring the entire infrastructure down. I felt that government should enforce the importance of cybersecurity in schools as it will be very helpful to teach during young age.

2. **How effective is the vertical communication within organization in considering adopting and implementing cybersecurity practices?**

Not very effective. In many organization that we see, most would not hire an internal IT. Rather, I have seen many outsource to external IT Service provider just like what our company is doing. For us, we generally do not have much knowledge to convince our people. Thus, it can be quite hard to either get management to buy new cybersecurity equipment or convince our employees to adopt preventive measures diligently. However, most of the time, we are lucky to have our service provider to conduct free course or online training to share out some knowledge.

3. What are your challenges when convincing your peers or management level to adopt your perspective towards cybersecurity adoption? How do you overcome it?

To me, I will always go for the sentence "depending on the needs". Because, in the current modern society, even if I am not working in the IT industry, in every business environment, IT has become relatively important as compared to the core business. We absolutely can't afford to have any equipment going down for several hours or even days. Some of the ways

to convince them would be using the word “Speed”. I generally will tell the CEO that investing in new servers for security will not only decrease cyberattacks but will have much more disk performance for our developers to access the file faster. This relates to faster performance in job as well. Even as a CFO, I still prioritize IT a lot.

Decision Making & Power

1. Is the management’s advice been rationale all the time? Why? Could it be better?

Yes, most of the time they are rationale. As usual, it’s all about the “needs” & the amount of capital investment. Sometimes, our management would want to invest in purchasing cybersecurity products which could cost up to $20,000. Most importantly, our government has certain grant that can subsidised up to 80% which could save us a lot of cost incurred.

2. Does your team have any influencer that is able to influence the management decision making process? What are their roles? And how do they influence them?

Usually, the influencer will be me, as a CFO. To be able to influence my CEO and president, I will need to weight the advantages and disadvantages of the product. Definitely, I will call our service provider to give me a write-up and reasons of upgrading certain software. They have to be able convince me first before I can influence my management. For instance, just 3 months ago, we implemented a new CRM customized software easily with a $50,000 investment. As it is something that can be replaced with manual control processing as well as managing client base data easily. Thus, I used these reasons to draw the management attention and proceed to procure it. Most importantly, we have 80% grant from government. Thu, it is like a win-win situation.

Individual & Group Motivation

1. How often do you use Cybersecurity practices when instructed by management?

Personally, I don’t really practise that often. I feel that most of the time, I will be occupied with many other things. If there’s any suspicious or malicious activities, my service provider team should announce or inform us immediately so actions can be taken to mitigate any unforeseen attacks. As a customer, we are not expertise in the area of cybersecurity thus, we

rely a lot on our IT specialist to monitor.

Change Management

1. How often does your company prioritize and constantly update on Cybersecurity latest trend?

As per mentioned above, we don't really prioritize it as our priority is different; our professional is not in the IT field. As an CFO, I would always take good care of my accounting (APAC) application first. Other than that, I will leave it to my service provider to provide me any latest trend.

2. **What is the biggest challenge in convincing the management that resist change in your view?**

Again, it depends on the needs of the company. Sometimes, it can be quite urgent that I feel some cybersecurity products should be in placed such as anti-virus. However, management is sometime reluctant to change. We have no choice but to wait for the opportunity such as additional government grant or wait for the price to drop.

Leadership

1. How does the management bring across Cybersecurity practices to everyone? If there is anyone refuse to accommodate to such instructions, what would be the consequences?

So far, our employees are quite obedient in terms of taking instructions. Instruction can be either via email or a small gathering sometimes. However, it is still up to individual to practise it as the interest level might be different. Any major disciplinary issue such as attempting to deliberately open a malicious website or file will then go through HR process for any penalty.

2. Are there any incentives for employees to adopt cybersecurity practices in order to show its value for better work commitment?

No such thing, we don't practice that. In today's world, Computer has become a necessity for every common user. Almost all the company would need to have a computer for a user. Even

our employees have their personal computers, we felt that it should be own responsibility to take care of the security of personal or work computer such as not putting any malicious data in the USB drive.

a. Due to the current global pandemic (covid-19) that has affected many organizations, how did your company sustain? Do they spend more money to enhance cybersecurity?

Not really, we don't really spend more because of global pandemic. However, as the government has announced employees to work from home, the challenges would be lacking of laptops. Most of our developers are using a desktop which is heavy and bulky. Thus, I actually get my IT service provider to standby laptops for our employees to bring back home to work. They are also required to support and ensure our employees can still function at home.

Economical Behaviour

1. Was there any personal bias seen in the management when spending more money to invest in their employees?

As much as possible, as part of the management, we usually try our best to put across everyone to attend cybersecurity training to raise their awareness. Unless if it is a very specialise course, we would re shuffle the team to go. It depends on case by case basis.

Appendix 6

Interview Transcript: Interviewee C3

The interview was conducted on 13th Sept 2020 at 11.00am.

Interviewee C3 was invited to be part of the interview through video conferencing via Microsoft Teams. Some of the questions were given beforehand as C3 would like to know if questions are confidential to be revealed. The interviewer took him through the Consent Form and proceed with the interview.

Interviewee C3 is working as a principle system engineer which is accountable for the entire internal IT infrastructure. It was a fruitful experience having him to providing informative responses especially a law firm company which is very particular towards regulatory compliance.

Working Environment/Culture

1. Can you give us a brief overview of your job at company XYZ? How long have you been in your company?

I have been in company for 9 years, since it was setup in year 2011. My job scope is to manage IT infrastructure, data centre. Managed on premise such as Office365 Email, Microsoft Infrastructure and daily operation. In charge of deploying endpoint solution such as antivirus. I assist IT director to define IT policy and documentation. We do users training.

2. Can you describe team working culture in your company when undertaking projects?

Usually we assign a project lead, so the project lead will be in charge of entire project, the other team members will assist when even needed, many projects require different expertise thus we work as a team.

Communication

1. What is the biggest challenges you faced in handling cyberattack? How do you manage and communicate it?

We do not have serious incident, we do have some incident. The challenges is the resource distribution. We only do the first level of support, we have incident and it caused by antivirus software itself. Could not do anything for whole day. End of the day, our service provider solved the issue and update the anti-virus to resolve it.

2. How effective is the vertical communication within organization in considering adopting and implementing cybersecurity practices?

I think the vertical communication within the company is very important because all the decisions are from management.

3. What are your challenges when convincing your peers or management level to adopt your perspective towards cybersecurity adoption? How do you overcome it?

The big challenge is to raise awareness of management. And also some human mistakes also involved. Need more user education.

Decision Making & Power

1. Is the management's advice been rationale all the time? Why? Could it be better?

I think our CIO being the part of the management has been very vigilant in Cybersecurity. Most of the time, he is very practical as he has done his homework and cross check with the respective cybersecurity vendors to ensure any proposed solution is workable. Our CIO should continue to stay updated and aware of cybersecurity trend and propose to the management.

2. Does your team have any influencer that is able to influence the management decision making process? What are their roles? And how do they influence them?

Our team have to evaluate the product and propose to management. As most of the management are not the subject matter expert in the IT field, we usually will discuss with our CIO and let him know the risk or difficulties on the ground.

Individual & Group Motivation

1. How often do you use Cybersecurity practices when instructed by management?

We often have phishing emails and previously some of our colleagues were not aware that the email contains malicious attack and thus they actually opened it. It was then we were being notified from one of the monitoring software that an attack has intruded into one computer. Luckily, we were able to savage the computer from backup. Since then, we often motivate and educate each other to be vigilant all of them including myself adopt cybersecurity practices daily.

Change Management

1. How often does your company prioritize and constantly update on Cybersecurity latest trend?

Our CIO will send emails to all users on the recent trends or incident reported so that it will raise user's awareness. It depends on how big is the case. Some of the case like a few years back, the notorious ransomware "Wannacry" has invaded many organization globally. Such incident was reported immediately even to our mobile, email and sometime calling employees to take note.

2. **What is the biggest challenge in convincing the management that resist change in your view?**

The biggest challenge would be to convince the management during peace time. When there is no major issue, they will not prioritize on cybersecurity but rather their core business in the law firm. Thus, it is only after some real incidents, our recommendation to the management will be easier. Otherwise, the management will be slightly reluctant and resist to change.

Leadership

1. How does the management bring across Cybersecurity practices to everyone? If there is anyone refuse to accommodate to such instructions, what would be the consequences?

The urgency and behaviour do not reflect the high level of awareness. Because the limited visibility and also sometimes. And many of the users may not know the new risks. I think the

people in the leadership position, they must update themselves. Within the organization, the cybersecurity leaders need to take very strong and good strategic leadership roles to lead all of us.

2. Are there any incentives for employees to adopt cybersecurity practices in order to show its value for better work commitment?

So far, I don't think there is incentives provided for our employees. Most cases, we have to enforce the employees to follow the practices and as much as possible if there's doubts, approach the IT team like myself for advice.

a. Due to the current global pandemic (covid-19) that has affected many organizations, how did your company sustain? Do they spend more money and enhance cybersecurity?

I don't think so. Especially with the current global pandemic situation, many organization including ourselves are affected. Thus, we are very cautious on spending money now. Most company like us will prioritize cost more than cybersecurity. The other main thing is that our management are not in the IT field thus showing lesser interest in upgrading technology.

<u>Economical Behaviour</u>

1. Was there any personal bias seen in the management when spending more money to invest in their employees?

Of course, when it comes to training, investment will be required regardless of its scale. Our company usually give training opportunities to better employees who have performed well in the past records. It will be more towards to selective employees rather than a whole.

Appendix 7

Interview Transcript: Interviewee C4

The interview was conducted on 14th Sept 2020 at 1.10pm.

Interviewee C4 was invited to be part of the interview through video conferencing via Microsoft Teams. Some of the questions were given beforehand as C4 would like to know if questions are confidential to be revealed. The interviewer took him through the Consent Form and proceed with the interview.

Interviewee C4 is working as an Operational director which is accountable for the entire company operationally and ensuring every work processes are following through the Standard Operating Procedure (SOP). It was a fruitful experience having him to providing informative responses especially dealing with multiple subsidiaries in different countries.

Working Environment/Culture

1. Can you give us a brief overview of your job at company XYZ? How long have you been in your company?

I have been since day 1. Almost 30 years. Well, I basically backend support to take care of operation side, administration, HR, finance, logistic.

.

2. Can you describe team working culture in your company when undertaking projects? (lead them with e.g. Teamwork)

We have many different divisions. On the broad one, we have projects team split up into different department such as marketing, sales, and technical support. My side is more towards to operation which I have mentioned earlier on. Very often, we need to have a proper ad detailed documentation so to keep track every single records. For instance, due to the current pandemic, most of us are working from home and we leverage on our CRM which is cloud based to communicate and work together. There are many formal and informal discussion such as through virtual meeting, emails and WhatsApp as well.

Communication

1. What is the biggest challenges you faced in handling cyberattack? How do you manage and communicate it?

We had a fraud case not too long ago which is early this year. It was through the email. Somehow this guy manage to understand our billing cycle and has been monitoring us for quite some time. They targeted on my finance side which happened that one of our colleague did not exercise carefulness in ensuring the email is legit. He could have verified the domain of the email before sending. As the email continued to correspond with the attacker, information like sending bill to 3rd party has been tracked. We did not know until the vendor alerted us that the bank account was not modified. As we do not have in-house IT, we very much rely on our IT service provider to monitor on this.

2. How effective is the vertical communication within organization in considering adopting and implementing cybersecurity practices?

This area is basically is handled by myself. I will be part of the decision making position. If there is a need to address the issue such as buying new cybersecurity products to protect our company asset. I will not hesitate to proceed with the solution. This also reduce the number of approval from my upper management as I can take over the control if necessary.

3. What are your challenges when convincing your peers or management level to adopt your perspective towards cybersecurity adoption? How do you overcome it?

Not really, we don't have much challenges. In operation side, we just have to make sure that our IT infrastructure is ready and good enough to cater for our present needs. In fact, sometime it is the other way round. For instance, if our project team finds some bugs or glitch in the CRM software, they will inform us and I will personally look for our CRM vendor to fix the issue.

Decision Making & Power

1. Is the management's advice been rationale all the time? Why? Could it be better?

Yes, most of the times, the management are being rationale and practical. For instance, we know the employees are not very IT savvy and thus would not be a person who is vigilant towards cybersecurity practices. In this case, we often send employees for courses to raise their cybersecurity awareness.

2. Does your team have any influencer that is able to influence the management decision making process? What are their roles? And how do they influence them?

Usually the influencer will be coming from the individual Head of Department (HOD). We actually gather all these information from the actual process users as the users are on working on the ground and best understand the situation. Ground users will be able to provide more practical feedback rather than theoretical perspective from the management. An example would the recent upgrade of our CRM software which our ground users found out that certain new features will be required to ease their operation and thus management proceeded to upgrade it.

Individual & Group Motivation

1. How often do you use Cybersecurity practices when instructed by management?

We have this protocol that anyone that received suspicious email. We will alert everyone in our WhatsApp group chat. We would quickly take snapshot and spread the information to everyone. We will then forward this to our IT consultant to check the legibility of the email.

Change Management

1. How often does your company prioritize and constantly update on Cybersecurity latest trend?

As long as IT consultant, if they find that it is necessary we will do it. There are so many things to be updated in the cyber space. After engaging IT consultant, we expect them to take good care of this area such as informing us on the latest trend or etc.

2. **What is the biggest challenge in convincing the management that resist change in your view?**

No. We did not have any issues in terms of resistance to change. It is quite smooth and never once we reject any good solution.

Leadership

1. How does the management bring across Cybersecurity practices to everyone? If there is anyone refuse to accommodate to such instructions, what would be the consequences?

One of the very classic example was before CB, from the announcement on Friday, Tuesday onwards it was beginning of CB, over the weekends, and we have to prepare a lot of things such as laptops. We loan from our IT service providers. Some of our staff are briefed beforehand. Still a few percentage of employees are quite rigid. They did not practise a good way of saving their work files. After multiple advice, if they continue to be stubborn, we will ask them to stop working rather than giving any penalty. Reason is simple, we do not want our organization to be put at risks. Until corrective actions have been implemented, the employees will go back home without any IT equipment.

2. Are there any incentives for employees to adopt cybersecurity practices in order to show its value for better work commitment?

We don't give carrot for complying cybersecurity practices. It should be employees' obligation and their responsibility. If there is anyone who is exceptionally performing well in this area, we will however give them additional task to lead the team. Giving incentives as an appreciation of token will not relate to any better work commitment in my opinion. It will more of commendation to show a sense of appreciation. Employees should always stay vigilant to protect their own asset just like their own personal data.

a. Due to the current global pandemic (covid-19) that has affected many organizations, how did your company sustain? Do they spend more money and enhance cybersecurity?

Yes, during this lock down period, we definitely spend more money to buy hardware such as laptops for our employees working from home. Currently we are also reviewing our contract

with our existing service providers to see if there's any new things to upgrade. We are definitely more than willing to prioritize cybersecurity practices as it is something that cannot be ignored, otherwise our data would be put at risk.

Economical Behaviour

1. Was there any personal bias seen in the management when spending more money to invest in their employees?

Basically, not everybody in the company. Unless we have a lot of resources in terms of financial. In the past, we used to send all the employees for short few days courses. However, we realised that majority of the juniors were not very much interested and thus not a fruitful event for them. Thus, we decided to only selective choose the respective HODs to attend cybersecurity course. After they have learnt the knowledge, they will be responsible to share and disseminate the information down to the team.

Appendix 8

Interview Transcript: Interviewee C5

The interview was conducted on 17th Sept 2020 at 12.10pm.

Interviewee C5 was invited to be part of the interview through video conferencing via Microsoft Teams. Some of the questions were given beforehand as C5 would like to know if questions are confidential to be revealed. The interviewer took him through the Consent Form and proceed with the interview.

Interviewee C5 is working as an operation manager which is accountable not only for operational task but also the entire internal IT infrastructure. It was a fruitful experience having him to providing informative responses especially when the shipping industry is declining due to the global crisis.

Working Environment/Culture

1. Can you give us a brief overview of your job at company XYZ? How long have you been in your company?

I work as an operation manager for more than 10 years. Typically, I manage the operation as well as some part of our IT infrastructure. Our IT equipment is quite basic with a firewall, switch and some servers.

2. Can you describe team working culture in your company when undertaking projects?

Our team is quite bonded. We usually give the project head to take the lead. About a few engineers will listen to his instruction and carry out the task accordingly. We are always quite punctual to meet the deadline.

Communication

1. What is the biggest challenges you faced in handling cyberattack? How do you manage and communicate it?

We did have a cyberattack quite recently, one of the endpoint was attacked as it was left turned on. When it was attacked, the biggest challenges was what to do next? As the IT manager, I immediately asked the person to turn off the entire machine by pushing the power off. Luckily, the damage was not too bad as it did not spread to our entire network. We began to contact our service provider who is taking care of our infrastructure.

2. How effective is the vertical communication within organization in considering adopting and implementing cybersecurity practices?

Our company have quite a number of departments. Usually most of us will encourage each other to ensure we do not open any suspicious emails. Most of the time, it's more about the user awareness, if the user awareness is weak, even with the best IT equipment, it would not help much. I would say our vertical communication is still relatively quite good and effective in a way that we do not resist much if the suggestion is for the sake of company.

3. What are your challenges when convincing your peers or management level to adopt your perspective towards cybersecurity adoption? How do you overcome it?

Our company focus is very much on managing the operation of vessels, containers and other shipping related thing. However, as I am also in charge of the IT infrastructure, sometimes I tend to be very particular about our security. The hardest part to convince my management level is that sometime they do not appreciate what I am trying to imply such as checking the domain of every senders to ensure we are not being tracked. However, the management always do not have the time to check every single senders' domain, thus I decided to buy an email filter device to mitigate the number of suspicious email.

Decision Making & Power

1. Is the management's advice been rationale all the time? Why? Could it be better?

Yes, most of the time they are being rationale. If there is anything that we felt not practical, we will voice out and counter propose the idea. Most of the time, management will heed our advice if there is not better suggestion from the management.

2. Does your team have any influencer that is able to influence the management decision making process? What are their roles? And how do they influence them?

Yes, we do have a lot of influencer. It doesn't matter what roles are they holding, so long any good suggestion is brought up at the right time, our management will take it up and proceed. Usually, it depends on whether if it's in favour to the entire organization.

Individual & Group Motivation

1. How often do you use Cybersecurity practices when instructed by management?

I am personally quite particular in security. Not just about the organization, I am also practising it for my own personal data. Thus, you can say that I practise it almost every single day and I am very cautious of handling cybersecurity practises. As we have seen that there were many cyberattack cases in the past, I often used this to motivate peers and try to influence them to practise it diligently.

Change Management

1. How often does your company prioritize and constantly update on Cybersecurity latest trend?

Even though, I am overseeing the entire IT infrastructure, my main role is however to focus more on the operational side. Thus, we still engage some third party service provider to assist us if there is any areas that requires technical expert. Since we have hired them, we would expect them to release any new updates to us as and when required. And if there is a need, we will adhere their advice and upgrade any hardware or software accordingly.

2. **What is the biggest challenge in convincing the management that resist change in your view?**

The biggest challenge is of course trying to get them invest in something that is more than 5 digits. As you might know, these days, when you want to invest on IT equipment, it can be quite expensive, not yet adding those maintenance fee. Sometimes, I find it hard to even convince my management about the necessity of the upgrade until I brought in the vendor to support me.

Leadership

1. How does the management bring across Cybersecurity practices to everyone? If there is anyone who refuses to accommodate to such instructions, what would be the consequences?

Other than our service provider updating us on latest cybersecurity trend, our management sometime will receive updates from their friends who are working as IT director in the IT industry. After receiving updates, our management will update our employees via email. We don't really have any penalty if anyone did not adhere to instructions.

2. Are there any incentives for employees to adopt cybersecurity practices in order to show its value for better work commitment?

No, we don't practise this. The company felt that it should be employees' responsibility to take care of their data. Like how they take care of phone.

a. Due to the current global pandemic (covid-19) that has affected many organizations, how did your company sustain? Do they spend more money and enhance cybersecurity?

Well, you know that covid 19 has affected so many organization. Our company was not spared either. For us, it might even worst as we are in the shipping industry line. As the exportation of goods are controlled strictly in terms of the complying our government regulation, there are months we are losing money. Thus, we did not have much capital and did not put our main focus on cybersecurity despite knowing that cyber attackers might take this chance to invade us.

Economical Behaviour

1. Was there any personal bias seen in the management when spending more money to invest in their employees?

Our company usually only send either or my IT team for Cybersecurity training. It depends on what kind of training it is. And how effective is the training to be able to help our organization bring in more benefits. Typically, our management will send the senior to management level.

Appendix 9

Interview Transcript: Interviewee C6

The interview was conducted on 19th Sept 2020 at 10.25am.

Interviewee C6 was invited to be part of the interview at his company. Some of the questions were given beforehand as C6 would like to know if questions are confidential to be revealed. The interviewer took him through the Consent Form and proceed with the interview.

Interviewee C6 is working as an IT manager which is accountable for the entire internal IT infrastructure as well as working with external IT vendors. It was a fruitful experience having him to providing informative responses and also how they adopt cybersecurity practises to protect their IT asset.

Working Environment/Culture

1. Can you give us a brief overview of your job at company XYZ? How long have you been in your company?

I am an IT Infrastructure Manager for my company. I've been here for close to 4 years. My job roles are managing the company infrastructure locally and remotely hosted. Implementing security measures in line with PDPA as we store customer's data on our servers.

2. Can you describe team working culture in your company when undertaking projects?

Any task is firstly gathered by Project director which in turn passed down to Project lead. They will then share those information with the teams involved e.g. Account Managers, Developers and IT and based on the flow that is communicate will discuss the best possible solution for the task taken.

Communication

1. What is the biggest challenges you faced in handling cyberattack? How do you manage and communicate it?

Local infrastructure will solely be managed by myself. Biggest challenges are from our end user's themselves who are not IT savvy and might start clicking on spams for eg that might open a whole gateway of malicious attack. To prevent such occurrence, frequent information sharing to end users on cyber security needs to be shared. And always thinking to be ahead of an attacker keeping oneself abreast of any new information security news that is latest.

2. How effective is the vertical communication within organization in considering adopting and implementing cybersecurity practices?

Management needs to take lead on telling staff of such exercise and information sharing is important. So the security team could be able to communicate to the staffs without being ignored

3. What are your challenges when convincing your peers or management level to adopt your perspective towards cybersecurity adoption? How do you overcome it?

Challenges could be from budget mainly to adopt such solutions will require a substantial amount of money to be spent on products and trainings. TO overcome that, we would need to plan ahead on the next fiscal year's spending.

Decision Making & Power

1. Is the management's advice been rationale all the time? Why? Could it be better?

As we held a very big amount of customer's P&C information, most of the times the management team are supportive. But on some occasions I did receive a lot of critics that the solution proposed is not necessary.

2. Does your team have any influencer that is able to influence the management decision making process? What are their roles? And how do they influence them?

Influencer would be myself. My role is to test it out and ensure that the solution fits our current environment. Requesting for a Proof of Concept (POC) is important. Once POC is completed gather all the data taken during that period and present it to the management.

Individual & Group Motivation

1. How often do you use Cybersecurity practices when instructed by management?

I practice it on a daily basis. Going through any latest news of threats and solutions in the market. Ensuring all staff adhere to security policies

Change Management

1. How often does your company prioritize and constantly update on Cybersecurity latest trend?

I go to cybersecurity training and seminars on my own accord very regularly whether its in a centre or online.

2. **What is the biggest challenge in convincing the management that resist change in your view?**

Usually it's because of budgetary. And whether such solutions are necessary. They also have an issue that I am the only IT personnel in our office so if I took a duration of time to go for courses, there will be no one to support any issues from clients and users.

Leadership

1. How does the management bring across Cybersecurity practices to everyone? If there is anyone refuse to accommodate to such instructions, what would be the consequences?

New hirers will be provided a copy of all IT policies, including Acceptable usage, security and VPN policies. Which then they will sign accordingly on all pages to acknowledged. When there is a breach on conduct it will start by a warning letter depending on the severity at worst, termination.

2. **Are there any incentives for employees to adopt cybersecurity practices in order to show its value for better work commitment?**

No there isn't.

a. **Due to the current global pandemic (covid-19) that has affected many organizations, how did your company sustain? Do they spend more money and enhance cybersecurity?**

Our company was already ready for such a scenario hence when the pandemic happened. We were already ready to be working from home accessing office and customer resources remotely and securely

Economical Behaviour

1. Was there any personal bias seen in the management when spending more money to invest in their employees?

There isn't any bias but it's hard when you only have 1 IT personnel, supporting and managing the entire organization.

Appendix 10

Interview Transcript: Interviewee C7

The interview was conducted on 19th Sept 2020 at 1.20pm.

Interviewee C7 was invited to be part of the interview through video conferencing via Microsoft Teams. Some of the questions were given beforehand as C7 would like to know if questions are confidential to be revealed. The interviewer took him through the Consent Form and proceed with the interview.

Interviewee C7 is working as an IT consultant in the distributor industry which is accountable to support System Integrator (SI) as well as working closely with IT vendors. It was a fruitful experience having him to providing informative responses especially the amount of IT experience he has gained that fits to answer this research questions.

Working Environment/Culture

1. Can you give us a brief overview of your job at company XYZ? How long have you been in your company?

I work as an IT consultant in the IT distributor industry. I have about close to 15 years of experience. I started working as an IT desktop engineer and grow my way up to consultant after going through many hurdles. Basically, I work very closely with a few business unit such as the project team, engineers as well as application team.

2. Can you describe team working culture in your company when undertaking projects?

We have a team of excellent engineers who are very friendly and always share their knowledge within the team. Whenever, there is any project, the project head will take the lead and manage the team accordingly. For instance, if the project is fall under application related tasks, it will be our developers who will be executing the project. Most of the time, our customers are SMEs and it is rather easy to fulfil their requirement.

Communication

1. What is the biggest challenge you faced in handling cyberattack? How do you manage and communicate it?

There are just simply too many cyberattacks in this world. The biggest challenge is not about upgrading software or hardware to mitigate cyberattack, as there is no way stop this completely. Most important is how our users or employees behaviour in terms of handling cyber threats. Often, we will launch a work shop either to our customers or even internally to build cybersecurity awareness.

2. How effective is the vertical communication within organization in considering adopting and implementing cybersecurity practices?

We are work very closely with our cybersecurity partners. Most of the time, we will get updates from them on the latest trend. Subsequently, as an IT consultant, I will then disseminate the information to the seniors or managers. Different departments will take charge to spread the information to others.

3. What are your challenges when convincing your peers or management level to adopt your perspective towards cybersecurity adoption? How do you overcome it?

Well, sometimes it depends on an individual's perception towards cybersecurity. Some can be very passionate about it, while some do not show interest. Thus, those that are not very much interested in adopting cybersecurity, I will use other ways such as trying to "scare" them that some of my customers went bankrupt due to data loss from cyberattack.

Decision Making & Power

1. Is the management's advice been rationale all the time? Why? Could it be better?

Not really, sometimes there is something that they only see it on the surface, thus without any in depth evidence, they concluded with an irrational advice. For instance, they mentioned that one of our internal software is not good and would like to change a new software. When asked why the software is not good, they replied as their friends gave a lot of negative feedbacks about it. However, it is actually not that the software is not good, it is more

towards to how the software is being configured based on certain requirement. Once a re-configuration is done correctly, it will work as effective as other software in terms of mitigating cyberattack threats.

2. Does your team have any influencer that is able to influence the management decision making process? What are their roles? And how do they influence them?

As an IT consultant, I ought to be initiative and give good suggestion to my management. However, we do not restrict who and what position, roles or job they are holding. We are all equal and appreciate any good recommendation. We influence the management by showing them how certain products such as cybersecurity software is necessary to protect the company assets.

Individual & Group Motivation

1. How often do you use Cybersecurity practices when instructed by management?

Even without my management instruction, I will do it very actively. As my stand is very clear that I have to protect the company data and asset, I am always looking at the internet to see if there's any new threats or new software which can be used in our organization.

Change Management

1. How often does your company prioritize and constantly update on Cybersecurity latest trend?

As an IT company, we are always changing to be better and constantly upgrading ourselves to keep updated on any latest news. Yes, we prioritize cybersecurity a lot as we think that is the key thing to safeguard our business.

2. **What is the biggest challenge in convincing the management that resist change in your view?**

We did not have much resistance in terms of the convincing the management. However, there may be some occasions when I tried to voice out my thoughts, they tend to divert it to other areas such as focusing on upgrading their core business strategy in the meeting. I guess

sometimes money drives them to focus on other areas which they think it is a better topic to discuss.

Leadership

1. How does the management bring across Cybersecurity practices to everyone? If there is anyone refuse to accommodate to such instructions, what would be the consequences?

Whenever there is any updates, emails will be broadcast to everyone. If there is anyone who refuses to take instruction, the supervisor will be to take responsibility as he or she should take care of the team. However, there won't be any penalty, it will be just a warning.

2. Are there any incentives for employees to adopt cybersecurity practices in order to show its value for better work commitment?

No, we don't practise this. It should be everyone's responsibility to take care of their own data.

a. Due to the current global pandemic (covid-19) that has affected many organizations, how did your company sustain? Do they spend more money and enhance cybersecurity?

You see, most of us are now working from home. Except those engineers that are required to be on site if there is any project. Luckily for us, as we are considered the essential service business which are allowed to continue our work, our impact is slightly lower as compared to the rest of the industries.

Economical Behaviour

1. Was there any personal bias seen in the management when spending more money to invest in their employees?

Not really, we spend money to invest on our employees to cybersecurity courses to ensure they are all well-educated and know what to do when it comes to a real cyberattack case. Whether the time is good or bad, our management point of view is to ensure everyone in the company are vigilant when adopting cybersecurity practises.

Appendix 11

Interview Transcript: Interviewee C8

The interview was conducted on 20th Sept 2020 at 11.40am.

Interviewee C8 was invited to be part of the interview through video conferencing via Microsoft Teams. Some of the questions were given beforehand as C8 would like to know if questions are confidential to be revealed. The interviewer took him through the Consent Form and proceed with the interview.

Interviewee C8 is working as a sales manager which is accountable for selling IT solutions and working closely with their solution architect. It was a fruitful experience having him to providing informative responses especially when he has a great exposure to clients who is particular about cybersecurity lately.

Working Environment/Culture

1. Can you give us a brief overview of your job at company XYZ? How long have you been in your company?

I am in an IT system integrator company providing IT Solutions to our corporate customers. I have been in the company for 4 years.

2. Can you describe team working culture in your company when undertaking projects?

We have many different departments and roles, and each personnel in their respective roles knows the requirements from their end in terms of deliverables. However the account manager would be the main bridge between the departments, to control and coordinate the flow of the projects.
From the Sales angle, we have the account managers, pre-sales and product managers. Technical side, we have our project engineers, service desk support engineers, project managers and Service Delivery managers. Operations includes our admin team that handles procurement and coordination of delivery, as well as contract admins who processes the paperwork for contract related services.

Communication

1. What are the biggest challenges you faced in handling cyberattack? How do you manage and communicate it?

I feel that the biggest challenge is educating the non-technical staff on the importance of cyber hygiene and compliance. Some of the staff were more reluctant when it comes to adapting new procedures, having to use newer software versions, etc.

2. **How effective is vertical communication within an organization in considering adopting and implementing cybersecurity practices?**

In my opinion, vertical communication is as important as horizontal communication. Younger generations who tend to be more IT savvy, should take the lead and assist the seniors who are less familiar with technology. This allows the team and the company to come up to speed quickly with the adoptions of cybersecurity practices.

3. What are your challenges when convincing your peers or management level to adopt your perspective towards cybersecurity adoption? How do you overcome it?

As we are a tech firm ourselves, it is quite easy to convince, in fact management could well be better informed than on this topic. We usually overcome issues easily as we are the subject matter expert in cybersecurity field.

Decision Making & Power

1. Is the management's advice been rationale all the time? Why? Could it be better?

They handle cybersecurity related advice with pride, as a failure or outage will result in a bad reputation for the company. We did not really have much cybersecurity incidents over the years.

2. Does your team have any influencer that is able to influence the management decision making process? What are their roles? And how do they influence them?

We have an open door concept in the company and management welcomes new ideas to implement, and should the use case be justified and pricing is reasonable, we are usually good to go.

Individual & Group Motivation

1. How often do you use Cybersecurity practices when instructed by management?

Cybersecurity practices are part of compliance for us and the team practises it as part of our company IT best practises protocol.

Change Management

1. How often does your company prioritize and constantly update on Cybersecurity latest trend?

As and when if there is an important announcement, management will notify the team via email and share what to do if any of the staff encounters the situation. Of course, our partners will also inform us of any latest trend. We all work very closely with each other especially in the IT industry.

2. **What is the biggest challenge in convincing the management that resist change in your view?**

Budget is the only resistance, especially if the price does not make sense for the solution to be implemented. Thus, a 3 quotation price comparison will always be called up to see which is the cheapest.

Leadership

1. How does the management bring across Cybersecurity practices to everyone? If there is anyone refuse to accommodate to such instructions, what would be the consequences?

We have a compliance to undertake when we join the company and all these security procedures have already been briefed and acknowledged. Thus, there is little to no resistance from the staff.

2**. Are there any incentives for employees to adopt cybersecurity practices in order to show its value for better work commitment?**

It is a responsibility and obligation to adopt the practises, and rewards should not be provided for complying. However we do have incentives when we recommend certain new practises.

a. Due to the current global pandemic (covid-19) that has affected many organizations, how did your company sustain? Do they spend more money and enhance cybersecurity?

Security is highly linked to our company's reputation and they generally do not hold back to enhance it.

Economical Behaviour

1. Was there any personal bias seen in the management when spending more money to invest in their employees?

As we operate in a fair environment where meritocracy is respected and looked upon, we are ok with it.

Plagiarism Certificate

Confirmation Certificate

Congratulations!

You have successfully completed the Library Plagiarism Quiz.

Student Name: Lim Jun Wen, Jawn

Student Number: **12258146**

Date: 18th Oct 2020

THIS IS TO CERTIFY THAT (signature)…… HAS COMPLETED THE PLAGIARISM QUIZ

Remember that the confirmation certificate is a statement by you that you understand plagiarism and know how to avoid it. If you think that you do not understand plagiarism and how to avoid it after working through this tutorial, you should confer with your module coordinator, no matter what score you have obtained on the test.