The Influence of Users' Addictive Behaviours on the Relationships Between Information Security Countermeasures and Risky Cybersecurity Practices

دراسة تاثير

السلوكيات الإدمانية للمستخدمين كوسيط في العلاقة بين الإجراءات المضادة

لأمن المعلومات وممارسات الأمن السيبراني الخطرة

by

ALI SAEED ALRASHDI

A thesis submitted in partial fulfilment

of the requirements for the degree of

DOCTOR OF PHILOSOPHY IN PROJECT MANAGEMENT

at

The British University in Dubai

June 2020

The Influence of Users' Addictive Behaviours on the Relationships Between Information Security Countermeasures and Risky Cybersecurity Practices

دراسة تاثير

السلوكيات الإدمانية للمستخدمين كوسيط في العلاقة بين الإجراءات المضادة لأمن المعلومات وممارسات الأمن السيبراني الخطرة

by

ALI SAEED ALRASHDI

A thesis submitted to the Faculty of Business and Law
in fulfilment of the requirements for the degree of
DOCTOR OF PHILOSOPHY IN PROJECT MANAGEMENT
at
The British University in Dubai
June 2020

Thesis Supervisor
Dr Maria Papadaki

Approved for award

_____	_____
Name Designation	Name Designation
_____	_____
Name Designation	Name Designation

Date: _____

DECLARATION

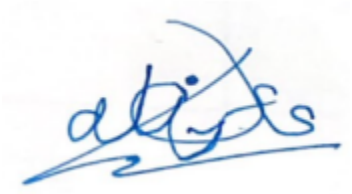
I warrant that the content of this research is the direct result of my own work and that any use made in it of published or unpublished copyright material falls within the limits permitted by international copyright conventions.

I understand that a copy of my research will be deposited in the University Library for permanent retention.

I hereby agree that the material mentioned above for which I am author and copyright holder may be copied and distributed by The British University in Dubai for the purposes of research, private study, or education and that The British University in Dubai may recover from purchasers the costs incurred in such copying and distribution, where appropriate.

I understand that The British University in Dubai institutional may make a digital copy available in the repository.

I understand that I may apply to the University to retain the right to withhold or to restrict access to my thesis for a period which shall not normally exceed four calendar years from the congregation at which the degree is conferred, the length of the period to be specified in the application, together with the precise reasons for making that application



Signature of the student

COPYRIGHT AND INFORMATION TO USERS

ABSTRACT IN ENGLISH

The emergence of the modern internet in 1990 and the development of web 1 was the first step on information sharing and reading-data, while the web 2 took a step closer and allowed peer-to-peer interactions with always an inter media system acting as a transmitter. Nowadays, web 3 is underway which will boost worldwide connectivity even further. The world is living the era of huge data flows, global scale interactions and social engagement of multicultural people in a worldwide network. People from various backgrounds and cultural dimensions are influencing the way that data are interpreted and managed through the technology driven system. Therefore, cyber security became extremely important and critical for organisations continuous operations. As the literature indicates the 95% of cyber security breaches are cause by a human error. Consequently, organisations worldwide are looking ways of minimising cyber threats that caused by human behaviour to improve information security. Currently, there is a lack of research on the role as well as the impact of the multi-behaviour countermeasures dimensions on information security. The main purpose of this research is to suggest a human behaviour information security countermeasures model for supporting investigation of and reasons for the main features of people's risky behaviours in the context of information security within public organisations in the UAE. The research methodology used descriptive quantitative with linear regression analysis. The research used a questionnaire that was analysed with the software (SPSS) 24.0.

Findings indicate that Attitude and self-efficacy have a direct influence on the attitudes towards cybersecurity countermeasures and Administrative, Managerial and Support countermeasures have a direct influence on the Security awareness countermeasures. The users' addictive behaviours can influence both information security countermeasures and risky cybersecurity

behaviour practices of the workforces of public organisations. Further research on employee behaviour can be studied over a longer period of time using a longitudinal study.

ABSTRACT IN ARABIC

كان ظهور الإنترنت الحديث في عام 1990 وتطور الويب 1 الخطوة الأولى في مشاركة المعلومات وقراءة البيانات، بينما اقتربت شبكة الويب 2 من ذلك وسمحت بالتفاعلات من نظير إلى نظير مع نظام وسيط دائمًا يعمل بمثابة الارسال. في الوقت الحاضر، الويب 3 قيد التنفيذ مما سيعزز الاتصال في جميع أنحاء العالم بشكل أكبر. يعيش العالم عصر تدفقات البيانات الضخمة والتفاعلات على نطاق عالمي والمشاركة الاجتماعية للأشخاص متعددي الثقافات في شبكة عالمية. يؤثر الأشخاص من خلفيات وأبعاد ثقافية مختلفة على طريقة تفسير البيانات وإدارتها من خلال النظام المدفوع بالتكنولوجيا. لذلك، أصبح الأمن السيبراني في غاية الأهمية والحيوية لعمليات المنظمات المستمرة. كما تشير الأدبيات إلى أن 95٪ من انتهاكات الأمن السيبراني ناتجة عن خطأ بشري. وبالتالي، تبحث المنظمات في جميع أنحاء العالم عن طرق لتقليل التهديدات السيبرانية التي يسببها السلوك البشري لتحسين أمن المعلومات. حاليًا، هناك نقص في البحث حول دور وتأثير أبعاد الإجراءات المضادة متعددة السلوكيات على أمن المعلومات. الغرض الرئيسي من هذا البحث هو اقتراح نموذج الإجراءات المضادة لأمن المعلومات للسلوك البشري لدعم التحقيق وأسباب السمات الرئيسية لسلوكيات الأشخاص المحفوفة بالمخاطر في سياق أمن المعلومات داخل المؤسسات العامة في دولة الإمارات العربية المتحدة. استخدم منهج البحث الكمي الوصفي مع تحليل الانحدار الخطي. استخدم البحث استبانة تم تحليلها بواسطة برنامج.24.0 (SPSS)

تشير النتائج إلى أن الموقف والكفاءة الذاتية لهما تأثير مباشر على المواقف تجاه التدابير المضادة للأمن السيبراني والتدابير المضادة الإدارية والإدارية والدعم لها تأثير مباشر على تدابير الوعي الأمني المضادة. يمكن أن تؤثر سلوكيات المستخدمين التي تسبب الإدمان على كل من الإجراءات المضادة لأمن المعلومات وممارسات سلوك الأمن السيبراني المحفوفة بالمخاطر للقوى العاملة في المؤسسات العامة. يمكن دراسة المزيد من الأبحاث حول سلوك الموظف على مدى فترة زمنية أطول باستخدام دراسة طولية.

ACKNOWLEDGEMENTS

First and foremost, praises and thanks to ALLAH, for His showers of blessings throughout my research work to complete the research successfully.

I would like to express my deep and sincere gratitude to my research supervisors, Prof. Halim Boussabaine and Dr. Maria Papadaki, for giving me the opportunity to do research and providing invaluable guidance throughout this research. Them dynamism, vision, sincerity and motivation have deeply inspired me. They have taught me the methodology to carry out the research and to present the research works as clearly as possible. It was a great privilege and honour to work and study under them guidance. I am extremely grateful for what they have offered me. I would also like to thank them for they friendship, empathy, and great sense of humour.

I am extremely grateful to my parents for their love, prayers, caring, sacrifices for educating and preparing me for my future. Also, I express my thanks to my sisters and brother for their support and valuable prayers. My Special thanks goes to my friend Dr. Mohammed Alaryani for the keen interest shown to complete this thesis successfully.

Would like to say thanks to my friends and research colleagues for their constant encouragement.

Finally, my thanks go to all the people who have supported me to complete the research work directly or indirectly.

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

LIST OF EQUATIONS

LIST OF TABLES

CHAPTER 1: DEVELOPING THE RESEARCH AGENDA/INTRODUCTION

1.1 Introduction

In the 21st century, globalization has created macroeconomic transformations that in turn have introduced new challenges in the management of critical organisational and information infrastructure, yet this is one of the most important organisational assets in the modern business environment. Increased globalization has resulted in corporate boundaries becoming increasingly invisible due to phenomena like globalization and increased computerization, and with this have come challenges in managing information assets. Automation has replaced most of the manual, human-mediated tasks such as decision making with technology-driven systems characterised by sophisticated technology; the effect has been a greater need for securing organisations' information systems (Moşteanu, 2020). As technological developments become more advanced and entrenched in everyday organisational operations, security threats increase proportionately; information security has become one of the enduring challenges to organisations, given the immense value information and data have to organisations, and the devastating effects of this information/data being breached (Kedrosky, 2019). In the modern corporate environment, it is common for critical information systems infrastructures to be run by non-computer experts, for instance soldiers in militaries, accountants in corporate environments, nurses in health care, and fire-fighters in emergency services (Ghafir *et al*., 2018). In such challenging applications, ensuring the protection of critical assets and data against insider threats and/or attacks becomes infeasible and economically impossible; however, the use of suitable strategies to manage these risks makes it possible to manage such insider

threats (Le and Zincir-Heywood, 2020). Security technologies such as data encryption and security firewalls can help protect data and information, as well as computer systems, from attackers and unauthorised access. However, a more critical and potentially high impact source of threats in cyber and information security is the human factor. Through techniques such as social engineering, malicious attackers are able to breach technology-mediated information systems' security through interactions with people (Ghafir *et al*., 2018). More and more organisations have capitalised massive resources on their information systems due to a significant increase in cyber risks in the workplace and because of the value attached to data, in order to combat increased risks. As a consequence, these organisations in return believe that they need to achieve higher returns on investment (ROI) on their investment in information systems security.

As internet technology is dynamic in nature, it leads to an increase in the volume and complexity of information security. Cyber incidents are growing regularly, thereby exposing organisations to elevated information security risks including cyber-attacks (Parekh, 2020). Different organisations have applied and deployed sophisticated monitoring systems in order to protect all types of organisation information systems and data assets; different types of monitoring systems used include prevention of data leak, password management, and information security technologies, such as antivirus, as well as content monitoring technologies, for perimeter defence. The latest research on cybersecurity has shown that the impact of applying information security countermeasures and policies on the organisation does not always have similar effects on different employees (Tam and Jones, 2018). Some of the employees in institutions do not give the information security policies high care and attention, and other groups of employees tend to misjudge risk events concerning information security, even after

receiving a clear instruction on policy security on a verbal and written way to guide them. Users who have received a high level of training on information security from their organisation will not necessarily show higher levels of healthy cybersecurity behaviour then other employees (Visvizi *et al.*, 2018). More and more organisations have capitalised a massive amount of resources on their systems after cyber risks increased significantly in the workplace to combat this issue and, as a result, those organisations in return need to achieve a positive return on their investment.

Information security experts should consider human information security behaviour countermeasures as well as technology in aspects of information security to create a secure environment. For example, according to Valizadeh *et al*. (2019), users may delay complying with a password change as they consider the change to be an unnecessary interruption. Safa *et al*. (2018) noted that employees failed to perform security behaviours that had been put in place to protect the information assets. Merhi and Ahluwalia (2019) pointed that, whilst users can understand the severe consequences of breaches of password protection, this does not change their attitudes or their resistance behaviour towards implementation of the information security policy. Jeong *et al*. (2019) demonstrated that the awareness of information security has significant effects on the information security attitude towards positive behaviour. Rahman Ahlan *et al*. (2018) highlighted the importance of information security awareness to influence security change behaviours among employees. In this research study, the researcher viewed people's management as a strategy to research and examined the mediating effect of the users' addictive behaviours on the relationships between information security countermeasures and risky cybersecurity practices.

With respect to information security, human factors remain under-appreciated and unexplored/under-explored, according to Nobles (2018). Mounting cyber-attacks, ransomware attacks and data breaches/data losses remain an enduring problem in information security and are as a consequence of human-induced errors: 95% of all cyber incidents are attributed to human factors and, according to Hadlington (2017), the present information security plans and strategies do not significantly incorporate human factors in evaluating and managing risks. Instead, information security stakeholders such as managers, corporate leaders and cybersecurity professionals extensively rely on technology as the primary means of averting cybersecurity issues and incidents. These stakeholders and manager's/decision makers believe, fallaciously, that the key to improving information security (IS) defences is the use of technology, despite research and existing relevant literature indicating that new technologies aimed at improving cybersecurity create unintended consequences, even though errors that are technologically induced are human enabled. The current perspective of managers on the problem of human factors with respect to IS has a very narrow scope and is more than an issue with training. Mounting human factor challenges, in addition to managing complex cybersecurity issues, exceed the expertise provided by a majority of cybersecurity professionals (Nobles, 2018). Despite this, managers and decision makers remain reluctant to seek the expertise of behavioural analysts, cognitive scientists and human-factor specialists to help in the development and implementation of effective strategies and objectives as a way of minimising human-enabled errors in IS that result in serious cybersecurity incidents.

An evaluation carried out in the United Kingdom to explore the size of organisations employees work for, and the employees' age as well as their attitudes towards the frequency of cybersecurity incidents and frequency of engagement in risky online behaviour, showed that

there is a negative association between risky cybersecurity behaviours and attitudes towards cybersecurity (Hadlington, 2017). In the study, participants aged between 18 and 84 were evaluated, with 515 participants, in full- or part-time employment, being involved in the research that involved self-administered questionnaires. Their general awareness of cybercrime and their attitudes towards cybersecurity as well as the risky cybersecurity activities they were involved in was evaluated. The findings showed that those with more negative attitudes towards cybersecurity were linked with much higher levels of risky cybersecurity behaviours. These findings showed appreciable differences with respect to the size of the organisation and the employee age groups, based on attitudes to cybersecurity and frequency of and attitudes towards engaging in risky cybersecurity behaviour. As such, the study concluded that employee attitudes and behaviours have a significant impact on cybersecurity and the organisation size is also a mediating factor.

Extensive research has been conducted on investigating and categorizing threats due to malicious attacks from currently disgruntled employees in organisations, or those motivated by quick financial gain. The information communication technology (ICT) threats related to employees are termed ‘insider threats’ and pose a growing information security menace, but, with the right strategies and approaches, they can be detected and arrested before damage is caused. However, human factors that are largely unintended, due to habit, or cultural, such as poor planning, ignorance and failure to pay attention to detail, are increasingly being linked to the rise in unintentional insider information security breaches and incidents. In such circumstances, there is no prior planning or malicious intent for the ‘attack’; instead, the actions of omission and/or commission by employees can be equally or even more disruptive and damaging than targeted and planned information security attacks (Hadlington, 2017). Even

without malicious intent, the biggest cybersecurity threats to organisations are its employees, and this is because controlling the human element is among the most challenging aspects of ensuring cybersecurity. There is slightly more predictability with machines than with humans. This is illustrated by organisations still being plagued by cybersecurity breaches despite increasing investments in information security technologies. Many attacks, for example, are as a result of employees misusing encryption in some way and the root cause is employees who may take requirements for cybersecurity too lightly, resulting in dramatic consequences for the organisation.

The researcher selected this research topic to develop various theories related to information security and suitable countermeasures for public organisations in the UAE's culture. The researcher also conducted various studies on the role of cultural dimensions in the society as well as different countermeasures used on this field. Galletta *et al*. (2019) argued that public organisations are required to make changes concerning information security to establish an effective informational security culture. Van Bavel *et al.* (2019) argued that information security is required to focus on human behaviours to mitigate the related risks and issues. It is indicated that a culture that is information-security aware reduces the risks to the information assets, because it reduces the rate of human misbehaviour and errors. The information is being protected by two of the strategies such as use of technology for protection of valuable information and the second is based on the human element, the 'end user'. Where the end user have high risk which could abuse the information security policy by passing it to a third party without the consent of the informational owners (Chin *et al.,* 2018). This research study is focused on the effect of the human element's culture in information security and the associated countermeasures used for the relevant behaviours. The key significant reason behind the role of

the human along with human factors is a challenge to monitor and predict, as well as control. Proper control over human errors is required to mitigate the risks relating to information security management systems.

The effective management of information security is an even bigger challenge for public organisations that use information technology in their daily processes. Rivis and Sheeran (2017) aver that human interventions in mitigating information security risks and threats fall under four categories: individual, third party, team and management. The human factors are uncontrollable forces which interact with the technological elements to secure the information system. The human errors occur due to a variety of factors including: inadequate skills, lack of information security awareness, lack of communication, weak countermeasures methods, and intentional as well as unintentional errors to pose risks to information security. Palau-Saumell *et al*. (2019) suggest that it is necessary for human factors to be better understood in the context of information security (IS) and their impacts on effective implementation of information security management systems. The purpose of this research study is to review the human factors in the information security as well as discuss how the information security countermeasures have become a major tool to overcome the human issues and errors (Katzenbeisser and Petitcolas, 2016). There has been an increase in threats to information technology which has resulted in new solutions, while the human threat factors have not been fully addressed'. Part of information security breaches are due to human factor issues which remain unaddressed (Maass *et al.*, 2018). The cultural dimensions have become an important part of organisations' information security strategies for promotion of performance as well as productivity.

The researcher selected this research topic to develop various theories related to information security and suitable countermeasures for public organisations in the UAE. The

researcher also conducted various studies on the role of cultural dimensions in the society and their impact on addictive behaviours that can impact information security, in relation to the different countermeasures used in securing information systems. Mikalef *et al*. (2018) argued that public organisations are required to make changes to the information security which establish an effective informational security culture. Mamonov and Benbunan-Fich (2018) argued that the information security is required to focus on the human behaviours to mitigate the risks and issues. It is indicated that a culture that is information-security aware reduces the risks to its information assets, which led to reduce on the rate of human misbehaviour and errors (Asadi *et al*., 2019).

1.2 Research Background

According to Ameen *et al*. (2021), public organisations implement information security strategies (policy, procedure and countermeasures) in order to reduce the risk of their information systems security being breached. Asadi *et al*. (2019) established that the user's behaviour is among the most important factors to consider when developing strategies for securing organisations' information systems security. Meoli *et al*. (2020) contend that organisations use various approaches for protecting their information system assets as well as resources. In this particular study, the participants are surveyed on different information security countermeasures for minimising the consequences of information security threats on public organisations within the UAE. According to Si *et al*. (2020), human factors are the most challenging aspects in managing risks to information systems. The majority of information security incidents that are a result of human behaviours, such as acts of human error and failure, compromise an organisation's intellectual property, and/or lead to blackmail in lieu of the threat

of unauthorised disclosure of confidential information such as health and personal financial records, unauthorised access to information and illegal confiscation of the equipment.

In the past quarter of a century, information security management has been growing and becoming ever more important in both private and public domains. Most information security incidents are a result of human acts of omission or commission, such as mistakes or deliberate jeopardy and misbehaviour. Based on these observations, the researcher focuses on the human factors relating to information security assurance. Ameen *et al*. (2021) state that, despite interest and increased efforts in ensuring information systems security, there are still gaps in one of the most critical risk surfaces to information systems security in public (and private) organisations: human factors and their addictive behaviour. Palau-Saumell *et al*. (2019) discussed that, in several cases of information security and data breaches, the main concern relates to humans, as errors are made due to different factors including lack of awareness of information security and poor countermeasures. The technology-related breaches are experienced due to both malicious and non-malicious individuals exploiting the vulnerabilities in information security technology systems on a regular basis, and the situation is expected to continue as the security hacks have become mainstream in the media sphere due to the general public's increased interest. Ameen *et al*.(2021) argue that there are various information security standards in existence, along with operations geared towards achieving cybersecurity assurances.

There are several examples of where human factors have played a major role in cybersecurity threats and incidents; one case is the '*Wanna Cry'* ransomware epidemic where human factors played a significant role in increasing vulnerabilities for many businesses worldwide. Even after technology vendor Microsoft had released updates to patch-up the identified vulnerabilities, many organisations had not updated their systems two months later.

As a result, several breaches followed, with the weakest link to the propagation of the '*Wanna Cry'* ransomware being accelerated by non-IT personnel within organisations. For instance, cases of employees unwittingly disabling security solutions in their workstation computers, leading to infections spreading to the rest of the organisation's network from their computers are numerous and varied. Some acts are a creation of habit: an employee, having opened several browser tabs with interesting information, elects to leave them unclosed, creating an increased cyber-attack surface. Yet many organisations believe they face minimal or no threats from within; a survey conducted by Kaspersky (*The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within | Kaspersky official blog*, 2021) established that just 52% of businesses believed they face information security risks from within. The major causes of these risks are employees who, either unintentionally or due to their lack of knowledge, are putting the organisations they work for in harm's way, in the context of information security risks.

Uninformed and irresponsible employees pose a great danger to an organisation's information security and this has elevated the sense of apprehension as 57% of organisations believe their IT systems will be breached. This risk creates fears in organisations, with the top three cybersecurity fears being due to employee behaviour and human factors. Some of the areas where organisations have reported top vulnerabilities include employees inappropriately sharing data through mobile devices (47%), physical device loss (mobile devices) that expose the organisation to increased risks (46%), and inappropriate use of IT resources by employees (44%). Other causes for concern as reported by the Kaspersky survey include incidents involving partners such as suppliers that an organisation shares data with (43%), and incidents involving connected, non-computing devices. Smaller organisations with between one and 49

employees reported feeling especially at risk from internal threats from their employees, compared to larger organisations with over 1000 employees (Kasperski Daily, 2020). This could be because smaller organisations do not spend a significant amount on cybersecurity while also giving their employees greater flexibility on how they use IT resources, while larger organisations may have stricter cybersecurity policies. And businesses are justified to be worried about employee-induced cybersecurity risks because staff can make mistakes that put at their organisation's data at great risk, either due to accidental slip-ups or due to carelessness, or, importantly, due to their habits. Further, these staff members may lack the requisite training and/or sensitization to teach them safe and appropriate behaviour to protect the IT resources of the organisations they work for.

In the UAE, 80% of organisations suffered at least a single cyber-attack incident in 2019, according to the study; yet as many as three-quarters of respondents in the survey admitted to only training their staff on best practices as regards cybersecurity just twice or less each year, according to Mansoor (2020), Almost half of UAE organisations reported multiple cyber-attack incidents, based on research conducted by (Proofpoint, 2019) involving 150 organisations from various industries in the UAE. The leading method by which cyber-attacks were propagated in the UAE in 2019 was compromised accounts, which impacted 28% of the surveyed firms; this was followed by credential phishing that affected 20% of employees, and insider threats came third as the main point of cyber-attack propagation at 17%. Almost a third of the respondents said compromised accounts will continue to be a major (the leading) cybersecurity threat in the UAE, followed by DDoS (distributed denial of service) attacks (28%), and phishing at 19%. The biggest outcomes for data breaches for UAE organisations were financial loss (29%), data breaches (28%), and loss of customer base (23%), as per Mansoor (2020). These figures

illustrate the seriousness and level of damage that can be caused by data breaches. Human error is a major cause of security breaches and some of the common errors identified in the Proofpoint study include poor password hygiene (29%), sensitive information mishandling (25%), succumbing to phishing attacks (24%), and clicking on links that are malicious (20%). Further, criminal insider threat was cited by 19% of the respondents as a growing cybersecurity concern for businesses.

For UAE companies, cybersecurity policies must be 'people-centric' as cyber criminals increasingly target humans rather than IT systems and infrastructure, with the goal of siphoning sensitive data, stealing credentials, or transferring funds fraudulently, among other malicious objectives. With a survey on UAE companies showing that 39% of organisations believe employees are a source of vulnerability for the businesses to cyber-attacks, security awareness and education/sensitization is a critical factor in enhancing cybersecurity and can make the difference between at attempted cyber-attack and a successful cyber-attack. People-centric cybersecurity solutions should be augmented by technical controls and solutions, with a comprehensive training programme being at the centre of any organisation's cybersecurity strategy and policy (Mansoor, 2020). One aspect of human factors and elevated cybersecurity threats is addictive behaviour; behaviour is considered addictive when there is a stimulus related to the said behaviour that is both reinforcing and rewarding, and is associated with the development of the addiction. When the addiction is about addictive human behaviour, then it is termed a behaviour al addiction. Research has shown, for instance, that internet addiction is a significant predictor of risky cybersecurity behaviours by employees; positive attitudes with regard to cybersecurity have also been shown to have a negative association with risky cybersecurity behaviours (Hadlington, 2017).

The use of technology in information security is negated when employs engage in risky activities or fail to follow information security protocols, placing themselves and the organisation at great risk, and this has led to increased research on the role humans play in information security. Consistently, research has shown that employees underestimate the risk of falling victims to cybersecurity breaches, despite their risky actions and behaviours, especially addictive behaviours. The environmental, organisational and behavioural factors all work to influence the extent by which employees are able to follow and adhere to safe cybersecurity practices. Personality traits influence addictive behaviours; these personality traits differ among individuals within an organisation and consequently affect the person's adherence to laid-down cybersecurity and safe -use procedures. It has been posited that personality traits such as conscientiousness and agreeableness are associated with greater willingness by people to adhere to information security protocols and practices. Further, people who are more extroverted have a greater tendency to violate information security policies when compared to those who are more conscientious and neurotic. Behavioural intent and actual behaviour have exhibited discrepancies in research on human behaviour and information security, and so it is more difficult to accurately use behaviour as a predictor of behaviours that comply with information security guidelines. Key personality factors have been shown as well to be predictors of susceptibility to social engineering attacks (Hadlington, 2017)

Addictive behaviours such as the use of smartphones even in the workplace, and accessing corporate information through smartphones, including accessing e-mails and information databases, are an addiction, for instance, that creates a new security threat surface. Smartphone use with the internet has a number of functions in addition to making calls; users can use smartphones to play games, use messaging systems, chat with others, access the web,

and search for information, as well as use corporate IT resources, including internet access (Wi-Fi). This has made smartphones popular and their use in corporate settings or mixed with corporate IT resources has become common (Derevensky *et al.*, 2019). There are various types of internet addictions and this is because the use of the internet is now ingrained in modern society; computer and internet use have changed the way people do business or transactions. Many people connect to the internet daily, and, while many believe connecting to the internet and watching videos or surfing is an activity that is relatively harmless, some people have become addicted. Behavioural addiction pertains to people being predisposed to entities that can cause stimulation and result in addictive behaviour. These addictions can be akin to substance addiction; behavioural addictions such as internet addiction can be analogous to substance/drug addiction, except that, in behavioural addiction, a person is not addicted to any substance; instead, they are addicted to the feeling the get when they engage in a relevant action (Mahapatra, 2019). Further, physical drug addiction signs are absent in behavioural addiction.

People respond in different ways to phishing attacks and this is related to their behaviour on social networks. When prize phishing e-mails are used, neuroticism is the most correlated factor in responding to such an e-mail and this is an addition to differences in responses based on gender. Persons that score highly on the openness factor tend to post messages to social media sites such as Facebook and have privacy settings that are less strict, and this can cause them to be more susceptible to privacy-type attacks. Susceptibility to becoming a victim of phishing attacks has no relation to a lack of awareness of the risks posed by phishing. Further, it is difficult to predict in advance among online computers/internet users (Cain *et al*., 2018). It is therefore imperative to understand better the traits that contribute to vulnerability online in order to understand how addictive employee behaviour increases cyber-attack risks for

organisations, to help in the development of custom policies and user interfaces along with developing sensitization and educational campaigns to increase the security of corporate information systems from addictive behaviour mediated cyber-attacks.

1.2.1 Human Factors in Information Security

People are at the centre of technological design along with use of designed products, and this makes technological systems, in the context of information systems, an asset as well as a threat. Due to the value placed on data and corporate information, organisations place a premium on addressing the human elements and risks in information security in order to effectively deal with the incidents of information security breaches (Katzenbeisser and Petitcolas, 2016), and this is among the motivating factors for undertaking this research. In public organisational policies as well as standards, there are codes of conduct which are designed for people to adhere to concerning information systems security; further, it is humans that execute organisational information security policies. The human factors are major forces which are behind the effectiveness as well as the failure of security systems. Asadi *et al*. (2019) state that the technical solutions are not sufficient as insider threats have become a fundamental issue in the public sector. There is evidence that the human factors undermine information security with devastating effects, as the examples in the UAE and globally (covered in the background section) show, in addition to public organisations having underdeveloped information security systems and policies. The direct factors are those that are dependent on the individual's characteristics and have a significant impact on the information security management system. Sheeran and Rivis (2017) explained that the indirect factors are based on external issues like the organisational issues related to adequate budget, types of culture as well as governmental policies which have proper influence to the direct factors and the information security system.

Human errors are defined as intrusions into systems which otherwise work properly; putting greater focus on human factors and internal threats will serve to significantly reduce the threats and risks to public information systems. Tsai *et al.* (2016) contend that security policies are being designed to restrain human behaviours (especially addictive behaviours) to mitigate the threats to information systems due to them (human errors and misbehaviour). Human behaviour is hard to define and measure as well as control in public organisations, especially when such behaviour is mediated by addictive behaviour. Public organisations are apprehensive about their employees adhering to information security policies and following the rules and guidelines geared towards ensuring information security, such as careful management of access codes, safe browsing, avoiding clicking e-mail links from unknown sources, and not using external devices such as flash disks to store company data, among other security policies. It is clear that there is a gap in the research, as well as a lack of understanding and appreciation of addictive human behaviour and its effects on information security threats and countermeasures. Further, there is a dearth of adequate sensitization programmes to educate public organisation employees on information security policies and procedures (Zhang *et al.*, 2019). Public sector staff without the requisite skills on information security, coupled with inadequate training on information security, are contributing to the weak performance of information security and increasing threats and risks to data and information systems. For instance, when people in critical areas such as the finance department are not aware of how to use email encryption, the end result is unencrypted emails containing sensitive information being sent to the customers. Meoli *et al*. (2020) determined that unsecure information is being exposed to the public domain and then it is obtained by criminals who use it for malicious purposes, including ransomware and fraud. Public organisations are not focused on insiders' behaviour with respect to information security and their technological competency although training programmes are

supposed to be held regularly, based on a competent information security policy (ISP) to provide employees with adequate skills and knowledge as well as to control their behaviour in order to confront the challenges of information security.

Dwivedi *et al.* (2019) stated that human behaviour is affected by the dimensions of the culture. The organisational culture is related to the employees' perceptions of their shared beliefs as well as the values among the employees in the working environment. The organisational culture influences the beliefs of individuals and their human behaviour. In the context of information security, this cultural effect has been tested by researchers. For example, the effect of the organisational culture has been tested in alignment with information security principles such as confidentiality, integrity and accountability (Asadi *et al*., 2019). The results showed that the organisational culture is influencing examined principles of the information security. Hofstede's cultural framework has been used for the organisational cultural in the information security investigation context. It has been applied in an empirical information system study and identified changes that existed in the cross-organisational behaviour at the time of testing the technology acceptance model (TAM). Hofstede defines culture as the collective programming of mind that can distinguish one group of people from another (Soomro *et al*., 2016).

The countermeasures for the cultural effect on human behaviour are information security policy, training and cultural awareness as well as management support. D'Arcy and Teh (2019) mentioned that the information security measures are shifting from technology towards the human factors. Asadi *et al*. (2019) investigated the influence as well as effect of information security policies on culture. The policies will set guidelines to influence human behaviour by means of using the system. The security policies are created for communicating the security

protocols, assigning roles as well as responsibilities, along with providing guidance to employees to make sure they correctly handle security incidents. Hina *et al*. (2019) discussed that creating, updating and communicating as well as promoting policies is an element of the security management programme to make employees aware of information security incidents.

Training as well as awareness is required for people to thrive in the culture of information security. It provides the employee with the knowledge and skills required to use the information system. The training aligned with employee awareness should be based on information security policies as well as responsibilities (Yu *et al*., 2020) without ignoring the organisational culture aspect. The training is focused on the forming of habits in relation to users' perception as well as procedural options. It enables the employees to retain experience in using the information system. Finally, management support is an important factor in the information security culture as it is required to create a supportive working environment in the organisation. Support as well as management leadership is a contributor in implementing efforts towards information security. Birkel *et al*. (2019) mentioned that it is imperative that managers should develop strategies to protect assets as well as formulate the organisational budget. Therefore, compliant employees are the result of implementing countermeasures that encourage or/and force them to comply. Additionally, rewards or threats that could motivate the potential non-compliant insiders will also motivate the compliant insiders.

The countermeasures philosophy is described as the philosophical method information system management practices to guarantee compliance or to minimise non-compliance between employees. There are two leading philosophies regarding methods to guarantee compliance. The first approach is a positive developmental one, with a focus on the inspiration to comply, as this is the development philosophy. The next one is more negative, which is the deterrence

philosophy, with a focus on generating fear in a situation of failure to comply. An example of the development philosophy is describing why compliance is favourable for the employees (for example, as it may offer a sense of personal fulfilment). An example of the deterrence philosophy is advising employees that individuals who do not fulfil the existing or/and newly established policies will be punished in different ways.

The deterrence theories warn employees, with sanctions to push them to obey IS policies, while the development theories encourage employees to follow the policies and procedures by proposing a reward or by notifying employees of the inherent benefits and general safe environment they will have when the policies are complied with.

Theories of deterrence have been utilized in dealing with criminal acts as well as in information security research and in governmental actions during the last decade, particularly the General Deterrence Theory (GDT), which was adapted, contextualised and adopted in IS research in the 1990s. There is another potential explanation why deterrence theory is generally used in IS security research: IS security shortages indigenous theories on IS, and there is lack of sufficient and healthy developmental theories (if we make exception on Protection Motivation Theory, PMT) that was adapted, contextualised and adopted in IS research.

The growth of security incidents related to employee actions led some researchers to explore the idea that the deterrence theory was not successful enough. Therefore, they began looking at another approach, the development theory, which uses encouragement to motivate insiders to obey information system policies. However, the increase in incidents cannot be definitely stated to be due to the futility of the deterrence theory.

1.3 Research Problem Statement

Information security is focused on technological remedies like encryption, detection of viruses, and firewalls as well as anti-spyware. Investing in a technological information system is not enough, however, as the information security incidents within public organisations result both directly and indirectly from misuse and errors by employees. Improvement in information security requires investment in two main areas, technical as well as organisational resources. Scholars have focused attention on the human dimensions of information security by applying philosophies of social as well as behaviourism thinking and investigating the suitable countermeasures for this specific organisational culture. There are various reasons behind the information security breaches such as communication technology, policy, computer science and achievement of success in areas such as managing as well as understanding the human factors (Zhang *et al*., 2019). Human factors play a key role in information security. The characteristics of human factors impact information security. This research studies behaviours and influences concerning effective information security management systems in public organisations.

In regard to all this, the information security awareness (ISA) of the employees is identified as an essential prerequisite of the information security behaviour. It plays a key role in the employees' policy compliances. ISA is termed a cognitive state of mind; therefore, it is identified as important to information security. As the increasing incidents could be simply because of the unsuccessful execution and assumption of the deterrence philosophy or/and the increasing number of employees. Additionally, sentencing cannot be discarded entirely. Employees who track policies to escape punishment and insiders with low self-control are more frightened by sentences than by ethical training (Yazdanmehr *et al*., 2020). Possibly, the reason why some studies are now focusing on development theory rather than deterrence theory may be rational in nature: the sentence in deterrence theories symbolises a negative method, and any

negative method is frowned upon in a culture motivated by political acceptability and keen to discover positive methods to improve societal manners. Tu *et al*. (2018), with others, inspired researchers to explore motivational approaches to ensure IS compliance. Thus, information system scholars have lately started to discover an extra positive aspect to compliance, although this is a very recent research area. The researcher can understand the drivers as well as the restraints of forces relating to human issues with obstacles to information security in public organisations. There are certain main implications of the role of human factors and challenges in the process of information security Moody *et al*. (2018). The information security risks are consequences on the organisation's operations along with its assets. This research study intends to address a number of problems, which are a lack of clear as well as effective regulations and countermeasures which are used to protect the information security along with the implementation of proper protection policies in different cultures. The main aim is to explore and identify the information security countermeasures and provide a framework to enhance the information security. One of the main challenges is implementation of information security policies due to the occurrence of cultural changes and the gap between knowing and doing. The researcher will take the public sector at both individual and management levels as the unit of study.

1.4 Research Questions

The main purpose of this research is to investigate whether addictive behaviours mediate the association between information security countermeasures and human risky cybersecurity behaviour practices. The outcome of this will highlight which measures can be adopted to mitigate employees' addictive behaviour. Several questions are formulated to accomplish this purpose. These are:

1. What are the information security countermeasures that may influence the human risky cybersecurity behaviour practices in public organisations?
2. What are the users' addictive behaviours that may lead to an increase in risky cybersecurity behaviour practices?
3. What is the association between risky cybersecurity behaviour practices and information security countermeasures?

The research questions were formulated after Hadlington's (2017) paper. Hadlington (2017) investigated human factors in cybersecurity, examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviour.

1.5 Research Aim

The aim of this research study is:

To examine the mediating effect of the users' addictive behaviours on the relationships between information security countermeasures and risky cybersecurity practices.

The study is focused on expanding the body of the knowledge based on various aspects of information security to support employees. This formulates the objectives of this particular research work. The study is focused on an extensive review of the existing body of literature. It aims to explore the reasons behind employees' non-compliance with their organisation's security policy and find out which security countermeasures will be necessary to encourage the employees' compliance and behaviour change. The study also investigates as well as analyses the role along with the impact of the employee's addiction behaviours on the information management system securities. It also explores an answer to the research question, "Does users' addictive behaviour mediate between information security countermeasures and employees'

risky behaviour"? We believe that this research context is particularly applicable for the emerging area of information security countermeasures.

1.6 Research Objectives

The objectives of this research study will lead to fulfilment of the research aim; they are as follows:

- Identifying countermeasures for information security that affects risky cybersecurity practices.
- Recognising addictive behaviour that can contribute to unsafe practices in information security.
- Analysing addictive behaviours that mediate between risky cybersecurity practices and counter-measurement of information security;
- Defining the link between risky cybersecurity practices and countermeasures of information security.
- Recognizing employees' risky behaviour practices that can affect public sector information security.

1.7 Research Scope and Significance

The main scope of this research study is to cover the information security countermeasures, users' addictive behaviours that are associated with the local culture in the public sector, and human risky cybersecurity behaviour, in order to increase the level of information security. The human aspects are used to investigate the behaviour that affects information security in the public sector. The scope is to analyse the impact level of human behaviour on information security, along with developing a mitigation plan to minimise the

effects using users' addictive behaviour as a mediator (Pearlson *et al*., 2016). The cybersecurity strategies are used to design an information security countermeasures framework related to the human behaviour. As per the best practices, guidelines are recommended for training as well as awareness about using internet services. There is scope for using an information security countermeasures model in this research. The research is focusing mainly on public sector organisations.

The conceptual framework is developed based on the countermeasure's dimensions identified as well as an exploration of the relevant literature. The countermeasures constructs are identified and related to the role of cultural dimensions as well as sub-dimensions to the public organisational culture along with the behaviour of staff towards the information security culture. The information security countermeasures constructs help to inform the security culture policies (Pearlson *et al*., 2016). The mediator is used to mediate the independent variables (IV) and dependent variables (DV) to guarantee clear relationship between them from the comprehensive perspectives, and in this way detects of perils and affirmation level of information security countermeasures. Security mindfulness training is given to staff to keep them from making malicious connections or accidentally going to suspect sites (Martins *et al.*, 2014). At the point when the approaches and additional preparation are adopting, there will be better confirmation the innovation with the end goal that when employees resist being foul up and the malware cannot run and accomplish the objectives.

Implementation of an information security countermeasures system has become a key requirement for public organisational services. There is a huge amount of research which is focused on the technical elements of information security with a clear understanding of the impact of behaviour on the information security countermeasures. There are challenges to

establish as well as promote the proper information security culture and countermeasures in public organisations (Teh *et al.*, 2015). The conceptual framework of this particular research study is based on strategic planning relating to information security policies, training and awareness of employees, and proper countermeasures along with a structure and activities in the IT services. It is important to maintain security as well as safety in handling the information to maintain security policies in the organisation (Siponen *et al*., 2014). This particular study is based on reducing the human mistakes and misbehaviours which impact the data security.

Consequently, data security needs to be utilized to remove or reduce human interference. The human conduct-related hypotheses are broken down in this examination in order to research different speculations which are utilized to limit the human dangers from the data framework. The human conduct is part of data security. Prior studies into the information security domain are broad into nature, which provides a general overview of the information security research (Martins *et al*., 2014). The study not only critically analysed the behaviour of users but also helped to understand people's information security behaviour.

1.8 Research Hypotheses

The research hypotheses are as follows: attitudes towards cybersecurity countermeasures are positively related to the risky cybersecurity behaviour practices and security awareness countermeasures are positively related to the risky cybersecurity behaviour practices. Users' addictive behaviours are positively related to the risky cybersecurity behaviour practices and attitudes towards cybersecurity and countermeasures are positively related to the users' addictive behaviours. Users' addictive behaviours are positively mediating between the risky cybersecurity behaviour practices, and information security countermeasures and security

awareness countermeasures are positively related to the users' addictive behaviours. The research hypotheses were formulated after Hadlington's (2017) paper. Hadlington (2017) investigated human factors in cybersecurity, examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviour.

1.9 Thesis Structure

The following outlines the chapters contained in this thesis:

Chapter 1: Introduction: this particular chapter presents the aims as well as objectives of the research study. It also provides justifications for carrying out the research. The chapter also provides research background, research questions, and outlines the countermeasures along with the human factors relating to information security. Additionally, the researcher identifies that human behaviour is the main reason for and aspect of information security.

Chapter 2: Literature review: this particular chapter reviews the literature on human behaviour risks related to information security countermeasures to establish the research framework. The chapter is focused on the security culture along with the roles in implementation as well as the development of information security cultural polices and countermeasures. Human behaviour is being affected by the cultural dimensions as well as sub-dimensions which influence human errors. Mainly due to human errors, the information security risks are increased, which affects the brand reputation of public organisations.

Chapter 3: Conceptual framework: this chapter provides the structure and content for the investigation based on the literature and, to a certain extent, in-depth knowledge of the research topic. The concepts and variables incorporated into the framework should be derived from the literature. These should capture the underlying principles of the theories which are

required to investigate the research study. This particular chapter provides a framework with the independent variables, mediating variable and dependent variable. There are two independent variables, the attitude towards cybersecurity countermeasures and security awareness countermeasures and a mediating variable is user's behaviour towards information security. The dependent variable is risky cybersecurity behaviours.

Chapter 4: Research methodology: this particular chapter explains the research methodology and method adopted to achieve the research aim and objectives. It provides detailed justification for the adoption of tools and methods as well as the procedures used to collect data using a primary data analysis method consisting of an online questionnaire. This particular section presents as well as discusses the primary method in order to answer the research questions. In Chapter 4literature survey is conducted to review the related literature.

Chapter 5: Data analysis: this chapter presents the data analysis which is intended to identify the information security countermeasures dimensions which influence the risky cybersecurity behaviours.

Chapter 6: Results of the hypotheses testing: in this particular chapter, the findings of a research paper and the hypothesis based on the results of the study contained in Chapter 5 and the hypotheses contained in Chapter 1 will be analysed. These steps are important to find out the population's opinions that could add value to the research topic. The checking of hypotheses is very important in understanding the relationship of the thesis paper's variables. Together with hypothesis testing, mutually exclusive population statements can also be categorised. Therefore, hypothesis testing can be used to consider the statistical value of analysis.

Chapter 7: Discussion: this chapter discusses and evaluates critically the main outcomes of the research, which provides answers to the selected research questions as well as the research hypothesis.

Chapter 8: Conclusion and recommendations: this particular chapter is summarised the outcomes along with contributions of the research study. This chapter also provides recommendations in order to improve the information security culture. It provides suggestions for the future research into areas of information security culture.

1.10 Summary

Technological innovation is required to secure data while humans are in charge of outlining, executing and working the mechanical instruments. People are considered as the weakest connection in the security of information and data because they make mistakes. Public organisations utilize data security strategies to ensure the advanced resources and countermeasures has been adopted to keep the data from theft. The significance of this research study is to become familiar with the human errors and misbehaviours which affect information security. Therefore, the human activities are to be mitigated with the use of proper information security countermeasures. The human behaviour-related theories are analysed in this study in order to investigate various theories which are used to minimise the human risks to the information system. Human behaviour is an aspect of information security. All through the threats to the data security alongside forms and additionally instruments, there is a zone which stays steady alongside the predictable threats. Because of increments in internal and in addition external digital threats, people's conduct and additionally mechanical vulnerability have stayed noticeable obstacles to corporate certainty. The organisation administers data security by the actualizing of data security norms and rules. The measures are utilized by the organisation to

ensure that it can administer data security from an all-encompassing viewpoint, and in this manner limit the dangers and improve the awareness level of data security in the organisations' societies. Employees' conduct affects progress and increases the inability to secure and protect data.

CHAPTER 2: LITERATURE REVIEW

2. Introduction

The research topic is based on examining the mediating effect of the users' addictive behaviours on the relationships between information security countermeasures and risky cybersecurity practices. Risky behaviours in a public organisation are considered as the main threat for the organisation; they are seen as the weakest link. It is hard to create an information security culture and protect the data and information (Siponen *et al*., 2014). The protection of information security could be achieved by innovative prevention technology along with understanding the ways in which humans interact with this technology. In this chapter, the researcher summarises the background of information security, its principles, and relevant theories along with models, different countermeasures, and the methodology used, threats of information security and standards and guidelines of information security (Peltier, 2016). This literature chapter analyses the security of information and computer data from breaches by insider misbehaviours and errors. Development of a theoretical model for information security is challenging work as there are diverse countermeasures, covering strategic as well as operational challenges based on legal and organisational perspectives.

2.1.1 Information Systems

In any organisation, there are usually people, computers and networks which collect, process, store and distribute information. All these put together make the information system. Therefore, an information system (IS) can be defined as a sociotechnical system in an organisation that is composed of tasks, people, structure and technology which is used to collect, process, store and share information (Pearlson *et al*., 2016). A typical information system is made up of the following components:

a) Hardware: this includes the computers and the input-output devices.
b) Software: these are the computer programs which are used to store, process and share information.
c) Data: data is the information being stored or processed by the programs.
d) Procedures: these are the set policies and guidelines that define how the hardware and the programs are to be used.
e) People: this includes the users of the information as well as those who operate and maintain the hardware and the software components.

When we talk about information system security, the security should be enforced in all of these components to ensure they are working correctly and are not compromised.

2.1.2 What is Information Security?

Information security, which is sometimes shortened as InfoSec, has been defined differently by many authors. However, all the definitions point to secure information processing, storing and access. For instance, it can be defined as the process of mitigating risks associated with information systems so as to secure the information (Moody *et al*., 2018). Safa *et al.* (2016) stated that information security is a practice preventing the unauthorised access, disclosure, inspection and destruction of the information. Crossler *et al.* (2013) argued that the security of information is required to protect confidentiality as well as data availability by focusing on policies and standards of information security. It is achieved through the use of risk management processes such as identification of assets, threat sources and vulnerabilities. He *et al.* (2017) defined information security as a set of strategies to manage the process, tools and policies to detect along with counter the threats to the digital information. Proper cryptography tools are used to mitigate the security threats. The possible responses to the security threats are

implementation of countermeasures to reduce the vulnerabilities, and evaluation of the countermeasures due to threats. Those types of countermeasures are used to minimise and mitigate the risks to the organisation's information that accrue due to the misbehaviour of current employees.

2.1.3 Threats to Information Security

A threat to information can be defined as any illegal act conducted with the purpose of corrupting or stealing an organisation's data or disrupting the normal operation of the organisation. The threats lead to exposure of the organisation's data or network. There are various sources that can compromise the security of information in organisations (Snitsarenko *et al.*, 2020). Regardless of the type of threat, all the threats are risky to the organisation and must be mitigated. According to Snitsarenko *et al*. (2020), some of the common types of information security threats are:

a) Insider threats: these types of threats occur where a person(s) working in the organisation who has authorised access to the information performs an act, whether intentional or accidentally, that compromises the data or the system.
b) Viruses and worms: these are malware programs which are often send by hackers to destroy an organisation's data and systems. These programs usually replicate themselves throughout the network or in other programs without the knowledge of the system administrator or user.
c) Botnets: botnet threats usually aim at manipulating vulnerable devices within the system by triggering activities that will consume much of the resources and eventually lead to denial of service. These activities normally run in the background, which makes them difficult to notice. The botnets are usually controlled remotely by hackers.

d) Drive-by download attacks: these are downloads that occur automatically via a browser without permission from the user of the system. Hackers use these attacks to install Trojans in an organisation's computers.

e) Phishing attacks: phishing attacks are threats to security information which override the set security measures to access confidential information such as login credentials and credit card numbers. Hackers use fake information that looks legitimate and causes users to perform certain actions.

f) Distributed denial of service (DDOS): this threat occurs when a number of compromised machines attack a single system, making it stop functioning. The attackers end multiple connection requests and messages to the target, which causes the target to crash.

g) Ransomware: in this type of attack, the target machine is locked through remote encryption, which prevents the legitimate users from accessing the information stored in the system. This forces them to pay a ransom to the hacker before they can use the system again.

h) Exploit kits: these are used by system attackers to distribute malicious programs which exploit vulnerabilities in an organisation's systems. The malicious programs will be used to fetch sensitive information from the organisation or create botnets.

i) Maladvertising: this is a technique used by attackers to compromise legal advertisement networks and websites with malicious code. When a user clicks on a genuine advert, they are redirected to a malicious website or program which is later installed in their machine automatically.

The risks associated with whichever kind of threat can highly compromise the operations of an organisation (Snitsarenko *et al*., 2020). Therefore, measures need to be set in any

organisation that will counter the impact of the attacks as soon as one happens. The most important measures should be to prevent the attacks from happening. This thesis addresses information security countermeasures and users' addictive behaviours that can result in security breaches and how the behaviours can be managed.

2.2 Information Security Behaviour

This section of the thesis examines information security behaviour, as it is considered to be an information stream of this research study. It is mainly focused on the human dimensions of information security. Abbasi, Sarker and Chiang (2016) mentioned that information security behaviour not only includes behaviour that threatens information security but also positive as well as desired security practices. It is defined as compliance of the users with the security policies of the organisation. Gerber *et al.* (2016) classified a taxonomy of six various types of behaviour using the technical expertise as criteria. The taxonomy of end user information security behaviour is as follows:

Intentional destruction: Humphries (2017) mentioned this type of behaviour requires technical expertise with stronger intention to harm the IT as well as technical resources of the organisation. For example, the employee can break into the employer's protected files to steal information relating to trade secrets.

Detrimental misuse: according to Layton (2016), this behaviour requires the minimal usage of technical expertise while it includes an intention to harm through harassment, breaking of rules, as well as annoyance. For example, by means of using company emails for SPAM messages to market a side business.

Dangerous tinkering: this behaviour does require technical expertise, while it is not based on an intention to harm the IT as well as the resources of the organisation. Sheeran and Rivis (2017) provided an example of this behaviour as the employee can configure a wireless gateway that can allow wireless access to the organisation's network like passwords.

Naïve mistakes: Ab Rahman and Choo (2015) argued that this behaviour is better as it requires minimal technical expertise and there is no intention to harm the organisation's resources. For example, choosing a bad password for keeping the data secret.

Awareness assurance: Malekian *et al*. (2017) mentioned that this behaviour requires a high level of technical expertise, with a higher intention of preserving as well as protecting the organisation's IT resources. For example, it is required to identify a backdoor program through observation of the PC.

Basic hygiene: according to Soomro *et al*. (2016), this behaviour requires no such technical expertise, while it includes intention to protect the resources of the business organisation. For example, a trained as well as aware worker can resist social engineering request to reveal their password to a caller demanding to share the password.

Technology is required to secure the information while humans are responsible for designing, implementing and operating the technological tools. Insiders are considered as the weakest link in the security of data and information due to intentional and unintentional errors. The five major human errors in information security that could affect the security and cause security breaches are as follows: the first error is involved with failure while changing passwords. The second error involves the incorrect use of procedures while writing down the password (Safa *et al*., 2016). The third error is the number of errors which are caused by some

extraneous acts, and the fourth is caused due to sequential acts. The final one is time errors, which are caused by people failing to complete a task in the scheduled time. Public organisations employ information security policies to protect their digital assets in addition to intellectual rights to prevent the theft of information (Gritzalis *et al.,* 2014). Apart from this, information security principles are also used to mitigate the human errors to prevent the associated risks. The information system is not dependent on the technical issues being prevented, but it is based on human use of the system and the way that they behave.

2.3 Information Security Principles

Safa *et al*. (2016) stated that principles are the core requirement of information security for the safe utilization and flow of information. The storage of that information is a CIA triad, which stands for confidentiality, integrity and availability of the data. Based on the CIA model, there are three principles of information security, which are summarised as follows:

Confidentiality: this means that the information is seen only by those who have authorised access to see it. A bank protects the confidentiality of users' information by users having to enter a PIN which is only known by them to check their balance or conduct other banking activities (Gritzalis *et al.,* 2014). It requires identification before someone can conduct a transaction on the account.

Integrity: this involves ensuring that the information is not changed and removed without the permission of the authorised person. The information is expected to be secure and when anyone changes it, the user should know. For example, banks have put safeguards in place to prevent their employees from changing customers' balances without their knowledge (Taylor and Bean, 2017). Most banks are protecting the integrity of the information by sending an alert

via SMS when any money is withdrawn from an account. It also provides information about where the money is being withdrawn from. Therefore, there is no problem with data integrity.

Availability: this ensures information is available when the authorised user requires it. It is no good to have a bank account when the user is not able to receive information on how much money is in the bank and what transactions have occurred (Safa *et al*., 2016). The banks provide this information in various ways such as online banking, ATM balance enquiry and monthly statement via email.

2.4 Relevant Theories and Methods

Theory is characterised by Peltier (2016) as an arrangement of interrelated factors, definitions and recommendations that exhibit an orderly perspective of wonders by indicating relations among factors, with the motivation being to clarify common beliefs. Another meaning of the hypothesis is provided by (Malekian *et al*., 2017) as a deliberate explanation for the perceptions that identify with a specific part of life. A socio-specialised hypothesis has at its centre that the plan and execution of any authoritative framework must be comprehended and enhanced if both 'social' and 'specialised' perspectives are united and regarded as associated parts of an intricate framework. Authoritative change programmes regularly come up short since they are excessively centred on one part of the framework, generally innovation, and neglect to break down and in addition comprehend the perplexing interdependencies that exist (Safa *et al*., 2016). This is straightforwardly comparable to the plan of an unpredictable design item, for example, a gas turbine motor. Similarly, as any change to this intricate design framework needs to address the thump on impact through whatever is left of the motor, so too does any change inside an authoritative framework.

Human behaviour theories are a set of theories used to describe various kinds of cognitive situations. In order to conduct a study in this research area, there is a requirement that those theories understand the characteristics of human behaviour within the information security context (Montano and Kasprzyk, 2015). The risky cybersecurity behaviours are to be minimised, which is related to the information security countermeasures. There is a group of theories which need to be presented which help to understand the research topic properly. Organisations need to pay more attention to these theories with regard to the human elements along with the organisational context of human interaction (Mishra *et al.*, 2014). The human behaviour theories are the theory of reasoned action (TRA), theory of planned behaviour (TPB), protection motivation theory (PMT), general deterrence theory (GDT) and technology acceptance theory (TAT). Those are chosen as the point of departure for this study as it has explicit focus on the behavioural intention. According to Paul *et al.* (2016), there are five dominant applied behavioural theories which are used in the context of information technology, and which are explained below:

Theory of reasoned action (TRA): this theory was introduced by Fishbein and Ajzen in 1975. Kautonen *et al.* (2015) stated that this theory is used in communication for disclosure as a theory of understanding. This particular theory is aimed at illustrating relationships among attitudes as well as behaviours in human actions. TRA theory is used for predicting individuals' behaviours based on pre-existing attitudes as well as behavioural intentions. An individual's decision to engage in human behaviour is related to the outcomes of their individual

expectations, which will come as a result of performing the behaviour. Montano and Kasprzyk (2015) argued that, using this theory, individuals are motivated to perform actions to minimise the human factors from the context of information security. According to this theory, intention to perform a certain behaviour precedes the definite behaviour. The behavioural intention is a key significant requirement in this theory as this intention is being determined by attitudes to the behaviours along with subjective norms (Leeuw *et al.*, 2015). The theory predicts that the behavioural intent is being created and caused by two of these factors. Fishbein and Ajzen called it the evaluation as well as strength of belief.

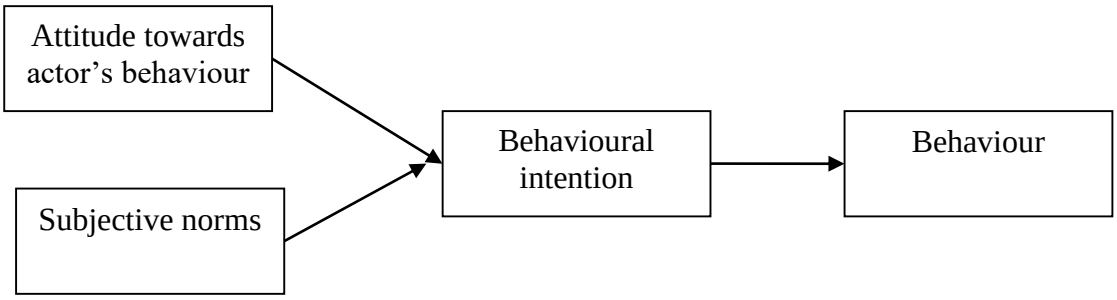


Figure 2.1: Theory of reasoned action

(Source: Montano and Kasprzyk, 2015, p. 97)

Theory of planned behaviour (TPB): this theory was developed by Ajzen in 1991. The behaviour of the employees influences the information security within the organisation. This pertains to user behaviours in accordance with security policies when using or accessing IT resources. Behavioural theories have been used widely in literature related to security compliance to understand the factors that motivate compliance with user security. The TPB is among the most important theories of human behaviour which relates to information security.

Sheeran and Rivis (2017) discussed that this theory is linked with one's beliefs as well as behaviour. This theory was developed from the theory of reasoned action. It is mainly about predicting the intention of an individual to engage in a certain behaviour at a particular time as well as place. Chen and Tung (2014) stated that this theory is dependent on motivation along with the person's ability. The theory consists of four constructs. The first one is attitude, which refers to the thinking or way of feeling that affect a human's behaviour. Mullan *et al.* (2015) illustrated that the second is behavioural intention, referred to as the motivational factor which influences the behaviour where there is a requirement for a stronger intention of behaviour. Third is a subjective norm which is based on approval and disapproval of a behaviour. The fourth construct is perceived behavioural control, which refers to the person's perception of the ease or difficulty of performing the behaviour of interest. This theory mainly explains the intention of individuals to perform the behaviour. Therefore, it postulates that behaviour can be explained by behavioural beliefs, normative beliefs and self-efficacy as antecedents of attitudes, subjective norms and perceived behavioural control, respectively.

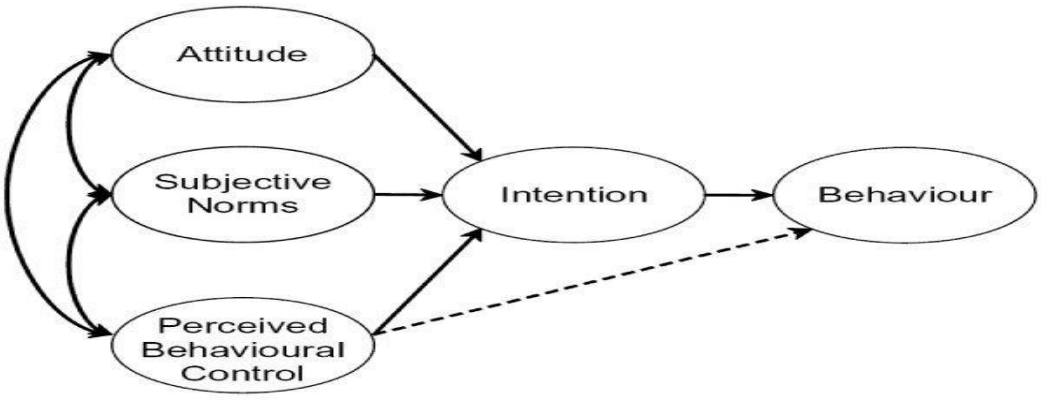


Figure2. 2: Theory of planned behaviour

(Source: Sheeran and Rivis, 2017, p. 61)

Protection motivation theory (PMT): this theory is most important as it proposes that people can protect themselves based on certain factors such as perceived severity of the threatening events, perceived probability of occurrence, efficacy of recommended preventive behaviour as well as perceived self-efficacy. The theory was developed by Rogers in 1986 (Rogers, 1975). This model explains why people engage in risky practices and provides suggestions to change human behaviour. The first prevention step is to take measures to mitigate the risks and the second is prevention from entering into worse conditions. Tsai *et al.* (2016) explained that this theory is concerned with how individuals are processing the threats along with selecting the responses to cope with the threats. Crossler *et al.* (2014) concluded that this particular theory is used as a framework to understand the use of protective measures in information security.

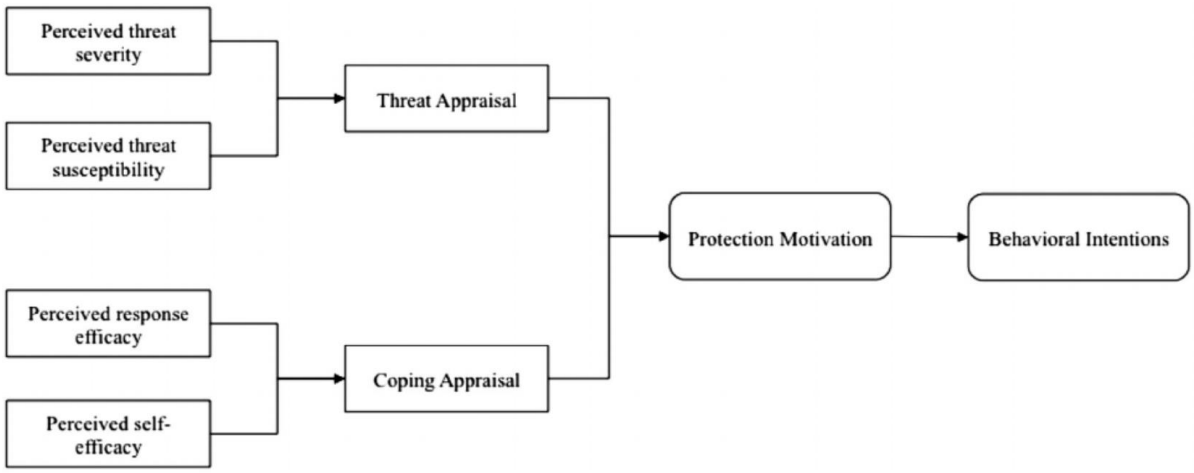


Figure 2.3: Protection motivation theory

(Source: Tsai et al., 2016, p. 141)

General deterrence theory (GDT): this is a legal theory which is sending messages to the general public about the risks which arise from information security risks due to human

factors. Cheng *et al.* (2014) stated that this theory posits that individuals should be dissuaded from commitment of antisocial actions through the use of proper countermeasures. This theory used countermeasures to eliminate the threats and mitigate them. Useful countermeasures include education, training, backups and tools to mitigate the risks. Tittle (2018) argued that the theory is used to prevent threats in the general population. This theory states that the perceived severity and certainty of the sanctions along with the punishment influence people's decisions regarding engagement in crime by balancing the costs and benefits of doing so. Martins *et al.* (2014) stated that information security is focused on the countermeasures of security and preventive strategies which impact the employees' intention to misuse and misbehave.

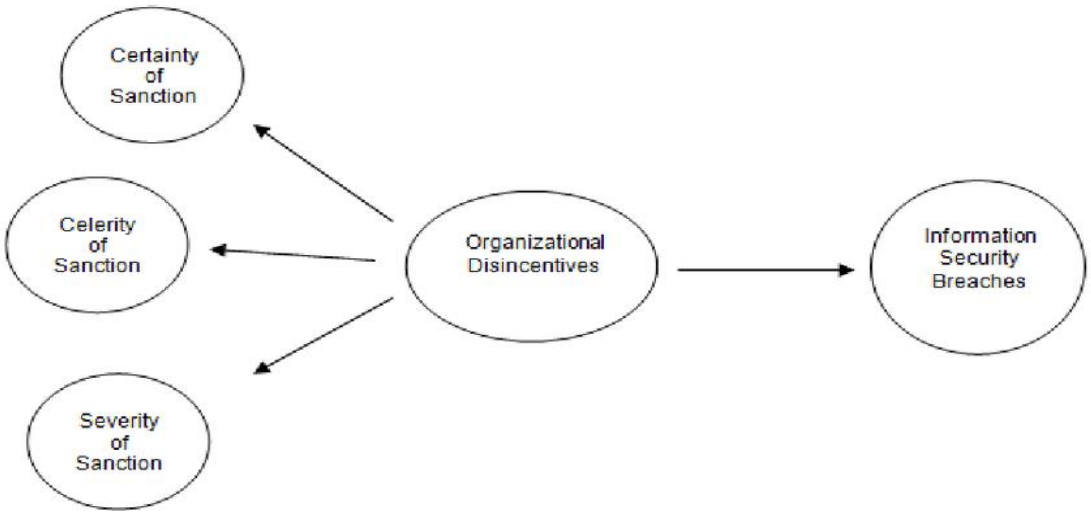


Figure 2.4: General deterrence theory

(Source: Cheng *et al.*, 2014, p. 224)

Technology acceptance theory (TAT): this theory was introduced by Fred Davis in 1986. Mishra *et al.* (2014) explained that it is an information theory which models how users come to accept as well as use the technology. Venkatesh *et al.* (2016) suggested that, when users are presented with new technology, then there are various factors which influence their decisions

about how as well as when to use it. The aim of this theory is to study how the individual's perceptions affect their intentions to use information technology in a useful way. Williams *et al.* (2015) stated that this theory is an adaption of the theory of reasoned action in the field of information security. It uses perceived usefulness and perceived ease of use to determine the intention of individuals to use the system for serving the mediator of actual use of the system. It is the degree to which the person believes that use of the system would raise the performance of the human behaviour (Peltier, 2016). Therefore, it explains the intentions of users to use the information system along with the ability and productivity to use it.

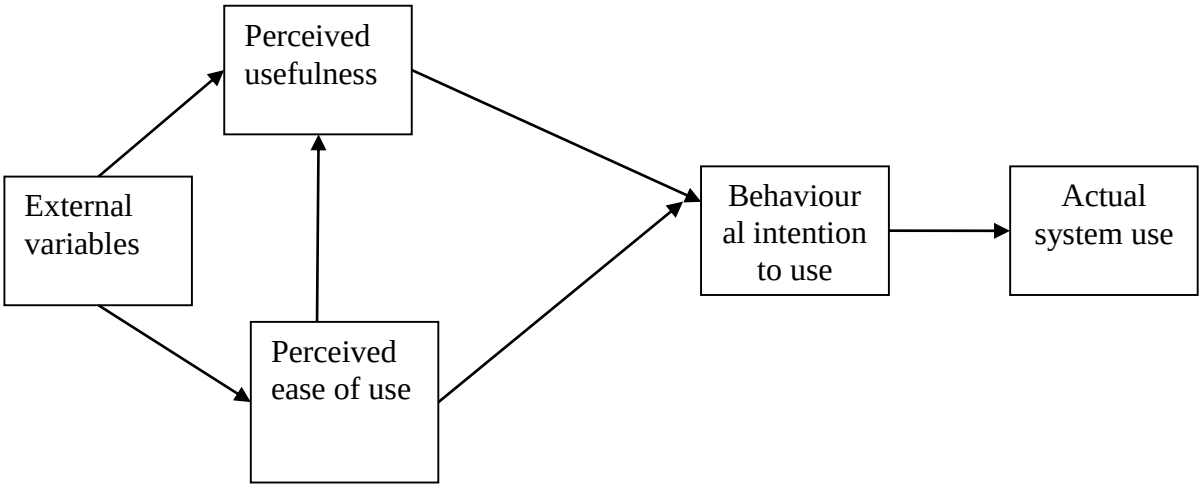


Figure 2. 5: Technology acceptance theory

(Source: Williams *et al.*, 2015 p. 447)

The theory of reasoned action is a broad model so it does not identify the beliefs that are effective for a specific behaviour (Davis *et al*., 1989). Thus, scholars using this theory first need to find out the beliefs that are salient for individuals regarding the investigated behaviour. Additionally, the theory of reasoned action, instead of dealing with the outcome of behaviour,

deals with the prediction (Foxall, 1997). As the theory determines behaviour by behavioural intentions, there is a limitation on the predictability of the model to circumstances in which behaviour and intention are correlated.

The largest correlates between behaviour and intention exist where the time-based gap between their expressions is minimal. To take the extreme case of overcoming this, however, measuring intention and behaviour simultaneously fails to ensure a true test of the model's power to predict the future. At best, it corroborates the attitudinal basis of current behaviour. Davies, Foxall, and Pallister (2002) suggested that, in order to test TRA, actual behaviour should be measured objectively, and unobtrusively, without signalling in any way its connection to the prior intention measurement phase. A further requirement of the TRA is that behaviour must be under volitional control. Hence, the TRA is ill equipped to predict situations in which individuals have low levels of volitional control (Ajzen, 1991).

The TPB is a theory that linked with one's beliefs as well as behaviour. This theory was developed from the theory of reasoned action, nevertheless, this theory has problematic on several grounds. First, like the TRA, the TPB assumes proximity between intention and behaviour; thus, the precise situational correspondence is still vital for accurate prediction (Foxall, 1997). As Eagly and Chaiken (1993) pointed out, the assumption of a causal link between PBC and intention presumes that people decide to engage in behaviour because they feel they can achieve it. Second, the operationalization of the theory is troubled by the problem of measuring PBC directly, as opposed to recording control beliefs (Davies *et al*., 2002; Manstead and Parker, 1995). Third, the theory introduces only one new variable, when there is continuing evidence that other factors add predictive power over and above the measures formally incorporated in the TPB (Davies *et al*., 2002). For example, Manstead and Parker

argued that personal norms and affective evaluation of behaviour may account for variance in behavioural intentions beyond that accounted for by the TPB Davies *et al*. (2002). Ajzen (1991) himself described the model as open to further expansion.

Weak support for discriminant validity was a result of the fact that all constructs of the TAM are self-reported and, when correlated with self-reported use, common-method variance becomes an important factor. Straub *et al*. (1995: p. 1336) argued that "research that has relied on subjective measures for both independent variables . . . and dependent variables, such as system use . . . may not be uncovering true, significant effect, but mere artefacts". Another key limitation of the TAM is that, while it provides a valuable insight into users' acceptance and use of technology, it focuses only on the determinants of intention (i.e., PU and PEU) and does not tell us how such perceptions are formed or how they can be manipulated to foster users' acceptance and increased use (Mathieson, 1991).

Table 2. 1: Theories overview
(Source: Author)

Theory	Founder	Concept	Key components	Overview
BMT	Rogers in 1975	People can protect themselves based on some factors such as "perceived severity of the threatening events, perceived probability of occurrence, efficacy of recommended preventive behaviour as well as perceived self-efficacy".	Employees' attitude towards information security is shaped by the evaluation of two cognitive-mediated appraisals: threat appraisal and coping appraisal.	This model explains why people engage in risky practices and provides suggestions to change the human behaviour. The first prevention step is to take measures to mitigate the risks and the second is prevention from entering into worse conditions.
TPB	Ajzen in 1991	The intention of employees to fulfil with ISPs passed on	Behaviour which can be explained by behavioural	This theory was developed from the theory of reasoned

		the general evaluation of and normative beliefs of employees towards compliance-related behaviour.	beliefs, normative beliefs and self-efficacy as antecedents of attitudes, subjective norms and perceived behavioural control, respectively.	action. It is mainly predicting the intention of individuals to engage in behaviour at a particular time and place. This theory mainly explains the intention of individuals to perform the behaviour.
TRA	Fishbien and Ajzen in 1975	This particular theory aims to illustrate relationships among attitudes as well as behaviours in human actions.	An employee's attitude towards information security is shaped by the evaluation of two cognitive-mediated appraisals: threat appraisal and coping appraisal.	The behavioural intention is a key significant requirement in this theory as this intention is determined by attitudes to the behaviours along with subjective norms.
TAM	Fred Davis in 1986	Discussed that it is an information theory which models how users come to accept as well as use technology.	The technology acceptance model determines the employees' intention to comply with ISP, which is influenced by the perceived usefulness and perceived ease-of-use of information security.	That this theory is an adaption of the theory of reasoned action in the field of information security.
GDT	Cesare Beccaria and Jeremy Bentham in the 18th century	Adapted from criminal justice research, general deterrence theory is based on rational decision making.	General deterrence theory states that perceived severity of sanctions and perceived certainty of sanctions or punishment influence employees'	This theory uses countermeasures to eliminate the threats and mitigate them. The perceived severity and certainty of the sanctions along with punishment influence people's decisions regarding engagement in crime by balancing the

			decision regarding ISP compliance by balancing the costs and benefits.	costs and benefits of doing so.

2.5 Threats to Information Security: Human Behaviour is a Constant Risk

2.5.1 Threats to Information Security

Among the evolving threats to information security, public organisations have to account for one constant, human error. According to Soomro *et al*. (2016), the authors arranged the participants into a few groups to facilitate discussion on the threats to information security. Throughout the threats to information security along with processes as well as tools, there is area which remains constant along with consistent risks – human error. There are three information security processes which are able to mitigate human errors:

Classification and restriction of access to data: there are some types of data which are more sensitive than others. This is a way to protect enterprises' data. Financial data are sensitive as they provide identifiable information about the clients. After classification of the data, requirements to access the sensitive data need to be determined (Soska and Christin, 2015). Criteria need to be defined when data need to be segregated into various classifications. There is personally identifiable client information. There is an amount of data which is not fully protected. Restrictions in accessing the data need to define data roles as well as permissions (Siponen *et al*., 2014). As it is expensive and difficult for organisations to protect their data on a similar level, data classification is a tool to ensure the right level of security matches the right classification of data. Usually capacities, for example, validation and session administration, are wrongly executed, giving an opportunity for aggressors to trade-off conditions, for example,

passwords and logins, keys or session tokens, or accepting another enrolled individual's character.

Restriction access to sensitive data: processes as well as tools need to be implemented to login and access data. This implies that there is a need to get rid of generic user accounts such as admin accounts. In order to regular access reviews, there should be a review what data are required to access to fulfil job requirements (Teh *et al*., 2015). A review of access logs is required to refine the access rules. In some information systems, there is a way around generic admin accounts, which defeats the goal to know who can access the data. The key information management system is that in which the admin can check the use of generic admin accounts. The management wants to know who can access the sensitive data. Another way of restricting access to sensitive data is to create an owner for the data, using two ways of authentication with the data owner. This will ensure only acceptable people access these data.

Review ways of circulating sensitive client and financial data: ways in which sensitive client data as well as financial data are circulated need to be reviewed. When someone asks question about a client account, an email is sent which provides details of the account which should never be sent via email Kampas *et al.* (2016). It is helpful to spend time with the client services team as well as the accounts receivable team to observe how exchange of information occurs. It is also an issue where implementation of a secure approach is done for exchange of information. Using password data protection for shared data is a common method that should be implemented to protect the client’s shared data.

2.5.2 Human Behaviour as an Aspect of Information Security

Information system knowledge

Antecedents of information security on an individual level include some factors which originate from the users of information security. Siponen *et al*. (2014) and Tam and Jones (2018) discussed that information security knowledge like IT, self-efficiency in using computers, knowing about advanced technology and others plays a key significant role information security research. Mishra *et al*. (2014) found that personal innovativeness with computer self-efficacy has positive correlations with the level of respondents' knowledge, which is in line with protection motivation theory. Safa *et al.* (2015) argued that the employee's and human's understanding about security threats helps them to take proper countermeasures against security issues. Self-efficiency with a computer is defined as an individual's judgement about using a computer system in various situations. On the other hand, personal innovativeness is defined as an individual's willingness to try innovative information technology. Almost 97% of IT security practitioners agreed that human behaviour is considered to be the largest security threat by organisations (Malekian *et al.*, 2017). Therefore, humans need to have the knowledge required to understand the information security threats and incidents.

Due to increases in internal as well as external cyber threats, human behaviour as well as technological uncertainty remain prominent barriers to public organisations' confidence. The greatest vulnerability in information security is human behaviour. The percentage increased to 88% in 2013 as well as 93% in 2014 (Safa *et al*., 2016). The entire program is designed to take account of human behaviour, and then the organisation provides training to show the individuals how to act with regard to the policies in place to guide those (Kim *et al*., 2014). Unless the staff are trained to identify scams as well as avoid risks, then there is no elimination of information

security issues. Education awareness is not just for the internal staffs; it rests on the third parties as well (Malekian *et al*., 2017). In order to reduce vulnerabilities, 24% of companies responding to a survey stated that they used fear, 41% included best practices and 83% are encouraging their employees through policies, awareness and training to become part of cybersecurity solutions (Soomro *et al.*, 2016).

Negative experience with information security threats

Hajli and Lin (2016) mentioned that, if individuals have a negative experience related to understanding information security incidents, then they will gain awareness of the security risks concerning information security. Soomro *et al*. (2016) argued that people's awareness of information security can stem from their life experiences, such as their experience of virus attack on the computer system.

Individual education

Vance *et al.* (2014) found that students from technical universities tend to be aware of the issues related to information security. Therefore, other students should be required to be more focused on understanding information security incidents. This indicates that students in some subjects require specific IS-related education.

User's Perception of security

In their research study on users' security awareness regarding information security threats, Hsu *et al.* (2015) argued that the perception of information in information security countermeasures is significantly influencing the awareness of risks as well as the issues. According to Abbasi, Sarker and Chiang (2016), security perception covers the user's sense of isolation about the computer system. The users have high expectations of the service provider as well as IT expertise to keep their system protected. Security awareness helps to keep confidential data in a protected place on the computer devices.

2.6 How Human Behaviour can be influenced by Standards, Guidelines and COBIT

The information security culture has been developed in public organisations due to certain actions by the IT department. An organisation's management implements information security components like policies as well as technical security measures with which the employees interact. The employees develop human behaviours like ignore reporting of security incidents and sharing of passwords, which lead to threats to the security of information assets (Heckmann *et al.*, 2015). The organisation manages its information security by implementing information security standards and guidelines. The standards are used by the organisation to make sure that it can manage information security from the holistic perspective, therefore minimising the risks and the acceptance level of the information security culture (Pearlson *et al*., 2016).

According to Peltier (2016), information security guidelines and policies are very important for any organisation. The IT department should come up with clear guidelines that

define what employees and the administration should do in order to secure the organisation's information system against any form of attack. Once the guidelines have been drafted, the users of the system should be educated on what the various guidelines mean (Peltier, 2016). The common guidelines that must be drafted include: not sharing computer passwords, employees should never leave their workstation before shutting down the computer, and the necessary steps that employees should take in case they suspect that a security breach has occurred. These guidelines will enable the employees to assist in enforcing information security countermeasures in the organisation (Peltier, 2016).

The IT department has to ensure that the organisation's information system conforms to the established international standards. The standards include use of genuine software, as well as all the security standards described in ISO 27001 and 27002. Standardised systems are less prone to security attacks as compared to nonstandard systems (Peltier, 2016).

2.6.1 COBIT

COBIT stands for Control Objectives for Information and Related Technology. It is a structure created by the ISACA (Information Systems Audit and Control Association) for IT administration and administration (Sheeran and Rivis, 2017). The COBIT standard helps IT professionals to fulfil IT governance as well as management responsibilities particularly in the areas of security, control and risk within the business. This standard is focused on human factors to protect the public organisation from malicious insider (Pearlson *et al.*, 2016). Public organisation development is required by making changes to the actual behaviour of the workforce. Basic training is required for humans to integrate security awareness in addition to understanding the organisational culture. Insiders change the human behaviour to protect access

to the information and confidential data (Abbasi, Sarker and Chiang, 2016). This standard requires increasing staff awareness and developing a security value culture among them.

According to Soomro *et al*. (2016), the organisation is dependent on the information security resources. COBIT is considered as an IT governance framework used by IT experts to bridge the gap between control needs, technical challenges and business issues. Taylor and Bean (2017) mentioned that the main focus of this information security standard is to develop clear policies as well as security practices and for public as well as professional organisations to control their IT. As issues are raised in information security management in relation to COBIT, therefore confidentiality and availability along with integrity are areas covered by this standard. The significant option to meet the information security management in the COBIT infrastructure is the ISO/IEC 27001 standard (Abbasi, Sarker and Chiang, 2016). This framework provides auditors as well as IT users with accepted measures and best practices to maximise the benefits of using information technology in business organisations. It is used to develop IT governance as well as control within organisations.

Kim *et al*. (2014) mentioned that COBIT's mission is to develop and promote up-to-date information with an international set of the accepted information security objectives. Managers and auditors have benefited from the development of COBIT as it helps in understanding IT systems as well as the level of security controls. Organisations are required to protect their assets through developing IT governance models. The COBIT security framework covers security and risks that occur due to usage of IT resources. Effective information security requires an integrated set of security management tools as well as governance procedures to plan and counter security risks. According to Abbasi, Sarker and Chiang (2016), COBIT is supporting the needs of security and addressing part of the business functions. It is devoted to security and

controlled security objectives along with addressing security in a business. Safa *et al*. (2016) discussed that documents on the COBIT security baseline highlighted security control objectives related to information security.

2.7 Human Factors and End User's Behaviour

Among the identified threats relating to information security, human behaviour is considered as a constant risk. The insider threats are become malicious due to human factors. It is necessary to monitor human behaviour outside the threat domain to better inform on the mitigation of threat. Safa *et al*. (2016) stated that technology lowers barriers to malicious insider activities. Stealing files from a USB drive requires a human factor and it occurs due to the behaviour and attitudes of humans towards the information security risks (Siponen *et al*., 2014). Human behaviour has a higher impact on success as well as failure to secure and protect information. According to Gerber *et al.* (2016), human error is stated as the greatest security weakness, followed by the technology. The human factor can be divided into two groups, factors which belong to the management and factors related to end users. The following are the human factors which have implications for the end user's behaviour:

Lack of motivation: Gritzalis *et al.* (2014) believed that humans are motivated to adopt secure behaviours and management are required to identify what motivates employees. Motivation for human behaviour is required when the security risks are shared and the users are involved in decision making to follow the security methods. Layton (2016) believed that employees need to be motivated to adopt secure human behaviours as well as practices, and management need to be able to identify what motivates the staff. According to Sinha (2015), motivation happens when the security issues are shared and the users are involved in making decisions to follow security procedures.

Lack of awareness: this is related to a lack of knowledge about attacks. The humans have no knowledge about how to recognise signs of spyware on their computer or that they need a strong password (Taylor and Bean, 2017). The data are not protected from identification of theft and the humans have no understanding about how to control access to the computer. Gritzalis *et al.* (2014) stated that this is related to lack of knowledge about human attacks. The employees are not aware of how to control others' access to their computer.

The administration of any organisation should therefore invest in educating its employees on various aspects of information security. Uninformed users can expose the system to attacks that might never be recovered, such as exposing sensitive information to competitor organisations. Making the employees aware of information security measures and practices is the first step of ensuring information security (Agarap, 2017).

Improper human behaviour: Siponen *et al*. (2014) explained different types of behaviour which interpreted as the improper behaviour of human. Hsu *et al.* (2015) claimed that documented requirements of expected behaviour regarding information security have a small effect on the behaviour of users. The users are considered as user involving approach to become effective to influence the user's awareness in addition to their behaviour. It is interpreted as the risky behaviour of users and loss of prevention of human behaviour. Vance *et al.* (2014) claimed that documented requirements regarding expected information security behaviours have few effects on user behaviour.

Inadequate use of technology: technology cannot succeed in solving the risks related to information security without the cooperation of humans along with the effective use of the technology (Abbasi, Sarker and Chiang, 2016). Examples of technology risks are unauthorised

re-configuration of the information system, access to the passwords, retrieval of improper information and others. Kautonen *et al*. (2015) believe that IT security basics such as threats and risks allow individuals to adapt to constant changes and allow the prediction of expected behaviour.

Belief: Abbasi, Sarker and Chiang (2016) conducted a qualitative study about users' views on information security as well as their beliefs. The users believed that installation of anti-virus software is not crucial to information security, and they were ready to click on links when they received an email from an unknown person.

Computer security risks: certain factors are computer security risk factors, such as error and omission, denial of services, unauthorised access, and miss identification of theft, malware as well as unauthorised copying of data (Sheeran and Rivis, 2017).

In recent decades, information security as well as human behaviour research has focused on the behavioural models and theories. In most of the theories, intentions rather than actual human behaviours are assessed due to the difficulty of observing the security behaviours (Pearlson *et al*., 2016). The theory of reasoned action is based on two notions: people are reasonable, and make use of information when deciding among human behaviours; and they consider the implications of the human behaviours. Errors from the human side are constant among the threats to information security. Safa *et al*. (2016) found that most of their respondents agreed with the statement that the biggest vulnerability is human behaviour. This theory was designed to account for human behaviour, then the organisation provide training for the individuals on how to act as well as put in place information security policies to guide them.

The organisation needs to be concerned about the human behaviour tools, which requires the human factors to be addressed.

2.8 Human Behaviour Risks Related to Information Security

As public organisations are made up of people, therefore human-related threats are pervasive at these levels. Siponen *et al*. (2014) stated that a degree of human-related risk is inevitable; therefore, the proper way to mitigate them is to structure public organisations in such a way that no single person can cause critical damage. The following are the information security risks which have been identified in most organisations:

Lack of management support: Soska and Christin (2015) stated that the values which create a stronger security environment come from the management and organisational culture. Investment in IT security reduces the cost of organisational finances while maintain organisations' reputation (Safa *et al*., 2016). It is also termed as an insider threat, as the management members are not interested in support and communication throughout the organisation.

Provide password to any unauthorised person: any unauthorised person can access information when someone provides their password details to them (Ab Rahman and Choo, 2015). The person can hack the information across the internet by stealing the account or database passwords. This causes loss of data in addition to information from the database system. Personal as well as financial information is stored on the computer, and then at that instant it is possible that someone can hack or steal it from the computer through the use of certain hacking software (Siponen *et al*., 2014).

Unaware of information security policies: any careless and uninformed staff can impact the security of a company and cause a serious security breach. Sometimes, employees are not aware of whom they should and should not provide confidential data and information to (Kim *et al*., 2014). Staff are not aware of the information security policies; therefore, they share information with others.

2.9 Public Organisation Information Security Culture

Public organisations require a strong security culture in their mode of operation. Malekian *et al*. (2017) stated that a sustainable security culture is required to secure the information in addition to the data. When the security culture is sustainable, then it transforms security from an event to part of the company's lifecycle, which generates security. The information security is not relying on the technology (Siponen *et al*., 2014). The culture encourages the employees to comply with the informational policies related to collecting in addition to managing the information, which will improve the information security.

2.9.1 Organisational Culture

Pearlson *et al*. (2016) stated that organisational culture includes the organisation's expectations and experiences as well as the values which hold it together, and its interactions with the outside world along with its future expectations. The organisational culture affects its productivity and performance along with guidelines concerning customer care. Organisational culture is different for each organisation and one of the critical aspects is the ability to respond to change.

2.9.2 Information Security Culture

Siponen *et al*. (2014) discussed that information security culture is based on how things are to be done within the organisation with regard to information security, with the aim being to protect the information assets along with influencing employees' security behaviour. Information security culture is a part of the organisational culture as the security of information is an organisational function. In order to gain a secure environment for the information assets, the practices of information security have become a part of corporate culture within the organisation (Kim *et al*., 2014). The culture guides activities within the organisation and the employees by placing constraints on the organisational activities and employee behaviour. The culture influences the human behaviour; therefore, there is a requirement to establish information security behaviour of the organisational employees. Malekian *et al*. (2017) defined information security culture as the perceptions, attitudes and assumptions of employees within the organisation based on information security. The culture develops as a result of employees' interactions with the information security controls.

Abbasi, Sarker and Chiang (2016) suggested that the information security culture is considered as accepted behaviour as well as actions by the employees. The culture involves identifying the security-related issues and beliefs along with values of the group that shape the security-related behaviours. Safa *et al*. (2016) defined the information security culture as the totality of the human attributes like behaviours and attitudes as well as the beliefs held by the organisation. This could impact the security of the organisation, which may or may not be explicitly linked to the impact (Siponen *et al*., 2014). The procedures which the employees are using in their daily work represent the weakest link in the chain of information security. It is

necessary to develop as well as improve the information security culture through a structured model to address the human behaviour.

2.9.3 Cultural Change

Cultural change is a term used in policy making to emphasise the influence of the cultural capital on individuals along with community behaviour. Vance *et al*. (2014) stated that cultural changes places a stress on social along with cultural capital which lead to determining the decision make to interact with the people (Pearlson *et al*., 2016). The cultural capital influences include the role of management.

2.9.4 Cultural Impact on Human Behaviour

Comparative research from other research studies shows that human social behaviour varies across various domains such as cooperation, culture, trust and morality. In order to better tackle human behaviour, work on cultural evolution is required. San Martin *et al.* (2018) stated that people are surprised when they witness how others behave when they are travelling across various cultures. Apart from regular observations, the cultural differences in behaviour are documented by means of psychological research. As an example, comparing Chinese and Canadian toddlers, Chinese toddlers spend more time in direct contact with their mothers and take more time to approach and play with strangers (Fuentes, 2017). This is an example of cultural differences in human behaviour in early childhood time. Taylor and Bean (2017) argued that there are theoretical accounts of various cultural differences in human behaviour, which can emphasise cognitive as well as affective processes. Perreault and Mathew (2016) proposed that Westerners hold a self-governing self-concept which is not affected by means of social contexts.

Varnum and Grossmann (2016) discussed that human behaviour is affected by genetic inheritance as well as by means of experience. In this way, people can develop and be shaped by their social experiences as well as situations in the context of inherited genomic. Each person is born into cultural as well as social settings; therefore, they are required to build social connections with community and family, close ones. Characteristics of the social settings among children are affected by how they think and behave. Each culture contains dissimilar webs of patterns plus meanings, ways to earn a living, social roles, and civilizations besides beliefs. Abbasi, Sarker and Chiang (2016) mentioned that the culture is induced by behavioural patterns, like patterns of speech, body language and type of humour. In a large society, there are various groups from different cultures linked by a region and social classes. Mishra *et al*. (2014) argued that, when a single culture is dominant in a large region, then its social value is considered as accurate as well as promoted. In each culture, there are fair as well as unfair social differences and wanted or unwanted believes. The distinctions among class are due to wealth, occupation and education. According to Siponen *et al*. (2014), class affects what opportunities and threats people experience; therefore, it affects people's paths and their living standards.

2.10 Significance of IS across Public Organisations

There are diverse categories of security challenges faced by public organisations such as the disclosure of information and unauthorised access to sensitive documents (Kautonen *et al*., 2015). Each of these security challenges can have a direct adverse impact on an organisation's business reputation and on its business sales. Hence, the reasons behind the occurrence of the security challenges have to be addressed in the first place. The three basic principles of IS are availability, integrity and confidentiality, which have to be followed in every public organisation as the progress of these organisations depends hugely on their ability to protect the information

from security challenges (Ab Rahman and Choo, 2015). Safe operations of the public organisations can be maintained if information is protected from the security challenges. IS can be very beneficial for the protection of the business assets of public organisations such as their intellectual property. IS challenges not only come from outside the business environment but also from inside the work environments. The IS threats coming from inside the organisation are more dangerous as compared with the challenges coming from social engineers. All the financial records and the business data can be secured with the help of IS.

IS behaviour such as intentional destruction allows the workforce to destroy the physical as well as the intellectual property of the business, whereas detrimental destruction allows the workforce to send bullying emails to their colleagues (Siponen *et al*., 2014). A 'dangerous thinker' makes the most out of their IT knowledge to destroy the organisation's resources. A naïve mistake is a mistake by an employee who does not have any intention to harm the organisation's resources. Awareness assurance is the most desired IS behaviour from every employee in a public organisation as it helps them to protect the organisation's IT resources, and its presented as the following table:

Table2. 2: Types of behaviours
(Source: Author)

	Types of Behaviours	Action
1	Intentional destruction	Destroy the physical as well as the intellectual properties of the business.
2	Detrimental destruction	Sending bullying emails to colleagues.
3	Dangerous thinker	Makes the most out of their IT knowledge to destroy the resources of the organisation.

4	Naïve mistake	Mistake by an employee who does not have any intention to harm the resources of the organisation.
5	Aware assurance	Is the most desired IS behaviour from every employee in a public organisation as it helps them to protect the IT resources of the organisation.

IS has three goals: prevention of loss of integrity, loss of availability and loss of confidentiality. Most of the IT-related risks in a public organisation can be addressed using IS; at the same time, IS is also very significant for commercial establishments to maintain a long-term relationship with consumers. IS can play a leading role to address the accountability issues of an organisation as well.

Workforces of public organisations are usually the weakest link regarding data security as both intentional and unintentional mistakes are committed by them (Vance *et al.,* 2014). There are numerous common mistakes which can be a source of concern regarding the protection of information, such as setting up weak passwords and sharing them with unauthorised stakeholders of the business. An incorrect procedure when setting the password is the other common mistake committed by most of the workforces of public organisations. The errors which occur while setting a new password or recovering an old password are also one of the major mistakes which are committed by the workforces of public organisations. Most public organisations have their own set of guidelines which can help them to address the security challenges (Gritzalis *et al.,* 2014). These guidelines are very beneficial to protect the digital assets of the business as well as the intellectual rights. Apart from the guidelines, there are IS principles that are also very beneficial to protect the assets of public organisations.

Hence, it can be stated that IS can be very significant across public organisations as it can help them to protect their confidential information. It can be understood that information is considered as the biggest asset in most commercial and public organisations and IS is very significant to protect this organisational asset from diverse categories of threats coming from both the workforce and from outside the business setting.

2.10.1 Factors Influencing IS

Employee behaviour is considered as a constant risk in most of the public organisations around the world as employees have access to both personal data and commercial data (Kim *et al*., 2014). The IS chain is very significant to protect the integrity of all the sensitive data which are circulated across numerous business environments. There are diverse categories of factors which have to be considered in the first place by the IS strategist of a public organisation, such as the lack of motivation and security awareness. Motivation is one of the driving factors which have a major influence on the IS countermeasures. Some of the employees of public organisations lack motivation and this has a direct impact on the decision-making procedures. Lack of motivation is one of the most significant factors which affect the IS practices of a public organisation. Lack of awareness about the IS challenges can also be considered as one of the key factors of IS practices. Employees working with sensitive information must be aware of security challenges such as spyware and malware, and each of them must understand the procedure to protect the integrity of the information. Lack of awareness can also lead to issues such as identity theft in public organisations. Improper human behaviour is one of the other factors which usually has an impact on the IS practices of public organisations (Taylor and Bean, 2017). Most of the security challenges associated with IS are due to the inappropriate behaviour of the employees. There are numerous practices which come from the employees which can

lead to IS challenges, such as clicking on improper or unidentified links. At the same time, sharing of data from devices which contain essential information is one of the other prime vulnerabilities coming from the employees. Inappropriate deployment of the IT resources is also considered as one of the major reasons behind the security challenges in most public organisations (Gerber *et al.,* 2016). Security vulnerabilities of non-computing devices is the other major human factor related to the IS practices.

Inadequate use of technologies which are deployed by the workforces of public organisations is one of the most significant technological factors which can have a huge impact on the IS practices of these organisations (Malekian *et al*., 2017). There are diverse categories of information systems which are deployed across public operations for optimizing business operations; however, security concerns arise whenever an unauthorised person, mostly an external service provider, gets permission to re-configure the function. Retrieving of information from shared technologies such as cloud computing can also lead to IS challenges. At the same time, users' belief in dedicated computer systems can also lead to IS challenges. Apart from these factors, computer security risks such as malware and DoS are the other factors which can influence the IS practices of any public organisation.

2.10.2 Impact of the Factors Affecting IS

Lack of both intrinsic and extrinsic motivation on the part of the employees of public organisations can have a huge impact on both their intention and the behaviour (Safa *et al*., 2016). The intentions of the employees of any commercial establishment can be affected due to a lack of motivation, and the establishment's security vulnerabilities can be increased due to employees' wrong intentions. The users' addictive behaviour can also be affected due to lack of motivation, organisational skills, analytical skills and cognitive abilities.

Lack of awareness can have a big influence on the IS countermeasures of any public organisation as the employees must be qualified enough to understand the significance of IS countermeasures (Pearlson *et al*., 2016). At the same time, the workplace culture can also be affected due to lack of awareness. Lack of awareness can have the biggest impact among all the other impacts in terms of security breaches, and usually results in loss of essential data. The entire database of a commercial establishment can be affected due to lack of awareness. At the same time, it can also be said that the cost to organisational finances is also increased due to lack of awareness.

Improper human behaviour can have a direct influence on the organisational culture of public organisations (Abbasi, Sarker and Chiang, 2016), and this can affect the productivity of the human resources. The expectation from the workforce is also greatly affected due to the improper behaviour of the human resources. Improper human behaviour can also have an adverse impact on the consumers of a public organisation (Siponen *et al*., 2014). Fraudulent activity in and across the business unit is one of the other constraints associated with this factor.

Inadequate use of technology can have a huge impact on IS countermeasures as well as on the behaviour of the employees (Cheng *et al*., 2014). Most of the organisational activities of public organisations can be affected due to this factor. The human computer interaction procedure can also be influenced due to the inadequate use of emerging technologies such as data encryption which can help to minimise the data security concerns of public organisations.

Computer security risks which are created with the help of malware can have a direct influence on both the behavioural practices and on the growth of the business (Taylor *et al.*, 2015). Loss of business reputation is one of the biggest effects of computer security risks.

Security risks can also have a cultural influence on the behaviour of the employees working in the UAE's public organisations.

2.10.3 Additional Factors

Apart from these factors, there are other factors which have an effect on the IS of a public organisation such as negative experience with the IS threats (Safa *et al*., 2016). Awareness of employees might be influenced as a result of the negative experience. At the same time, it can also be said that individual training can be one of the most significant factors which has an effect on IS incidents (Malekian *et al*., 2017). Employees who understand the causes and the ways to prevent IS challenges can play a key role in addressing IS concerns (Kim *et al*., 2014). IT users' perceptions of the systems in public organisations are also a very significant factor which can help the organisations to deal with the security challenges of IS.

IS standards and guidelines can also be considered as a major factor which can help public organisations to deal with security incidents. The technical security measures are very beneficial to minimise the security risks and maintain an acceptance level of IS culture. Using the guidelines, an appropriate organisational culture can also be created which can help to understand the behaviour and intention of the employees and make the employees understand the business values of business information (Culture Soska and Christin, 2015). Cultural changes required in a public organisation which can help to address the threat coming from inside the organisation can be identified if the IS standards are followed in the organisation in systemised modus. It can be said that maintaining a professional organisational culture has a huge impact on the behaviour and the intention of the employees (Taylor and Bean, 2017). Challenges which occur in public organisations such as inappropriate human behaviour are sometimes affected by genetic inheritance; hence, the cultural and social setting of the

employees can be monitored if an appropriate organisational culture and the necessary countermeasures are maintained across each business unit.

COBIT is defined as the type of framework which can also be very beneficial to maintain the security of the IT systems of public organisations. Threats coming from malicious insiders and human errors can be significantly minimised if this IT governance framework is successfully incorporated in these organisations (Pearlson *et al*., 2016). This framework can also help a public organisation's strategic team to identify the actual behaviour of the workforce. This framework has numerous advantages: it can help the public organisation to maintain a professional organisational culture, which can help the organisation to check the behaviour and the intention of the employees (Vance *et al*., 2014). Maintaining this framework can help the public organisation to protect its online assets; hence, it can be stated that the control needs of the organisation can be fulfilled using this IT governance framework.

Creation and enactment of IS policy is one of the other major factors which might have an influence on the security controls of the IT systems; hence, most of the intellectual property of the business can be secured from IS challenges using this framework (Malekian *et al*., 2017). The IS culture can be very beneficial to protect the information assets both inside and outside the business. A secure environment can be created if the best practices of IS culture are incorporated into the organisational culture (Safa *et al*., 2016). Acceptable employee behaviour can also be identified if an IS culture is maintained in public organisations.

Human factors are the most significant factors which are very closely associated with the IS as the users of the IT systems have the capability to protect or destroy the essential information at the same time (Gerber *et al.,* 2016). Human intention and behaviour have a direct

impact on the protection of information in any public organisation. If the user of an IT system provides a password to unauthorised personnel, this can lead to a cyber-attack (Taylor and Bean, 2017). Cyber-attacks can have an adverse effect on public organisation, as they can encrypt or alter essential business information (Heckmann, Comes and Nickel, 2015). Any of these illegal activities can cause business loss or loss of reputation for any public organisation. Hence, it can be said that users of IT systems in a public organisation must be aware of the IS policies (Sheeran and Rivis, 2017). The policies are very significant in addressing the security threats coming from an uninformed or careless workforce.

2.11 Information Security Policy

2.11.1 What is an Information Security Policy?

Ifinedo (2014) stated that an information security policy is a set of policies issued by an organisation to make sure that the users of information technology comply with the rules and guidelines related to the security of information stored at any point within the network. Each organisation is required to protect its data and control those data which are distributed within as well as without the organisational boundaries. Gerber *et al.* (2016) argued that the policies are used to ensure the networks that storing data are secured into the organisational boundaries and users interpreted with that stored data are awarded and able to keep the data secured into the organisational boundaries. It is a method which defines how the information is being protected and the consequences of violated the rules to maintain access to the information. Siponen *et al*. (2014) discussed that an effective IT security policy is a model for an organisational culture where the rules as well as procedures are driven from the employees' approach to the information. It is such a document for any public organisation that is cultivated from people's perspectives on the tolerance of risks.

The main objectives of an IT security policy are confidentiality and integrity as well as availability of the information used by the organisation's staff. Information security policies are linked to subjective norms and attributes as changes in a policy may affect organisational change, which may result in violation within the organisation (Teh *et al*., 2015). The personal norms, information security standards, benefits, attitudes and values matter with regard to how the employees perceive the information security issues and those related to the information security policies. Privacy is achieved by two approaches: protection of the organisation's operational practices and maintenance along with control of data management procedures throughout the product lifecycle (Crossler *et al.*, 2013). The approaches are used to promote the employees' informational security awareness, which is implemented through an effective educational programme. Training is provided to promote in addition to enhance informational security.

2.11.2 User Behaviour Related to the Information Security Policy

In the field of information security, the human factor is considered as a vulnerability and an unpredictable one. Heckmann, Comes and Nickel (2015) mentioned that the human factor is a variable which is most hard to control. Most information security issues arise due to the human factor and human errors. Humphries (2017) discussed that, when an organisation is dealing with the human factor, the method to place the staff at the right level of commitment is based on information security policies. The policies contain an assessment of the security behaviour of humans and individual employees. Kim *et al*. (2014) suggested that, when there is a level of compliance with acceptance of the security policies, then control over humans is being measured to achieve the success of the information security policies.

Teh *et al*. (2015) named the levels of compliance relating to the information security policies and user behaviour. The first compliance level is culture, which means the security is a natural part of the daily behaviour of individuals. The second is commitment, which means the security is not part of the users' behaviour. The users should be required to provide guidance and leadership for proper understanding of information security policies. The third level of obedience is where the users are required to instruct rather than providing guidance. Gerber *et al.* (2016) mentioned that awareness is where the users can become aware of the security risks and threats at a level and then present high level of adverse effects of the security incidents. The fourth is awareness, where the users are required to be aware of the security risks and show the required human behaviour. Ignorance is the fifth level, where the users are not aware of the security risks at this level and then represent a high risk of accidental adverse effects. The sixth compliance level is apathy, where the users are aware of their role in preventing security threats but not acting as the roles requires. Hsu *et al.* (2015) mentioned that the seventh level is resistance, which means the users are aware of their role regarding security but they are working against aspects of the security practices. Disobedience is the final compliance level, where the users are breaking information security rules and failing to comply with the security controls.

2.11.3 Compliance with the Information Security Policy

Information security policy compliance protects the information assets of public organisations. Information security has significant effect on employee attitudes towards compliance with the organisational security policies (Sinha, 2015). Employee attitude has a significant effect on behavioural intention regarding compliance with information security. Kampas *et al*. (2016) illustrated that it is a key factor in reducing the risks. Understanding of employees' compliance behaviour is a step to leverage worker assets towards reduction of risks.

The main aim of those policies is to design and provide the employees with guidelines on securing the information resources while performing their job regarding information security. Employee compliance is required to prevent as well as reduce the misuse of information system resources in addition to abuse by insiders (Safa *et al*., 2016). Behavioural theories are employed to study people's compliance intentions with prevention of misuse of an information system. Therefore, proper actions need to be taken by public organisations to comply with the associated information security issues.

Pearlson *et al*. (2016) stated that professionals are dedicated to maintaining the confidentiality of organisational information but they are resistant to maintaining information security environments. Based on the theory of planned behaviour and protection motivation theory, the behavioural factors are identified which influence the compliance with the information security policy. Based on the theory of planned behaviour, people's attitudes towards compliance and belief are believed to determine their intention to comply with the information security policy. Dependent on the protection motivation theory, expected efficacy impacts compliance intentions. Taylor *et al.* (2014) mentioned that the main requirement of their research study was to identify the human factor's perspectives of information security that connect end users 'behaviours along with compliance with the information security policy within an organisation. Mistakes and human errors are to be mitigated in order to achieve a proper information security policy.

2.12 Human Computer Interaction (HCI) and Behaviour Change

HCI is an initial study in which people use difficult technological inventions. HCI occurs when users and computer systems work together to accomplish something. Attig, Wessel and Franke (2017) mentioned that HCI and social interaction is the study of interaction among

humans as well as computers. It is a study related to the field of computer science and behavioural science. Zafar *et al*. (2017) discussed that HCI consists of three main elements – users, computers and the way the two elements get together, i.e. interaction. Groups of users in HCI are working together as well as carrying the users' perceptions for controlling the broadcasting of information. As people as well as machines are distinguished, therefore HCI field can allow to work with the functional system (Gotsis and Jordan-Marsh, 2018). HCI is developed with an ability to identify simulation of the human beings.

Kautonen *et al*. (2015) stated that there are three groups involved in human and computer interaction. The first group is explored with the interaction between computers and people in the form of data processing. The second group is explored with action-oriented interactions for those who are focused on projects like activity theory. The third group is explored by interactions linked with social as well as object-oriented contexts (Sheeran and Rivis, 2017). Despite the huge rise in the media reporting of information security, the human behaviours demonstrate a lack of information security awareness. Human-computer interaction is required in an organisation to make individuals aware about the security threats which arise due to human errors (Glanz, Rimer and Viswanath, 2008). HCI researchers are engaged in the design of such a system, which is required for behaviour changes: how the interventions for the behaviour changes are evaluated based on the context of HCI research. Mishra *et al*. (2014) concluded that behavioural changes are required in an organisation so that all the individuals are aware of the information security threats.

Martins *et al*. (2014) stated that the theory of reasoned actions assumes that individuals consider the consequences of their behaviour before performing the specific human behaviour. The result of this theory is that intention is a factor to determine behaviour along with the

behavioural changes. The intention is developed from the individual's perceptions of behaviour as positive as well as negative together with their impression. Therefore, the personal attitude as well as social pressure shape the intention that is required to perform the behaviour along with the behavioural changes (Williams *et al*., 2015). As per the theory of planned behaviour, it is based on the role of intention within human behaviour performance; however, it is intended to cover the cases in which the individual is not under control of the factors that affect the actual performance of the behaviour. This theory states that the incidence of actual behaviour performance is to be proportional to the amount of control along with the strength of the individual's intention to perform the behaviour (Katzenbeisser and Petitcolas, 2016). The most important theory is technology acceptance theory, which is adapted for reasoned action in the field of information security. It uses perceived usefulness and perceived ease of use to determine the intention of individuals to use a system for serving the mediator of the actual use of the system (Safa *et al*., 2016). It is the degree to which the person believes that use of the system would raise the performance of the human behaviour.

2.13 Insider Threats Behaviour

Cheng, Zhai and Smyth (2014) mentioned that the insider threat behaviour allows people to detect users who pose an increased risk as malicious insiders as well as to prepare for potential insider attacks. Each insider has a different level of access as well as a different level of threats. An insider threat is such people who can authorise access to confidential resources such as facilities, networks and systems as well as the equipment those use to access to harm the security of sensitive data. The insider threat concerns are related to criminal activities including theft as well as fraud, safety, including active shooter incidents, and financial harms by stealing of organisational sensitive data (Alexander, 2014). Insider threats include contractors as well as

employees. The organisation is required to develop close relationships with third-party vendors as well as partners who need access to the information (Kim *et al*., 2014). The following are the common types of dangerous insider threats that occur in public organisations:

Disgruntled employees: Heckmann, Comes and Nickel (2015) mentioned that there are various things which can make employees dissatisfied in their work, including being turned down for promotion and poor relationships with managers. This insider threat can use their position to take revenge as well as cause harm to the company.

Inside agents: employees as well as other corporations and governments may spy on a company. The inside agent is not a newcomer but a trusted employee (Taylor and Bean, 2017). They intend to steal professional secrets for the organisation's competitor, for an exchange of rewards.

Malicious insiders: Pearlson *et al*. (2016) discussed that there are some employees who misuse as well as abuse access to steal as well as delete valuable data out of malicious intentions. The difference between malicious insiders and disgruntled workers lies in motivation. The disgruntled employees are abusing data as an emotional response.

Third party providers: Layton (2016) suggested that there is little control over cybersecurity on the side of third-party providers. Security controls are audited as part of the selection processes, but this does not guarantee the complete safety of sensitive data. It is best to defend the remote connections from malicious subcontractors as well as cooperative accounts.

Hajli and Lin (2016) stated that the insider threats impact on access to account information. There is unauthorised access to sensitive data, which is a data breach in the securing of information on the network. As a solution to this threat, data encryption is used to transfer

data from one computer to another within the organisation so that no other person is able to hack and access the data (Siponen *et al*., 2014). The data encryption prevents unauthorised users from misusing data if they can gain access to the underlying file storage. The organisation should contain policies with regard to employee conduct that define the expectations of what the employees have to report with regard to potential insider threat behaviours (Safa *et al.,* 2015). Most of the incidents caused by insiders are a result of employee negligence. The malicious insider threats are hard to detect as it is based on trust in employees and their honesty.

2.14 Modelling Human Behaviour to Anticipate Insider Attacks

Abbasi, Sarker and Chiang (2016) discussed that insider threats such as espionage and leakage of data involve computer networks, which are among the pressing challenges of information security which threaten the governmental as well as industry information infrastructures. Today, unfortunately there is no single intrusion detection and assessment of insider threats technique for the insider threat problems (Kautonen *et al*., 2015). Battleday, Peterson and Griffiths (2017) mentioned that, in the operational context, the security analyst should review as well as interpret a huge amount of data to draw conclusions about suspicious human behaviours. This includes violations of policy as well as malicious policies. It applies domains of knowledge to observe as well as categorise patterns in the data. In domain knowledge, the analyst is facilitated by a process to identify the relevance of connections among data. According to Heckmann, Comes and Nickel (2015), the analyst is focused on preventing cybersecurity attacks and therefore monitors various data to provide alerts and reports about suspicious activities. Incorporation of psychosocial data into cyber data analysis offers additional dimensions to assess potential insider threats and integrate a threat analysis framework.

Battleday, Peterson and Griffiths (2017) mentioned that cybersecurity emphasises protection against attacks that can arise from external threats. An insider can be an employee, third-party provider or contractor; those who have access to the network and systems along with organisational data. The malicious insider is seeking to exploit access for improper gain, whether it is personal or financial. According to Schmitt *et al.* (2016), the insider threat problem is growing; therefore, it requires attention. There are early indicators of an insider threat. Warning signs are included when any unauthorised user accesses a server as well as organisational data. Indicators are provided when users gain unauthorised access and request information which is unrelated to their job responsibilities. It is considered as a theft of authorised credentials of the users. The employees apply domain knowledge to perceive as well as recognise the data patterns. The research analyst uses a number of tools to monitor various types of data in order to provide alerts in addition to reports about suspicious activities. The research analyst integrates analysis as well as sense making across various domains (Siponen *et al*., 2014). No systematic methods have yet been developed to provide complete and effective solutions to insider threats.

2.15 Intrinsic and Extrinsic Motivators in Information Security Behaviour

Teh *et al*. (2015) developed an information security behaviour model based on previous intrinsic and extrinsic motivation models that influences the individual's or public organisation's intention to comply with the information security policies as well as intention to lead to compliance behaviours. The extrinsic motivation model includes penalties as well as social pressure for employees' compliance with information security (Taylor *et al*., 2014). Social pressure consists of peer behaviour and normative beliefs. Apart from this, the intrinsic

motivation model includes the perceived effectiveness of penalties, perceived ownership and perceived self-efficacy as well as perceived value congruence for policy compliance.

Table 2. 3: Intrinsic and extrinsic motivators in information security behaviour
(Source: (Kautonen *et al*., 2015, p. 271))

Motivation	**Factors**	**Description**	**Theory used**
Extrinsic	Sanctions	The insider should comply with the security policies to avoid the penalties.	General Deterrence Theory (GDT)
	Normative beliefs	The insider should comply with the security policies as they believe that the IT management expects them to comply (Abbasi, Sarker and Chiang, 2016).	Protection Motivation Theory
	Monitoring	The insider should comply with the security policies as they know that the activities are monitored (Montano and Kasprzyk, 2015).	Theory of Planned Behaviour
	Rewards	The insider should comply with the security policies for attainment of rewards.	Theory of Planned Behaviour
	Social climate	The insider should comply with the security policies as it is observed that the management and supervisors provide greater emphasis to prescribe	Protection Motivation Theory

		the security procedures (Kautonen *et al*., 2015).	
Intrinsic	Perceived effectiveness	The insider should comply with the security policies as it is perceived that the security actions are taken for the betterment of the organisation.	
	Perceived ownership	The insider should comply with the security policies as it is perceived that they own the assets such as computer, internet (Mullan *et al.*, 2015).	
	Perceived self-efficacy	The insider should comply with the security policies as it is perceived that the employees have the skills and competency to perform the security activities.	Self-efficacy theory
	Perceived value congruence	The insider should comply with the security policies as it is perceived that the security values and goals are congruent with their values (Cheng *et al.*, 2014).	

Williams *et al*. (2015) suggested that intrinsic as well as extrinsic motivators influence employees' IS security behaviours. Siponen *et al*. (2014) examined the impacts of perceived

certainty as well as severity of the sanctions such as extrinsic motivation model, and perceived legitimacy, along with the perceived value, such as intrinsic motivation model of the IS security policies compliance among the employees. Both the motivational models are assessed for research significance. Martins *et al*. (2014) found that the contribution of the intrinsic motivational model exceeds the extrinsic motivation. It is proposed that the intrinsic motivation model generates explanations and solutions for the compliance with the organisational IS security policies. The public organisation should increase its emphasis on the intrinsic motivational-based approaches and rely less on the extrinsic-based approaches.

The extrinsic motivator for information security compliance that has received attention in the literature study is sanctions. A sanction is a negative stimulus and negative incentive for discouraging individuals from acting and taking decisions which are not aligned with the public organisational goals. According to Bae, Han and Moura (2019), the current research into IS security policy compliance is focused on the value to employees of extrinsic rewards where the employees tend to value intrinsic in addition to extrinsic rewards. In this study, sanctions are classified into two types, certainty and severity. Williams *et al*. (2015) mentioned that the certainty of a sanction refers to the possibility that the employee can commit a wrong act and is caught. On the other hand, severity refers to the degree of punishment on being caught. This concept of sanction assumes that humans are rational. The importance of the intrinsic motivator in information security research is incorporated with feelings of competence. The factors of intrinsic motivational are self-efficacy, perceived effectiveness, perceived value congruence and psychological ownership, which influence employees' decisions. It is clear that intrinsic factors explain information security policy compliance better than extrinsic factors do.

Montano and Kasprzyk (2015) conceptualised empowerment as intrinsic task motivation. Empowerment refers to a set of cognitions for reflecting the perceptions about the tasks and its ability to control the shape as well as influence the tasks (Sheeran and Rivis, 2017). The contract between two of the motivational theories is focused on the managerial practices which share power with the employees (Conner and Norman, 2015). In other words, the individuals are considered as intrinsically motivated when they experience cognition. Siponen *et al*. (2014) discussed various practices which indicated structural empowerment, such as access to opportunity and access to information, as well as participation in decision making.

2.16 Insider Misuse and Incident Responses

Cultural aversion leads to public organisations avoiding creating solid incident response plans. Human behaviour risks can be mitigated by an incident response plan which helps to identify the possible incidents which lead to information security risks due to human errors, and the causes and control factors to prevent such risks. Malekian *et al*. (2017) stated that the incident responses understand security incidents. The breach events are to be compromised with confidentiality as well as availability of information assets. Such incidents include attacks, which are intentional attempts to gain unauthorised access to damage as well as destroy the network. Siponen *et al*. (2014) suggested that the incident responses are formal as well as organised approaches to deal with all kinds of security incidents. They involve an incident response plan which outlines the steps that the organisation should follow after an incident has occurred. The plan includes the incident response process for common types of incidents. Safa *et al*. (2016) discussed that insider incident response plans define responses that include extended teams such as the legal department and human resources along with departmental management when the employees are involved. The security programme helps to evaluate the

entire state of a public organisation's security by providing an objective view of its policies and controls as well as its processes.

Gritzalis *et al.* (2014) illustrated that the development of threat vulnerability along with information security management programmes help to identify the organisation's vulnerability to exposure to malicious activities. There is an assessment to determine whether malicious activities are taking place in the network. Gerber *et al.* (2016) argued that this assessment should be regularly scheduled as part of the vulnerability management practices along with integration of the incident response capabilities. The organisational as well as cultural factors affect insider responses to the security environment. Soomro *et al*. (2016) stated that the technical approaches use system policies to identify as well as minimise the damage done by threatening insiders. Incident response techniques are used to reduce the insider threats, which reduces the risks. The information security policies are based on the motivation and feelings of the insiders. The attitude of employees towards information security is the main challenge for implementation of information security policies (Siponen *et al.*, 2014). Employees' understanding along with awareness of information security issues and implementation of information security policies play a key significant role to protect a public organisation's information

2.17 Conclusion

The research topic is based on examining the mediating effect of the users' addictive behaviours on the relationships between information security countermeasures and risky cybersecurity practices. Risky behaviours in the public organisation are considered as the main threat to the organisation. In any organisation, there are usually people, computers and networks which collect, process, store and distribute information. All these put together make the information system. In this literature study, various information security dimensions have been

identified such as culture, information security countermeasures and attitude towards cybersecurity. Different theories, methods and procedures were covered and different international standards were analysed. Von Solms and Furnell (2016) stated that information security is a practice preventing the unauthorised access, disclosure, inspection and destruction of information. Crossler *et al.* (2013) argued that information security is required to protect the confidentiality as well as data availability while it is focused on policies and standards of information security. The risks associated with whichever kind of threat can highly compromise an organisation's operations (Snitsarenko *et al*., 2020). Therefore, measures need to be set in any organisation that will counter the impact of attacks as soon as one happens. Human behaviour theories are a set of theories used to describe various kinds of cognitive situations. In order to conduct the study in this research, there is a requirement to understand those theories and the characteristics of human behaviour within the information security context. The IT department has to ensure that the organisation's information system conforms to the established international standards. The standards include use of genuine software, as well as all the security standards described in ISO 27001 and 27002. Insider threats have become malicious due to human factors. It is necessary to monitor human behaviour outside the threat domain to better inform on the mitigation of threat. Information security culture is a part of the organisational culture as the security of information has become an organisational function. In order to gain a secure environment for the information assets, the practices of information security have become a part of corporate culture within the organisation.

CHAPTER 3: RESEARCH CONCEPTUAL FRAMEWORK

3.1 Introduction

This particular chapter contains a description of the conceptual framework used in the research study. The conceptual framework for this particular study is derived from the literature review above. The literature review helps the researcher to understand the problems as well as guides the data gathering as well as analysis. The conceptual framework describes two independent variables, one dependent variable and a mediating variable regarding how they are related and how they impact the human behaviour (Wong *et al.*, 2019). The relation between two variables is used to answer the mentioned research questions. This particular research is carried out in two phases: in the first phase, the information security countermeasures are identified to examine the mediating effect of the users' addictive behaviours on the relationships between information security countermeasures and risky cybersecurity practices in public organisations in the UAE. In the second phase, the human perception of information security countermeasures is analysed (Safa *et al*., 2018). The conceptual framework is used to analyse that there are various countermeasures which influence the human information security behaviour based on organisational culture and the empirical study is to be performed to provide both negative and positive influences.

3.2 Theoretical Development

After the review of the literature, the research paper analyses the problem area to identify the information security threats for organisations due to human behaviours such as:

- Lack of people's understanding about the insider threats and issues (Libby, 2017).

- There are limited human resources for the management of security.
- There is a lack of understanding about the importance of the human factors.
- There is a lack of priority of information security (Jeong *et al*., 2019).
- There is a lack of understanding about the variety of information security countermeasures used for different organisational cultures.

As a result of the literature review, a number of relationships have been detected to identify the internal threats, countermeasures and human factors along with human behaviour, as detailed in the following figure.

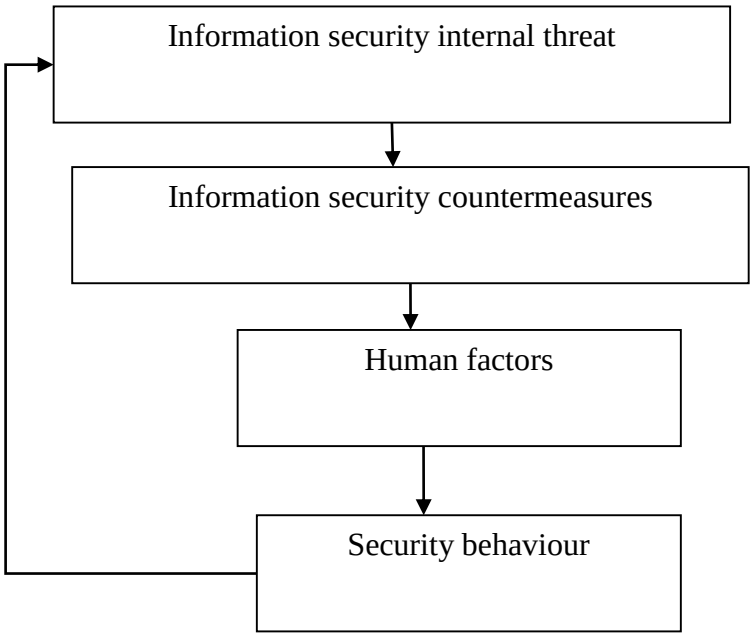


Figure 3. 1: Relations among threat countermeasures and human behaviour
(Source: Safa *et al.*, 2015, p. 71)

In order to reduce the internal threats to public organisations due to human errors, different countermeasures can be implemented and maintained, but the employees should

understand the countermeasures which influence the human behaviour which are not properly clear. This study intends to research the end users' perceptions of the information security countermeasures (Aldawood and Skinner, 2019). In public organisations, there are insider threats which have a huge impact on sensitive as well as confidential data. The implementation of an information security system in a public organisation is based on safeguarding the network and data from penetration by hackers (Neneh, 2019). The insider threats also have an impact on the account information. Some unauthorised access to sensitive data causes a data breach; therefore, the organisation is required to secure information on the network. The analysis of insider threats is correlated with various sources used to recognise the potential threats (Moody *et al.*, 2018). The research analyst uses various monitoring tools to alert the organisation about the suspicious activities. The specialised methodologies utilize framework approaches to recognise and in addition limit the harms which are caused by insiders. Episode reaction procedures are utilized to lessen and decrease the insider dangers. The data security arrangements depend on the insiders' inspiration. The state of mind of representatives towards data security is the primary difficulty in the usage of data security approaches (Van *et al*., 2019). The comprehension of representatives alongside their consciousness of data security issues with their execution of data security arrangements assumes a key critical part to ensure the safety of the organisation's data.

3.2.1 Security Awareness Countermeasures

Security awareness countermeasures are the first part of information security countermeasures and are considered as an independent variable. Security awareness countermeasures can be divided into three sub-sections: managerial countermeasures, support countermeasures and administrative countermeasures. The term 'security awareness' is

currently researched in combination with behaviours and attitudes that protect the organisation's information. To be aware of cybersecurity means that the organisation's users are familiar with and understand the information security threats and take the right steps to avoid them. Recently, the information technology industry has boomed, taking care of almost all of our everyday jobs, the administration of the whole of government and legislative frameworks. Public organisations have at all times been processing information and, in today's world, governments' schedules are seeking to maintain digital networking as well as the changes in society which are based on information technology. Nevertheless, digitalization is enforcing the changes in most businesses as they try to provide services that are user friendly to citizens and businesses (Butavicius and Pattinson, 2017). Despite this, new security measures should be applied in the form of data protection and IS that is legally compliant. Adequate protection in an IT environment can no longer be disputed in most industries, commerce and administration. The repercussions from IT security incidents can be severe for businesses and organisations or can obstruct the functioning of their duties, which might lead to high costs being incurred. All areas of life are quickly being affected by digitalization, and the underlying ICT sends, processes electronically and stores a huge amount of data and information (Van *et al*., 2019). The more the organisation connects to the internet, the more it connects to cybersecurity risks and harms as well as opportunities. One should be able to differentiate between the words' safety and security. Safety refers to the machine's safety function, and it should be addressed as the process of keeping the environment safe against irregular operations. Security refers to the protection of systems that are supported by IT against errors that are deliberate and undesired. The protection of safety systems against attacks must be put in place at all times.

Digitalization offers a greatly advanced form of industrialization, which most organisations cannot do without, but cybersecurity is creating new challenges each day. Information security comprises just IT security. The main objective of information security is to protect all kinds of information regardless of where that information is stored, whether on paper or in employees' minds. IT security, on the other hand, focuses more on the protection of information that is stored and processed electronically. Cybersecurity deals with various forms of security information and communication technology (González, 2019). Employees of an organisation are a factor that is necessary and important to consider in realizing information security (IS) in the organisation successfully and efficiently. This, therefore, requires all the employees to understand their particular duties and be mindful of the information systems management (ISM). According to the BSI, it is important that all an organisation’s employees of the organisation understand its information security goals and understand the countermeasures that have been put in and must be willing to support them effectively. In short, they must understand what is expected from them in terms of information security and the way to respond in critical cybersecurity situations.

Information security has technical solutions that are important to find particular vulnerabilities like denial of service attacks and viruses. Certificate Server (CS), IS and IT are more than just technology; they involve users, and at times humans do not always perform as they are expected to. This characterises humans as a critical factor within the processes of information security (IS) (Dahbur Bashabshed and Bashabshed ,2017).

Just using technological solutions is not enough to confirm countermeasures for IS. This highlights the problems of information security management in organisations as behavioural as well as management aspects are important in building an information security management

system in an organisation. The human security side should be managed to protect the organisation's assets, include information and systems which are prone to attacks (Patiño and Yoo, 2018). The human aspect has an important responsibility to deliver information security in organisations, and information security behaviour is largely affected by the perception of users concerning risk. However, through awareness and IS training, these perceptions can change. The tasks and duties of the organisation play a key role in all the activities. In all processes in the organisation, IS must be integrated and the management of that organisation has a responsibility for this as the most effective measures in protecting the information are not always expensive.

An organisation requires constant analysis of threats to understand the plans of attackers which keep on evolving every day; this enables the organisation to create defences that are reliable and more efficient (Al-Daeef *et al.*, 2017). Cyber-attacks are directed at people mainly, not technologies. The reason why there are a lot of attacks is because the internet- and web-based systems have been used and are still being used by millions of people around the world without enough information security. As a result of this, attackers have shifted their attention to the users.

The idea that considers the employees as the weakest link can be found in most studies where they try to describe the obedience to or non-compliance of the employee with the IS. The efforts made by organisations in relation to IS are threatened by the negligence of the employees and breaches (Hadlington, 2017). Ignorance, apathy and resistance are some of the users' mistakes that lead to the vulnerability of the systems. In research by Kessler *et al.* (2020), they found out that most employees underestimate the likelihood of security breaches occurring. If a single action by a user can compromise the whole security program, then the problem lies with

the security program itself. Some of the vulnerabilities are characterised by inadequate knowledge of regulations, inadequate awareness of information security, and handling of information in a careless manner. Employees should decide on ways to implement information security in their context specifically and this requires high-level skills and motivation factors.

Learning the methods that can be used to clarify threats, attacks, damage and vulnerabilities is essential in information security and for protection of data. The basic values that should be used are integrity, confidentiality and availability. Protection against access by unauthorised people and disclosure of information is what confidentiality is required for. Confidential information should only be disclosed and accessed by authorised personnel in the organisation. When an unauthorised person accesses the information, this is referred to as loss of confidentiality. Integrity is ensuring the correctness of the information or data that been developed by authorised users. When data are changed without authorization or are incomplete, then integrity is violated. There can be serious repercussions when data or any other information are falsified. Availability implies that the services, functions, applications or networks of IT are accessible and obtainable and that they can be used by the employees at any time (Anwar *et al.*, 2017).

In most organisations, training with suitable presentations that are aided by posters and flyers, or online training, is seldom used as an awareness campaign which has to be completed by the employees at a particular time or place of their choosing. Focusing on knowledge transfer does not provide long-lasting safety or security awareness for employees. Different approaches can be used to create awareness to sensitise the employees and create emotions that can be used in securing the organisation's information and in creating the measures. Students are future employees and therefore they should be educated and engaged in practices in organisations and

companies (Howard, 2018). This builds knowledge to assemble a general comprehension of sensitivity and technology development to deal with current issues of information security. This awareness and competence apply not only to IT professionals but also to businesses. Every employee in the organisation must contribute to information security and be responsible for it in their respective environments.

Information security does not exempt anyone; it concerns everyone in the organisation. Damage can be avoided when they all act responsibly and with awareness, which in effect contributes to success. The fundamental prerequisites for IS are increasing information security awareness and training that been provided to all employees in the management team. The necessary skills are essential in implementing the security measures as planned. The top management in the organisation is the role model. Knowledge about the operation of the security mechanism also involves an understanding of the purpose as well as the spirit of security measures. Some of the factors that influence IS are the work atmosphere, ideals and commitment. When new users are enrolled or the current ones are tasked with different duties, training should be provided to them so that they are able to adjust to the new situation. Security aspects that are related to their jobs must be taught to them. If an employee leaves the organisation or changes their responsibilities, security safeguards must also change, for instance the withdrawal of authorization or return of ID.

Employees should be made aware of hazards that may occur, and they should know what effects they might bring to the organisation. When risky situations are known by the employees, the acceptance of the security measures will be easier. They should have the correct knowledge to be able to comprehend and adopt measures in the right way (Lazar *et al.*, 2017). Safety culture and awareness of security can be designed and set up for this. Countermeasures awareness is a

significant indicator of information security. Raising users' awareness of security through training and education could be an appropriate technique to encourage acceptance of information security systems that lead to safe technology use.

The level of emotions should be addressed explicitly because participation socially in the process of a communicative team is an important factor in raising the awareness of activities that are based on psychological approaches. Students must see or experience the results as outcomes of their actions.

All of the above-mentioned facts give rise to the need for both public and private workers to improve their knowledge of workplace safety and confidentiality so that sensitive and confidential information is not misused and mismanaged by opposing market players. There are two hypotheses related to this section: Security awareness countermeasures are positively related to the risky cybersecurity behaviour practices, and Security awareness countermeasures are positively related to the users' addictive behaviours.

3.2.2 Attitudes towards Cybersecurity Countermeasures

Attitude towards cybersecurity countermeasures is the second part of information security countermeasures and it is considered as the independent variable. Attitude towards cybersecurity countermeasures is divided into two sub-sections, attitude and self-efficiency. One of the responsibilities of employees in an organisation is cybersecurity responsibility. According to Tischer (2016), people are devolving obligations for their cybersecurity to technical interventions and senior executives. The attitude is taken to be that when they are in a place of employment they fail to see cybersecurity as their fundamental concern. This attitude would fit into a framework of risk compensation, where people believe that they are made safe

by technical interventions that are provided by their employer (organisation) which in effect may engage in risky cybersecurity behaviours (Peter, Asrar and Kuchinke, 2016).

Though an understanding between humans and computers in terms of interaction helps in managing information risk, users and the management are refocusing their resources on aspects of attitude to IT as they try to gain the benefits obtained from positive behaviour in computer usage. The sluggish shift can be explained by the fact that there have not been many pieces of research done to explain the usability of cybersecurity (Albarracin and Shavitt, 2017).

Before analysing cyber usage and security, it is important to comprehend the meaning of attitude since it would probably describe the significance of a positive attitude towards cybersecurity. Attitude is the psychological tendency that is expressed by assessing a certain enterprise with some degree of favour or disfavour (Aldahmash *et al.*, 2019). Other scholars describe attitude as a learned predisposition to respond positively or negatively to a certain situation, object or person.

One point that stands out is the fact that attitude can be used as a predictor of human behaviour. Attitude towards the utilization of cybersecurity can act as a useful predictor of ways that cyber users can approach secure cyber use.

Education level is an important factor that influences the user's attitude towards cybersecurity. If the cyber user has a higher level of education, then they have a greater level of concern for security (Newhouse *et al.*, 2017). The principle behind this is the belief that education helps in increasing the ability to use the internet securely and it also creates the necessary awareness for using the internet securely. Many educated individuals are likely to be more informed about the effects associated with cybercrime and be well aware of the

repercussions of a cyber-attack for organisations or businesses. Education is not just training but rather the process of providing knowledge in learning institutions (Proctor, 2016). The more a person advances up the ladder of education, the more equipped they become in terms of understanding and using the internet in a secure way.

Gender cannot be ignored because it plays an important role in cybersecurity and also because the internet is being used by all genders regularly (Anwar and Xu, 2017). There is a noticeable gender gap in the IT profession and computer education. There is a smaller number of females in the IT workforce as compared to men. In terms of attitudes towards the use, security and adoption of computers, some argue that the history of men and women is long and disproportionate. Women are likely to not use computers as compared to men because they are more interrupted than men and they are also technophobic and are mostly not liable to adapt to technology as compared to men (Peacock and Irons, 2017). This view may be biased but it exists nonetheless.

Gender is a better steward of cybersecurity and many researchers consider it a factor of cybersecurity usability. Most researchers argue that males are more interested in computers and enjoy doing work with them than their female counterparts. Men also hold views that are gender-biased when it comes to computer competence. The more females are exposed to computers, using them in a proportion equal to that of men's usage, the more the cybersecurity issues will decrease (Vilceanu and Johnson, 2018).

Age is also a determinant in attitude towards cybersecurity and therefore cannot be ignored because people of all ages use the internet. According to Pencheva *et al.* (2020), people aged 65 years and above are less likely to use ATM cards and few of them own a computer or a laptop,

while younger people are most likely to use the devices (Broady *et al.*, 2010).

People in urban areas are connected to high-speed networks and the probability of using the network securely is high; people living in rural areas that are sparsely populated may not be able to access the internet. This is due to the unavailability of a broad infrastructure and to the gap between demographic groups (Cobb, 2019). Two hypotheses are related to this section: Attitudes towards cybersecurity countermeasures are positively related to the risky cybersecurity behaviour practices, and Attitudes towards cybersecurity and countermeasures are positively related to the users' addictive behaviours.

3.2.3 Users' Addictive Behaviours

The internet user's addictive behaviour is a type of personality trait that has been absorbed within the research around information security behaviours (Beauchaine *et al.*, 2017). The sub-categorization of the user's addictive behaviour is impulsive. The definition of impulsiveness is "the urge to act spontaneously without reflecting on an action and its consequences (Coutlee *et al.*, 2014). In this research impulsive contain two elements, premeditation and urgency. The deliberate intention to do any action, mainly a crime is the definition of premeditation (Barratt *et al*., 2003). The research has also identified a second factor that influences the users 'addictive behaviour, which is the urgency (Argyriou *et al*., 2018). The urgency is the ability of the user to respond to any action in a timely way without minimising the efficiency of that action. Due to this action response, significant threat to cybersecurity appears as a state of urgency; the internal user can create a harmful effect to the information security of the organisation, and there are different types of addictive behaviours, as detailed below.

3.2.3.1 Addiction to and Abuse of the Internet

In day-to-day working, the internet has become an integral part of people's lives. Issues that surround the use and abuse of, and addiction to, the internet have emerged. It is not a surprise that employees spend work time on activities that are not related to work. Internet access in places of work is mostly spent on browsing that is not related to work (Milková and Ambrožová, 2018). The abuse of the internet in the workplace can result in productivity decreasing, network clogging and rising incidents of breaches in organisations. This kind of activity is a serious concern for the management and they highlight the abuse of the internet.

Excessive use of the internet can be addictive and pathological and such behaviour is termed as technological addiction. Behavioural addiction is no different from other forms of addiction such as alcoholism and marijuana addiction in terms of components such as tolerance, withdrawal, mood modification, conflict and relapse. Internet addiction is quite broad and it covers wide forms of behaviours and problems (Qi *et al.*, 2019). According to Wellbeing (2012), there are five types of internet addiction:

1) Overloading of information – uncontrolled web surfing and database searches.
2) Net compulsion – employees become obsessed with online gambling or trading.
3) Addiction to computers – especially playing games.
4) Addiction to cybersex – uncontrollable use of websites that are meant for cybersex.
5) Too much involvement in relationships especially online ones.

However, most employees may not be addicts but they may use the internet to accelerate other addictions. Internet abuse can be caused by many factors in workplaces. A virtual

environment in communication that is computer-mediated provides comfort and also acts as a distraction. This is why staff may enter in non-work internet use.

3.2.3.2 Social Media Addiction

Over-usage of social media has become a behavioural addiction in recent times due to similarities that it shares with other forms of addiction. Due to the connectivity of Wi-Fi in most organisations, it is easy for employees to access the internet. Many organisations do not stop their employees from carrying their mobile devices with them, especially smartphones, and therefore it is easier for them to access many things using the apps on their phones and they can do so frequently. However, social media usage can present several experiences especially from a psychological perspective, and this can result in patterns in behaviour which can be problematic. Socially inclined employees may tend to spend more time on Facebook, frequently checking who has posted and what has been posted, or even posting just to get likes from their viewers. Others may find platforms such as Instagram to be more addictive because they spend most of their time taking selfies to present them to others. Addiction to social media can be fuelled by social anxiety (Perera and Samaraweer, 2019).

Nowadays, mobile phones offer nearly all the internet applications such as video and voice call, video recording and even text messages. Employees spend most of their time focusing on them, consuming valuable time when they should be being productive. There are many apps that people can engage with, and moreover they have an element of accessibility that is different from that of previous computers (traditional). Obsession concerning those devices can interfere with work, especially if there is a requirement for face-to-face interaction.

Committing more time to social media does not only lead to loss of work time but also procrastination in terms of core job responsibilities in order to check social media updates (Tunc-Aksan and Akbay, 2019). Excess usage of social media causes distractions at work and most employees are helpless about it. Seeking approval using social media platforms is turning out to be a trap, but it reflects more or less the real-life settings everywhere. Two hypotheses are related to this section: Users' addictive behaviours are positively related to the risky cybersecurity behaviour practices and Users' addictive behaviours are positively mediating between the risky cybersecurity behaviour practices and information security countermeasures.

3.2.4 Information Security Countermeasures

Information security countermeasures is considered as an independent variable and it is divided into two sub-sections: attitude towards cybersecurity countermeasures and security awareness countermeasures. Different researchers are reviewed in the conceptual part with aim being to recognise as well as define the information security countermeasures influencing the risky human cybersecurity behaviour practices in public organisations. The type of information security countermeasures which are analysed in the literature part such as:

Documentation related to the information security: each public organisation should have documentation whose objective is to influence the human behaviour. Documented norms should describe the responsibilities of the employee, authorised use of confidential information as well as organisational system, and what human behaviour is being prohibited as well as the consequences of a violation (Aldawood and Skinner, 2019). Therefore, the employees should follow the organisational rules and regulations to implement a good culture in the working environment.

Training and awareness: this is provided to employees to raise knowledge about the security issues, and influences the emotional aspects of how they perceive the information security (Abbas *et al.*, 2019). Proper training is provided to all the employees to make them aware of the good human behaviour which is required for any public organisation.

Reward: each organisation should have some reward process for preventing the employees from performing unacceptable human behaviour. When the information security incidents and the reaction to the incidents are integrated, therefore the process becomes effective, then the employees have improved their security behaviour (Nelson and Staggers, 2016). Reward system encourages the employees to work properly and motivates them to work more so that they are recognised by others.

Internal security culture: Hodgson (2017) concluded that there are cultural dimensions which are used in the conceptual framework for identifying and assessing the internal culture in an organisation. The management as well as employees believe in the importance of information security, motivation of human behaviour, changes in the public organisation, social interaction and the responsibility of employees to minimise the information security risks. Culture plays a key significant role in shaping society as well as the country (Yang *et al.*, 2015). The culture is developed as result of employees' interactions with the information security controls. The above-mentioned cultural factors would influence the end user's behaviour.

Access limitations: there are effective methods to reduce the internal threats, including the implementation of access rights, which is based on a need to know with the internal information system. The internal limitations are used to reduce the possibility of information

leakages (Arnott, Lizama and Song, 2017). The limitations to physical and/or electronic access help to secure the information from physical threats.

Identification and authentication: a strict user name, password and technological countermeasures are used in public organisations to identify the end users along with authentication to enforce access to the information as well as offer accountability (Jahromi *et al.*, 2019).

Therefore, the conceptual framework is showing different types of countermeasures to prevent as well as mitigate the internal threats which are required for user perception to make sure that the internal threat levels are not raised.

3.2.5 People's Addictive Behaviour and the Information Security System

Different researchers are reviewed in the conceptual part with the aim of recognizing as well as defining the users' addictive behaviours that mediate between risky cybersecurity behaviour practices and information security countermeasures. Most of the literatures states that information security breaches are based on human behaviour. Senyo *et al*. (2018)stated that humans are proactive regarding information security. When an organisation is recommended to use information security measures, then the level of human awareness is increased and the successful implementation of the information system is impacted. The security of information is defined as the capability of the information system measures to protect against unauthorised use as well as misuse of information system assets (Moody *et al*., 2018). This particular study believes that focusing on information security is important, security incidents need to be decreased and the effectiveness of the information systems needs to be increased. The acceptable human behaviour will increase the effectiveness of the human information security system. As

per the organisational policies along with standards, various codes of conduct need to be designed for people to follow up. People are educated about the public organisational information security policies which help the users to prevent and minimise the human activities, and this leads to an enhanced information system (Safa *et al*., 2018). The human factors are major forces behind the effectiveness as well as the failure of security systems.

There are many different researchers reviewed in the conceptual part with the aim being to evaluate the association between risky cybersecurity behaviour practices and information security countermeasures in public organisations. Most of the studies have focused little attention on organisational attitudes, human behaviours or interaction among individuals and its context (Hadlington, 2017). The interaction contributes to the beliefs of individuals along with their values concerning information security. There are various cultural components in humans' personal culture and it is better to focus on the values to promote human behaviour. Based on the literature review findings, the frameworks of four modes are analysed in three cases (Ahmad, Maynard and Park, 2014; Stewart and Jürjens, 2017). Based on the three cases, the participants are asked to recognise the causes of the security incidents and the obstacles to achieving improved information security compliance in the organisation. The following table shows the four modes of the information security behaviour which are presented in three cases which are related to the four modes.

Table 3. 1: Human security culture
(Source: Tsohou, Karyda and Kokolakis, 2015, p. 134)

Modes	**Case A**	**Case B**	**Case C**
Mode 1: Not knowing-not doing	Some of the employees are not sharing related information as they are not aware of the information security mechanisms.	Most of the employees are unaware of information security policies. There are no such instructions provided to them by IT departments (Mishra *et al*., 2014).	Most of the employees are unaware of information security policies as no such instructions are provided to them. Their non-compliance behaviour is seen as a result of related rules as well as consequences of taking information security risks (Luthans, Luthans and Luthans, 2015).
Mode 2: Not knowing-doing	There is sharing of cultural information as well as knowledge which is related to the security of information among IT staff.	In the public organisation, the employees are relied on to solve work issues. The cultural values prevent the users from viewing illegal web	There is an informal approach to the sharing of information among staff. Some of the cultural values dictate the user's actions (Parsons *et al*., 2014).

		content (Morosan, 2014).	
Mode 3: Knowing-not doing	The employees are not aware of information security procedures as they conduct non-compliant behaviour such as downloading of internet software (Khaitan and McCalley, 2015).	The employees are not ignoring the procedures by downloading internet software (Ahmad, Maynard and Park, 2014). The employees have a tendency not to report violation for the sake of their group's image.	The users are downloading software, shortcuts. The functional manager tends to enforce the rules to discipline their sub-ordinates due to protection concerns (Tsohou, Karyda and Kokolakis, 2015)
Mode 4: Knowing-doing	There is a level of information security culture which indicates that most of the members in the three cases fit into the modes.		

From the above table, the data indicates that the cultural values impact the individual's security-related behaviour and this influences the information security culture in the proper manner.

3.2.6 Risky Cybersecurity Behaviour Practices

Risky cybersecurity behaviour practices are considered as the dependent variable and it is divided into three sub-sections: risky behaviours, digital trusted behaviours and mitigating behaviours. The cultural framework is based on six distinct dimensions: power distance, individualism versus collectivism, uncertainty avoidance, indulgence, masculinity vs.

femininity and pragmatism. The cultural analysis is based on those six dimensions, analysing differences between the cultures.

As per Hofstede's cultural framework, people from the UAE are high on the power distance dimension with a score of 90, as people can accept the hierarchical order and it requires no justification. Public organisational hierarchy is reflected in inherent inequalities and the existence of subordinates, and centralization is important. The UAE has a score of 25 as it is considered to be a collectivistic society. People have a long-term commitment to their peers and extended relations (Litz and Scott, 2017). Loyalty in a collectivist culture is dominant in addition to overriding other societal regulations. People foster stronger relationships with the fellow members of their group. As the UAE scores 50 on the masculine vs. feminine dimension. Therefore, the society is neither driven by competition and success nor has dominant values for quality of life or care. The UAE scores 80 in the uncertainty dimension as there is a high cultural preference to avoid uncertainty. The country exhibits high avoidance as it maintains a rigid code of beliefs as well as human behaviour (Grey *et al.*, 2018). In this culture, there is an emotional need for rules, people are busy in their daily work as well as punctual. For the long-term orientation and indulgence, the UAE has no score.

Furthermore, Individuals often take the requirements of cybersecurity too lightly, resulting in severe consequences for the organisations they work for. The human factor plays a key role in making business either vulnerable or more secure. Many companies and organisations have not updated their systems, which makes them a target for attackers outside or within. There are many cases where non-IT personnel have been targeted because they have been considered to be the weakest link. Most companies believe that they face risks from within.

Employees, whether intentionally or carelessness or through lack of proper knowledge, put the businesses that they work for at risk (Hadlington, 2017).

3.2.6.1 The Risk from Employees

Businesses assume that their IT security is more prone to attacks due to the increase in the cyber-threat landscape but at the same time they have to realise that one of the biggest chinks in their armour against cyber-attacks is their staff. Most organisations admit that their biggest weakness in IT security is their employees, especially those with careless actions that put the business's IT security measures at risk.

The risk from employees is brought out clearly in the fact that, for many business organisations, the top cybersecurity fears are associated with human factors and the behaviour of employees (Hadlington and Murphy, 2018). The worry is mostly about the sharing of inappropriate data by the employees using their mobile devices, and the physical loss of those devices (mobiles), which ends up exposing the company they are working for to risk, and the inappropriate usage of IT resources by employees. Inappropriate IT usability by employees varies according to the size of the organisation, with small organisations feeling more at risk from the threat than organisations with a huge number of employees. Small organisations task their staff with a greater degree of flexibility in terms of the way they use the business's IT resources.

3.2.6.2 Employee Actions that Result in Cybersecurity Incidents

Businesses do have a reason to be worried when it comes to employees' contribution to cybersecurity risks. They may make blunders, whether accidentally or through careless behaviour, putting the organisation's data or system at risk. They may lack the required training

to teach them how to carry themselves appropriately and maintain the safety of the business they work for (Anwar and Yuan, 2019).

Employees who are careless or uninformed are likely to cause serious security breaches after malware attacks. These incidents have contributed to attacks on some organisations in the past. Human error is an attack vector that employees fall victim to. Internal staff also cause security issues through their malicious actions, working against their employers.

The major contributors to malware and targeted attacks are the staff's carelessness and phishing, which have risen in the past years. Many organisations worldwide report being attacked by malware and viruses, and they consider the carelessness of employees and them being uninformed as the top factors contributing to the threat. Other organisations believe that phishing and social engineering contribute to attacks (Li *et al.*, 2016). If attack scenarios continue to rise, and staff are contributing to them, whether willingly or unwillingly, organisations need to expend more efforts to reduce these attacks to which they are exposed and protect their systems better.

3.2.6.3 Incident Reporting

Incidents regarding security happen in businesses, and employees should be able to spot the attacks or breaches, or come up with ways to mitigate those risks. They have a responsibility in helping to protect the organisation they are working for. However, employees do not always act when their organisation is attacked or a security incident occurs. Most employees hide when those incidents happen. When an incident happens and it is hidden by staff, the consequences could be catastrophic and damage could be higher. Unreported events can result in a breach of the entire organisation’s system.

Regular detection and forensic analysis of a targeted attack can help minimise the threats that organisations may face. Relying on employees' ability to report incidents when they occur and their vigilance is not sufficient, as attacks and human factors are changing every day. It is therefore prudent for organisations to come up with solutions and technologies that automatically monitor and reduce the chances of irresponsibility and errors. Hide and seek is challenging, especially for larger organisations where employees hide cybersecurity incidents.

Hiding problems should be communicated to the entire business, employees and the high managements. Employees do not just hide incidents, there must be a reason why; for instance, strict and unclear rules and businesses imposing more responsibilities on their employees. Policies that instil fear in employees leave them with a single option that they can utilize to avoid being punished at all costs (Parker and Brown, 2018).

3.2.6.4 Irresponsible Employees Causing Damage

The irresponsibility if any employee may result in the organisation's system being hit, especially the data and its integrity, when linked to security incidents (Fimin, 2017). Loss of customers' information deemed to be sensitive and confidential may be a result of irresponsibility. Above all, the organisation may lose its reputation internally and externally.

3.2.6.5 Mobility Trends and Digital Trust

The idea of 'bring your own device' (BYOD) varies with the size of the business. Regardless of the size of the organisation, BYOD causes headaches to businesses all over the world. For small businesses, their concern revolves around the practices of employees' BYOD, while the likelihood of struggling with issues of security management is high. Employees

sharing the company's data inappropriately using the mobile devices that they work with is a worry to most employers. It is practically impossible to manage the security of the users' devices.

BYOD is dependent entirely on the responsibility of each employee and the capability to treat the data on their devices well is a concern to most businesses. People may lose their devices or they can be stolen and this makes the process difficult. The more the device is not in the work environment, the more it poses risks to the business (Topping, 2017).

Whenever the employee has a responsibility to BYOD when working in an organisation, carelessness may result a primary problem experienced with the trends. The contribution of employees' carelessness to cybersecurity incidents is high; it accounts for more incidents than those associated with the theft of devices.

3.3 Proposed Conceptual Framework of the Research Study

The conceptual framework in this particular study is being conceptualised by protection motivation theory as well as technology acceptance theory. Both theories are used in human behaviour studies which are significant for predicting human behaviour. The protection motivation theory refers to how people change their attitudes as well as behaviours in response to human risk (Van *et al*., 2019). The research study found that most of the factors, like the attitude towards cybersecurity, as well as self-efficacy influenced the users in practising security behaviour. This theory is based on four factors which are believed to motivate users to protect themselves: “perceived severity, perceived vulnerability, perceived benefits in addition to self-efficacy” (Sunarta *et al.,* 2019). This particular model is used to assess engagement in risky practices and offer suggestions to change human behaviour (Menard *et al.*, 2018). This theory is concerned with how individuals are processing the threats along with selecting the responses

to cope with them. The factors are divided into threat and coping appraisal. Threat appraisal consists of the perceived severity as well as perceived vulnerability, and coping appraisal includes the perceived benefits in addition to self-efficacy. Threat appraisal is such that when people have a stronger perception of the severity of as well as the vulnerability to the threats, it motivates to avoid the security incidents (Wu, 2020). Coping appraisal refers to people's ability and belief to avoid security risks.

Technology acceptance theory examines how users come to accept as well as use technology. This theory is based on how the individual's perceptions affect their intentions to use information technology. It is such a degree where a person believes that the use of an information security countermeasures raises them performance and productivity (Tamilmani *et al.*, 2021). This theory uses perceived usefulness as well as perceived ease of use to determine the intention of individuals to use a system for serving the mediator of actual use of the system. This particular theory is easier to apply across various research settings. It consists of security factors; in addition, it is used as a mediator with a direct as well as indirect relationship with the factors and also the user's intention to use a single platform (Aldawood and Skinner, 2019). A few studies present the technology acceptance model which is used to evaluate information system acceptance. Khaitan and McCalley (2015) stated that the TAM model is designed for comprehending the causal relationship among external variables of the user's acceptance along with their real-time use of the computer. It is required to understand the user's behaviour through utility of the knowledge along with the user's facility as perceived by the organisation.

In this research study, there are two independent variables: attitude towards cybersecurity countermeasures and security awareness countermeasures. The mediating variable is users' addictive behaviour towards the information security. The dependent variable

is risky cybersecurity behaviour practices. The information security countermeasures are recommended as the practice for protecting the public organisation's data. Most previous research studies found that employees have a low awareness of human behaviour in addition to understanding information security (Li *et al.*, 2019). The conceptual framework in this particular study is conceptualised by protection motivation theory. The theory is used in human behaviour studies which are significant for predicting human behaviour. The critical factors which influence the behaviour of humans towards information security are included. The concepts as well as the variables are derived from the literature review. It captures the underlying principles of the theories which are required to investigate the research study.

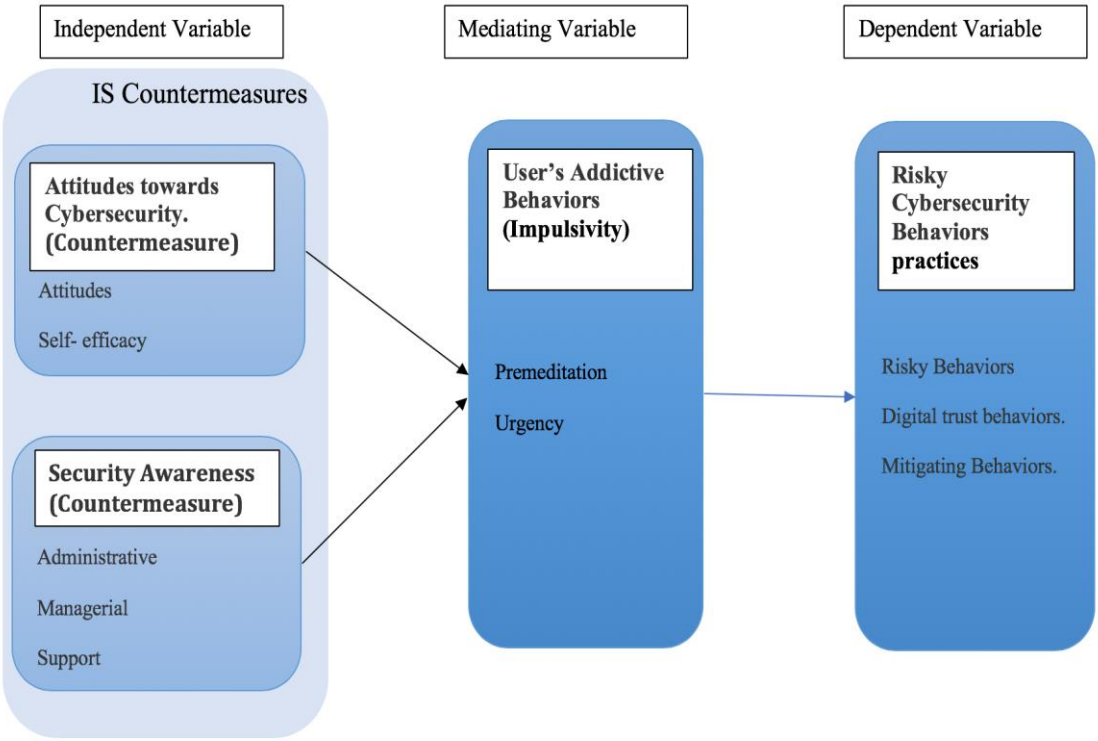


Figure 3. 2: Conceptual framework of the research study
(Source: Created by author)

The research study is based on six hypotheses: Hypothesis 1: Attitudes towards cybersecurity countermeasures are positively related to the risky cybersecurity behaviours practices. Hypothesis 2: Security awareness countermeasures are positively related to the risky cybersecurity behaviour practices. Hypothesis 3: Users' addictive behaviours are positively related to the risky cybersecurity behaviour practices. Hypothesis 4: Attitudes towards cybersecurity countermeasures are positively related to the users' addictive behaviours. Hypothesis 5: Users' addictive behaviours are positively mediating between the risky cybersecurity behaviour practices and information security countermeasures. Hypothesis 6: Security awareness countermeasures are positively related to the users' addictive behaviours (Hadlington, 2017).

The information security principles are also used to lessen the human errors to avoid the connected risks. Human behaviour has a higher impact on success along with failure in securing and protecting information (Wu, 2020). Human-related resources are responsible for making use of both physical and natural resources in order to transform traditional behaviour into modern behaviour (Safa *et al*., 2018). Differences in behaviour development provide a huge reflection on the quality of the human resources. The term managing of human resources encompasses various ideas. Most of the time, the success of a public organisation is based on the human resources who lead and motivate as well as encourage teamwork.

3.4 Conclusion

In summary, the conceptual framework is synthesised from results of the research investigation which argues that the strategic analysis deliberately includes information security. The research approaches in this thesis suggested that there are limitations to the conducted

investigations as well as the direction of the study. Analysing of the human behaviour theories helps to identify the human-related factors which become risks for information security. The human factors play a key role in information security. They have a high impact on information security as the human factors used to analyse and influence the information security management system. The organisation is not focused on human factors with technological competency. The human factors are dependent on the individual's characteristics, which have an impact on the information system management. The IT security arrangement is such a model for a hierarchical culture where the values and methods are driven from the representative way to deal with the data. This particular research also influences as well as evaluates information security management systems.

CHAPTER 4: RESEARCH METHODOLOGY

4.1 Introduction

The research methodology is the technique or approach that is used to conduct the research (Kumar, 2018). There are different research methodology techniques that can be used, and the choice of a research methodology depends on the type of research and the research question (Taherdoost, 2016). According to Taherdoost (2016), some of the most widely used methodologies are: (1) questionnaires; in this methodology, questionnaires are administered to a research community. It can be done either through physical questionnaire forms or online. The sample community should be selected with no favouritism. (2) Interviews; this is where the research population is directly interviewed on the selected topic. (3) Observation; in this methodology, the researcher observes the various elements of the research topic in order to understand the exact state. (4) Experimental; some researches require an experimental methodology where samples of the research population are analysed in the lab. Experimental methodology also includes taking measurements. (5) Literature survey is also a research methodology used to obtain data from secondary sources. In some cases, it is important to use more than one research methodology in some studies.

Methodology also involves the data collection approaches, how the data are analysed, recorded and stored for future reference. The approaches in which these aspects are handled are very important as they ensure the research is systematic and has covered every relevant sector (Taherdoost, 2016). The success of the research mainly depends on the methodology. There is a high chance of getting the wrong impression of the research topic if the methodology is poorly conducted.

The purpose of this chapter is to describe the research methodology which is used in this thesis. There are two sections, which describe the research purpose along with research approaches (Clark and Creswell, 2014). At end of this particular chapter, the research data are gathered and analysed using the described methods. The purpose of this thesis is to identify the proper countermeasures in information security that the public organisation uses to minimise and mitigate the internal threats in the UAE. The researcher will be able to understand the information security issues along with the countermeasures (Fletcher, 2016). The knowledge related to the internal threats as well as security countermeasures is being affected by the human factors which help to choose the proper control mechanisms and reduce the level of risks and mitigate the impacts. Flick (2015) determined that the research questions are required and considered as an important part to review the existing literature. The main objective of the research methodology is to identify as well as justify the possible methods, data collection methods, research sample and questionnaire using an online survey. This particular section presents as well as discusses the primary methods used in order to answer the research questions. A literature survey is performed to review the related literature (Humphries, 2017). It is required to develop the initial framework of this research study as well as the benefits from research which is related to the selected research topic to cover the research objectives.

4.2 Research Philosophy

Research philosophy is the belief where the data about the phenomenon are gathered, analysed and utilized (Dougherty, Slevc and Grand, 2019). Before identifying the research philosophy to use, one has to be aware of the various philosophies and be able to formulate one's own beliefs and assumptions (Edson, Henning and Sankaran, 2016). One has to define one's research strategy by use of a 'research onion'. According to the research onion, the

outermost layer is the one to be occupied by the identification of the research philosophy. This means that the first step in a research methodology should be to identify the research philosophy to be used. Assumptions about the nature and source of knowledge define each phase of the research process. The key assumptions of the researcher are reflected in the research philosophy (Webster, 2017). The strategy for the research is based on the researcher's assumptions. The type of research philosophy depends on the scope and purpose of the research (Webster, 2017).

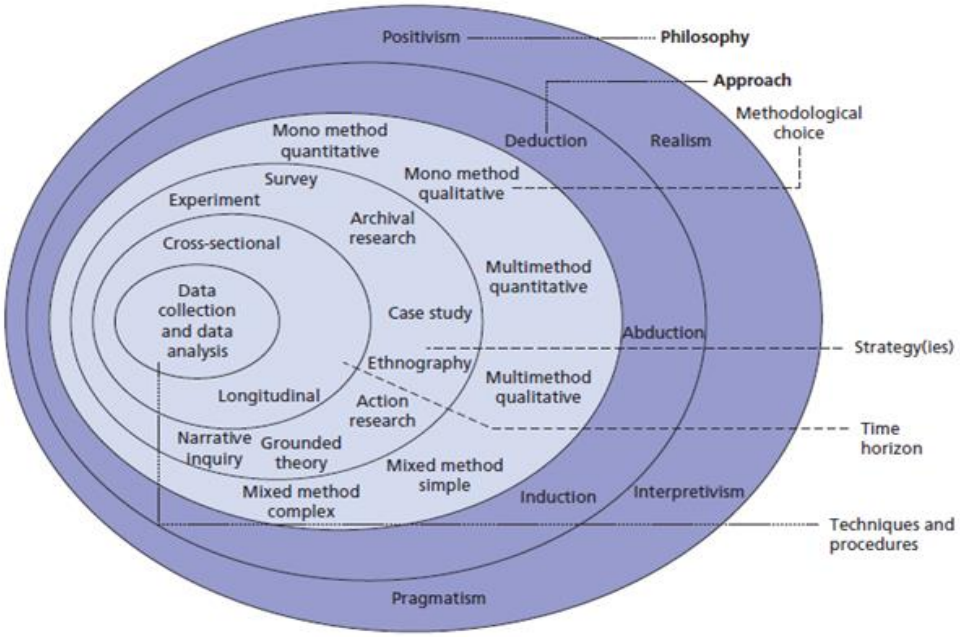


Figure 4.1: Research onion
Source: (Sahay, 2016)

Lewis (2015) expressed that examination rationality encourages the researcher to obtain some data identified with the chosen enquiry about the theme and space being contemplated. It additionally adds different measurements for the directed research to think about. Matthews and Ross (2014) intimated that the determination of appropriate logic ensures that the speculations and ideas are accessible to a specialist to use the productivity of this particular research. The theory enables the specialist to lead the examination in a legitimate way. It deals with sources

and nature as well as the development of the knowledge. Most people will tend to think that the aspect of knowledge creation is so deep that it can rarely be achieved. This is however not the case. The process of creating and completing the thesis actually leads to the acquisition of new knowledge. During the research, the researcher is involved in collecting both primary and secondary data, and technical analysis of the collected data in order to obtain answers to the formulated research questions and come up with conclusive answers (Kogut *et al.*, 2020). By obtaining the answers, the research gains new knowledge.

McCusker and Gunaydin (2015) argued that a research philosophy addresses and involves awareness as well as formulating the beliefs along with assumptions. There are four types of research philosophy: positivism, interpretivism and realism. Positivism is highly structured, using larger samples along with the measurement of the collected data and information. Interpretivism uses smaller samples, which provide an in-depth analysis of the research study (Neuman and Robson, 2014). It investigates collected data. Realism is the method that is chosen to fit with the subject.

Table 4. 1: Showing the structures of different research philosophies
(Source: Jeeragal, 2018)

	Pragmatism	**Interpretivism**	**Realism**	**Positivism**
Common methods for collecting data	Multiple data collection methods. Both quantitative and qualitative.	Deep analysis is done to small samples. It involves investigations and is qualitative in nature.	The data collection method should exactly fit the research topic. It can be both qualitative and quantitative.	It is highly structured. Large samples are analysed through quantitative methods and measurement. However, in some cases qualitative analysis can be done.

Practical implications determine the research philosophy to be used. There is a big difference in terms of philosophies for studies that are based on numbers and facts and those that are based on quality; for example, the analysis of how organisational approaches influence employees' behaviours in combating cyber-crimes. For a long time, many people have debated the choice between interpretivist and positivist research philosophies or the qualitative and quantitative approaches. However, in the last decade, a lot of interest has been shifted to realism and pragmatism research philosophies (Jeeragal, 2018).

Justification for the chosen research philosophy

In this particular study, positivism is used as the research philosophy. Positivism is a belief that is based on objective reality and is described from an objective viewpoint (Ryan, 2018). According to Ryan (2018), positivism philosophy believes that experiments, observations and mathematical proofs can be used to verify whatever exists. As this study was observing the behaviours of participants accessing the organisation's network through multiple answers to specific questions and there were no wrong or right answers, positivism was the best fit. Positivism categorises the statements or beliefs as either true, false or meaningless. Meaningless beliefs are ones which are neither true nor false. It is not possible to use positivistic means to test such statements. Positivism contends that phenomena which are isolated in addition to the observations are repeatable. It involves manipulation of reality with the variations into a single independent variable for identifying the regularities that form relationships between constituent elements of the social world. Panneerselvam (2014) stated that positivism has a rich historical tradition.

In this thesis, the various organisational policies, strategies and beliefs were tested through the positivism philosophy to identify the influence of the employees' behaviour on cybersecurity (Žukauskas *et al.*, 2018). The philosophy was also used to test whether the relationship between peer employees can influence their reaction towards responding to information security countermeasures.

4.3 Research Approach

Deductive, abductive and inductive research approaches are three different types of research approach. A deductive research approach is used when the hypotheses are formulated

and the research is required to reject or confirm those hypotheses; whilst the abductive research approach is used when the thesis is devoted to an explanation of an observation that has not been completed at the start of the study. An inductive research approach is helpful if there is no hypothesis, and the research starts with only an aim, objective and research questions. A research approach is the plan and procedure of how the research will be conducted (Tuffour, 2017). The approach is carried out in steps ranging from broad assumptions to comprehensive data collection, analysis and interpretation methods (quantitative and qualitative approaches) (Queirós *et al.*, 2017). The complexity of the procedure depends on the nature of the problem in question. In this thesis, the problem being addressed requires qualitative analysis of the various factors. The first step of the research was to identify the population to be used for the research. This involves the online community since the research was conducted through an online survey. Once the population was identified and selected, a questionnaire was formulated with questions corresponding to the research objectives, and then administered to the identified population. Step three was to analyse the responses obtained in order to get the finest details possible. The analysis comprised tables, graphs and comparison charts. As there was a shortage of time in this research study, depth analysis for larger samples was unattainable.

Justification for the chosen research approach

A deductive approach was chosen for this particular research study as this research is based on six hypotheses. This approach is one which is associated with scientific investigations (Matthews and Ross, 2014). The researcher reads the existing theories of the research phenomenon where the research hypothesis is tested from the theories. This particular approach begins with the hypothesis which emphasises causality. It also designs the research strategy for testing the research hypothesis. It is explained by means of the research hypotheses that are

derived from the propositions of existing theory. Viswanadham (2017) stated that a deductive approach is concerned with the deduction of conclusions in order to find the research patterns with them.

As the name suggests, this approach deducts false theories from the list of theories explaining a certain phenomenon. Scientific methods are used to perform the elimination so that only true beliefs are identified. This research addresses various beliefs about information security countermeasures in organisations within the UAE (Alhosani, *et al*., 2019). The beliefs tend to explain the relationship between information security countermeasures and the risky behaviour practices of employees towards enforcing the information security policies. With a deductive approach, the positive beliefs are isolated from the negative ones.

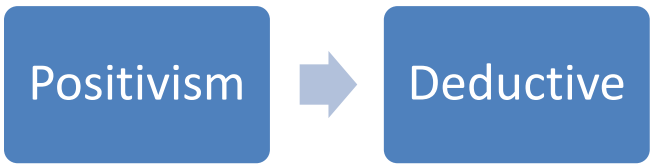


Figure 4. 2: Approach selection
(Source: Created by author)

4.4 Research Design

A research design is the collection of procedures and methods that are used to collect and analyse the measures of the objectives specified in the research question (Leavy, 2017). The design is the framework that is used to enable the researcher to obtain answers for the formulated research questions. The design of the research questions defines the type (experimental, correlational or survey) and subtypes of the research design to be used (Leavy, 2017). The common design of scientific research involves data collection, and measurement and analysis of the collected data. In the research design phase, the tools to be used in collecting the data are

identified. The researcher also learns how to use the tools they have identified. When an appropriate research design is used in the research, biasness in the collected data is minimised, thus increasing trust in the data.

For a research design to be considered effective, it must produce the least margin for errors (Leavy, 2017). Such a design must have the following elements:

a) It should contain the exact research questions.
b) It must define the techniques that will be used in collecting and analysing the research.
c) The method used to analyse the research details must be explained.
d) It must explain the research methodology to be used.
e) It must define the timeline in which the research will be conducted.
f) The environment for the research must be defined.

Clark and Creswell (2014) discussed that utilization of a research configuration creates a system to gather, and in addition break down, the information. Appropriate utilization of a research plan strategy uncovers the examples alongside the sources of information. There are three types of research design: descriptive, exploratory and explanatory. An exploratory research design provides insights into as well as comprehension of the research issues along with situations (Flick, 2015). This type of research is conducted because the issues are not clearly defined. It helps to determine the proper research design and method of data collection along with the selection of research subjects. Descriptive research is defined as statistical research, which describes the data as well as the characteristics related to the population along with the studied phenomenon (Humphries, 2017). It answers the research questions and, based on one of the research designs for the present study, it is required to gauge different projects

which are specific to the risks which impact the projects and understand the dynamics of organisations' principle on the projects (Clark and Creswell, 2014). An explanatory research design is conducted for problems that are not well researched, and provides a better research model.

The choice of the research design depends on the research problem being addressed and not the other way around (Leavy, 2017). A well-defined research design should have the following characteristics:

i) Neutrality; before conducting the research, the researcher normally comes up with assumptions concerning the data expected to be collected. The projected results should be neutral and free from any biasness.

ii) Reliability; the design should be able to produce similar results when the research is repeated multiple times. Guidelines on how to generate the research questions should be provided by the research design.

iii) Validity; although there are many measuring tools available, the researcher should adopt methods that will help them gauge the results obtained in relation to the research objectives. If the result can be gauged, then the design is considered to be valid.

iv) Generalization; the design should focus on the general research population and not just a few selected samples. This means that different parts of the population should provide the same result when tested.

Justification for the chosen research design

A descriptive research design is adopted due to the nature of this research study. It is a research design which is used to depict the participants in the proper way. It is about describing the people that take part in the research study. There are three procedures the researcher can use in a descriptive research study: observational, case study and survey. McCusker and Gunaydin (2015) discussed that this type of research design collects information from the target population in order to describe the preferences and characteristics as well as practices. An example of a descriptive survey is using a questionnaire to solicit the information from the participants based on the selected research topic. The descriptive statistical techniques consist of three purposes: describe the relationships among the variables, describe the variables and describe the distributions (Matthews and Ross, 2014). A descriptive design is accurate for this particular study as it examines the mediating effect on the users' addictive behaviours on the relationship between information security countermeasures and risky cybersecurity behaviour practices.

Figure4.3: Design selection
(Source: Created by author)

4.5 Data Collection Process

The process of collecting research data ranges from identifying the research population and collecting the actual data, to analysing the data, and interpreting and presenting it to the relevant audiences (Stieglitz *et al.*, 2018). This is the most important phase of the research

process. Therefore, it should be carried out with the utmost care and accuracy in order to obtain the desired results.

While conducting the research, the information is being accounted as the most critical data which is required for this specific investigation. Sensitive information is valuable to provide knowledge relating to the selected topic. Matthews and Ross (2014) indicated that use of the best possible data is significant to the investigation resource to convey the exactness of information while maintaining the research standard. At the time of collecting the survey data, it is necessary to verify the research settings which are discussed in Chapter 3 in the conceptual research framework. The tools as well as techniques of data collection help to collect the required data (Clark and Creswell, 2014). With the help of the data collection tools, it is necessary to transfer facts from the field into data as well as tables. In the process of data collection, there is the possibility that some of the data information will be lost (McCusker and Gunaydin, 2015). Proper information is being collected as well as utilized for the purpose of data analysis as well as interpretation.

4.5.1 Data Sources

In this research study, the data collection tool or instrument used for collecting data is an online survey questionnaire. It is the main instrument used for a survey research study. A set of standardised questions on the selected research topic –which is examining the mediating effect of the users' addictive behaviours on the relationships between information security countermeasures and risky cybersecurity practices– is prepared to collect data from the individuals. The questionnaire is designed so that statistical analysis of the collected responses can be performed (Matthews and Ross, 2014). At first, the researcher prepared the survey questions based on the selected research topic. While preparing the survey questions, the

researcher should ensure that there is no influence on the received responses. The question design should reflect the aims of this research study as well as the objectives. Then, the researcher shared the survey link with the target sample population via email and WhatsApp, to obtain their responses. After obtaining their responses, the researcher collected raw data in SPSS format. The collected data are analysed the various views of the group of people from the selected population are interpreted (Humphries, 2017). The variables for the questions are taken from the identified research hypotheses, which are considered as the main data set from the survey instruments. At the time of data interpretation, the data are analysed in the form of pie charts and tables.

4.5.2 Data Analysis

Data analysis is the process of inspecting, critically analysing and transforming the collected data to meaningful information (Mi *et al.*, 2017). The obtained information is used to come up with a conclusive report on the research questions. The purpose of analysing the data is to enable the researcher to create an informed conclusion which will help them to make precise decisions. Data analysis is performed to create a visual representation of the collected data. In other words, the purpose of analysing the data is to generate graphs, charts and tables which show the trends of the aspects being researched. The collected data cannot be interpreted if it is not analysed. The process of analysing the data can be carried out through a qualitative approach or a quantitative approach. In qualitative analysis, fine details are sorted from the data to enable the researcher to come up with accurate conclusive information. On the other hand, quantitative analysis is where a general view of the research topic is created (Jacobi *et al.*, 2016).

A quantitative approach is used in this particular study. The data from the research survey, such as regarding the UAE's public organisation services, are required to provide the

raw data used to recognise as well as explore the information security culture. They also explore the challenges to promote as well as enhance the information security culture. McCusker and Gunaydin (2015) stated that the data collection process aims to provide raw data as well as information which helps to develop the information security model culture. This particular stage is involved to distribute the structured questionnaire to the organisation. It involves the conduction of an in-depth analysis of the key personnel's feedback. The key personnel give their opinions as well as attitudes towards the information security culture along with the factors influencing the information security culture. The main purpose of the questionnaire method is to explore as well as identify the culture and help with the development of an initial information security culture model (Simonsohn *et al.*, 2017).

The purpose of quantitative analysis is referred to emergent of the research methodology developments with systematic integration. The purpose of this data analysis is expanding and strengthening the conclusions of the research study, and therefore contribute to the published literature. The quantitative analysis method contributes to answering the research questions (Matthews and Ross, 2014). The core characteristics of the quantitative data analysis method are:

I. Collection and analysis of quantitative data such as closed-ended questions (Panneerselvam, 2014).
II. Ensuring a specific sample size for the quantitative analysis of the study.
III. Integration of data by means of data collection and analysis
IV. Framing of theoretical models of the research study to understand the various perceptions of various authors on the relationship between human behaviour and information security (Simonsohn *et al.*, 2017).

Quantitative data analysis is performed by considering the respondents from the UAE's public organisation and using a survey questionnaire data instrument. The value of raw data is considered in the form of numerical values where each piece of data has a unique numerical value linked with the research study. It is collected for performing statistical analysis by means of a survey across the sample population.

There are various types of data analysis which can be performed (Mi *et al.*, 2017). The analysis types are text analysis, statistical analysis, diagnostic analysis, prescriptive analysis and predictive analysis. The analysis conducted in this thesis is text analysis. This type of analysis creates a pattern of traits from the sample results that were obtained. In this context, the data were analysed to give a logical pattern of how information security countermeasures influence employees' risky behaviours towards managing cybersecurity.

Figure 4. 4: Research approach
(Source: Created by author)

4.5.3 Data Interpretation

The last phase of data collection is the interpretation of the analysed data (Fetters and Molina-Azorin, 2019). This is the phase in which the researcher comes up with a conclusion on the research they were undertaking. The purpose of data interpretation is to find out the outcome of the research in relation to the research question. In this thesis, the researcher developed a conclusive report on the findings of the research (Fetters and Molina-Azorin, 2019). Data interpretation can be conducted through comprehensive reports, tables, charts or graphs. At this point, the findings can be presented to the relevant audience for decision making. The conclusion

can be positive or negative to the research question. In this case, it can either agree or disagree that the information security countermeasures can truly influence the employees' risky behaviours. Sometimes, data interpretation is referred to as data visualization since the data are represented in the form of graphics (Fetters and Molina-Azorin, 2019).

4.5.4 Data Presentation

Once all the data have been analysed and interpreted and reports generated, the reports are made available to the target organisation (Gray, 2019). The organisation uses the reports to make informed business decisions on the problem being addressed. The reports can be submitted directly to the specific organisation or made available online for multiple organisations. The purpose of this research was to identify the relationship between organisations' information security countermeasures and minimising risky behaviour practices. Therefore, the results of the research can be presented to different organisations. If the research findings are not presented but remain with the researcher, then the research can be considered to be of no use (Viswanadham, 2018).

4.6 Sample and Sampling Method

The sample is the total population involved in this research study. It is considered for studying human behaviour regarding information security. In this study, the sample is small in number and can suit the criteria for the investigation (Simonsohn *et al.*, 2017). Sampling method refers to observations which are selected from the sample population selected for performing the research survey. The sampling method used for this research study is simple random probability sampling, where there are no specific criteria chosen for selecting the sample population. This type of sampling method is selected to demonstrate specific traits which may exist in the target sample population. It is used when the researcher is aiming to perform a

quantitative study. It benefits the researcher when there are limited costs and time to carry out the research study.

The employees of the UAE's public organisation services are considered as the sample for this work. By means of an online questionnaire, the employees were asked to participate in this investigation work (McCusker and Gunaydin, 2015). The sample size for performing this quantitative research study is 124 employees, selected on a random basis. This is because the percentage of employees in the UAE's public sector is 3.8% of the total employees in the country. There are 7,219,000 employees across the UAE in all sectors and 274,322federal employees in the public sector, which is the study population size (*Workforce in the UAE - The Official Portal of the UAE Government*, 2021). The research accepts 8% as the margin of error, 90% as the confidence level and 0.5 as the standard deviation.

The following equation was used to determine the sample size:

(z- Score) ^ 2 * StdDev * (1- StdDev) / (Margin error) ^ 2. (Daniel and Cross, 2018)

(1, 65) ^ 2 * 0.5 * 0.5 / (0.08) ^ 2=106

4.7 Validation and Verification

A research design reduces the possibility of error in the investigation study as the researcher should focus on two main research design factors, validation and verification. Verification is a process to check that the research study meets the research aim and validation is a process to check whether the research specification meets the research requirements (Taylor *et al*., 2015).

Table 4. 2: Validation and verification of the research

Area of concern	**Research stage**	**Solutions to increase the validation and verification in the research study**
Respondents from UAE public organisation	Quantitative data research	Limitations of the theoretical framework are to be discussed with the IT professionals for data validation. For validating the proposed theoretical framework of this investigation study, the IT professionals provided responses based on their viewpoints.
Empirical work findings	Quantitative data research	Testing of the research hypothesis through using survey research will allow the researcher to compare results of quantitative research. Various perceptions of the author and research participants will enhance the validation of the research data (Vaioleti, 2006).

In the research that was conducted, validation was done by ensuring the research was conducted according to the objectives of the research defined in the research design (Magazzeni, Mcburney and Nash, 2017). The objectives of the research were the guidelines used to carry out the research. As such, it can be concluded that the research was conducted accordingly. The conclusion reports generated were used to verify the validity of the research. Since the outcomes of the research were in line with the research questions and objectives, then the research can be considered to be valid.

4.8 Ethical Considerations

The current research study is liable to moral issues. While conducting the information gathering alongside information examination, the researcher has to think about various issues to ensure that the exploration meets the required moral standards. The researcher is required to distinguish the contrasts between wrong and right arrangements of the human practices leading this specific investigation. The participants are educated about the purpose of the research destinations, as they are assured that their information is kept secret and also is only utilized for scholarly purposes and for just this specific research. The information is being put away and being secured by strict codes of morals. There are restriction and lawful access to the data. The researcher guarantees that the information and in addition data utilized in this examination consider are not utilized industrially. The researcher maintains a moral code to provide an expected standard for the examination (Simonsohn *et al*., 2017). The secondary information is being referred to by utilization of Harvard referencing.

4.9 Summary

In summary, the collected data are analysed to provide results which are used to support the research as well as to present the main findings with regard to the information security cultural dimensions. The chapter has identified as well as justified the research methodology, data collection methods, research sample and questionnaire. The next charter provides the research finding, and includes the tools for analysing the data collected from the questionnaire. This specific part depicts the different research strategy apparatuses which are utilized to better examine the chosen subject. The researcher has attempted to adjust the idea of this examination to think about the variable for different research procedures to such an extent that the best research strategies are to be utilized. The examination devices are appropriate for dissecting the

ideas regarding examining the mediating effect of the users' addictive behaviours on the relationships between information security countermeasures and risky cybersecurity practices. Essential and in addition secondary information accumulation strategies enable a better examination, with the goal that the examiner should better comprehend the chosen research topic. The entire research study is mainly based on the primary data collection method where all the data are collected through the use of an online survey, and the participants – those who are interested in the study – are only considered to provide their feedback based on the questionnaire. The data collection process is aimed at providing raw data as well as information which help to develop the information security model culture. This particular stage is involved to distribute the structured questionnaire to the organisation.

CHAPTER 5: RESEARCH FINDINGS

5.1 Introduction

According to Lewis (2016), data analysis is one of the most significant chapters of a thesis as it helps to understand what the collected data interpret. The researcher stated that human errors in the data collection procedure in a research paper can be addressed in the analysis chapter. The researcher also helped in understanding that the analysis which is conducted in this chapter helps in determining the conclusive statements in the ensuing chapter of the thesis. The coding of the responses gathered from the participants is conducted by the analyst in this chapter of a thesis. This chapter starts with the descriptive statistics, which will be followed by demographics, Common Method Variance, Normality, and Frequency Analysis. The discussions of the methods of analysing the collected data are provided in this chapter of the thesis as well. The common patterns of the responses coming from the primary data sources can be categorised using this chapter (George and Mallery, 2016). This chapter will be very useful to critically analyse the data collected from the primary sources. The critical analysis of the data will be conducted using the research questions created by the researcher in the first chapter.

5.2 Data Analysis Types and Tools

Most research papers have two different categories of data analysis procedures, qualitative data analysis and quantitative data analysis (Shields, 2017). There are drawbacks and advantages related to each method. The data which do not have any sort of numerical value but which are full of theories and models are evaluated on the basis of qualitative analysis and the data which have numerical value are evaluated on the basis of the quantitative technique (Awang *et al.*, 2016). Quantitative data are considered by the researcher in this study.

Analysis of research papers deploys diverse categories of tools to analyse the data which are gathered from primary foundations such as R programming, which is a type of analytic tool, tableau, which is much useful to create a data visualization, dashboards and data maps (Disman, Ali and Education, 2017). Programming languages like Python are also very significant to analyse diverse categories of raw data sets. Data manipulation can be performed with the help of another programming language such as SaS, which was developed in 1966. Large-scale processing of data can also be performed using a data processing engine known as Apache Spark (Lajoie, 2016). Microsoft Excel is also very useful to summarise any type of raw data with the help of pivot tables. Rapid Miner is one of the most popular data science platforms and is very useful to analyse any type of real-time data. The predictive analytics capabilities of Rapid Miner are increasing due to the incorporation of machine-learning algorithms (Bloomberg and Volpe, 2018). Knime is also considered as one of the biggest data tools which is very useful to interpret any data using visual programming (Lewis, 2016). Splunk is a statistical tool which is very useful to analyse any type of text-based data (Disman, Ali and Barliana, 2017). The other essential data analysis tool which is often used by academic students is Statistical Package for Social Sciences (SPSS); this tool is one of IBM's most popular products and is very useful to analyse any type of data organised as a database.

The data analysis tool which has been selected in this thesis is SPSS; this tool imports data from other data sources and then analyses those data with the help of graphical illustrations and figures (Friese, 2019). There are drawbacks as well as benefits associated with the deployment of this software. Research analysts can add variables as per the paper's hypothesis using this tool. This tool is also much useful to assign different properties to the research variables (Disman, Ali and Barliana, 2017). This software is much more reliable in terms of data

analysis than the other data analysis tools which were identified in the previous part of this chapter. Creation of the output file from the data is one of the advantages related to the use of this tool as well (Paulus and Bennett, 2017). Frequency distribution of any type of data set can be maintained using this statistical tool as well. This tool is also very useful to draw graphs directly from the SPSS data. All the statistical transformations of the data can be maintained using SPSS (Lewis, 2016). There are other advantages related to this statistical tool as well, such as the control over the data, and a wide range of graphs and charts can be generated using this statistical tool.

On the other hand, there are a few limitations associated with SPSS as well, such as the quality of the graphics which are automatically generated from this software. Although these graphics can be used in academic assignments, they cannot be used in any corporate commercial establishments (Samuels, 2019). This software is also very expensive as compared with all the other statistical tools which are used for analysing raw data. Documentation of the algorithm is very complex and very challenging to decide on.

Descriptive statistics are an integral part of the data analysis method, and were performed using SPSS (Wang and Zhang, 2019). Summarizing the given data set is one of the prime functionalities of descriptive statistics, and the measures of the central tendency and variability are an integral part of descriptive statistics (Green and Salkind, 2016). There are diverse categories of descriptive statistics as well, such as the measure of the frequency of the data, the analysing of the central tendency of the data, measures of data variation, measures of data positioning, etc.

Primary data for this thesis were collected from participants from different cultural backgrounds (Bhatti *et al.*, 2019). A detailed survey questionnaire was created by the researcher prior to the start of the data collection procedure (Hall, Hume and Tazzyman, 2016). All the participants of this online survey work in public services across the United Arab Emirates. A simple random sampling method was considered as the sampling method to collect the primary raw data. The sample size of the population is 124, and each one of is the sample was made aware of the topic and the purpose of this research.

5.3 Data Collection Analysis

The questionnaire created by the researcher has two sub-sections, the demographic questions and the questions which are directly associated with the research hypotheses. The different categories of demographic questions in the survey questionnaire are gender, highest educational qualification, availability of any sort of IT related qualification, and questions about IT related training, years working in the current position in the organisation, designation of the participants, and type of work performed in the workplace by these participants. Thus, all the measurable characteristics of every participant can be successfully evaluated using these demographic questions (Józsa and Morgan, 2017). The structure and the distribution of the population can also be understood using these demographic questions.

The degree to which the participants disagree or agree with a statement can be measured using a Likert scale (George and Mallery, 2016). The Likert scale data can be analysed as interval data; the intensity of the attitude of the participants of a survey can be understood using this scale. The data collected from the participants can be easily interpreted using this scale, which is the most important reason for its selection. Using this scale, it is much easier to draw conclusions about any issues or problems for which the research is being conducted (Awang,

Afthanorhan and Mamat, 2016). Results and graphs can be easily generated using this scale; at the same time, it can be said that this scale was much easier for the researcher to construct. On the other hand, there are a few drawbacks associated with the use of this scale as well; one of the prime drawbacks is that it judges a question on the basis of the total score obtained from every sample of the population.

5.3.1 Sample Size

It is defined as the term which indicates the number of subjects in a sample; the general population of a specific study can be understood in the first place using the sample size of the population. The number of individual samples in a survey is also termed as the sample size of the population in the thesis. The sample size of the population in this thesis is 124. Individuals come from a different cultural background; hence, the validity of this research will be very important in identifying the ways to manage the employees' behaviour in multi-cultural organisation.

5.3.2 Gender

The orientation of the samples can be successfully understood from this demographic question. Out of the 124 individuals who took part in this data collection method, 80 of them are males and 28 of them are females, and the rest 16 of them have not stated their gender. Thus, of those who did, 64.5% are male and the rest (22.6%) are females. The valid percentage of females is 25.93% and the valid percentage of males is 74.07%. Thus, based on the above, it can be understood that most of the population of this sample are males. The gender biasedness of the survey is shown in the following diagram.

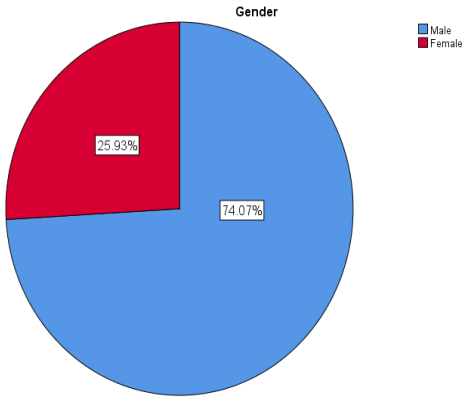


Figure 5. 1: Gender of the participants

5.3.3 Education

This demographic question will be very significant to understand the highest educational achievement of the participants who have taken part in the online survey. Out of the total 124 participants, six of them do not have even a high school degree, nine of them only have a high school qualification, nine of them have their diploma certificate, 44 of them have a bachelor's degree and 38 of them have successfully completed their master's degree; however, 18 participants have not stated their educational qualification. Thus, it can be said that most of the sample are very well educated and have the minimum qualifications required to take part in this online survey. The following diagram is be very significant in understanding the distribution of the participants' educational history.

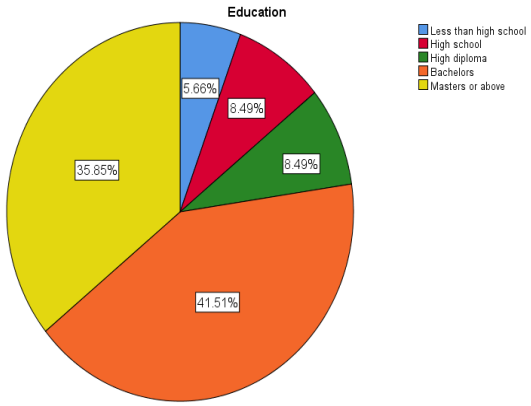


Figure 5. 2: Education of the participants

5.3.4 Training to UG/PG level

This demographic question will be very useful to understand whether the survey participants have any IT-related qualification at any level. Out of the 124 participants, 57.94% of them have IT-related educational qualifications, whilst 42.06% of them do not. Thus, this question was very useful to understand the fundamental IT knowledge of the participants who have been a part of this online data collection procedure. The distribution of these results is provided in the below figure.

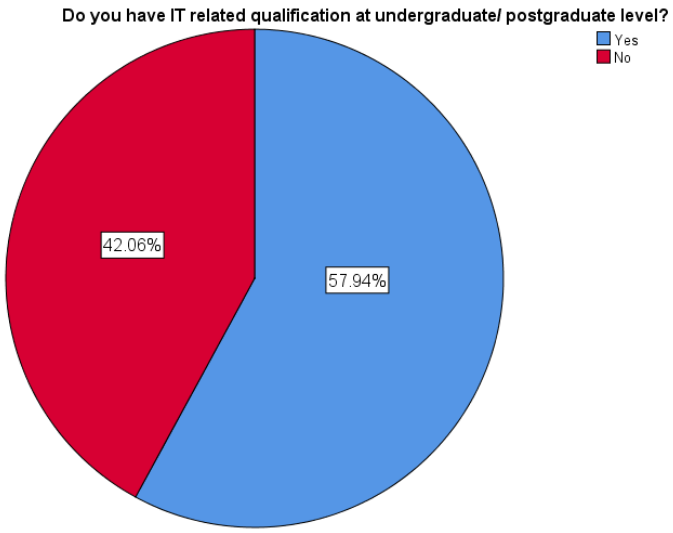


Figure 5. 3: Qualification of the participants

5.3.5 IT-Related Training Courses

This demographic question will be very useful to understand the basic IT knowledge of the participants who have stated their opinion in the online survey. Out of the 124 respondents, 22.6 % of them have not gone through any type of IT-related training course, 18.69% of them have a minimum of one training course, 31.78% of them have been a part of two to five training courses and 20.36% of them have been through more than five training courses. Thus, out of the 124, 28 of them have not gone through any IT-related training courses and the rest have.

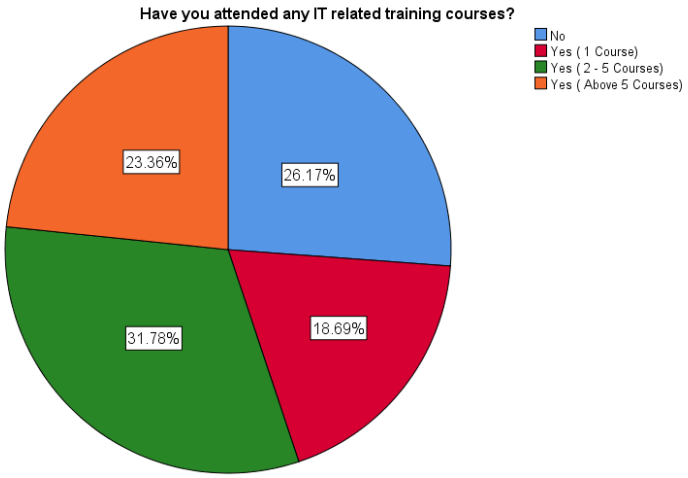


Figure 5. 4: Attendance on IT-related training courses

5.3.6 Years Working in Current Position

This demographic question is very significant for the readers of this thesis to comprehend the experience of all the participants, who have worked for several years in their existing position. Out of the 124 participants, 20.19% of them have over 20 years of experience working in their current position, 23.08% of them have between 11- and 20-years' experience, 25.96% of them have six to 10 years' experience and the rest (30.77%) have one to five years of work experience in the current position. Thus, it can be identified that most of the sample population are very experienced in working in the same position over the years.

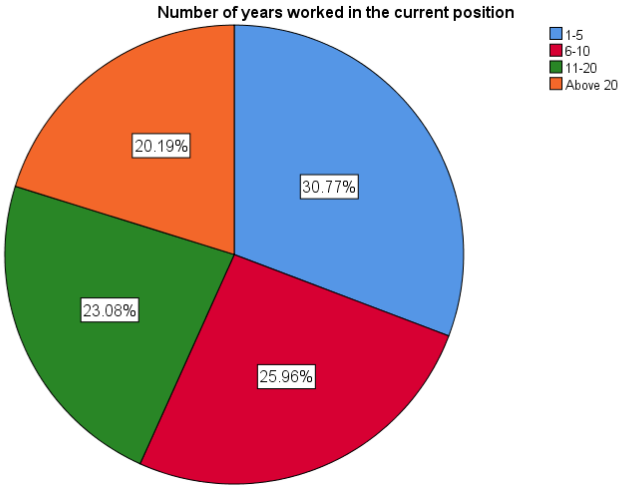


Figure 5. 5: Years in current position

5.3.7 Position Held at Work

The designation of each survey participant can be understood in the first place using this demographic question. Out of the 124 participants, 19 skipped this question, 20% work as supporting staff or in the administrative units, 10.5% work as IT staff, 36.2% work as management staff, and 33.3% of the sample work in other positions. Thus, it can be understood that most of the survey participants work in a managerial role in their respective organisations. The entire distribution of the participants' designations can be successfully understood from the below pictorial presentation as well.

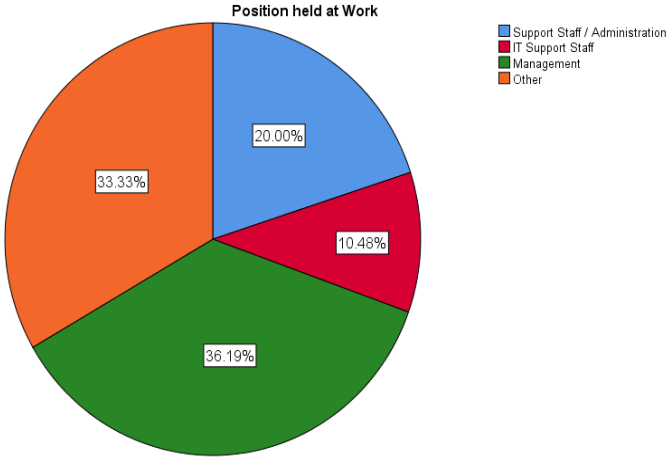


Figure 5. 6: Position held at work

5.3.8 Nature of Task Performed in the Workplace

The nature of the work performed by each of the survey participants can be understood from this demographic question. Data gathered from the population help in understanding that 107 of the participants have stated the nature of their work whereas the other 17 have not stated this. Out of the 124 participants, 11.21% of them work as typing experts, 12.15% of them work as data entry operators, 10.28% of them work as data administrators, 8.41% of them work as communication experts, 3.74% of the population works in a general secretarial role, 6.54% of them work in computer maintenance, another 6.54% of the population works as system development experts or as software programmers, and the rest (41.12%) of the population work in a management role.

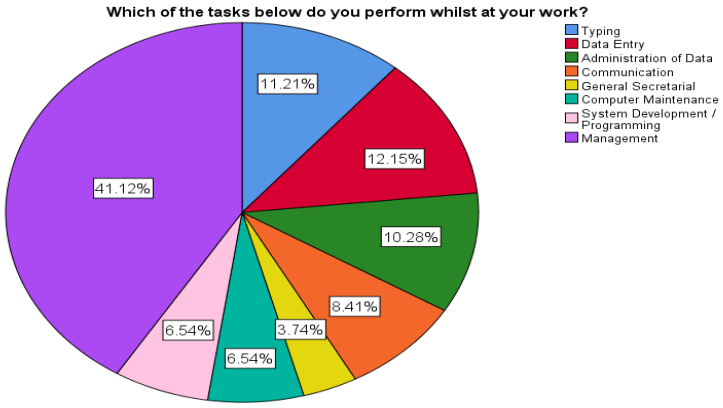


Figure 5. 7: Nature of task

5.3.9 Common Method Variance (CMV)

All the variables of a research paper can be measured in accurate modus using CMV; the biasedness of any data which might influence the research analysis is addressed using this measurement method. This thesis factor will make the most out of Harman's single factor so that the total variance of one of the factors does not exceed 50%. Identifying the common method variance can be done with the help of Harman's single factor as well, and the majority of the covariance among the factors can also be identified using Harman's single factor. The relationship between the variables of this project can also be identified with the help of CMV. The initial Eigenvalues are analysed using the CMV; based on the analysis of all the 124 components of this research, it can be concluded that the first component rotation extraction sum of squared loading is 42%, which is much less than 50%, which is the general standard to identify the biasedness of the instruments which are being used to analyse the collected data. Hence, it can be stated that the instruments do not have any biasedness.

Table 5. 1: Data total variances

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	52.430	42.282	42.282	52.430	42.282	42.282	36.595	29.512	29.512
2	16.435	13.254	55.536	16.435	13.254	55.536	23.925	19.294	48.807
3	4.218	3.401	58.938	4.218	3.401	58.938	4.916	3.965	52.771
4	3.113	2.510	61.448	3.113	2.510	61.448	4.130	3.330	56.102
5	2.752	2.219	63.667	2.752	2.219	63.667	3.546	2.860	58.961
6	2.310	1.863	65.530	2.310	1.863	65.530	3.033	2.446	61.407
7	2.053	1.656	67.186	2.053	1.656	67.186	2.873	2.317	63.724
8	1.935	1.561	68.747	1.935	1.561	68.747	2.660	2.145	65.870
9	1.793	1.446	70.193	1.793	1.446	70.193	2.229	1.798	67.668
10	1.705	1.375	71.568	1.705	1.375	71.568	2.187	1.764	69.431
11	1.673	1.349	72.917	1.673	1.349	72.917	1.923	1.551	70.982
12	1.523	1.228	74.146	1.523	1.228	74.146	1.650	1.331	72.313
13	1.468	1.184	75.330	1.468	1.184	75.330	1.565	1.262	73.575
14	1.362	1.098	76.428	1.362	1.098	76.428	1.560	1.258	74.833
15	1.319	1.064	77.492	1.319	1.064	77.492	1.548	1.249	76.082
16	1.248	1.006	78.498	1.248	1.006	78.498	1.516	1.223	77.304
17	1.205	.972	79.470	1.205	.972	79.470	1.515	1.222	78.526
18	1.113	.898	80.368	1.113	.898	80.368	1.502	1.211	79.737
19	1.064	.858	81.225	1.064	.858	81.225	1.481	1.194	80.931
20	1.010	.815	82.040	1.010	.815	82.040	1.375	1.109	82.040
21	.973	.784	82.825						
22	.948	.764	83.589						
23	.912	.735	84.324						
24	.885	.714	85.038						
25	.864	.697	85.735						

Extraction Method: Principal Component Analysis.

The Eigenvalues of the extracted components can be comprehended from the below pictorial representation.

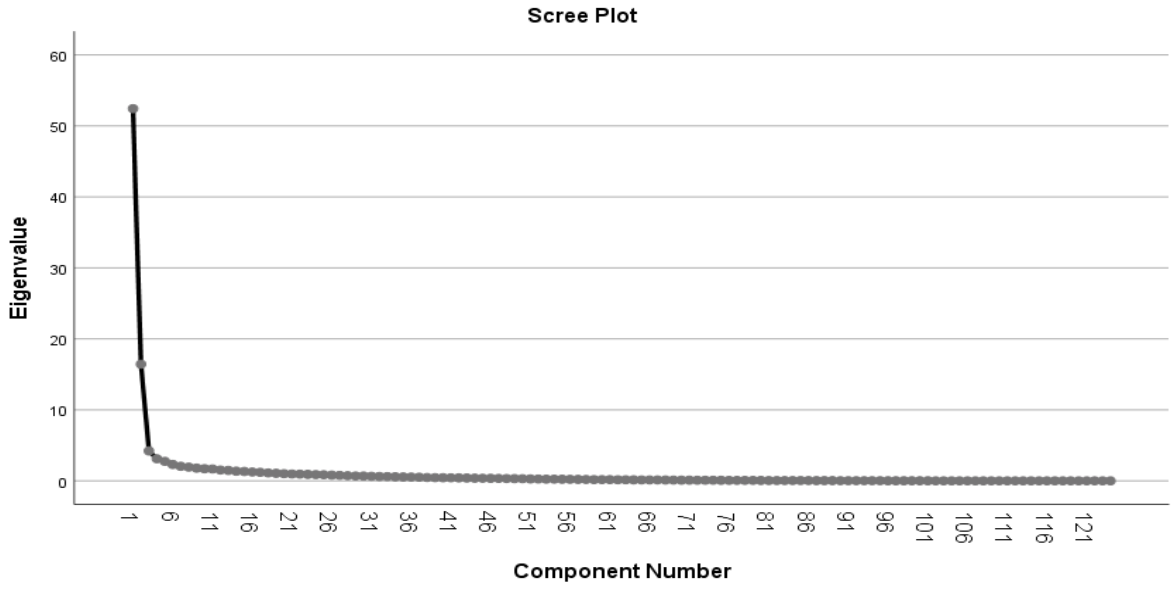


Figure 5. 8: Screen plot for the eigenvalues

5.4 Reliability Analysis

The internal consistency of the collected data can be measured in the first place using the Cronbach's Alpha test. The relationship between each set of components can be identified with the help of this test. Alpha $= \frac{n \times r}{(1+(n-1)) \times r}$ Is the formula where n is the number of components (10); at the same time, the means of co-relation among every dataset is denoted by r. The Cronbach's Alpha score is very essential to understand the consistency of the collected data. If the score of the test is 0.7 or above, then it is considered as a good score and a score above 0.9 is the best. The following table illustrating the reliability test is significant regarding the identification of the reliability score for each component of this research study.

Table 5. 2: Reliability test

No	Components	Number of entered items	Cronbach's Alpha
1	Attitude towards cybersecurity		
1.1	Attitudes	11	0.935

1.2	Self- efficiency	8	0.938
2	Risky cybersecurity behaviours		
2.1	Risky behaviours	18	0.970
2.2	Digital trust behaviours	4	0.907
2.3	Cybersecurity mitigating behaviours	4	0.895
3	Countermeasures (Security awareness)		
3.1	Administrative countermeasures	4	0.895
3.2	Managerial countermeasures	10	0.950
3.3	Support countermeasures	7	0.944
4	Impulsivity (Users' addictive behaviour)		
4.1	Premeditation	13	0.965
4.2	Urgency	8	0.930

5.5 Normality Test for the Dependent and Independent Variables

The normality test of this research study is conducted in the basis of skewness and kurtosis. The procedure for identifying the degree of lopsidedness in a frequency is termed skewness, whereas the procedure for measuring the degree of tailedness in the frequency distribution is commonly termed kurtosis. The acceptance intervals of these concepts are very different from each other. The acceptance levels are either ±1.96 at 0.05 or ±2.58 at 0.01. However, any sort of discrepancy in the acceptance level can have a huge impact in a thesis. The summary of each variable can be understood with the help of the following table:

Table 5. 3: Skewness and kurtosis

NO	Components	N	Skewness		Kurtosis	
		Statistic	Statistic	Std. Error	Statistic	Std. Error
1	Attitude towards cybersecurity					
1.1	Attitudes	124	0.455	0.217	-1.004	0.431
1.2	Self- Efficiency	124	-0.889	0.217	0.9	0.431
2	Risky Cybersecurity Behaviours					
2.1	Risky Behaviours	124	0.438	0.217	-1.158	0.431
2.2	Digital trust behaviours	124	0.054	0.217	-1.159	0.431
2.3	Cybersecurity mitigating Behaviours	124	-1.185	0.217	0.656	0.431
3	Countermeasures (Security Awareness)					
3.1	Administrative Countermeasures	124	-1.387	0.217	1.545	0.431
3.2	Managerial countermeasures	124	-1.23	0.217	1.787	0.431
3.3	Support countermeasures	124	-0.934	0.217	0.083	0.431
4	Impulsivity (Users' Addictive behaviour)					
4.1	Premeditation	124	-1.483	0.217	2.175	0.431
4.2	Urgency	124	-0.93	0.217	0.51	0.431

A normality test such as the Kolmogorov-Smirnov test can be very useful to analyse research with fewer components. Interpretation of the Kolmogorov-Smirnov test has to be performed in an accurate order, whereas the null hypothesis can be conducted with the help of Shapiro-Wilk tests. The two types of test on each of the components can be understood from the following table:

Table 5. 4: Tests of normality

NO	Components	Kolmogorov-smirnov		Shapiro- Wilk	
		Statistic	df	Statistic	df
1	Attitude towards cybersecurity				
1.1	Attitudes	0.186	124	0.903	124
1.2	Self- efficiency	0.156	124	0.9	124
2	Risky cybersecurity behaviours				
2.1	Risky behaviours	0.183	124	0.885	124
2.2	Digital trust behaviours	0.132	124	0.934	124
2.3	Cybersecurity mitigating behaviours	0.199	124	0.849	124
3	Countermeasures (security awareness)				
3.1	Administrative countermeasures	0.235	124	0.82	124
3.2	Managerial countermeasures	0.185	124	0.869	124
3.3	Support countermeasures	0.218	124	0.872	124
4	Impulsivity (users' addictive behaviour)				
4.1	Premeditation	0.266	124	0.81	124
4.2	Urgency	0.14	124	0.949	124

Based on the above table, it can be stated that none of the research components are violating the acceptance standards stated in the previous section.

5.6 Frequency Analysis

The number of occurrences of each response to the online survey is managed with the help of frequency analysis. The mean median mode of each component can be categorised with the help of frequency analysis. All the categorical variables of a research study can be conducted with the help of frequency analysis. Illustrations such as bar charts and pie charts can be created

with the help of frequency analysis. The influence of the dependent variables on the independent variables and the role of the mediator can be understood from frequency analysis as well.

5.6.1 Attitudes towards Cybersecurity Countermeasures

5.6.1.1 Attitudes

Insights into the frequencies of the responses of the 124 participants will be gained using a Likert scale. The Likert scale selected for the frequency analysis is a 7-point Likert scale; all the frequencies have seven options: strongly disagree, which is denoted by 1, disagree denoted by 2, somewhat disagree denoted by 3, neither agree nor disagree denoted by 4, somewhat agree by 5, agree and strongly agree by 6 and 7 respectively.

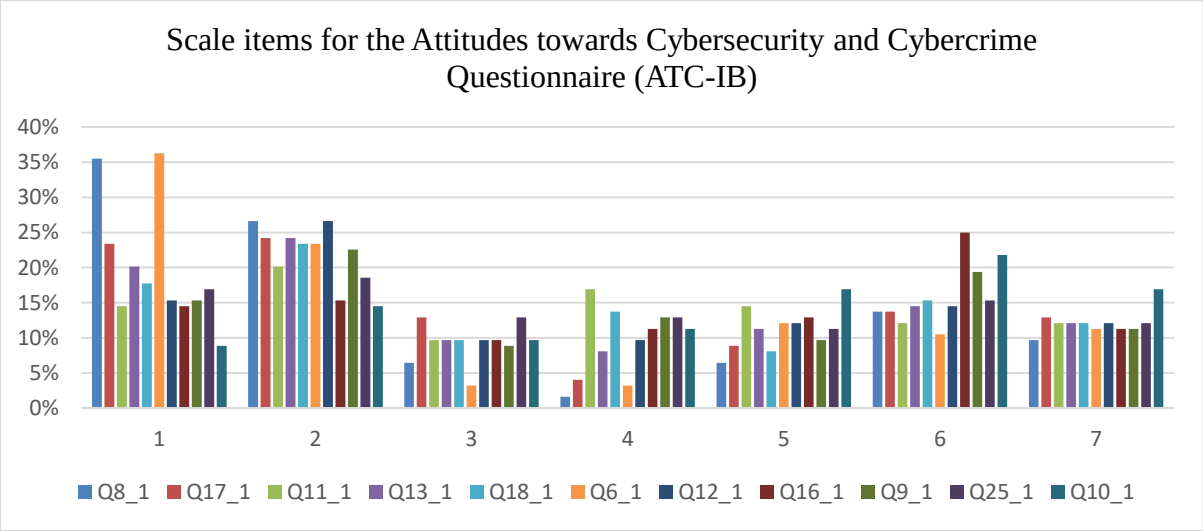


Figure 5. 9: Attitudes

Based on the responses gathered from the respondents about their attitude towards cybersecurity, it can be said that 35% of them strongly disagreed that reporting cybercrime is a waste of action and 27% of them also disagreed, whereas 14% agreed with the fact that reporting cybercrime is required and 10% strongly agreed with the statement; 6% of the entire population somewhat disagreed and 2% neither agreed nor disagreed with this topic of discussion, whilst

6% of the population somewhat agreed with the statement. Next, 9% of the total population strongly disagreed with the fact that cybercriminals are more advanced than other people, 15% of the population disagreed, 10% somewhat disagreed, 11% of the population neither agreed nor disagreed, 17% agreed with the statement, 22% of the respondents agreed and 17% of the population strongly agreed. Regarding paying attention to the company material sent by the organisation, 18% of the population strongly disagreed that they do not pay attention to the company material, 23% of the population disagreed, 10% of them somewhat disagreed, 14% neither agreed nor disagreed, 18% somewhat agreed with the statement, 15% agreed and 12% strongly agreed on this point.

5.6.1.2 Self-efficacy

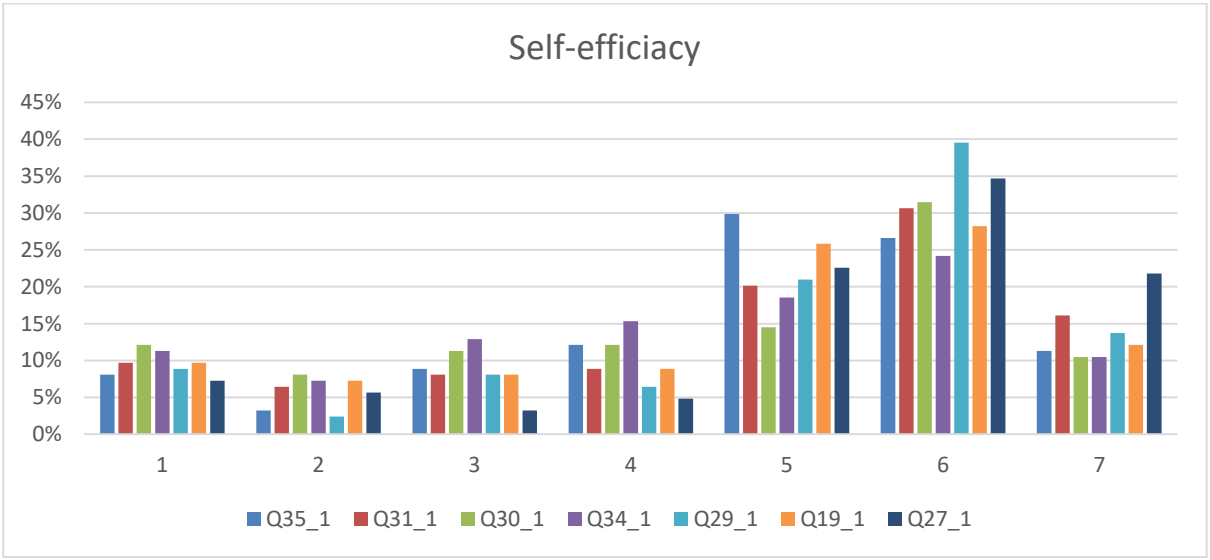


Figure 5. 10: Self-efficacy

From the results gathered from the respondents of this survey, it was understood that 8% strongly disagreed with that fact that other employees comply with the security policy adopted by organisations, 3% disagreed, 9% somewhat disagreed, 12% neither agreed nor disagreed, 30% of the population somewhat agreed, 27% agreed and 11% strongly agreed that other

employees comply to the security policies of the commercial establishments. Next, 12% strongly disagreed with the fact that they can manage virus-infected files, 8% of them disagreed that they did not feel confident to handle virus-infected files, 11% somewhat disagreed with this statement, 12% neither agreed nor disagreed, 15% of the participants somewhat agreed, 31% agreed and 10% felt confident in handling virus-infected files. Moving on to the next statement, 11% strongly disagreed that other employees back up their computers, 7% disagreed, 13% somewhat disagreed, 15% of the total population neither agreed nor disagreed, 19% somewhat agreed, 24% of the respondents believed that other employees back up their computers on a regular basis and the rest (10%) strongly agreed with this question. For the next statement, 10% of the entire population strongly disagreed that they felt confident about getting rid of spyware and malware from a computer system, 6% of them disagreed with this statement and 8% somewhat disagreed with the statement. However, 9% of the population neither agreed nor disagreed, 20% somewhat agreed with it, whereas 31% agreed and the rest (16%) strongly agreed.

5.6.2 Risky Cybersecurity Behaviour Practices

5.6.2.1 Risky Behaviours

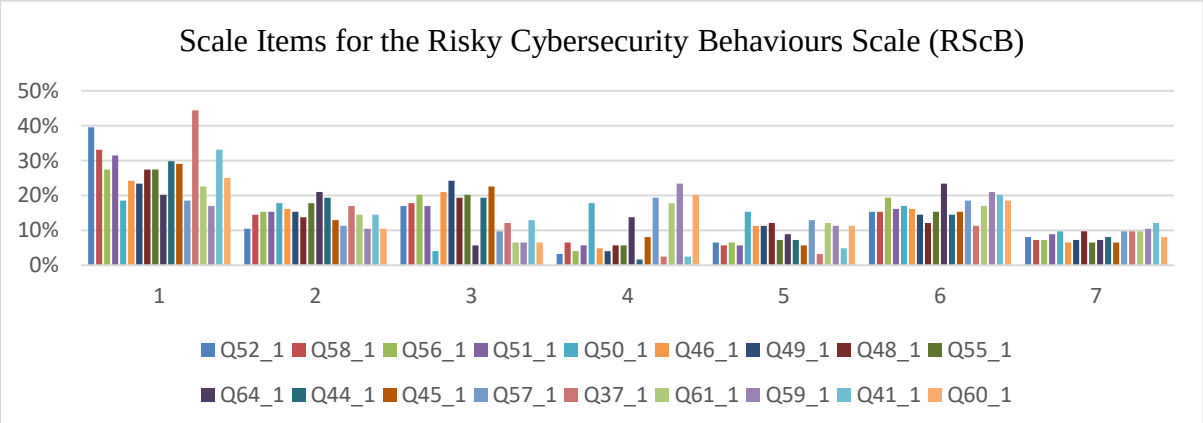


Figure 5. 11: Risky behaviours

Based on the results obtained from the respondents, it can be said that 40% strongly disagreed with the fact that they sent personal information to strangers, 10% of the respondents disagreed with this statement, 17% somewhat disagreed with it, 3% neither agreed nor disagreed, 6% of the population somewhat agreed, 15% of the population agreed that they send personal information over the internet and 8% of them strongly agreed. Moving on, 31% of the respondents strongly disagreed with the statement that they click on links in unsolicited emails from unidentified sources, and 15% disagreed, 17% somewhat disagreed, whereas 6% neither disagreed or agreed, and 6% of the total population somewhat agreed on this question. However, 16% agreed that they click on links from unsolicited emails and the rest (9%) of the population strongly agreed with this statement. Regarding the next statement, 23% of the total population strongly disagreed that they like to share their location across social media platforms, 15% of the population disagreed with the fact that they share their current location on social media, 24% somewhat disagreed with this statement, whereas 4% of the respondents neither disagreed nor agreed, 11% somewhat agreed, 15% of the total population agreed that they share their location on social media and 7% stated that they synchronise their current position in most of the social media platforms.

5.6.2.2 Digital Trust Behaviours

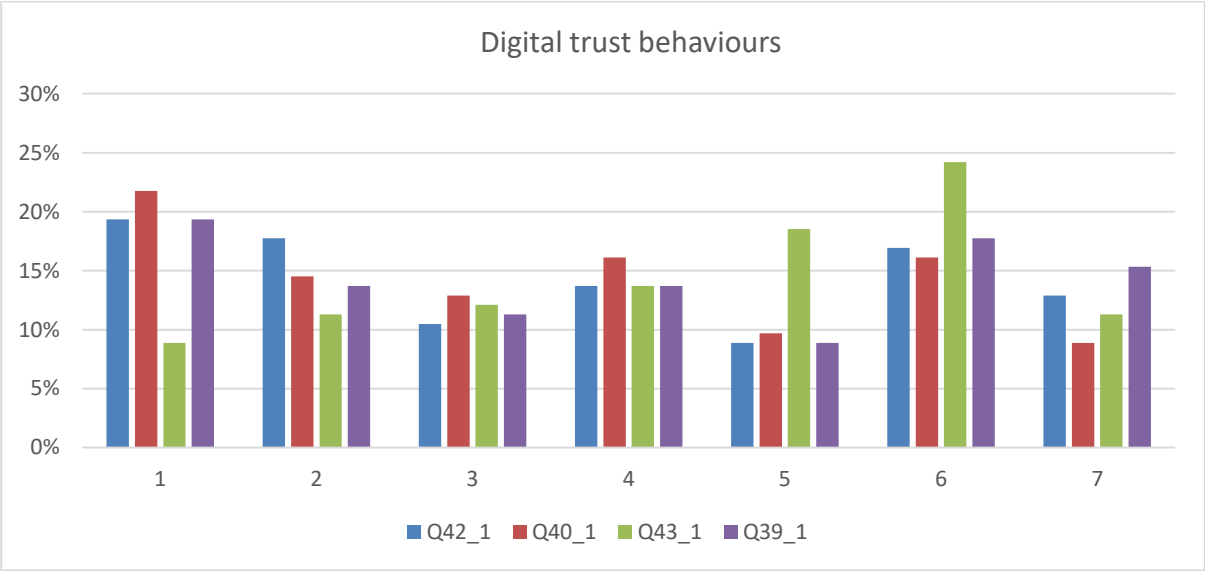


Figure 5. 12: Digital trust behaviours

Data gathered from the respondents helped in understanding that 19% of the total who took part in the online survey strongly disagreed that they have free access to public Wi-Fi, 18% disagreed, 10% somewhat disagreed with this fact, and 14% neither agreed not disagreed. However, 9% of the population agreed that they have unrestricted access to public Wi-Fi, 17% agreed and 13% of the population strongly agreed with the fact that they have free Wi-Fi. Moving on, 22% of the total population strongly disagreed that they use online storage systems to keep and exchange their sensitive or personal information, 15% disagreed with the fact that they use online storage systems to protect their sensitive data, 13% of respondents somewhat disagreed with this statement, whereas 16% of the participants of the online survey neither agreed nor disagreed, 10% of the participants somewhat agreed that they make the most of the online storage systems, 16% agreed and the rest (9%) strongly agreed. Concerning passwords, 19% of the total participants strongly disagreed that they use the same passwords for different websites, 14% disagreed with this topic of discussion and 11% somewhat disagreed, and 14% neither agreed nor disagreed; meanwhile, 9% somewhat agreed that they use the same password

for different websites, 18% agreed and 15% of respondents strongly agreed with this topic of discussion.

5.6.2.3 Cybersecurity Mitigating Behaviours

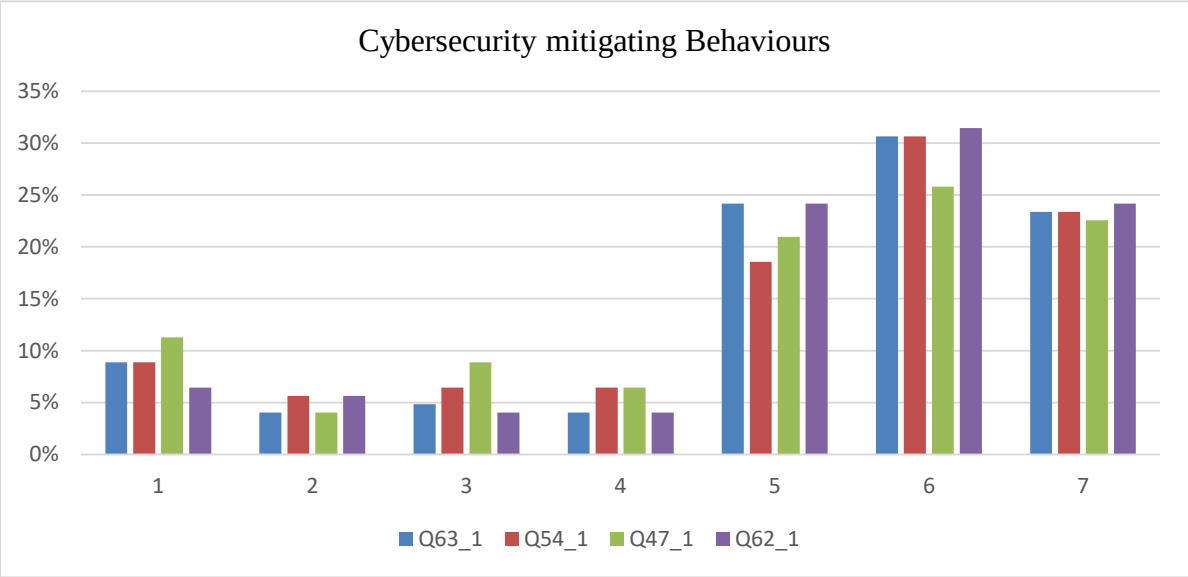


Figure 5. 13: Cybersecurity mitigating behaviors

Based on the data gathered from the respondents, it can be said that 9% of the respondents strongly disagreed that they back up their computer regularly, 4% disagreed that they back up their computer regularly, 5% somewhat disagreed, 4% neither agreed nor disagreed and 24% somewhat agreed. However, 31% agreed that they back up their computer regularly and the rest (23%) of the participants of this survey strongly agreed about this topic of discussion as well.

Regarding email security, 6% strongly disagreed that they check the security of an email with an attachment, 6% disagreed with this topic of discussion, 4% of the population somewhat disagreed and 4% neither agreed nor disagreed. However, 24% somewhat agreed that they check

the security of an email with an attachment. 31% agreed and 24% strongly agreed with this discussion as well. Concerning updates, 9% strongly disagreed that they check for updates to any antivirus software which is installed, 6% disagreed with this statement, and 6% somewhat disagreed. Another 6% neither agreed nor disagreed with this statement. However, 19% somewhat agreed that they check for updates for anti-virus software which is already installed, 31% agreed with this statement and the rest (23%) strongly agreed with the statement as well.

5.6.3 Countermeasures

5.6.3.1 Administrative Countermeasures

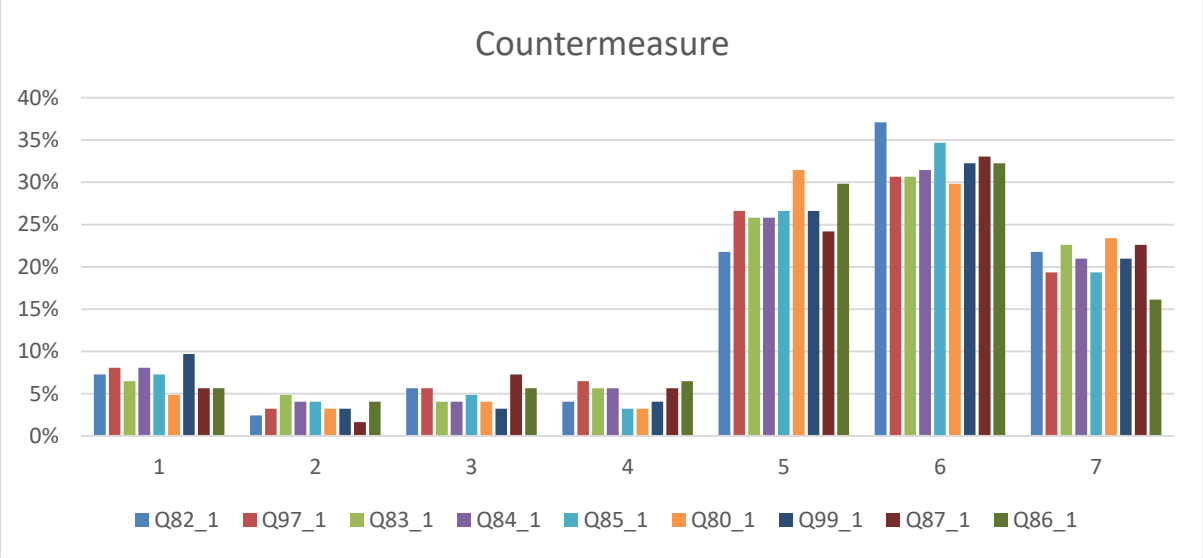


Figure 5. 14: Administrative countermeasures

Looking at the data gathered from the respondents of the online survey, it can be stated that 7% of the total population strongly disagreed that organisation policy requests the regular use of an antivirus, 2% of the respondents disagreed with this statement and 6% somewhat disagreed and 4% neither agreed nor disagreed with this statement, whereas 22% somewhat agreed that their organisation's policy requests them to use an anti-virus regularly, and 37% of

the respondents of this online survey agreed with this statement as well and the rest (22%) also strongly agreed with this statement as well.

Relatedly, 6% of the responders stated that their organisation's policy requests them to update their antivirus regularly, 5% of the total population disagreed and 4% of them somewhat disagreed with the statement, 6% of them neither agreed nor disagreed, whilst 26% of them somewhat agreed with this topic of discussion, 31% of the respondents agreed and the rest (23%) strongly agreed with this statement as well.

Moving on, 8% of the responders from the survey strongly disagreed that their organisation's policy requests them to scan files and devices before using them, 4% disagreed and 4% somewhat disagreed, whilst 6% of them neither agreed nor disagreed, 26% of the total population somewhat agreed that their organisation requests them to scan files before using them, 31% of the survey respondents agreed and whereas the rest (21%) strongly agreed with this statement.

5.6.3.2 Managerial Countermeasures

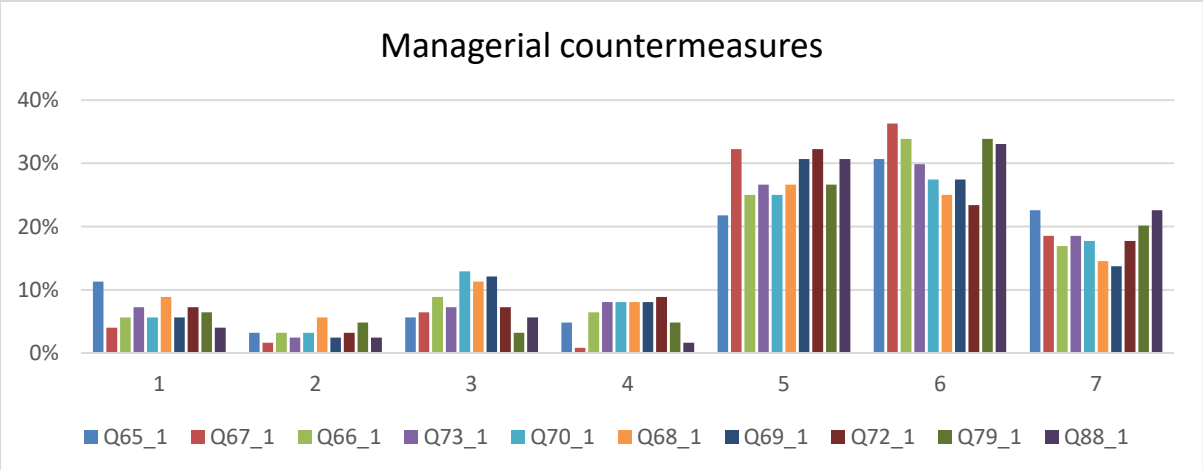


Figure 5. 15: Managerial countermeasures

Based on the results obtained from the respondents, it can be said that 11% of them strongly disagreed that their management team encourages them to improve information security policies, 3% disagreed with this and 6% somewhat disagreed, whereas 5% neither agreed nor disagreed, 22% somewhat agreed, 31% agreed and the rest (23%) strongly agreed. Relatedly, 17% of the respondents to the online survey strongly agreed that their management educates them regarding the significance of practising IS behaviour, 34% agreed, 25% somewhat agreed, 6% neither agreed nor disagreed, 9% somewhat disagreed, 6% disagreed with this question and the rest (6%) strongly disagreed with this statement. Furthermore, 6% strongly disagreed that their management takes serious action regarding the workforce who do not comply with the IS policies, 3% of them disagreed with the statement, 13% somewhat disagreed, 8% neither disagreed nor agreed, 25% of the respondents somewhat agreed that their management takes decisive action against employees who are not following the IS policies, 27% agreed and the rest (18%) strongly agreed with this statement.

5.6.3.3 Support Countermeasures

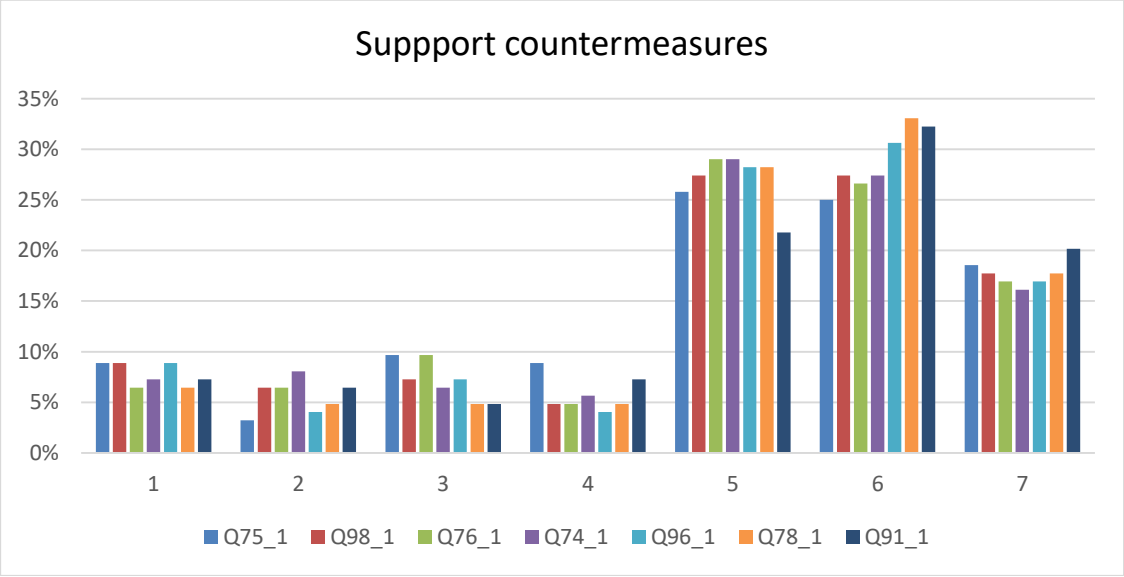


Figure 5. 16: Support countermeasures

Considering the answers coming from the respondents of this online survey, it can be said that 9% of the total population strongly disagreed that their management encourages them to attend information security training, 3% of them disagreed and 10% somewhat disagreed, 9% neither agreed nor disagreed, 26% somewhat agreed, 25% agreed that their management team encourages them to take part in information security training sessions and the rest (19%) of the total population strongly agreed. Relatedly, 9% of the respondents strongly disagreed that they have been through computer security training sessions and 6% disagreed, 7% somewhat disagreed. Only 5% of the online survey neither agreed nor disagreed about the training sessions, whilst 27% of the population somewhat agreed that they have conducted training sessions and another 27% agreed, whereas the rest (18%) strongly agreed that they have already participated in a formal training session.

Relatedly, 9% of the respondents of the online survey strongly disagreed that their organisation organised security talks and training, 4% disagreed with this statement, 7% somewhat disagreed, 4% neither agreed nor disagreed, 28% somewhat agreed that their organisation organises security talks and training, 31% agreed and the rest (17%) strongly agreed with this statement. Similarly, 6% of the respondents strongly disagreed that the IS policy training helps them to understand the behaviour required to work with the concept of IS, 5% disagreed, 5% somewhat disagreed and another 5% who neither agreed nor disagreed about this topic of discussion, whilst 28% of the online survey somewhat agreed with the statement and the rest (33%) agreed that the training module is very useful for them to work on IS projects, and 18% strongly agreed with this.

5.6.4 Impulsivity (Users' addictive behaviours)

5.6.4.1 Premeditation

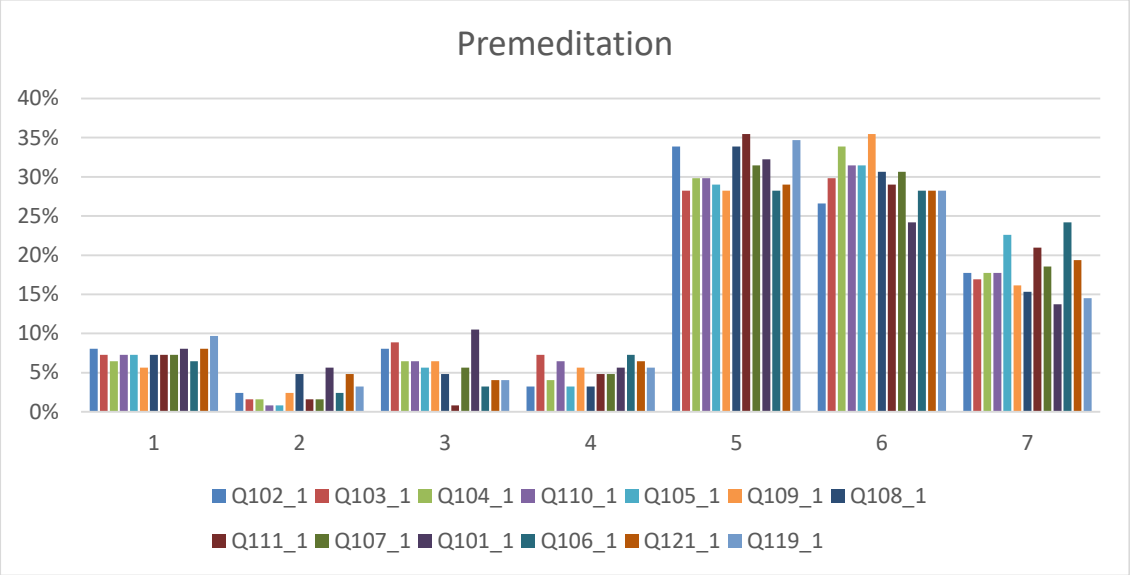


Figure 5. 17: Premeditation

Based on the results obtained from the participants, it can be stated that 8% strongly disagreed with the fact that their thinking is careful and purposeful, 2% of the population disagreed that their thinking is clear and purposeful and 8% somewhat disagreed that their thinking is careful and purposeful. However, 3% neither agreed nor disagreed with this topic of discussion, whilst 34% of the population somewhat agreed with the selected discussion, 27% of them agreed and the rest (18%) strongly agreed. Moving on, 7% strongly disagreed that they stop and think before doing anything, whilst only 1% of the participants, which is a very low figure, disagreed with the statement and 6% of the population somewhat disagreed with this statement. At the same time, 6% of the total population neither agreed nor disagreed with this selected discussion topic, 30% somewhat believed that they think before doing anything, 31% agreed that they think before doing anything and 18% strongly agreed with this statement. Relatedly, 8% strongly disagreed that they are reserved and cautious towards life, 6% of the

total population disagreed about the statement, 10% somewhat disagreed, 6% of the respondents neither agreed nor disagreed with this statement, 32% of them somewhat agreed, 24% agreed and the rest (14%) strongly disagreed.

5.6.4.2 Urgency

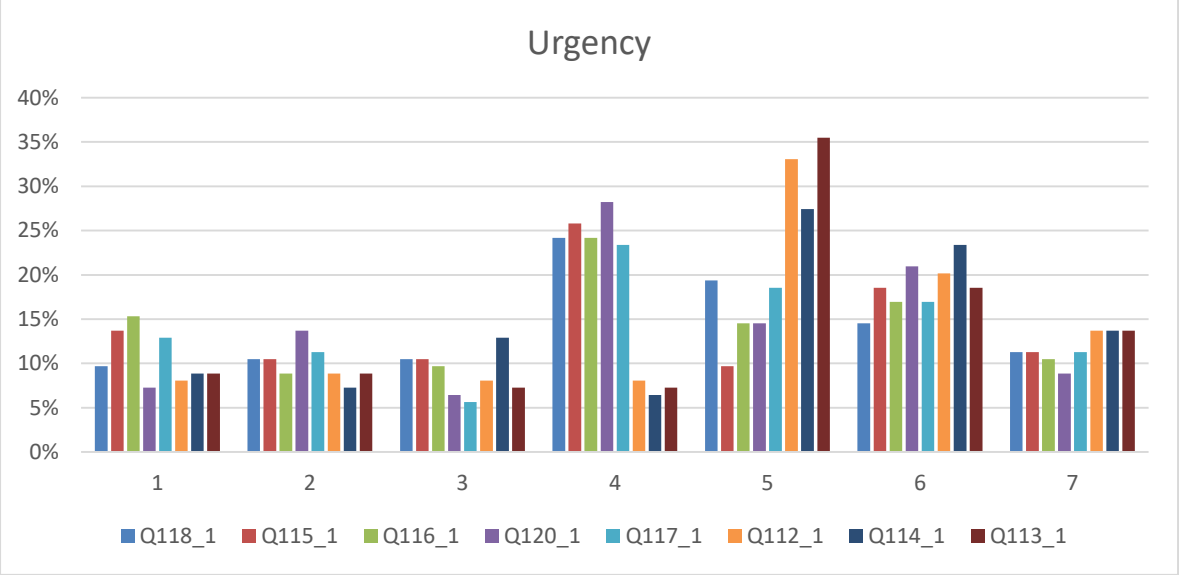


Figure 5. 18: Urgency

The data obtained from the online survey indicated that 10% of respondents strongly disagreed that it is very difficult for them to resist acting on their feelings, and another 10% of them disagreed with this selected topic of discussion, a further 10% somewhat disagreed with this statement, whereas 24% neither agreed nor disagreed, 11% strongly agreed, 15% agreed and 19% somewhat agreed with this statement. Similarly, 15% of respondents strongly disagreed that, when they are upset, they act without thinking, 9% of the population disagreed and 10% somewhat disagreed, whilst 24% of the participants who showed an interest in the online survey neither agreed nor disagreed with this topic of discussion. At the same time, the results showed that 15% somewhat agreed with this topic of discussion, 17% agreed that they act without thinking when they are upset and the rest (10%) strongly agreed with this statement. Moving on, 9% of the respondents strongly disagreed that they get involved in things where

they can get out of doing so, 9% disagreed, 7% somewhat disagreed, 7% of them either agreed or disagreed with this topic of discussion, 35% somewhat agreed, at the same time 19% of the respondents who have stated their opinion in the online survey agreed and the rest (14%) strongly agreed with this statement.

5.7 Dependent and Independent Variables

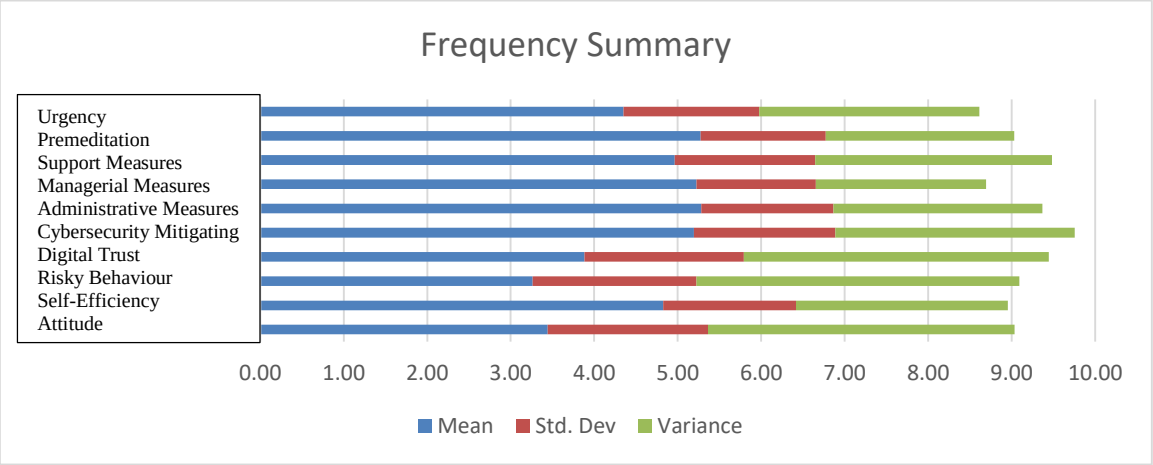


Figure 5. 19: Frequency summary

The following table will be very useful to understand the description of each component such as mean, 95% of the confidence interval, mean, variance and standard deviation.

Table 5. 5: Variable descriptive statistics

Descriptive Statistics

			Bootstrap[a]			
					95% Confidence Interval	
		Statistic	Bias	Std. Error	Lower	Upper
Attitude	N	124	0	0	124	124
	Mean	3.4446	-.0043	.1733	3.0953	3.7943
	Std. Deviation	1.91702	-.01239	.08564	1.72682	2.06316
	Variance	3.675	-.040	.325	2.982	4.257
Self-Efficiency	N	124	0	0	124	124
	Mean	4.8260	-.0129	.1438	4.5029	5.0864
	Std. Deviation	1.59270	-.00295	.10370	1.37036	1.78948
	Variance	2.537	.001	.329	1.878	3.202

Risky Behaviour	N	124	0	0	124	124
	Mean	3.2612	-.0098	.1769	2.8972	3.6009
	Std. Deviation	1.96572	-.01001	.08169	1.79415	2.10780
	Variance	3.864	-.033	.318	3.219	4.443
Digital Trust Behaviours	N	124	0	0	124	124
	Mean	3.8832	-.0059	.1680	3.5431	4.2004
	Std. Deviation	1.91080	-.00613	.07800	1.74108	2.06059
	Variance	3.651	-.017	.297	3.031	4.246
Cybersecurity Mitigating Behaviour	N	124	0	0	124	124
	Mean	5.1956	-.0070	.1494	4.9111	5.4876
	Std. Deviation	1.69347	-.00363	.12342	1.43472	1.91258
	Variance	2.868	.003	.415	2.058	3.658
Countermeasures	N	124	0	0	124	124
	Mean	5.2831	-.0073	.1373	5.0012	5.5474
	Std. Deviation	1.58247	-.00338	.13390	1.30265	1.82098
	Variance	2.504	.007	.419	1.697	3.316
Managerial Countermeasures	N	124	0	0	124	124
	Mean	5.2252	-.0066	.1268	4.9763	5.4734
	Std. Deviation	1.42791	-.00265	.12476	1.17293	1.67326
	Variance	2.039	.008	.356	1.376	2.800
Support Countermeasures	N	124	0	0	124	124
	Mean	4.9629	-.0047	.1543	4.6505	5.2471
	Std. Deviation	1.68444	-.00521	.11129	1.44442	1.89294
	Variance	2.837	-.005	.372	2.086	3.583
Premeditation	N	124	0	0	124	124
	Mean	5.2734	-.0062	.1336	4.9961	5.5221
	Std. Deviation	1.50201	-.00708	.13703	1.22496	1.75925
	Variance	2.256	-.002	.409	1.501	3.095
Urgency	N	124	0	0	124	124
	Mean	4.3529	-.0027	.1503	4.0424	4.6343
	Std. Deviation	1.62351	-.00492	.08944	1.44567	1.79938
	Variance	2.636	-.008	.290	2.090	3.238
Valid N (listwise)	N	124	0	0	124	124

a. Unless otherwise noted, bootstrap results are based on 1000 bootstrap samples

The residual statistics of the population can be understood from the following table.

Table 5. 6: Variable residual statistics

Residual Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.5949	4.3331	3.4901	.63077	124

Residual	-3.33313	3.43091	.00000	1.81744	124
Std. Predicted Value	-3.005	1.337	.000	1.000	124
Std. Residual	-1.819	1.872	.000	.992	124

a. Dependent Variable: Dependent

Based on this table, it can be said that the minimum predicted value of the dependent variables is 1.5949, the maximum predicted value of this frequency is 4.3331, and their mean is 3.4901. The standard deviation of the predicted value is 0.63077. The minimum residual is - 3.33313, whereas the maximum residual value is 3.43091 and their mean is found to be 0.00000.

The standard deviation of the residual value is 1.81744. The minimum of the standard predicted value is -3.005, the maximum standard predicted value is found to be 1.3337, the mean of the standard predicted value is 0.000 and the standard deviation of the standard predicted value is 1.000. The minimum of the standard residual value is -1.819, the maximum of the standard residual value is 1.872, and their mean is 0.000. The standard deviation of the standard residual value is 0.992.

Table 5. 7: Variables' descriptive statistics

Descriptive Statistics

	N	Minimum	Maximum	Mean	Std. Deviation
Attitude	124	1.00	7.00	4.1465	1.72132
Dependent	124	1.00	7.00	3.4901	1.92379
Information Countermeasures	124	1.00	7.00	5.2687	1.45260
Mediator	124	1.00	7.00	5.1342	1.41365
Valid N (listwise)	124				

Standard deviation and mean of the variable of this thesis can be understood from the descriptive statistics; it can be comprehended that the minimum of attitude is 1.00 whereas the maximum of attitude is found to be 7.00. The mean of attitude was found to be 4.1465 and its standard deviation is 1.72132. The minimum of the dependent variable is 1.00 whereas the maximum of the dependent variable is 7.00. The standard deviation of the dependent variable is found to be 1.92379 as the obtained mean value is 3.4901. The minimum of the Information countermeasures was found to be 1.00 and the maximum value was found to be 7.00. Hence, the mean value of the Information countermeasures is 5.2687 and the standard deviation was found to be 1.45260. Considering the mediator, the minimum value is 1.00, whereas the maximum value was found to be 7.00. The mean of the mediator is 5.1342 and the standard deviation of the mediator is 1.41365.

CHAPTER 6: DATA ANALYSIS

6.1 Introduction

A hypothesis is a proposition or a projected outcome about a particular subject that is developed before the research is conducted (List, Shaikh and Xu, 2019). The research is then carried out to verify the hypothesis. After completion of the data collection and analysis process, the obtained outcome is compared to the formulated hypothesis or hypotheses. This comparison can turn the hypotheses to be either true or false. There are different types of hypotheses that can be formulated (List, Shaikh and Xu, 2019). The type of hypothesis to be used depends on the researcher's choice and objectives. Some of the widely used types of hypotheses are: (1) working hypothesis; this is a hypothesis that tries to explain various relationships between certain facts that have been observed. It provides guidelines to the researcher while looking for solutions for the research question. (2) Null hypothesis; this hypothesis is formulated to oppose the working hypothesis (Mellenbergh, 2019). In other words, a null hypothesis disproves a working hypothesis. (3) Alternate hypothesis; when the researcher is disagreeing with the null hypothesis, they often create an alternate hypothesis (Thinh, Dall'Arno and Scarani, 2019). This usually only happens in rare cases.

Hypothesis testing is the method used to confirm the claim made about a particular subject in the hypothesis by use of the data acquired from the research (List, Shaikh and Xu, 2019). The test is performed to find out if actually what was proposed is true or false. Hypothesis testing is carried out in four steps (Thinh, Dall'Arno and Scarani, 2020):

(i) Identifying the stated hypothesis; the first step in testing a hypothesis is to identify the hypothesis that was stated prior to the research.

(ii) Come up with a criterion to determine if the stated hypothesis is true or false. For the hypothesis to be true, the results obtained should be within a given range of the stated hypothesis.

(iii) Take sample results of the research and compare them with the projected results stated in the hypothesis.

(iv) Conclude whether the hypothesis is true or false based on the comparison that was made in step (iii) above.

6.2 Correlation Test (Pearson)

Specifications of a variable can be understood with the help of correlational testing. This testing procedure is very significant to understand the position of the variables and the mediators of a statistical technique. A degree of association among the variables can also be identified using the co-relational test. Pearson correlation coefficient is defined as a type of coefficient that is very beneficial to understand the linear co-relation among the research variables. The role of the variance is very significant in correlational testing. In this thesis, this type of test is carried out to identify how various aspects of the information security countermeasures control risky cybersecurity behaviour practices (Cox, 2019). The research variables are risky cybersecurity behaviour practices and the information security countermeasures. A correlation test was carried out in six different aspects involving the organisations and employees.

A description of the six sections where a correlation test was performed is provided in the below table.

Table 6. 1: Description of the correlation sections

Section 1	Correlation between attitudes towards cybersecurity countermeasures and risky cybersecurity behaviour practices.

Section 2	Correlation between security awareness countermeasures and risky cybersecurity behaviour practices.
Section 3	Correlation between users' addictive behaviours and risky cybersecurity behaviour practices.
Section 4	Correlation between attitudes towards cybersecurity countermeasures and users' addictive behaviours.
Section 5	Correlation between peer relationships and IS countermeasures.
Section 6	Correlation between security awareness countermeasures and users' addictive behaviours.

Section 1: Correlation between attitudes towards cybersecurity countermeasures and risky cybersecurity behaviour practices.

Correlations

Table 6. 2: ATCC and RCB correlation

				Independent	Dependent
Attitudes towards cybersecurity countermeasure	Pearson Correlation			1	.612**
	Sig. (2-tailed)				.000
	N			124	124
	Bootstrap[b]	Bias		0	-.003
		Std. Error		0	.065
		95% Confidence Interval	Lower	1	.468
			Upper	1	.735
Risky cybersecurity behaviour practices	Pearson Correlation			.612**	1
	Sig. (2-tailed)			.000	
	N			124	124
	Bootstrap[b]	Bias		-.003	0
		Std. Error		.065	0
		95% Confidence Interval	Lower	.468	1
			Upper	.735	1

**. Correlation is significant at the 0.01 level (2-tailed).

b. Unless otherwise noted, bootstrap results are based on 1000 bootstrap samples

Based on the above table, it can be understood that there is a moderate positive co-relation with the variables chosen for this co-relation analysis and it is significant with $p<0.01$. The variables that were used in this test were the attitude towards cybersecurity countermeasures

against risky cybersecurity behaviour practices (Adam Bujang *et al.*, 2016). The bias of this co-relation is found to be 0 at 99% significance. This means that the attitude of employees towards enhancing security in information systems is directly influenced by the risky cybersecurity behaviours (Guhr, Lebek and Breitner, 2019). Hence, based on this result, it can be said that enhancement of the attitudes towards cybersecurity countermeasures will surely have an influence on the risky cybersecurity behaviour practices of the UAE's public organisations.

Section 2: Correlation between security awareness countermeasures and risky cybersecurity behaviour practices.

Correlations

Table 6. 3: SAC and RCB correlation

				Independent	Dependent
Security awareness countermeasures	Pearson Correlation			1	.568**
	Sig. (2-tailed)				.000
	N			124	124
	Bootstrap[b]	Bias		0	-.003
		Std. Error		0	.065
		95% Confidence Interval	Lower	1	.428
			Upper	1	.681
Risky cybersecurity behaviour practices	Pearson Correlation			.568**	1
	Sig. (2-tailed)			.000	
	N			124	124
	Bootstrap[b]	Bias		-.003	0
		Std. Error		.065	0
		95% Confidence Interval	Lower	.428	1
			Upper	.681	1

**. Correlation is significant at the 0.01 level (2-tailed).

b. Unless otherwise noted, bootstrap results are based on 1000 bootstrap samples

This correlation test was carried out to determine the relationship between the security awareness countermeasures in managing risky cybersecurity behaviour practices (Masih, 2018). The correlation results about the stated variables obtained are shown in the above table. According to the table, there is a positive correlation between the two variables. The correlation is positive and is about 0.568 where $P<0.01$, which makes it significant. The correlation has a significance of 99% with no biasedness. From the results discussed above, it can be concluded that the policies communicated by the security awareness countermeasures can highly impact on how employees react to information security issues. This means that organisations which

have strict information security policy communication are most likely to be secure from cyber-attacks.

Section 3: Correlation between users' addictive behaviours and the risky cybersecurity behaviour practices.

Correlations

Table 6. 4: UAB and RCB correlation

				Independent	Dependent
Users' addictive behaviours	Pearson Correlation			1	.572**
	Sig. (2-tailed)				.000
	N			124	124
	Bootstrap[b]	Bias		0	-.006
		Std. Error		0	.071
		95% Confidence Interval	Lower	1	.409
			Upper	1	.693
Risky cybersecurity behaviour practices	Pearson Correlation			.572**	1
	Sig. (2-tailed)			.000	
	N			124	124
	Bootstrap[b]	Bias		-.006	0
		Std. Error		.071	0
		95% Confidence Interval	Lower	.409	1
			Upper	.693	1

**. Correlation is significant at the 0.01 level (2-tailed).

b. Unless otherwise noted, bootstrap results are based on 1000 bootstrap samples

The biasedness of the users' addictive behaviours on the risky cybersecurity behaviour practices can be understood from the above table. The results obtained from the above table help in understanding that there is a moderate positive co-relation (0.572) which is significant at $p<0.01$. The biasedness of this co-relation was found to be 0 at 99% significance. Hence, based on these results, it can be suggested that users' addictive behaviours in public organisations are co-related to risky cybersecurity behaviour practices.

Section 4: Correlation between attitudes towards cybersecurity countermeasures and the users' addictive behaviours.

Correlations

Table 6. 5: ATCC and UAB correlation

				Independent	Dependent
Attitudes towards cybersecurity countermeasures	Pearson Correlation			1	.276**
	Sig. (2-tailed)				.002
	N			124	124
	Bootstrap[c]	Bias		0	-.002
		Std. Error		0	.088
		95% Confidence Interval	Lower	1	.099
			Upper	1	.440
Users' addictive behaviours.	Pearson Correlation			.276**	1
	Sig. (2-tailed)			.002	
	N			124	124
	Bootstrap[c]	Bias		-.002	0
		Std. Error		.088	0
		95% Confidence Interval	Lower	.099	1
			Upper	.440	1

**. Correlation is significant at the 0.01 level (2-tailed).

c. Unless otherwise noted, bootstrap results are based on 1000 bootstrap samples.

This correlation test was carried out to understand the relationship between attitude towards cybersecurity countermeasures and users' addictive behaviour (Kokolakis, 2017). The biasedness of the dependent variable on the independent variable can be understood from the above tabular description. The results obtained from the above table help in understanding that there is a correlation (0.276), which is significant at $p<0.01$. The biasedness of the correlation is found to be 0 at 99%. Significance Hence, on the basis of these results, it can be said that the dependent variable is directly related to the independent variable in this correlation. Although there is correlation between the two variables, it can be said that the attitude countermeasures can have a positive influence on users' addictive behaviours in organisations (Ahmad *et al.*, 2019).

Section 5: Correlation between peer relationships and IS countermeasures.

Table 6. 6: Peer relationships and cybersecurity

				Peer relationships	dependent
Peer relationships	Pearson Correlation			1	.612**
	Sig. (2-tailed)				.000
	N			124	124
	Bootstrap[b]	Bias		0	-.006
		Std. Error		0	.071
		92% Confidence Interval	Lower	1	.389
			Upper	1	.0.715
Cybersecurity	Pearson Correlation			.612**	1
	Sig. (2-tailed)			.000	
	N			124	124
	Bootstrap[b]	Bias		-.006	0
		Std. Error		.071	0
		92% Confidence Interval	Lower	.409	1
			Upper	.693	1

**. Correlation is significant at the 0.01 level (2-tailed).
b. Unless otherwise noted, bootstrap results are based on 1000 bootstrap samples

This test was carried to determine if the IS can be enhanced by improving the relationship between peer employees (David *et al.*, 2020). According to the tabulated results, there is a moderately strong correlation between the peer relationships and the information systems security. The correlation was found to be 0.612, which is significant at $p<0.01$. There is 0 biasness of the result, which makes it 99% significant. From the calculations above, it can be concluded that enhancing relationships between peer employees can have a positive impact on the fight against information insecurity.

Section 6: Correlation between security awareness countermeasures and the users' addictive behaviours.

Correlations

Table 6. 7: SAC and UAB correlation

				Independent	Dependent
Security awareness countermeasures	Pearson Correlation			1	.276**
	Sig. (2-tailed)				.002
	N			124	124
	Bootstrap[c]	Bias		0	-.001
		Std. Error		0	.087
		95% Confidence Interval	Lower	1	.099
			Upper	1	.433
Users' addictive behaviours	Pearson Correlation			.276**	1
	Sig. (2-tailed)			.002	
	N			124	124
	Bootstrap[c]	Bias		-.001	0
		Std. Error		.087	0
		95% Confidence Interval	Lower	.099	1
			Upper	.433	1

**. Correlation is significant at the 0.01 level (2-tailed).

c. Unless otherwise noted, bootstrap results are based on 1000 bootstrap samples

There is a weak correlation between the two variables of this hypothesis (0.276). The above table helps in understanding the biasness of the dependent variable and the independent variable. From the above calculations, it can be said that there is a weak correlation (0.276), which is significant at $p<0.01$. Like the previous sections, the biasedness was also found to be 0 at a significance of 99%. Hence, it can be understood that users' addictive behaviours are related to security awareness countermeasures in this correlation.

6.3 Correlation Results Summary

The results obtained from the chapter are very significant to understand that all the variables of this thesis are positive and each one is significant. Enhancement of the organisational IS countermeasures is very significant to the behaviour of the public organisation

workforces towards IS. It can be concluded that the risky behaviours of users in the UAE's public organisations can have a direct influence on the organisations' IS countermeasures. It can also be concluded that users' addictive behaviours have a direct influence on impulsivity.

Table 6. 8: Association summaries

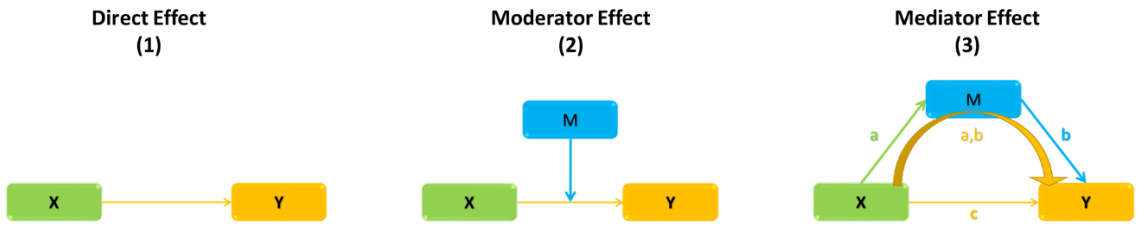
Number	Independent variable	Dependent variable	Mediating	Correlation summary	Hypothesis (Accepted)	Hypothesis (Rejected)
1	Attitudes towards cybersecurity	Risky cybersecurity behaviour practices	None	Positive Correlation (0.612) significant p< 0.01	Accepted	
2	Security awareness countermeasures	Risky cybersecurity behaviour practices	None	Positive Correlation (0.568) significant p< 0.01	Accepted	
3	Users' addictive behaviours	Risky cybersecurity behaviour practices	None	Positive Correlation (0.572) significant p< 0.01	Accepted	
4	Attitudes towards cybersecurity	Users' addictive behaviours	None	Positive Correlation (0.278) significant p< 0.01	Accepted	
5	Peer relationships	Information security countermeasure	Users' addictive behaviours	Positive Correlation (0.612) significant p< 0.01	Accepted	
6	Security awareness countermeasures	Users' addictive behaviours	None	Positive Correlation (0.276) significant p< 0.01	Accepted	

6.4 Regression Analysis

Regression analysis of the hypothesis is carried out to determine how one or more independent variables influence a dependent variable (Darlington and Hayes, 2016). The purpose of this type of analysis is to enable the researcher to validate the null hypothesis that was formulated before the research was conducted. In this research, the dependent variable is the information security countermeasures.

This section of this chapter conducts three tests for each independent facet so that the dependent facet can be predicted. The independent facets refer to the attitude towards cybersecurity countermeasures (Attitude countermeasures, Self-efficacy countermeasures),

security awareness countermeasures (Administrative countermeasures, Managerial countermeasures, Support countermeasures), and users' addictive behaviours (Premeditation, Urgency) of employees is consider as the mediator. The dependent facet is the employees' risky cybersecurity behaviour practices (Risky behaviour, Digital trust behaviour, Mitigating behaviour) (Darlington and Hayes, 2016). The three tests are direct effect, mediator effect and moderator effect. The following illustration may be beneficial in understanding the three tests.



Equation 6. 1: Influence of users' addictive behaviours on information security countermeasures and risky cybersecurity behaviour practices

- **Equation 6. 1: Direct effect between variables (independents and the dependent) using linear regression followed by brief interpretations of the results.**

Prediction Equation $y = b_1 + b_2 * x$

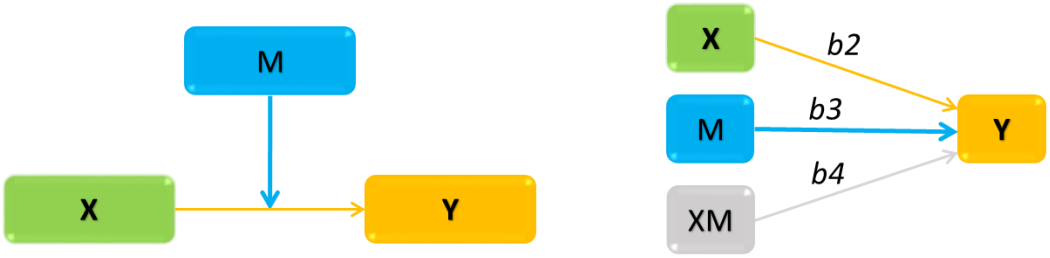
Equation 6. 2: Direct effect

- **Equation 6. 2: CQ as a moderator on the relation between the dependent and independent variables followed by brief interpretations of the results.**

The interactions between the independent variables, dependent variable and CQ as moderator will be tested through the hierarchical regression method analysis via Process v3 by Andrew F. Hayes, equation 6.1, which will be followed to test if the independent facets significantly predicted the dependent facet using the moderator's influence on these interactions.

The first entry will be **y** = dependent variable, the second entry will be **x** = independent variable, and the third entry will be **m** = moderator. Equation 6.3 shows the moderator's effect on the relationships between the variables.

Prediction equation $y = b_1 + b_2 x + b_3 m + b_4 x*m$



Equation 6. 3: Moderator effect

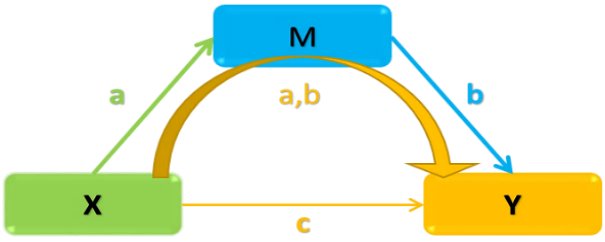
This section will follow the Baron and Kenny (1986) causal steps, and the regression will be through Process v3 by Andrew F. Hayes, equation 6.4, following the below steps that summarise the mediator method, as follows:

1- First path: x variable predicts y – the direct path c.

2- Second path: x variable predicts m – the direct path a.

3- Third path: x and m together predicting y – the indirect path a, b.

Prediction equation $Y = b_1 + b_2 x + b_3 m$



Equation 6. 4: Mediator effect

The following questions are created from the research hypotheses:

1. How do the attitudes towards the cybersecurity countermeasures influence the risky cybersecurity behaviours practices?
2. How do the security awareness countermeasures influence the risky cybersecurity behaviour practices?

   How do the users' addictive behaviours influence the risky cybersecurity behaviour practices?
3. How do the attitudes towards the cybersecurity countermeasures influence the users' addictive behaviours?
4. How do the users' addictive behaviours mediate between countermeasures and the risky cybersecurity behaviour practices?
5. How do the security awareness countermeasures influence the users' addictive behaviours?

6.4.1 The Result for the First Hypothesis

The first hypothesis of the study is posited as:

Hypothesis 1: Attitudes towards the cybersecurity countermeasures are positively related to the risky cybersecurity behaviour practices.

Regression analysis is defined as the type of relationships which helps in quantifying the dependent variables to the independent variables. In this thesis, regression analysis was conducted by the researcher using SPSS software and the results for the hypothesis are illustrated in the following figures.

Table 6. 9: Model summary for the first hypothesis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.612[a]	.374	.369	1.52800

a. Predictors: (Constant), Attitude

Table 6. 10 : ANOVA[a] for the first hypothesis

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	170.373	1	170.373	72.971	.000[b]
	Residual	284.845	122	2.335		
	Total	455.218	123			

a. Dependent Variable: Dependent

b. Predictors: (Constant), Attitude

Table 6. 11: Coefficients[a] for the first hypothesis

Coefficients[a]

Model		Unstandardized Coefficients		Standardised Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	.655	.359		1.824	.071
	Attitude	.684	.080	.612	8.542	.000

a. Dependent Variable: Dependent

Table 6. 12: Collinearity diagnostics[a] for the first hypothesis

Collinearity Diagnostics[a]

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions	
				(Constant)	Attitude
1	1	1.924	1.000	.04	.04
	2	.076	5.036	.96	.96

a. Dependent Variable: Dependent

Table 6. 13: Residual statistics[a] for the first hypothesis

Residual Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.3387	5.4411	3.4901	1.17692	124
Residual	-3.75736	3.97756	.00000	1.52178	124
Std. Predicted Value	-1.828	1.658	.000	1.000	124
Std. Residual	-2.459	2.603	.000	.996	124

a. Dependent Variable: Dependent

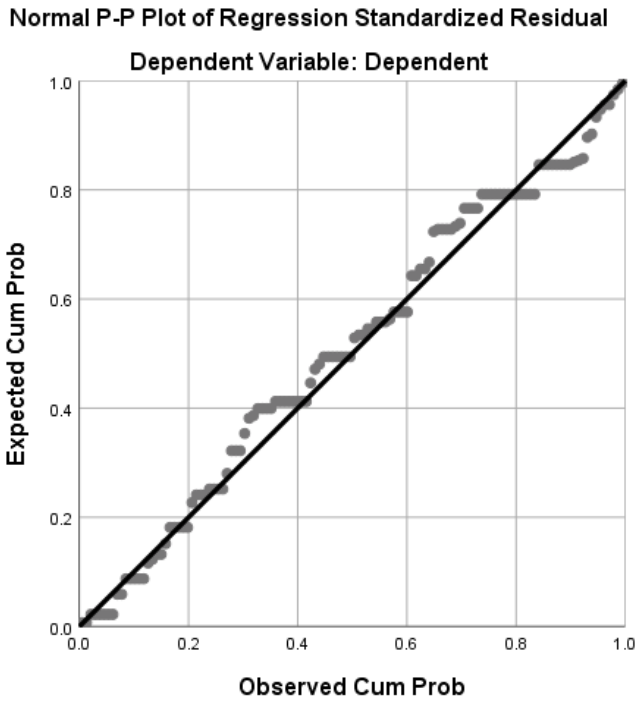


Figure 6. 1: EIO normality test for the first hypothesis

Linear regression analysis was used to test if attitudes towards the cybersecurity countermeasures predicted risky cybersecurity behaviour practices. The result shown in the tables above indicated that the coefficient of R=0.612 suggests a positive relationship between

attitudes towards cybersecurity countermeasures and risky cybersecurity behaviour practices. Also, the R^2= 0.374, which indicates an acceptable level of goodness in this model, were 37.4% of the variance of attitudes towards cybersecurity countermeasures could be explained by risky cybersecurity behaviours practices. Furthermore, based on ANOVA test results, this model is predicting the dependent variable risky cybersecurity behaviour practices well because F (1,122) = 72.971 at significant value p< 0.01. Finally, b1= 0.655, b2=0.684, and t (1,122) =8.542 with Beta positive value = 0.612 indicates that a higher level of attitudes towards cybersecurity countermeasures might decrease risky cybersecurity behaviour practices. Below is the prediction equation:

Risky cybersecurity behaviour practices = 0.655 + 0.684 Attitudes towards cybersecurity countermeasures.

6.4.2 The Result for the Second Hypothesis

The second hypothesis of the study is posited as:

Hypothesis 2: Security awareness countermeasures are positively related to the risky cybersecurity behaviour practices.

Table 6. 14: Model summary for the second hypothesis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.568[a]	.323	.317	1.20050

a. Predictors: (Constant), Attitude

Table 6. 15: ANOVA[a] for the second hypothesis

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	83.708	1	83.708	58.082	.000[b]
	Residual	175.826	122	1.441		

	Total	259.534	123			

a. Dependent Variable: Risky cybersecurity behaviour practices.
b. Predictors: (Constant), Attitude

Table 6. 16: Coefficients[a] for the second hypothesis

Coefficients[a]

Model		Unstandardized Coefficients		Standardised Coefficients		
		B	Std. Error	Beta	T	Sig.
1	(Constant)	3.281	.282		11.630	.000
	Attitude	.479	.063	.568	7.621	.000

a. Dependent Variable: Risky cybersecurity behaviour practices.

Table 6. 17: Collinearity diagnostics[a] for the second hypothesis

Collinearity Diagnostics[a]

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions	
				(Constant)	Attitude
1	1	1.924	1.000	.04	.04
	2	.076	5.036	.96	.96

a. Dependent Variable: Risky cybersecurity behaviour practices.

Table 6. 18: Residual statistics[a] for the second hypothesis

Residual Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	3.7607	6.6363	5.2687	.82496	124
Residual	-2.76073	2.76001	.00000	1.19561	124
Std. Predicted Value	-1.828	1.658	.000	1.000	124
Std. Residual	-2.300	2.299	.000	.996	124

a. Dependent Variable: Risky cybersecurity behaviour practices.

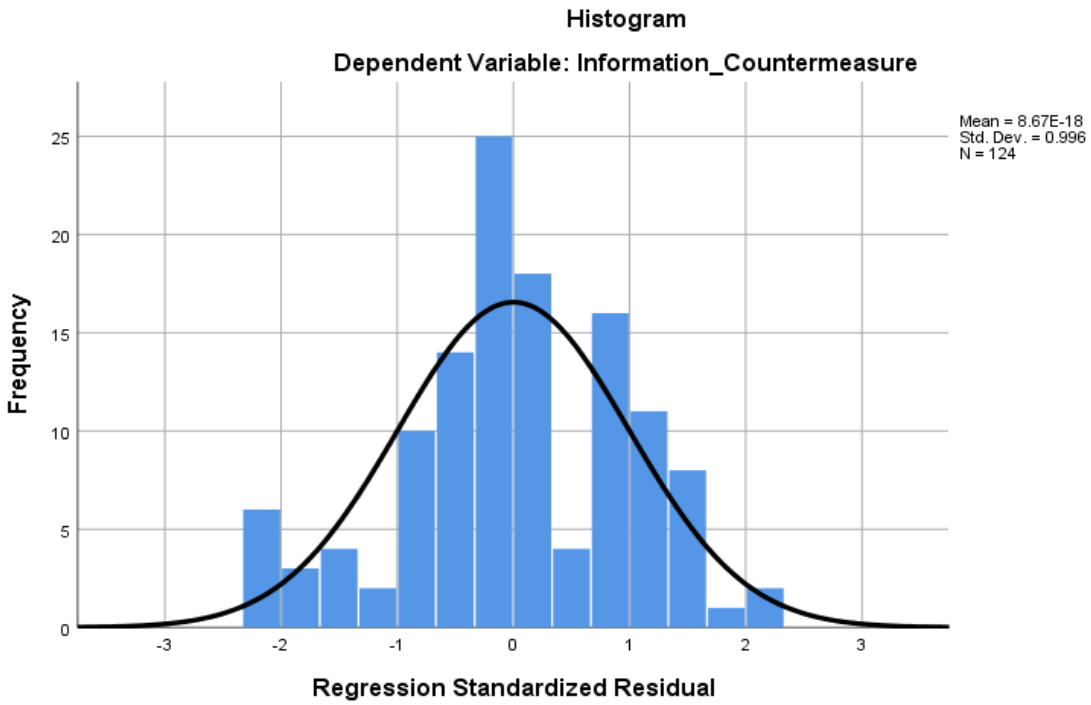


Figure 6. 2: EIO normality test for the second hypothesis

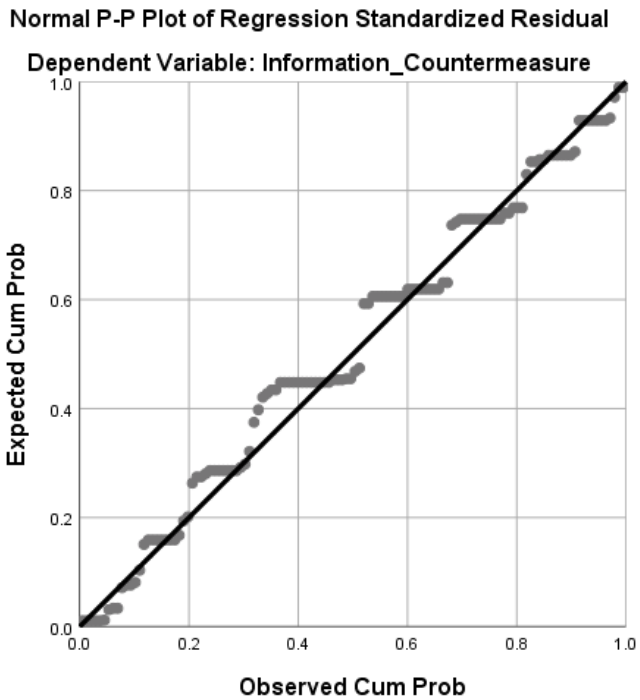


Figure 6. 3: EIO normality test for the second hypothesis

Linear regression analysis was considered to check if the security awareness countermeasures are positively related to the risky cybersecurity behaviour practices. The

results, which can be seen above, can be very beneficial for the readers of this thesis to understand the coefficient of R= 0.568; hence, it can be understood that there is a positive relationship between the two variables of this hypothesis. From the same table, $R^2 = 0.323$, which indicates an acceptable level for goodness in this model, where 32.3% of the variance of the security awareness countermeasures can be explained by the risky cybersecurity behaviour practices. From the calculations of the ANOVA table, this model is predicting that dependent variable risky cybersecurity behaviour practices because F (1,122) = 58.082 at the significant value p<0.01. Finally, it can be said that b1= 3.281 and b2= 0.479 and t (1,122) = 7.621 with a beta positive value = 0.568 and it helps in understanding that a higher level of security awareness countermeasures might minimise risky cybersecurity behaviour practices. The predicted equation is:

Risky cybersecurity behaviour practices = 3.281+0.479 Security awareness countermeasures.

6.4.3 The Result for the Third Hypothesis

The third hypothesis of the study is posited as:

Hypothesis 3: Users' addictive behaviours is positively related to the risky cybersecurity behaviour practices.

Table 6. 19: Model summary for the third hypothesis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.612[a]	.374	.369	1.36719

a. Predictors: (Constant), Dependent

Table 6. 20: ANOVA[a] for the third hypothesis

ANOVA[a]

Model	Sum of Squares	Df	Mean Square	F	Sig.

1	Regression	136.399	1	136.399	72.971	.000[b]
	Residual	228.045	122	1.869		
	Total	364.444	123			

a. Dependent Variable: Risky cybersecurity behaviour practices.
b. Predictors: (Constant), Dependent

Table 6. 21: Coefficients[a] for the third hypothesis

Coefficients[a]

Model		Unstandardized Coefficients		Standardised Coefficients		
		B	Std. Error	Beta	T	Sig.
1	(Constant)	2.236	.255		8.765	.000
	Dependent	.547	.064	.612	8.542	.000

a. Dependent Variable: Risky cybersecurity behaviour practices.

Table 6. 22: Collinearity diagnostics[a] for the third hypothesis.

Collinearity Diagnostics[a]

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions	
				(Constant)	Dependent
1	1	1.877	1.000	.06	.06
	2	.123	3.900	.94	.94

a. Dependent Variable: Risky cybersecurity behaviour practices.

Table 6. 23: Residual statistics[a] for the third hypothesis

Residual Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	2.7835	6.0678	4.1465	1.05306	124
Residual	-3.52043	3.21652	.00000	1.36163	124
Std. Predicted Value	-1.294	1.824	.000	1.000	124
Std. Residual	-2.575	2.353	.000	.996	124

a. Dependent Variable: Risky cybersecurity behaviour practices

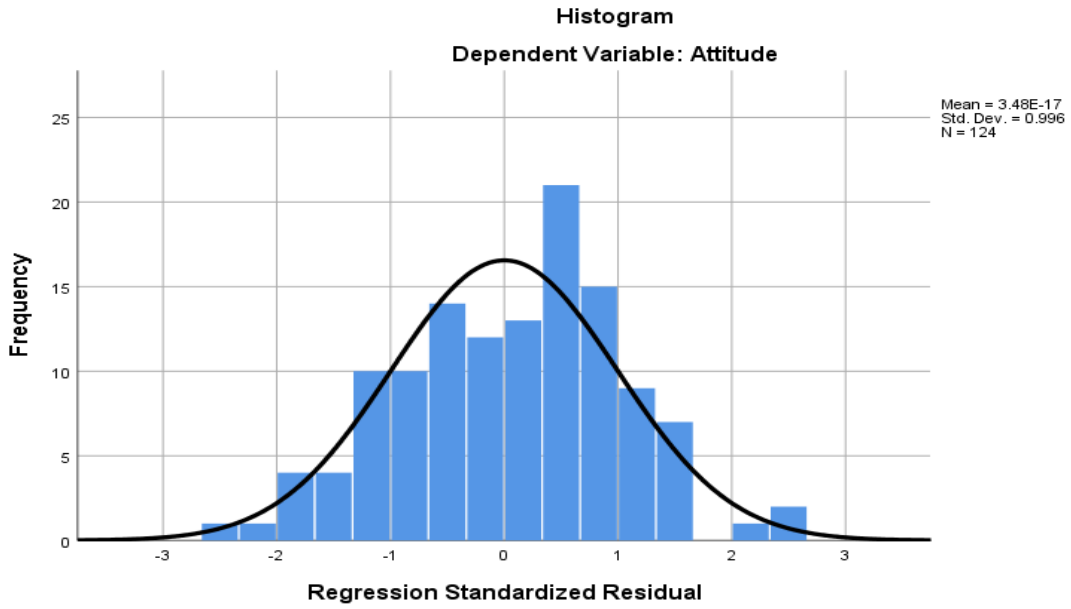


Figure 6. 4: EIO normality test for the third hypothesis

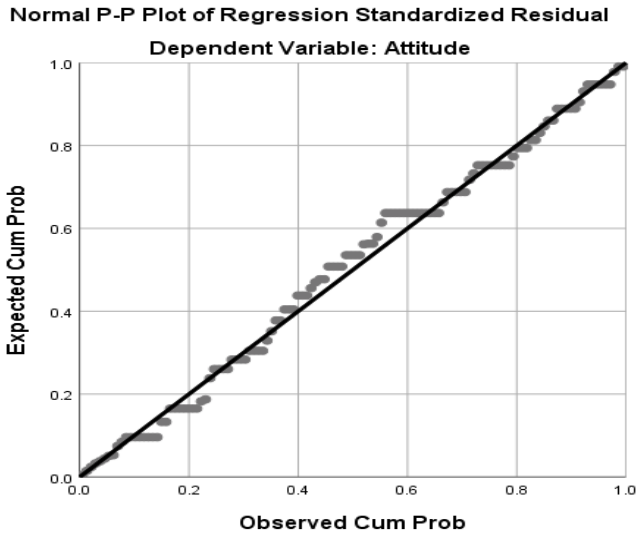


Figure 6. 5: EIO normality test for the third hypothesis

Linear regression analysis was deployed across the two variables of this hypothesis to test whether the users' addictive behaviour is positively related to the risky cybersecurity behaviour practices. The results shown in the above table indicated that the coefficient of R is 0.612, which suggests that there is a positive relationship between the two variables of this

hypothesis. $R^2 = 0.374$, which also helps in understanding the acceptable level of goodness in this model where 37.4% of the variance of the users' addictive behaviours must be explained by the risky cybersecurity behaviour practice. Based on the results obtained from the ANOVA table, it can be said that this model is predicting the dependent variable, which is the risky cybersecurity behaviour practice, towards the users' addictive behaviours because F (1,122) = 72.971 at the significant value of $p< 0.01$. Finally, b1 = 2.236, b2 = 0.547 and t (1,122) = 8.542 with beta positive value = 0.612 helps in understanding that a higher level of the users' addictive behaviours might increase the risky cybersecurity behaviour practice.

Risky cybersecurity behaviour practice = 2.236 + 0.547 users' addictive behaviours.

6.4.4 The Result for the Fourth Hypothesis

The fourth hypothesis of the study is posited as:

Hypothesis 4: Attitudes towards cybersecurity countermeasures are positively related to the users' addictive behaviours.

Table 6. 24: Model summary for the fourth hypothesis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.276[a]	.076	.068	1.85690

a. Predictors: (Constant), Dependent

Table 6. 25: ANOVA[a] for the fourth hypothesis

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	34.554	1	34.554	10.021	.002[b]
	Residual	420.665	122	3.448		
	Total	455.218	123			

a. Dependent Variable: Dependent

b. Predictors: (Constant), Attitudes towards cybersecurity countermeasures

Table 6. 26: Coefficients[a] for the fourth hypothesis

Coefficients[a]

Model		Unstandardized Coefficients		Standardised Coefficients		
		B	Std. Error	Beta	t	Sig.
1	(Constant)	1.568	.630		2.489	.014
	Information Countermeasures	.365	.115	.276	3.166	.002

a. Dependent Variable: Dependent

Table 6. 27: Collinearity diagnostics[a] for the fourth hypothesis

Collinearity Diagnostics[a]

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions (Constant)	Variance Proportions Information Countermeasures
1	1	1.964	1.000	.02	.02
	2	.036	7.418	.98	.98

a. Dependent Variable: Dependent

Table 6. 28: Residual statistics[a] for the fourth hypothesis

Residual Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.9325	4.1218	3.4901	.53002	124
Residual	-3.12179	3.06065	.00000	1.84933	124
Std. Predicted Value	-2.939	1.192	.000	1.000	124
Std. Residual	-1.681	1.648	.000	.996	124

a. Dependent Variable: Dependent

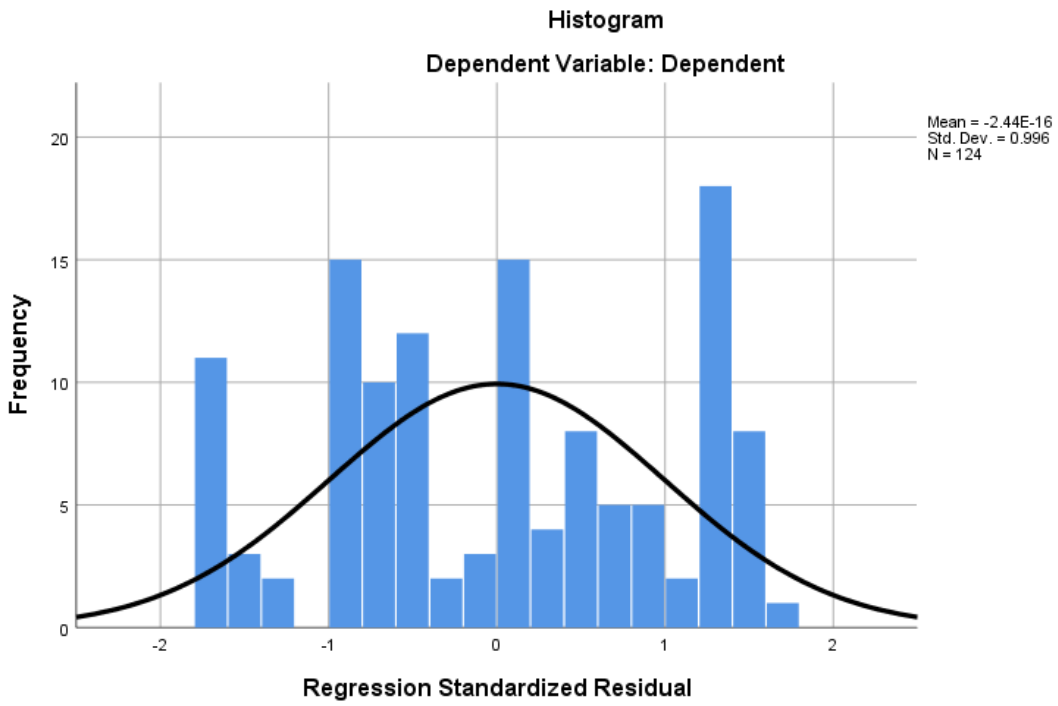


Figure 6. 6: EIO normality test for the fourth hypothesis

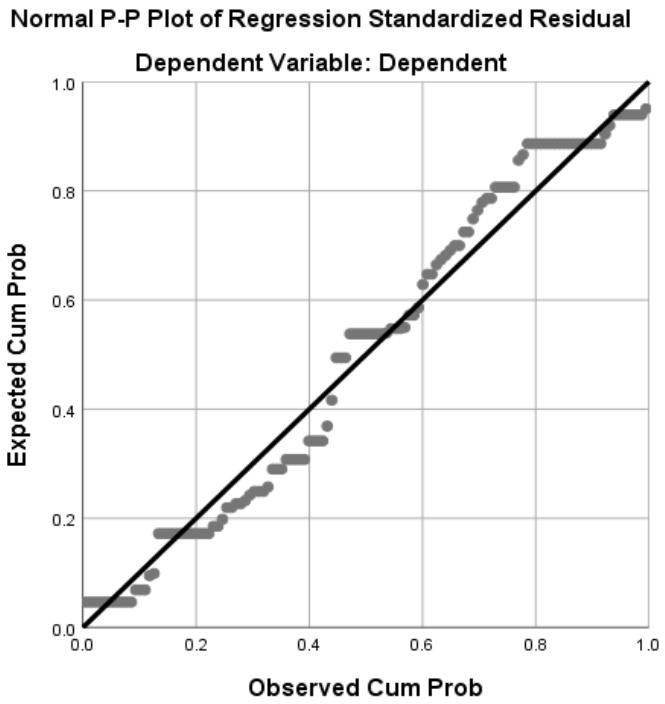


Figure 6. 7: EIO normality test for the fourth hypothesis

Linear regression analysis was considered to check if the attitudes towards cybersecurity countermeasures are positively related to the users' addictive behaviours. The results, which can be seen above, are very beneficial for the readers of this thesis to understand the coefficient of R= 0.276; hence, it can be understood that there is a positive relationship between the two variables of this hypothesis. From the same table, $R^2 = 0.076$, which indicates an acceptable level for goodness in this model, where 7.6% of the variance of the attitudes towards cybersecurity countermeasures can be explained by the users' addictive behaviours. From the calculations of the ANOVA table, this model is predicting that dependent variable users' addictive behaviours that influence IS countermeasures because F (1, 122) = 10.021 at significant value $p < 0.01$. Finally, b1= 1.568, b2= 0.365 and t (1, 122) = 3.166 with beta positive value = 0.276, and it helps in understanding that a higher level of attitudes towards cybersecurity countermeasures positively increase users' addictive behaviours. The predicted equation is:

Users' addictive behaviours = 3.281+0.479 attitudes towards cybersecurity countermeasures

6.4.5 The Result for the Fifth Hypothesis

The fifth hypothesis of the study is posited as:

Hypothesis 5: Users' addictive behaviours are positively mediating between risky cybersecurity behaviour practices and information security countermeasures. This hypothesis is divided into three sections:

a. Information security countermeasures – Risky cybersecurity behaviour practices (dependent).
b. Information security countermeasures – Mediator (Premeditation + Urgency).
c. Information security countermeasures + Mediator (Premeditation + Urgency) – Risky cybersecurity behaviour practices.

   The behavioural practices usually influence the personal traits of the employees in an organisation. A regression analysis is performed to explain how an observed independent variable (IS countermeasures) influences the mediator variable (non-observable), personal traits in this case, which later influences the dependent variable (behavioural practices). The analysis is carried out in a number of steps:

   Step 1; the dependent variable is regressed against the independent variable to prove that behavioural practices is a significant predictor.

   IS countermeasures $\longrightarrow$ Behavioural practices

   Y (IS countermeasures) $= \beta_{10} + \beta_{11} X + E_1$ where β_{11} is significant

   Step 2: The mediator is regressed against the behavioural practices to prove that the latter is a significant predictor.

Me= $\beta_{20} + \beta_{21} X + E_2$ where β_{21} is significant.

Step 3: The dependent variable is regressed against the independent variable and the mediator.

$Y = \beta_{30} + \beta_{31} X + \beta_{32}Me + E$. in this case β_{31} should be smaller than β_{21} above.

The researcher of this thesis used an impulsivity moderator while conducting the regression analysis. Mediators are simply third-party variables which strengthen or weaken the relationship between the dependent and the independent variables in question.

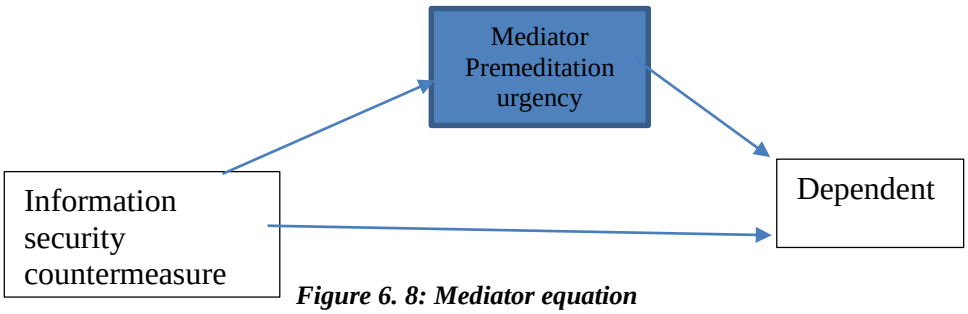


Figure 6. 8: Mediator equation

6.4.5.1 Information Security Countermeasures – Risky Cybersecurity Behaviour Practices

Table 6. 29: Model summary for the fifth hypothesis (a)

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.328[a]	.108	.093	1.83240

a. Predictors: (Constant), Mediator, IS countermeasures

Table 6. 30: ANOVA[a] for the fifth hypothesis (a)

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	48.938	2	24.469	7.287	.001[b]
	Residual	406.280	121	3.358		
	Total	455.218	123			

a. Dependent Variable: Dependent

b. Predictors: (Constant), Mediator, IS countermeasures

Table 6. 31: Coefficients[a] for the fifth hypothesis (a)

Coefficients[a]

Model		Unstandardized Coefficients B	Unstandardized Coefficients Std. Error	Standardised Coefficients Beta	t	Sig.
1	(Constant)	1.139	.655		1.738	.085
	Information Countermeasures	.063	.185	.048	.341	.734
	Mediator	.393	.190	.289	2.070	.041

a. Dependent Variable: Dependent

Table 6. 32: Collinearity diagnostics[a] for the fifth hypothesis (a)

Collinearity Diagnostics[a]

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions (Constant)	Variance Proportions Dependent
1	1	1.877	1.000	.06	.06
	2	.123	3.900	.94	.94

a. Dependent Variable: IS countermeasures

Table 6. 33: Residual statistics[a] for the fifth hypothesis (a)

Residual Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	4.7507	5.9989	5.2687	.40020	124
Residual	-3.75071	2.24929	.00000	1.39638	124
Std. Predicted Value	-1.294	1.824	.000	1.000	124
Std. Residual	-2.675	1.604	.000	.996	124

a. Dependent Variable: IS countermeasures

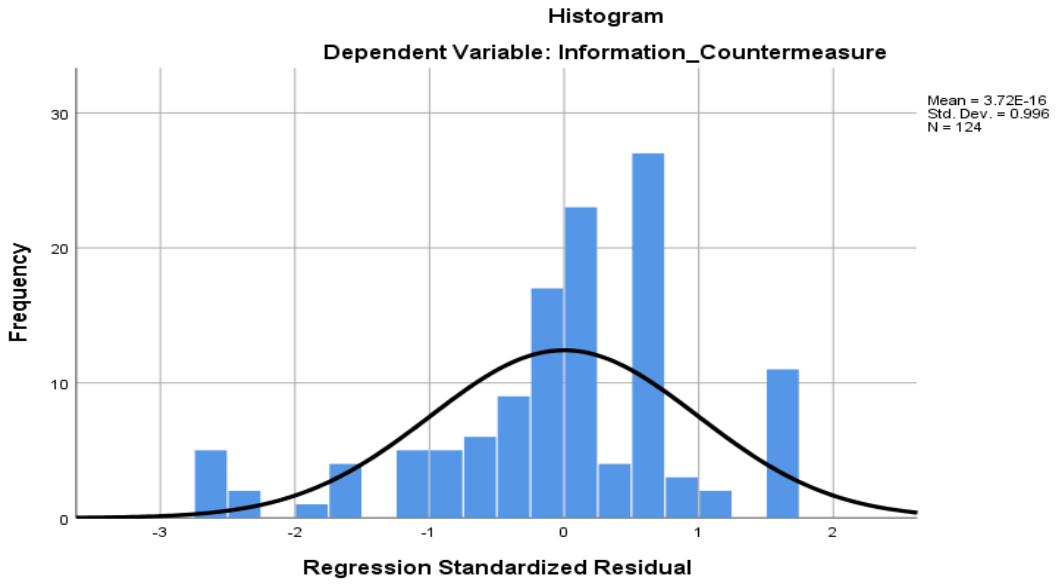


Figure 6. 9: EIO normality test for the fifth hypothesis (a)

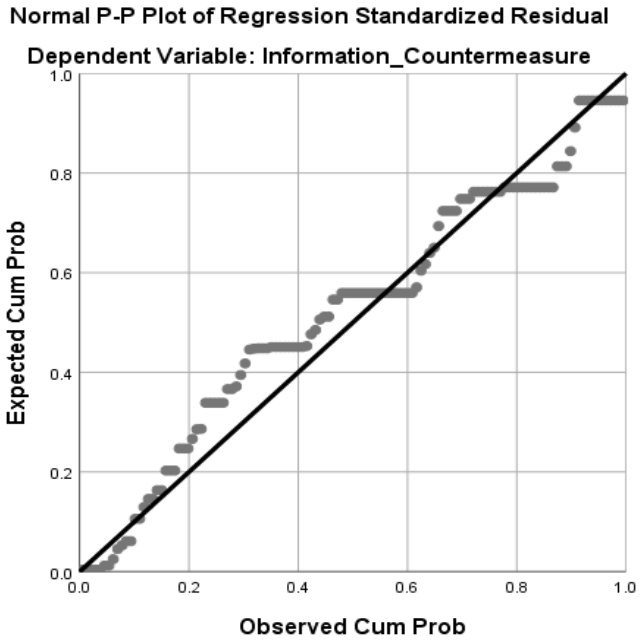


Figure 6. 10: EIO normality test for the fifth hypothesis (a)

Risky cybersecurity behaviour practices = 1.568 + 0.365 information security countermeasures.

6.4.5.2 Information Security Countermeasures – Mediator (Premeditation + Urgency).

Table 6. 34: Variables entered/removed[a] for the fifth hypothesis (b)

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	IS Countermeasures[b]	.	Enter

a. Dependent Variable: Mediator

b. All requested variables entered

Table 6. 35: Model summary for the fifth hypothesis (b)

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.789[a]	.622	.619	.87290

a. Predictors: (Constant), IS countermeasures

c. Dependent Variable: Mediator.

Table 6. 36: ANOVA for the fifth hypothesis (b)

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	152.847	1	152.847	200.600	.000[b]
	Residual	92.958	122	.762		
	Total	245.805	123			

a. Dependent Variable: Mediator

b. Predictors: (Constant), IS countermeasures

Table 6. 37: Coefficients[a] for the fifth hypothesis (b)

Coefficients[a]

Model		Unstandardized Coefficients		Standardised Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	t	Sig.	Tolerance	VIF
1	(Constant)	1.091	.296		3.685	.000		
	IS Countermeasures	.767	.054	.789	14.163	.000	1.000	1.000

a. Dependent Variable: Mediator

Table 6. 38: Collinearity diagnostics[a] for the fifth hypothesis (b)

Collinearity Diagnostics[a]

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions (Constant)	Variance Proportions IS_Countermeasures
1	1	1.964	1.000	.02	.02
	2	.036	7.418	.98	.98

a. Dependent Variable: Mediator

Table 6. 39: Residual statistics[a] for the fifth hypothesis (b)

Residual Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.8583	6.4628	5.1342	1.11475	124
Residual	-3.85553	2.83949	.00000	.86934	124
Std. Predicted Value	-2.939	1.192	.000	1.000	124
Std. Residual	-4.417	3.253	.000	.996	124

a. Dependent Variable: Mediator

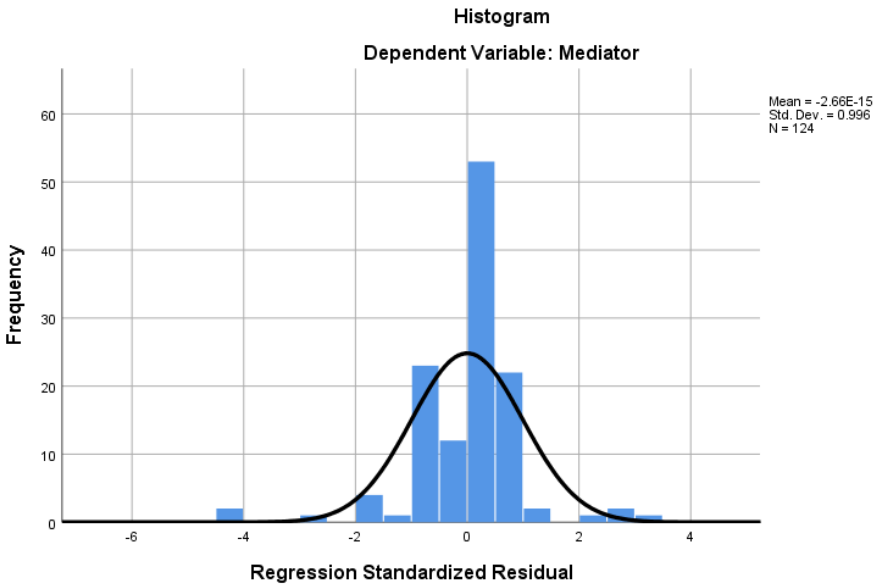


Figure 6. 11: EIO normality test for the fifth hypothesis (b)

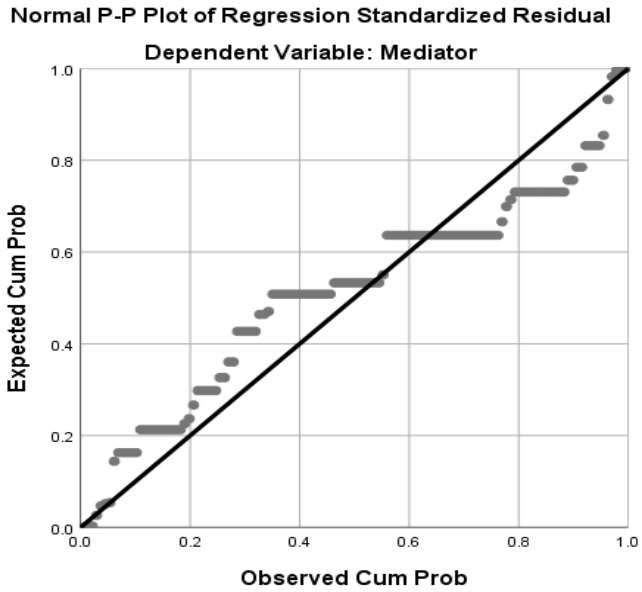


Figure 6. 12: EIO normality test for the fifth hypothesis (b)

Linear regression analysis was conducted on this fifth hypothesis (b) of this thesis to test if the addictive behaviours of the workforces of public organisations are mediating between

risky cybersecurity behaviour practices and the information security countermeasures. The results shown in the tables indicated that the coefficient of R= 0.789, which suggests that users' addictive behaviour is mediating between the two variables of this hypothesis. Also, $R^2 = 0.622$, which indicates the acceptable level of goodness in this model, where 62.2% of the variance in information security countermeasures can be explained by the risky cybersecurity behaviour practices. From the ANOVA test results, it can be understood that this model is predicting the dependent variable information security countermeasures which can minimise the risky cybersecurity behaviour practices because F (1, 112) = 7.287 at significant value $p<0.01$. Finally, b1 = 1.091 b2 = 0.067 and t (1, 12) = 0.341 with beta positive value = 0.048, which indicates that the users' addictive behaviours are positively mediating between risky cybersecurity behaviour practices and information security countermeasures.

Information security countermeasures = 1.091 + 0.067 users' addictive behaviours

6.4.5.3 Information Security Countermeasures + Mediator - Risky Cybersecurity Behaviour Practices

Table 6. 40: Variables entered/removed[a] for the fifth hypothesis (c)

Variables Entered/Removed[a]

Model	Variables Entered	Variables Removed	Method
1	Mediator, IS Countermeasures[b]	.	Enter

a. Dependent Variable: Dependent
d. All requested variables entered.

Table 6. 41: Model summary for the fifth hypothesis (c)

Model Summary[b]

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate

1	.328[a]	.108	.093	1.83240

a. Predictors: (Constant), Mediator, IS countermeasures

c. Dependent Variable: Dependent

Table 6. 42: ANOVA for the fifth hypothesis ©

ANOVA[a]

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	48.938	2	24.469	7.287	.001[b]
	Residual	406.280	121	3.358		
	Total	455.218	123			

a. Dependent Variable: Dependent

d. Predictors: (Constant), Mediator, IS countermeasures

Table 6. 43: Coefficients[a] for the fifth hypothesis (c)

Coefficients[a]

Model		Unstandardized Coefficients		Standardised Coefficients			Collinearity Statistics	
		B	Std. Error	Beta	T	Sig.	Tolerance	VIF
1	(Constant)	1.139	.655		1.738	.085		
	IS Countermeasures	.063	.185	.048	.341	.734	.378	2.644
	Mediator	.393	.190	.289	2.070	.041	.378	2.644

a. Dependent Variable: Dependent

Table 6. 44: Collinearity diagnostics[a] for the fifth hypothesis (c)

Collinearity Diagnostics[a]

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions (Constant)	Variance Proportions Information Countermeasures	Variance Proportions Mediator
1	1	2.943	1.000	.01	.00	.00
	2	.043	8.315	.99	.10	.10
	3	.015	14.097	.00	.89	.90

a. Dependent Variable: Dependent

Table 6. 45: Residual statistics[a] for the fifth hypothesis (c)

Residual Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.5949	4.3331	3.4901	.63077	124
Residual	-3.33313	3.43091	.00000	1.81744	124
Std. Predicted Value	-3.005	1.337	.000	1.000	124
Std. Residual	-1.819	1.872	.000	.992	124

a. Dependent Variable: Dependent

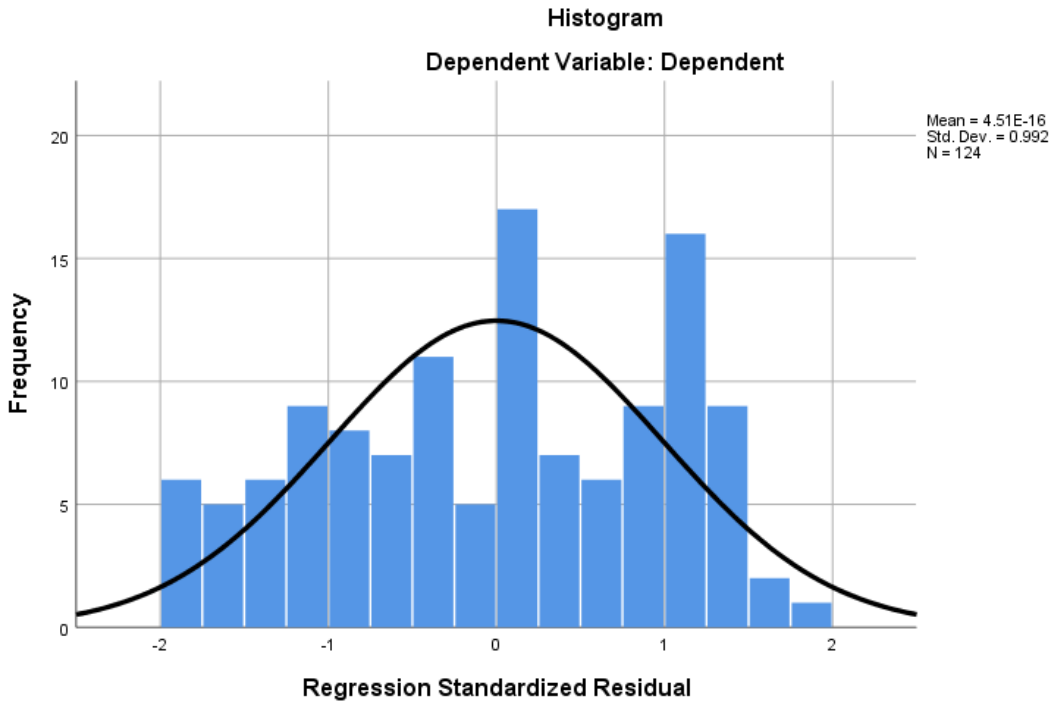


Figure 6. 13: EIO normality test for the fifth hypothesis (c)

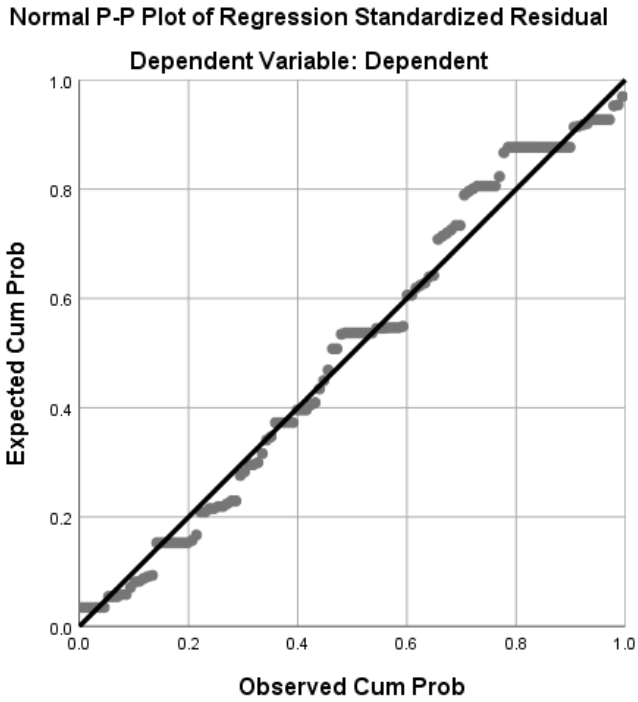


Figure 6. 14: EIO normality test for the fifth hypothesis (c)

Linear regression analysis conducted on this hypothesis was used to test if the independent variable plus the mediator is able to predict the dependent variable of this hypothesis or not. Based on the above tables, it can be identified that the coefficient of R= 0.328, which indicates that there is a positive association between the independent and the mediator to the dependent variable of this hypothesis. Also, the R^2= 0.108, which indicates the acceptable level of goodness in the model, where 10.8% of the variance which is the independent variable and the mediator should be explained by the dependent variable of this hypothesis. From the ANOVA test result, it can be understood that this model is predicting the dependent variable of this hypothesis because F (1, 121) = 7.287 at the significant value p <0.01. Finally, b1= 0.063, b2= 0.393 and t (1, 121) = 2.070 with a beta positive value = 0.289, which indicates that the users' addictive behaviours are mediating between the users' addictive behaviours and information security countermeasures.

Information security countermeasures = 1.139 + 0.063 Risky cybersecurity behaviour practices + 0.393 Users' addictive behaviours.

6.4.6 The Result for the Sixth Hypothesis

The sixth hypothesis of the study is posited as:

Hypothesis 6: Security awareness countermeasures are positively related to users' addictive behaviours.

Table 6. 46: Model summary for the sixth hypothesis

Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate
1	.276[a]	.076	.068	1.40209

a. Predictors: (Constant), Dependent

Table 6. 47: ANOVA[a] for the sixth hypothesis

ANOVA[a]

Model		Sum of Squares	Df	Mean Square	F	Sig.
1	Regression	19.700	1	19.700	10.021	.002[b]
	Residual	239.834	122	1.966		
	Total	259.534	123			

a. Dependent Variable: Security awareness _countermeasures

b. Predictors: (Constant), Dependent

Table 6. 48: Coefficients[a] for the sixth hypothesis

Coefficients[a]

Model		Unstandardized Coefficients		Standardised Coefficients		
		B	Std. Error	Beta	T	Sig.
1	(Constant)	4.543	.262		17.362	.000
	Dependent	.208	.066	.276	3.166	.002

a. Dependent Variable: Security awareness _countermeasures

Table 6. 49: Collinearity diagnostics[a] for the sixth hypothesis

Collinearity Diagnostics[a]

Model	Dimension	Eigenvalue	Condition Index	Variance Proportions (Constant)	Variance Proportions Support Countermeasures
1	1	1.964	1.000	.02	.02
	2	.036	7.418	.98	.98

a. Dependent Variable: Mediator

Table 6. 50: Residual statistics[a] for the sixth hypothesis

Residual Statistics[a]

	Minimum	Maximum	Mean	Std. Deviation	N
Predicted Value	1.8583	6.4628	5.1342	1.11475	124
Residual	-3.85553	2.83949	.00000	.86934	124
Std. Predicted Value	-2.939	1.192	.000	1.000	124
Std. Residual	-4.417	3.253	.000	.996	124

a. Dependent Variable: Mediator

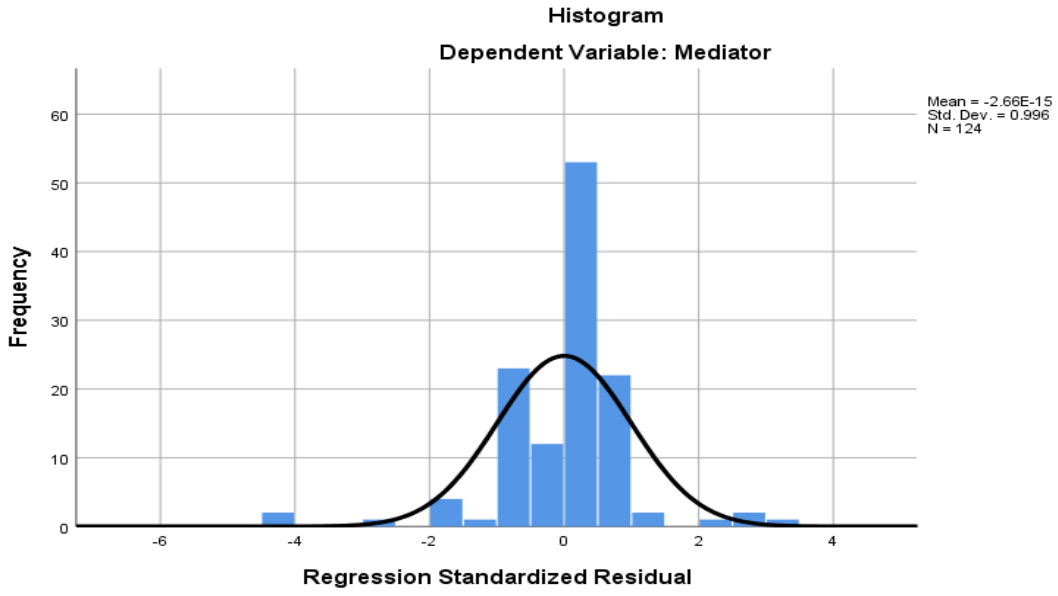


Figure 6. 15: EIO normality test for the sixth hypothesis

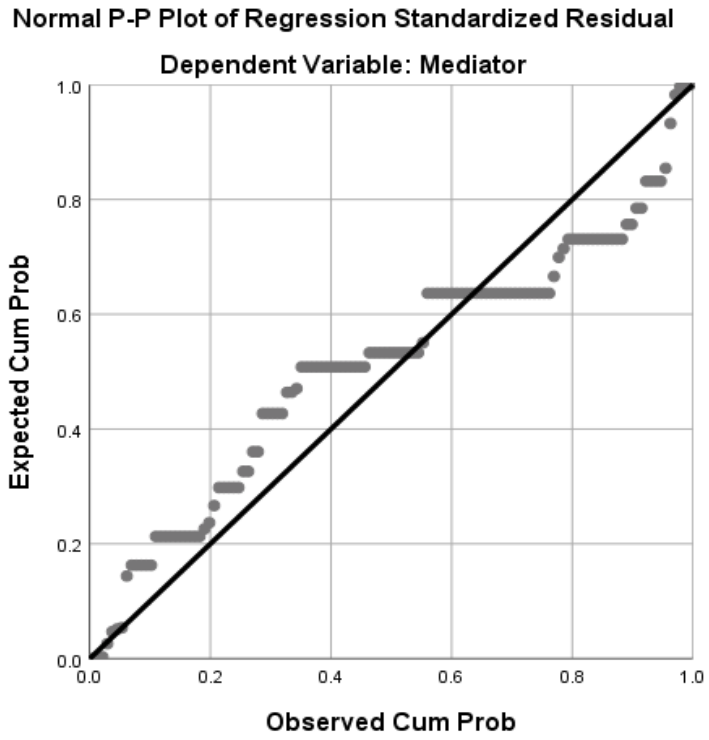


Figure 6. 16: EIO normality test for the sixth hypothesis

Linear regression was conducted to test if the addictive behaviours of the workforce are positively related to the security awareness countermeasures. Based on the above tables, it can be understood that the coefficient of R= 0.276, which indicates that there is a positive relationship between the two variables of this hypothesis. Also, the R^2= 0.076, which indicates the acceptable level of goodness in this model where 7.6% of the variance of users' addictive behaviours could be explained by the security awareness countermeasures. The results obtained from the ANOVA table help in understanding that this model is predicting the dependent variable users' addictive behaviours because F (1, 122) = 10.021 at the significant value p< 0.01. Finally, b1= 4.543 and b2= 0.2018 and t (1, 122) = 3.166 with a beta positive value = 0.276, which indicates that the higher level of security awareness countermeasures might have an influence on the users' addictive behaviours. The predicted equation is

Security awareness countermeasures = 4.543+ 0.2018 Users' addictive behaviours.

6.5 Confirming the Research Constructs Association

Structural model and hypotheses testing:

The results for the relationship between the dependent and independent variables using simple regression are reported in the previous sections. This section describes the results from the path models to confirm the direct and indirect relationships between the research constructs. For this purpose, several models were created using AMOS. The results from these exercises are reported in the following sections.

6.5.1 Relationship between Dependent and Independent Constructs

The first path analysis model that was created was intended to depict the relationship between risky cybersecurity behaviour practices and information security countermeasures. The path diagram is shown in the figure below

The purpose of the first SEM model was to portray the association between cyber risk variables and cyber action outcomes. The path diagram is shown in the following figure.

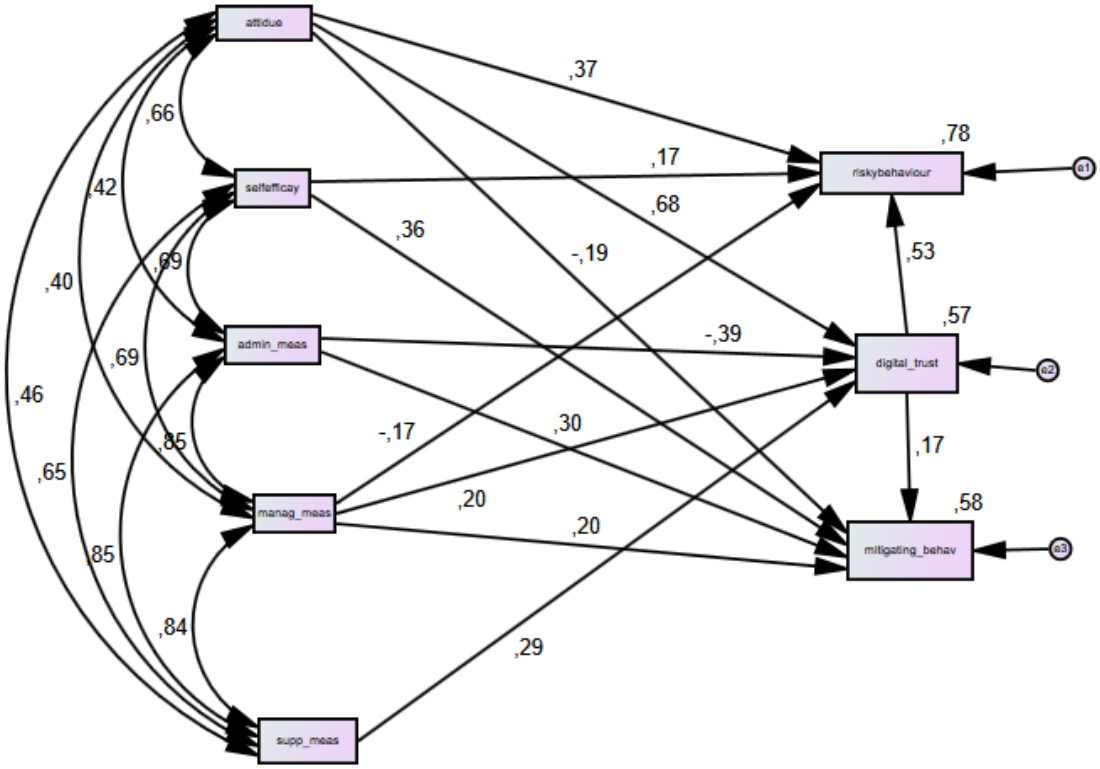


Figure 6. 17: Relationship between IV and DV

The model fit measures produced by AMOS are reported in in tables 6.51 and 6.50. These threshold vales showed that the structural model provided a good fit to the data. The hypothesised theory appears to be accepted. The CFI is 1; P close is 0.569; CMIN/df is 1.025; and the RMSEA is 0.014. The model predicts 78% of the variance in risky behaviour, 57% of digital trust and 58% of mitigating behaviours.

Table 6. 51: Model fitness measures

Measure	Threshold	Model fitness
CMIN/df	< 3, sometime < 5 is acceptable	1.025
CFI	> 0.9	1.00
AGFI	>0.8	0.964
RMSEA	<0.05 sometimes <0.05-0.08	0.014
P close	>0.05	0.569

Table 6. 52: Model standardised regression weight

			Estimate	C.R.	P	Label
digital_trust	<---	Attidue	.676	10.138	***	Accepted
digital_trust	<---	manag_meas	.200	1.601	.109	Rejected
digital_trust	<---	supp_meas	.286	2.233	.026	Accepted
digital_trust	<---	admin_meas	-.391	-3.028	.002	Accepted
riskybehaviour	<---	Attidue	.371	5.113	***	Accepted
riskybehaviour	<---	Selfefficay	.169	2.331	.020	Accepted
mitigating_behav	<---	manag_meas	.200	1.669	.095	Rejected
riskybehaviour	<---	manag_meas	-.166	-2.790	.005	Accepted
mitigating_behav	<---	Selfefficay	.360	3.523	***	Accepted
riskybehaviour	<---	digital_trust	.530	8.495	***	Accepted
mitigating_behav	<---	digital_trust	.167	1.908	.056	Partial
mitigating_behav	<---	admin_meas	.303	2.561	.010	Accepted
mitigating_behav	<---	Attidue	-.190	-1.885	.059	Partial

The above table showed that several paths between independent and dependent variables were found to be significant.

The digital_trust <--- manag_meas and mitigating_behav <--- manag_meas direct effect paths are the only ones which were found to be insignificant. Also, the paths mitigating_behav <--- digital_trust and mitigating_behav <--- attidue are marginally significant at 0.05 level. The other paths are significant at the 0.05 level.

6.5.2 Mediation Analysis Results

The following models were set to test the mediation of users' addictive behaviours (impulsivity) effect of urgency and premeditation on the relationship between the IV and DV variables. The process followed is in line with (Hayes, 2018) model shown in the following figure.

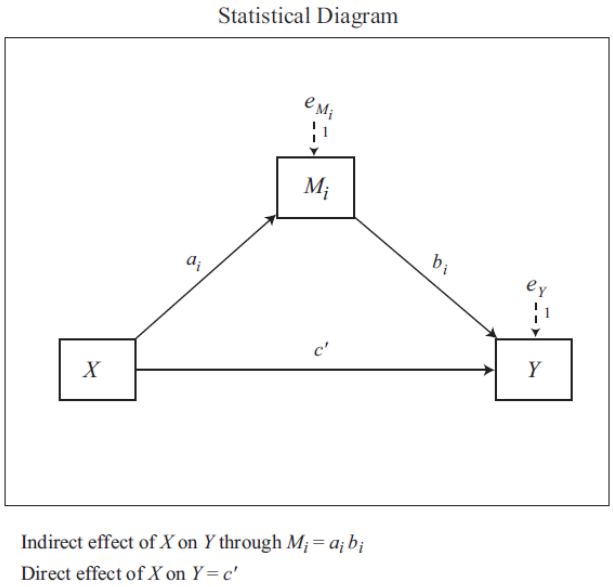


Figure 6. 18: Statistical diagram

6.5.2.1 The Mediating Effect of Impulsivity on DV and IV Relationship

The purpose of this model is to check the indirect effect of IV on DV through the users' addictive behaviours (Impulsivity) construct. The model will examine the direct effect of IV on DV. The path model developed for this purpose is shown in the following figure. The model showed that impulsivity mediates only between DV (digital trust and mitigating behaviour) and IV (self-efficacy, admin measures and management) (Adam *et al.*, 2020).

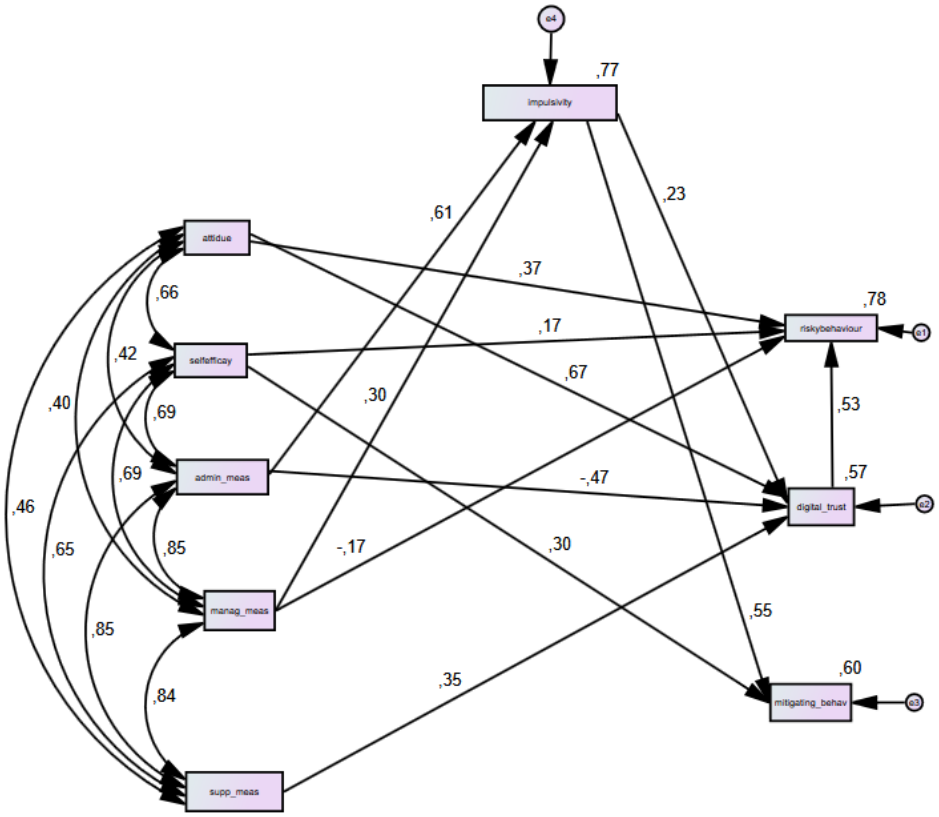


Figure 6. 19: The mediating effect of users' addictive behaviours (Impulsivity) on DV and IV relationship

The model fit measures produced by AMOS are reported in in tables 6.52 and 6.53. These threshold vales showed that the structural model provided a good fit to the data. The hypothesised theory appears to be accepted. The CFI is 1; P close is 0.691; CMIN/df is 1.031; and the RMSEA is 0.016.

The model predicts 78% of the variance in risky behaviour, 57% of digital trust and 60% of mitigating behaviours.

Table 6. 53: Model fit measures

Measure	Estimate	Threshold	Interpretation
CMIN	14,429	--	--
DF	14,000	--	--
CMIN/DF	1,031	Between 1 and 3	Excellent
CFI	1,000	>0.95	Excellent
SRMR	0,020	<0.08	Excellent
RMSEA	0,016	<0.06	Excellent
PClose	0,691	>0.05	Excellent

Table 6. 54: Model standardised regression weight

			Estimate	C.R.	P	Label
impulsivity	<---	admin_meas	,606	7,281	***	
impulsivity	<---	manag_meas	,301	3,618	***	
digital_trust	<---	Attidue	,668	9,991	***	
digital_trust	<---	admin_meas	-,469	-3,245	,001	
digital_trust	<---	supp_meas	,346	2,938	,003	
digital_trust	<---	Impulsivity	,235	1,990	,047	
riskybehaviour	<---	Attidue	,372	5,139	***	
riskybehaviour	<---	Selfefficay	,169	2,333	,020	
mitigating_behav	<---	Selfefficay	,304	4,147	***	
riskybehaviour	<---	manag_meas	-,167	-2,804	,005	
riskybehaviour	<---	digital_trust	,528	8,549	***	
mitigating_behav	<---	Impulsivity	,547	7,475	***	

The above table showed that all the model paths between the independent, dependent and mediator variables were found to be significant at 0.05 level and 0.001 level. Since all the paths are significant, this indicated that there is partial mediation between the IV and DV. However, these results need be checked against the indirect path results.

The results from the indirect path analysis are shown in the following table. The results showed that the standardised indirect (mediated) effect of impulsivity on the relationship

between admin measures and digital trust though path (admin_meas --> impulsivity --> digital_trust) and (admin_meas --> impulsivity --> mitigating_behaviour) is significant at the 0.05 level (p=.048). Similarly, the standardised indirect (mediated) effect of impulsivity on the relationship between admin measures and mitigating measures through path (admin_meas --> impulsivity --> mitigating_behaviour) is significant at the 0.001 level (p=0.001). Likewise, the standardised indirect (mediated) effect of impulsivity on the relationship between management measures and mitigating measures through path (manag_meas --> impulsivity --> mitigating_behav) is significant at the 0.05 level (p=0.012). These three paths showed that impulsivity is a partial mediator.

The indirect effect path analysis showed that impulsivity is not a mediator for the attitude, self-efficacy and supp-measures IV.

It is noticeable from the direct path analysis that digital trust has a mediating effect between attitude, supp_measures, admin measures and risky behaviour. The results appear to show that digital skills may influence cyber risk behaviour.

Table 6. 55: Model indirect effect path results

Indirect Path	Unstandardized Estimate	Lower	Upper	P-Value	Standardised Estimate
admin_meas --> impulsivity --> digital_trust	0,173	0,048	0,376	0,048	0,142*
admin_meas --> impulsivity --> digital_trust --> riskybehaviour	0,085	0,026	0,191	0,042	0,142*
admin_meas --> impulsivity --> mitigating_behav	0,359	0,182	0,580	0,001	0,332***
admin_meas --> digital_trust --> riskybehaviour	-0,280	-0,460	-0,070	0,039	-0,248*
manag_meas --> impulsivity --> digital_trust	0,092	-0,001	0,275	0,109	0,071

manag_meas --> impulsivity --> digital_trust --> riskybehaviour	0,045	-0,001	0,135	0,109	0,071
manag_meas --> impulsivity --> mitigating_behav	0,191	0,049	0,401	0,012	0,165*
attidue --> digital_trust --> riskybehaviour	0,359	0,267	0,464	0,001	0,352***
supp_meas --> digital_trust --> riskybehaviour	0,201	0,061	0,350	0,024	0,183*
impulsivity --> digital_trust --> riskybehaviour	0,150	-0,024	0,269	0,148	0,124

6.5.2.2 The Mediating Effect of Premeditation on DV and IV Relationship

The purpose of this model is to examine the indirect effect of IV on DV through the premeditation construct. The model will examine the direct effect of IV on DV. The path model developed for this purpose is shown in the following figure. The model showed that premeditation mediates only between DV mitigating behaviour and IV (admin measures and management measures).

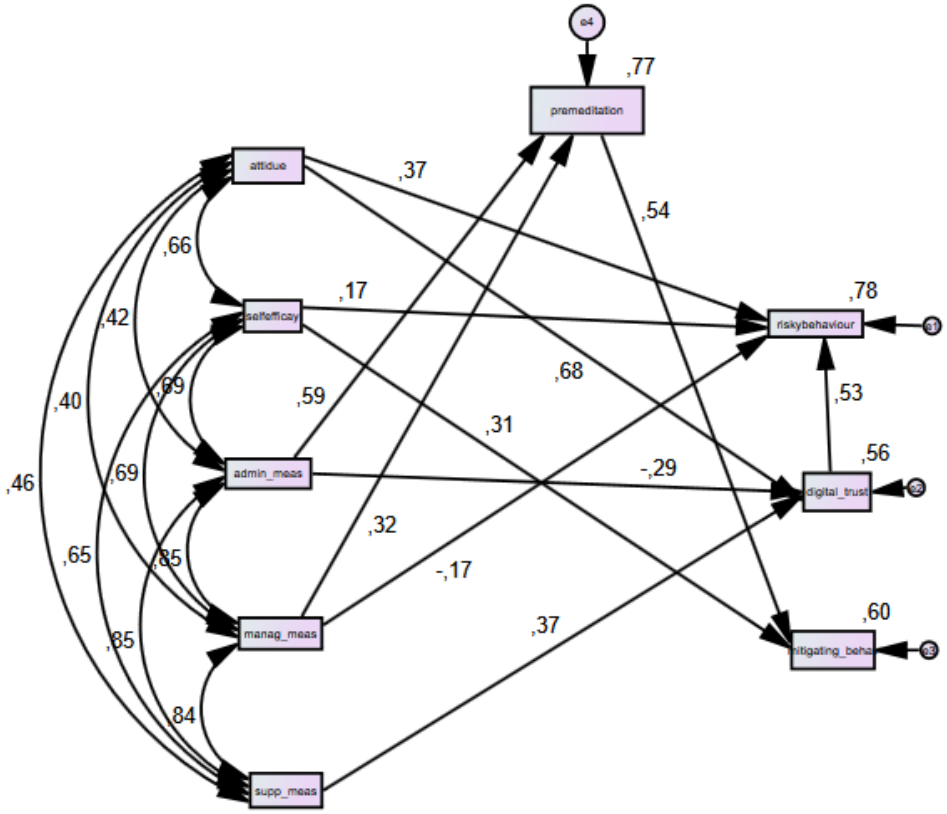


Figure 6. 20: The mediating effect of premeditation on DV and IV relationship

The model fit measures produced by AMOS are reported in in tables 6.55 and 6.56. These threshold vales showed that the structural model provided a good fit to the data. The hypothesised theory appears to be accepted for some of the mediation paths. The CFI is 0.998; P close is 0.573; CMIN/df is 1.173; and the RMSEA is 0.037. The model predicts 78% of the variance in risky behaviour, 56% of digital trust and 60% of mitigating behaviours.

Table 6. 56: Model fit measures

Measure	Estimate	Threshold	Interpretation
CMIN	17,590	--	--
DF	15,000	--	--
CMIN/DF	1,173	Between 1 and 3	Excellent
CFI	0,998	>0.95	Excellent
SRMR	0,028	<0.08	Excellent
RMSEA	0,037	<0.06	Excellent
PClose	0,573	>0.05	Excellent

Table 6. 57: Model standardised regression weight

			Estimate	C.R.	P	Label
digital_trust	<---	Attidue	,676	10,031	***	
digital_trust	<---	admin_meas	-,293	-2,550	,011	
digital_trust	<---	supp_meas	,371	3,143	,002	
premeditation	<---	admin_meas	,588	7,097	***	
premeditation	<---	manag_meas	,321	3,882	***	
riskybehaviour	<---	Attidue	,370	5,098	***	
riskybehaviour	<---	Selfefficay	,169	2,333	,020	
mitigating_behav	<---	Selfefficay	,310	4,211	***	
riskybehaviour	<---	manag_meas	-,166	-2,811	,005	
riskybehaviour	<---	digital_trust	,529	8,567	***	
mitigating_behav	<---	Premeditation	,538	7,293	***	

The above table showed that all the model paths between the independent, dependent and mediator variables were found to be significant at 0.05 level and 0.001 level. Since all the paths are significant, this indicated that there is partial mediation between DV and IV through premeditation. However, these results need be checked against the indirect path results.

The results from the indirect path analysis are shown in the following table. The results showed that the standardised indirect (mediated) effect of premeditation on the relationship between admin measures and mitigating behaviour through path (manag_meas -->

premeditation --> mitigating_behav) is significant at the 0.05 level (p=.004). This path showed that premeditation is a partial mediator.

It is also noticeable from the direct path analysis that the digital trust has a mediating effect between attitude, risk behaviour, support measures and risky behaviour. The results appear to show that digital skills may lead to risky cyber behaviour.

Table 6. 58: Model indirect effect path results from premeditation mediation analysis

Indirect Path	Unstandardized Estimate	Lower	Upper	P-Value	Standardised Estimate
attidue --> digital_trust --> riskybehaviour	0,366	0,273	0,470	0,001	0,357***
admin_meas --> digital_trust --> riskybehaviour	-0,176	-0,317	-0,033	0,044	-0,155*
admin_meas --> premeditation --> mitigating_behav	0,342	0,174	0,554	0,001	0,316***
supp_meas --> digital_trust --> riskybehaviour	0,217	0,073	0,366	0,019	0,196*
manag_meas --> premeditation --> mitigating_behav	0,200	0,071	0,402	0,004	0,173**

6.5.2.3 The Mediating Effect of Urgency on DV and IV Relationship

The purpose of this model is to examine the indirect effect of IV on DV through the urgency construct. The model will examine the direct effect of IV on DV. The path model developed for this purpose is shown in the following figure. The model showed that urgency mediates only between DV mitigating behaviour and IV support measures.

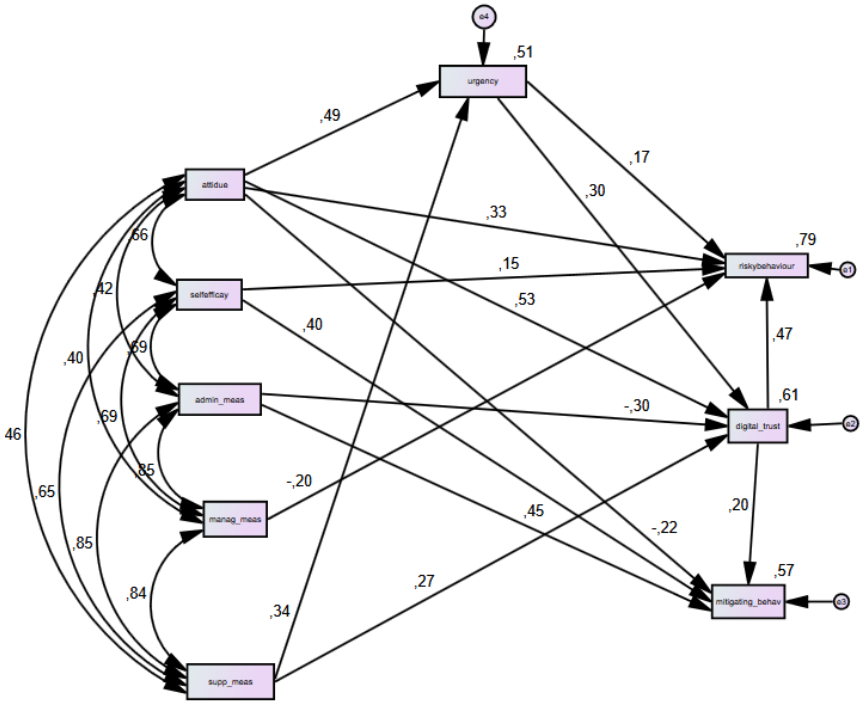


Figure 6. 21: The mediating effect of urgency on DV and IV relationship

The model fit measures produced by AMOS are reported in in tables 6.58 and 6.59. These threshold vales showed that the structural model provided a good fit to the data. The hypothesised mediation appears to be accepted. The CFI is 0.999; P close is 0.584; CMIN/df is 1.127; and the RMSEA is 0.032. The model predicts 79% of the variance in risky behaviour, 61% of digital trust and 57% of mitigating behaviours.

Table 6. 59: Model fit measures

Measure	Estimate	Threshold	Interpretation
CMIN	12,393	--	--
DF	11,000	--	--
CMIN/DF	1,127	Between 1 and 3	Excellent
CFI	0,999	>0.95	Excellent
RMSEA	0,032	<0.06	Excellent
PClose	0,584	>0.05	Excellent

Table 6. 60: Model standardised regression weight

			Estimate	C.R.	P	Label
Urgency	<---	Attidue	,487	6,814	***	
Urgency	<---	supp_meas	,342	4,784	***	
digital_trust	<---	Attidue	,528	7,059	***	
digital_trust	<---	admin_meas	-,296	-2,720	,007	
digital_trust	<---	supp_meas	,269	2,344	,019	
digital_trust	<---	Urgency	,303	3,765	***	
riskybehaviour	<---	Attidue	,329	4,559	***	
riskybehaviour	<---	Selfefficay	,147	2,099	,036	
mitigating_behav	<---	Selfefficay	,402	4,027	***	
riskybehaviour	<---	manag_meas	-,204	-3,458	***	
mitigating_behav	<---	admin_meas	,450	5,477	***	
mitigating_behav	<---	Attidue	-,221	-2,193	,028	
riskybehaviour	<---	Urgency	,174	2,892	,004	
mitigating_behav	<---	digital_trust	,199	2,315	,021	
riskybehaviour	<---	digital_trust	,470	7,395	***	

The above table showed that all the model paths between the independent, dependent and mediator variables were found to be significant at 0.05 level and 0.001 level. Since all the paths are significant, this indicated that there may be partial mediation between DV and IV through urgency. However, these results need be checked against the indirect path results.

The results from the indirect path analysis are shown in the following table. The results showed that the standardised indirect (mediated) effect of urgency on the relationship between attitude and digital trust though path attidue --> urgency --> digital_trust is significant at the 0.05 level (p=.002). Similarly, the standardised indirect (mediated) effect of urgency on the relationship between attitude and risk behaviour measured through path attidue --> urgency --> riskybehaviour is significant at the 0.05 level (p=.007). Likewise, the standardised indirect (mediated) effect of urgency on the relationship between support measures and digital trust through path supp_meas --> urgency --> digital_trust is significant at the 0.05 level (p=.001). These three paths showed that urgency acts as a partial mediator.

It is noticeable from the direct path analysis that the digital trust acts as a mediator between IV variable risky behaviour and the support measure DV variable. The results in this study appear to suggest that digital skills may have an influence on risky cyber behaviour and cyber mitigating measures.

Table 6. 61: Model indirect effect path results from urgency mediation analysis

Indirect Path	Unstandardized Estimate	Lower	Upper	P-Value	Standardised Estimate
attidue --> urgency --> digital_trust	0,163	0,078	0,274	0,002	0,147**
attidue --> urgency --> digital_trust --> mitigating_behav	0,029	0,007	0,065	0,024	0,147*
attidue --> urgency --> digital_trust --> riskybehaviour	0,071	0,033	0,130	0,001	0,147**
attidue --> urgency --> riskybehaviour	0,087	0,033	0,156	0,007	0,085**
attidue --> digital_trust --> mitigating_behav	0,103	0,020	0,190	0,046	0,105*
attidue --> digital_trust --> riskybehaviour	0,255	0,175	0,350	0,001	0,249***
supp_meas --> urgency --> digital_trust	0,124	0,069	0,213	0,001	0,104***
supp_meas --> urgency --> digital_trust --> mitigating_behav	0,022	0,006	0,051	0,019	0,104*
supp_meas --> urgency --> digital_trust --> riskybehaviour	0,054	0,029	0,102	0,001	0,104***
supp_meas --> urgency --> riskybehaviour	0,066	0,025	0,130	0,005	0,060**
supp_meas --> digital_trust --> mitigating_behav	0,057	0,004	0,148	0,070	0,054†
supp_meas --> digital_trust --> riskybehaviour	0,140	0,017	0,280	0,064	0,127†
admin_meas --> digital_trust --> mitigating_behav	-0,064	-0,150	-0,010	0,044	-0,059*
admin_meas --> digital_trust --> riskybehaviour	-0,158	-0,276	-0,049	0,020	-0,139*
urgency --> digital_trust --> mitigating_behav	0,065	0,016	0,136	0,028	0,060*
urgency --> digital_trust --> riskybehaviour	0,160	0,086	0,265	0,001	0,143**

6.6 The Discussion of the Indirect Influence

In the section of the research the author is set to test the mediating effect of users' addictive behaviours on the relationship between (ATC-IB) and risky cybersecurity behaviours (RScB). The users' addictive behaviours instrument is grouped into two constructs premeditation and urgency and those two instruments were equalled to impulsivity.

6.6.1 The Mediating Effect of Impulsivity

The hypothesis in this structural model was to test the influence of the mediating of impulsivity on relationships among ATC-IB and RScB. The summary of the hypothesis test is presented in Table 6.61.

The results demonstrated that seven hypotheses are supported. This suggested that attidue --> digital_trust --> riskybehaviour and admin_meas --> impulsivity --> mitigating_behav are important factors in the assessment of risky cybersecurity behaviour practices.

The results demonstrated that hypotheses manag_meas --> impulsivity --> digital_trust and manag_meas --> impulsivity --> digital_trust --> riskybehaviour were rejected. This indicates that managerial countermeasures are not important in the participants' viewpoint.

Table 6. 62: The influence of the mediating effect of impulsivity on relationships among ATC-IB and RScB.

Indirect Path: Hypothesis	P-Value	Standardised Estimate	Hypothesis status
admin_meas --> impulsivity --> digital_trust	0,048	0,142*	Supported
admin_meas --> impulsivity --> digital_trust --> riskybehaviour	0,042	0,142*	Supported
admin_meas --> impulsivity --> mitigating_behav	0,001	0,332***	Supported
admin_meas --> digital_trust --> riskybehaviour	0,039	-0,248*	Supported
manag_meas --> impulsivity --> digital_trust	0,109	0,071	Rejected
manag_meas --> impulsivity --> digital_trust --> riskybehaviour	0,109	0,071	Rejected
manag_meas --> impulsivity --> mitigating_behav	0,012	0,165*	Supported
attidue --> digital_trust --> riskybehaviour	0,001	0,352***	Supported
supp_meas --> digital_trust --> riskybehaviour	0,024	0,183*	Supported
impulsivity --> digital_trust --> riskybehaviour	0,148	0,124	Rejected

6.6.2 The Mediating Effect of Premeditation

The hypothesis in this structural model was to test the influence of the mediating of premeditation on relationships among ATC-IB and RScB. The summary of the hypothesis test is presented in Table 6.62.

The results demonstrated that five hypotheses are supported. This suggested that attidue --> digital_trust --> riskybehaviour and admin_meas --> premeditation --> mitigating_behav are important factors in the assessment of employee risky cybersecurity behaviour practices.

The results demonstrated that none of the hypotheses were rejected. This indicates that all of the hypotheses are working in the participants' viewpoint.

Table 6. 63: The influence of the mediating of premeditation on relationships among ATC-IB and RScB

Indirect Path: Hypothesis	P-Value	Standardised Estimate	Hypothesis status
attidue --> digital_trust --> riskybehaviour	0,001	0,357***	Supported
admin_meas --> digital_trust --> riskybehaviour	0,044	-0,155*	Supported
admin_meas --> premeditation --> mitigating_behav	0,001	0,316***	Supported
supp_meas --> digital_trust --> riskybehaviour	0,019	0,196*	Supported
manag_meas --> premeditation --> mitigating_behav	0,004	0,173**	Supported

6.6.3 The Mediating Effect of Urgency

The hypothesis in this structural model was to test the influence of the mediating of urgency on relationships among ATC-IB and RScB. The summary of the hypothesis test is presented in Table 6.63. The results demonstrated 14 hypotheses are supported. This suggested that attidue --> digital_trust --> riskybehaviour and attidue --> urgency --> digital_trust are important factors in the assessment of employee risky cybersecurity behaviour practices. The results demonstrated that one hypothesis was rejected and one hypothesis was partially supported. This indicates that (the bath of supp_meas --> digital_trust --> mitigating_behav and supp_meas --> digital_trust --> riskybehaviour) is not important in the participants' viewpoint.

Table 6. 64: The influence of the mediating effect of urgency on relationships among ATC-IB and RScB

Indirect Path: Hypothesis	P-Value	Standardised Estimate	Hypothesis status
attidue --> urgency --> digital_trust	0,002	0,147**	Supported
attidue --> urgency --> digital_trust --> mitigating_behav	0,024	0,147*	Supported
attidue --> urgency --> digital_trust --> riskybehaviour	0,001	0,147**	Supported
attidue --> urgency --> riskybehaviour	0,007	0,085**	Supported
attidue --> digital_trust --> mitigating_behav	0,046	0,105*	Supported
attidue --> digital_trust --> riskybehaviour	0,001	0,249***	Supported
supp_meas --> urgency --> digital_trust	0,001	0,104***	Supported
supp_meas --> urgency --> digital_trust --> mitigating_behav	0,019	0,104*	Supported
supp_meas --> urgency --> digital_trust --> riskybehaviour	0,001	0,104***	Supported
supp_meas --> urgency --> riskybehaviour	0,005	0,060**	Supported
supp_meas --> digital_trust --> mitigating_behav	0,070	0,054†	Partial
supp_meas --> digital_trust --> riskybehaviour	0,064	0,127†	Rejected
admin_meas --> digital_trust --> mitigating_behav	0,044	-0,059*	Supported
admin_meas --> digital_trust --> riskybehaviour	0,020	-0,139*	Supported
urgency --> digital_trust --> mitigating_behav	0,028	0,060*	Supported
urgency --> digital_trust --> riskybehaviour	0,001	0,143**	Supported

6.7 Summary of Data Analysis

The regression analysis was successfully conducted by the researcher to find out the extent to which the research outcome matches the hypotheses that were formulated prior to the research. The analysis was conducted to identify the relationship between the attitude towards cybersecurity countermeasures (Attitude countermeasures, Self-efficacy countermeasures), security awareness countermeasures (Administrative countermeasures, Managerial countermeasures, Support countermeasures) and Users' addictive behaviours (Premeditation, Urgency) of employees and their influence on information security countermeasures (Nudy *et al.*, 2019).

CHAPTER 7: DISCUSSION

7.1 Introduction

This chapter will critically examine the results which were obtained from both the literature review chapter and the data analysis chapter of the thesis. The significance of the results obtained from the data collection procedure will be analysed in this discussion chapter. This data analysis chapter will be very beneficial for the readers of this thesis to understand whether all the hypotheses are supported with regard to the public organisations in the UAE.

In this thesis, the relationship between the information security countermeasures and the risky behaviour measures against cybersecurity has been proposed in terms of a model to provide security to the employees' side (Safa *et al.*, 2016). The behaviour of employees in an organisation can be influenced by the countermeasures of the organisation. This is made possible through employees' beliefs and appraisal of threats relating to information security and how effective the coping strategies are. This was proposed by use of the Protection Motivation Theory (PMT) framework. This aspect has been widely surveyed and published in the literature. During the research, the conceptual model was tested using data from 124 employees in the United Arab Emirates (UAE) working for public organisations. From this survey, it was identified that employees in public organisations in the UAE have been organising ways in which they can enhance cybersecurity in the organisations.

The research led to the investigation and identification of two potential IS countermeasures types of employees that mainly influence the security of information in the PMT framework (Fine and Edward, 2017). The first one is the role of the attitude towards cybersecurity countermeasures and the second is the security awareness countermeasures. These two IS countermeasures can motivate the behaviours of employees towards information security

either in intrinsic or extrinsic ways. Most of the previous studies have been based on self-reported behaviours to enhance the future of information security. However, this research is different. The research combines both the efforts made by the organisations to enhance information security and the current actions towards information security based on self-reported behaviours. In general, the findings of the research support the conceptual model presented by the PMT framework. The research also identified that organisational factors on the beliefs and behaviours of employees play a very important role in enhancing their response to information security (Fine and Edward, 2017). This can best be performed in the PMT framework. From the research, it was also identified that the factors of the PMT framework model directly relate to the security policies set by organisations for information systems and the awareness directed to the employees in the set policies. As such, it can be concluded from the research that the behaviours towards information security can be enhanced through the application of the PMT framework. The research also implies that the beliefs of employees towards cybersecurity are motivated by their immediate working environment and policies set by the organisation. This enables them to develop protective behaviours against cyber-attacks.

7.2 Overview of the Research Questions

The researcher of this thesis created the research questions to identify the information security countermeasures which influence the risky cybersecurity behaviour practices. The researcher also wanted to identify the users' addictive behaviours which mediate between the risky cybersecurity behaviour practices and the information security countermeasures, and to identify the association between information security countermeasures and risky cybersecurity behaviour practices.

From the literature, information security countermeasures were divided into two sections: attitudes towards cybersecurity countermeasures and security awareness countermeasures. Then it was identified that attitudes towards cybersecurity countermeasures might have an influence on workforce behaviours. From the literature, it was identified that there are numerous behaviour practices which have a direct influence on the attitudes towards cybersecurity countermeasures, such as attitude and self-efficacy. On the other hand, Administrative, Managerial and Support countermeasures have a direct influence on the Security awareness countermeasures. The literature was very beneficial to understand that the users' addictive behaviours can influence both information security countermeasures and the risky cybersecurity behaviour practices of the workforces of public organisations. The literature also helped in understanding that a lack of management support, providing unauthorised access and a lack of IS policies can have an influence on the information security countermeasures and the risky cybersecurity behaviour practices as well.

From the literature, it was identified that IS countermeasures might have an influence on workforce behaviours, and that there are numerous behaviours which have a direct influence on the IS countermeasures, such as intentional destruction, dangerous tinkering and naïve mistakes. The literature was very beneficial to understand that the personal traits of the workforce can influence both IS countermeasures and the behavioural practices of the workforces of public organisations.

From the literature resources reviewed, it is clear that the behaviours of the employees in an organisation greatly depend on the security measures put in place by the organisation (Pearce, 2017). For instance, employees will tend to be more concerned about the security of the information systems in organisations that have strict security measures. Such organisations

usually keep their employees on their toes by always reminding them of the importance of enforcing information security for the organisation's data and information systems. Employees are usually made aware of any new security measure to be implemented in the organisation. This allows the employees to review it often in order to understand how it works and the associated risks if it is not properly implemented. On the other hand, managers who work in organisations that rarely make their employees aware of the security measures put in place tend to be less concerned about information security (Alshare, Lane and Lane, 2018). The research also identified that such managers might not be aware of any security risks associated with the organisation's information system. This shows that employees' response towards cybersecurity is directly influenced by their organisation's beliefs and behaviours. Therefore, the security of the organisation's information systems can be enhanced by making the employees aware of the security measures in place and not just putting the measures in place. By understanding the security risks associated with information, employees can come up with their own ways to combat the risks apart from the countermeasures set by the organisation.

Security countermeasures put in place by an organisation define the behaviour of the employees. Employees working in an organisation that has strict security measures will automatically be careful when handling that organisation's information (Call, Hidayat, Peacock and Yang, 2017). Such employees also understand the importance of securing the systems against cyber-attacks and thus they will be at the forefront of securing the information systems. The researcher therefore concluded that the security countermeasures set up by the organisation integrated with the employees' behaviours can help in improving the security of the information systems. Summarizing the overview of the research questions:

- Attitude and self-efficacy have a direct influence on the attitudes towards cybersecurity countermeasures.
- Administrative, Managerial and Support countermeasures have a direct influence on the Security awareness countermeasures.
- The users' addictive behaviours can influence both information security countermeasures and risky cybersecurity behaviour practices of the workforces of public organisations.
- The lack of management support, providing unauthorised access and lack of IS policies can have an influence on the information security countermeasures and the risky cybersecurity behaviour practices as well.
- IS countermeasures might have an influence on workforce behaviour.
- Intentional destruction, dangerous tinkering and naïve mistakes have a direct influence on the IS countermeasures.
- The personal traits of the workforce can influence both IS countermeasures and the behavioural practices of the workforces of public organisations.

7.3 Descriptive Analysis Findings Discussion

This research was conducted on various literature sources where a number of sources were identified. The selected samples were critically analysed to come up with a conclusive report (Gates *et al.*, 2018). The researcher of this study has remained unbiased while selecting the sample for the online survey, which was conducted on 124 samples. Most of the sample have a bachelor's degree and also have an IT-related qualification at undergraduate level. Even distribution of IT-related training was observed from the descriptive analysis; the researcher has successfully identified that most of the samples have a minimum of one year of experience.

Most of the sample works in diverse domains as well. Hence, from these findings it can be concluded that all 124 participants were perfectly chosen by the researcher without any sort of preferences or biasedness. The participants used for the survey were obtained from different sources. Each of the selected sample was analysed separately in order to avoid compromising the legitimacy of the findings. Once analysis of all the 124 was completed, a general conclusive report was generated. During the analysis, various objectives of the research were considered. The purpose of this was to ensure the research is in line with the stated objectives and not just general research. Various organisations' environments were used in order to find out how a business environment can influence the behaviour of employees towards information security.

7.4 Frequency Discussion of the Research Constructs

Based on the results obtained in the frequency discussion, it was understood that most of the sample believe that reporting cybercrime is a waste of time, and at the same time they also agreed that cyber criminals are far more advanced than the users of the IT systems across the public organisations. From the responses, it can be understood that most of the employees comply with the security policies adopted by their organisations. Most of the employees of the public organisations believe that they cannot get rid of spyware and malware from their IT systems. None of the employees share their personal information on internet platforms and they do not clink on unsolicited mails either. Employees of public organisations do not have free work access to Wi-Fi but they do use online storage systems.

Data backup is one of the most significant best practices to secure the data from cybersecurity challenges. Checking the security of an email having an attachment also falls under the best IS practices and most of the public organisations request their staff to use antiviruses to protect the intellectual business assets. IS training being very beneficial for the

employees to understand the procedure of protecting the integrity of business data. Having control over their feelings is greatly desired to resolve the data security challenges which are being faced in the UAE's public organisations. Summarizing the frequency discussion of the research constructs:

- The majority of the sample believes that reporting cybercrime is a waste of time.
- The cyber criminals are far more advanced than the users of the IT systems across the public organisations.
- The employees comply with the security policies adopted by their organisations.
- Most of the employees of the public organisations believe that they cannot get rid of spyware and malware from their IT systems.
- None of employees share their personal information on the internet platforms and they do not clink on unsolicited mails either.
- Employees of public organisations do not have free work access to Wi-Fi as well but they do use online storage systems.
- Data backup is one of the most significant best practices to secure the data from cybersecurity challenges.
- Checking the security of an email having an attachment also falls under the best IS practices and most of the public organisations request employees to use antiviruses to protect the intellectual business assets.
- IS training being very beneficial for the employees to understand the procedure of protecting the integrity of business data.

7.5 Association of Findings Discussion and Contribution to Knowledge

There is a moderate positive correlation between the attitudes towards cybersecurity countermeasures and the risky cybersecurity behaviour practices of the workforces relating to IS. Enhancement of the attitudes towards cybersecurity countermeasures across the public organisations has an influence on the risky cybersecurity behaviour practices of the workforces as well. On the other hand, there is a moderate positive correlation between the risky cybersecurity behaviour practices and the security awareness countermeasures. It can be understood that, if security awareness countermeasures are enhanced then this will have an influence on the risky cybersecurity behaviour practices of an employee in relation to IS. There is a moderate positive correlation between users' addictive behaviours and risky cybersecurity behaviour practices, and users' addictive behaviours have a direct influence on the risky cybersecurity behaviour practices maintained across the UAE's public organisations. There is a positive correlation between the attitudes towards cybersecurity countermeasures and users' addictive behaviours. Attitudes towards cybersecurity countermeasures have a direct influence on the users' addictive behaviours of the workforces working across the UAE's public organisations. There is a positive correlation between the security awareness countermeasures and users' addictive behaviours. Security awareness countermeasures have a direct influence on the users' addictive behaviours of the workforces working across the UAE's public organisations, and, finally, these is a positive mediation of users' addictive behaviours between the risky cybersecurity behaviour practices and information security countermeasures.

7.6 Regression Analysis Contribution to Knowledge

Higher levels of attitudes towards cybersecurity countermeasures have an influence on the risky cybersecurity behaviour practices of the workforces towards IS. It can also be

understood that maintaining higher levels of security awareness countermeasures might minimise the risky cybersecurity behaviour practices which are followed across the UAE's public organisations. Higher levels of workforce attitudes towards cybersecurity countermeasures can have an influence on the users' addictive behaviours towards IS. Higher levels of security awareness countermeasures may influence users' addictive behaviours as well. Higher levels of users' addictive behaviours might have an influence on the risky cybersecurity behaviour practices.

7.7 Discussion of Users' Addictive Behaviours as a Mediator on Predicting Risky Cybersecurity Behaviours

Users' addictive behaviours in the UAE are positively mediating between the IS countermeasures and the risky cybersecurity behaviour practices. The model is very successful in predicting the dependent variable of the hypothesis which is risky cybersecurity behaviour practices towards the IS countermeasures of the public organisations' workers.

Based on the data obtained from the first hypothesis, it can be stated that attitudes towards cybersecurity countermeasures are positively related to the risky cybersecurity behaviour practices.

This information is well supported by the theory of planned behaviour, which was obtained from Sheeran and Rivis (2017). The theory helps in understanding that the attitude of employees working in any commercial setting depends upon belief and behaviour. This theory is very beneficial to predict the behaviour of the employees of any commercial establishment; perceived behaviour control can also be understood from this theory. Hence, this theory was very beneficial in understanding that the attitudes towards cybersecurity countermeasures are

directly related to the risky cybersecurity behaviour practices. Employee behaviour depends on both the organisation and the regular business practices. Based on the theory, it was understood that attitudes towards cybersecurity countermeasures must have a set of subjective procedures and regulations which can help an employee to improve their workplace behaviour. At the same time, the discussions of Chen and Tung (2014) also strategically align with the results obtained in this hypothesis as they highlighted that the behaviour of the employees depends hugely on their motivation, which is directly associated with their attitudes towards cybersecurity countermeasures. The discussions of Mullan *et al.* (2015) also suggests that the motivation of the employees comes from the workplace practices and attitudes towards cybersecurity countermeasures. The researchers stated that the perceiving power of the employees in an organisation depends hugely on the attitudes towards cybersecurity countermeasures. In the view of Tsai *et al.* (2016), the behaviour of an employee depends only upon their intention; the researchers stated that perceived severity and perceived vulnerability usually affect employee behaviour and it is not organisational culture only. Hence, the discussions of these researchers can be significant in understanding that the organisational culture does not play an important role to affect the behaviour of the employees of any commercial setting. On the other hand, protection motivation theory discussed by the researchers also suggests that the behaviour and the motivation of the employees depend upon self-efficacy. Self-efficacy of an employee depends hugely on the attitudes towards cybersecurity countermeasures as well. Hence, the scholars' discussions are strongly aligned with the results obtained from this hypothesis, which stated that attitudes towards cybersecurity countermeasures might have an influence on enhancing risky cybersecurity behaviour practices.

Results obtained from the second hypothesis suggest that security awareness countermeasures are positively related to the risky cybersecurity behaviour practices. The results of this analysis are strongly supported by the discussion of Pearlson *et al*. (2016). The researchers stated that every organisation must have its information security countermeasures which can help it to address the cybersecurity risks. Based on the discussion of these researchers, it was understood that IS culture is directly related to the organisational culture, and each of these two cultures can have a huge impact on the information security countermeasures. Hence, it can be understood that the discussion of Pearlson *et al*. (2016) aligns with the results which were obtained from the hypothesis where it was found that security awareness countermeasures might minimise the risky cybersecurity behaviour practices. Supporting the hypothesis, Heckmann, Comes and Nickel (2015) also stated that IS countermeasures are very useful to address the internal risks coming from inside an organisation and security awareness countermeasures play a key role in governing the IS practices.

Cheng *et al.* (2014) highlighted general deterrence theory in support of the above discussion as well. The theory helps in identifying that any human errors can have a direct impact on IT security practices. Based on this theory, it can be stated that the commitment of the social engineers can be addressed if proper countermeasures are taken by an organisation's employees. The researchers stated that employees must be educated and trained about the ways to deal with security risks, and these training sessions can also be very useful to maintain professional cybersecurity behaviour practices. The results obtained from the analysis also align with the discussion of Abbasi, Sarker and Chiang (2016), as they stated that training sessions can help staff to understand the reasons behind the security issues and also maintain professional cybersecurity behaviour practices. Pearlson *et al*. (2016) stated that basic training is very

beneficial to help employees understand the cybersecurity behaviour practices of a business. The researchers of this journal article helped in comprehending that the behaviour of the employees can have an impact on the security practices of their organisation. Creation of a culture that values security is very significant for the information security resources before going through the training sessions. Hence, it can be understood that the discussion of all the scholars of the literature review supported the results obtained from this hypothesis.

From data collected from the third hypothesis it was understood that users' addictive behaviours are positively related to the risky cybersecurity behaviour practices. Humphries (2017) has successfully described the diverse categories of information security behaviour of the employees working in an organisational setting. The researcher highlighted addictive behaviours, which allow the employees to steal any sort of essential information from the consumers. The researcher stated that this attitude can have a direct impact on both the progress of the organisation and on the addictive behaviours of the employees. Humphries (2017) stated that the cybersecurity behaviour practices of the employees are closely associated with the addictive behaviours of the employees in any commercial setting. Supporting the hypothesis and the discussions of Humphries (2017), Martins *et al*. (2014) suggested that the theory of reason action can be very beneficial to link the cybersecurity behaviour practices with employees' addictive behaviours. This theory is very useful to predict the behaviour of an individual; moreover, it can also be said that the cybersecurity behaviour practices of the employees depend upon their behavioural belief, evaluation and the suggestive norms. The researchers discussed that normative beliefs are very significant in understanding the cybersecurity behaviour practices of an employee. The theory also suggests that addictive behaviours are closely related to the cybersecurity behaviour practices of a person. Hence, it can

be understood that this theory is greatly aligned with the results obtained from this hypothesis where it was understood that users' addictive behaviours are positively related to the risky cybersecurity behaviour practices.

Contradicting the above researcher, Mullan *et al.* (2015) stated that addictive behaviours are a motivation factor and are associated with the cybersecurity behaviour practices. The researchers stated that the motivation factors play a huge role in influencing the addictive behaviours of an individual. The researchers mentioned that the stronger addictive behaviours have an influence on the cybersecurity behaviour practices. They also stated that approval or disapproval of the behaviour can have a direct influence on the cybersecurity behaviour practices of an individual as well. On the other hand, as discussed by Malekian *et al*. (2017), the technical expertise of an individual can have a huge impact on the addictive behaviours. The researchers stated that the employees of a public organisation must be aware of the security risks, as this can have a direct influence on organisational performance as well as on mental health. Thus, the employees of public organisations must shape their addictive behaviours to protect the organisations' online assets and intellectual properties. Thus, the opinion of the scholars aligns with the results which were obtained from the hypothesis testing.

Kautonen *et al*. (2015) suggested that the addictive behaviours of employees are very clear from their plan of action. The researchers stated that the cybersecurity behaviour practices of the employees of any commercial establishment depend directly on the addictive behaviours of the employees. Thus, the discussion of Kautonen *et al*. (2015) is aligned with the results which were obtained from this hypothesis testing. Hence, it can be understood that the results obtained from the hypothesis match with all the discussions made by the researchers in the literature review.

Based on the results obtained from the fourth hypothesis, it can be comprehended that attitudes towards cybersecurity countermeasures are positively related to the users' addictive behaviours. Based on the discussion of Cheng, Zhai and Smyth (2014), employee behaviour depends upon numerous factors such as job satisfaction and workplace motivation. The researchers of this paper stated that the motivation level of the employees is strongly aligned with the behaviour and the attitude. The factors which influence the behaviour of the employees, such as positive work environment and customer demands, are the driving forces of the attitudes towards cybersecurity countermeasures as well. From this literature, it can be understood that the security policies which are planned by an organisation get accomplished only when the employees understand the reasons behind enacting them. Hence, from this discussion, it can be determined that attitudes towards cybersecurity countermeasures are positively related to the users' addictive behaviours.

Supporting the above discussion, Martins *et al*. (2014) highlighted that IS is focused more on the countermeasures of preventive. The researchers mentioned that employee behaviour is affected by numerous factors and attitude towards cybersecurity countermeasures is one of them. The researchers stated that private organisations have to balance costs as well as benefits, and employee behaviour is very significant to improve the benefits of the business; on the other hand, it is the responsibility of the employees to understand the security countermeasures which help them to reduce or minimise any security threats.

Based on the discussions of Siponen *et al*. (2014), general deterrence theory can be very useful to link attitudes towards cybersecurity countermeasures and the users' addictive behaviours. The theory can be very beneficial to understand the ways by which the illegal practices can be resolved. It can also restrict the employees of any commercial establishment

from committing any sort of crime which might have an impact on the growth and productivity of the business. The appropriate behaviour required to minimise the security risks can also be understood from this theory. The theory can help to manage the severity, celerity and certainty of the employees so that they can take all the decisive steps to secure the online assets of the business. Siponen *et al*. (2014) also discussed the IT skills of the employees, which are very closely associated with their behaviour, and are very useful for the creation of countermeasures against the security threats. Thus, it can be said that, if an employee wants to maintain the information security standards, at that point of time, their addictive behaviour is very significant in the decision-making procedure. Hence, it can be said that the discussions in the literature support the results which were obtained from the hypothesis testing which indicated that attitudes towards cybersecurity countermeasures might have an influence on the users' addictive behaviours.

The results obtained from the fifth hypothesis suggest that users' addictive behaviours are positively mediating between the risky cybersecurity behaviour practices and information security countermeasures. Based on the discussions of Cheng, Zhai and Smyth (2014), there are diverse categories of users' addictive behaviours associated with most of the employees working across private organisations, such as their leadership skills, cognitive abilities, organisation skills, honesty, urgency, premeditation and work ethic. Each these addictive behaviours are very beneficial for the employees to improve their workplace behaviour as well as to address the security risks coming from different sources. The researchers stated that the behavioural practices of an employee can be identified from their addictive behaviours and these addictive behaviours help them to be successful in their respective organisations as well. The researchers stated that employees must be aware of the IT risks the moment they join their organisation, and

the decisive step taken by them can help the organisation to address the security risks. The researchers indicated that risky cybersecurity behaviour practices and users' addictive behaviours are very closely associated with each other, and users' addictive behaviours have a huge influence on the risky cybersecurity behaviour practices as well. Hence, the data analysis is showing a supporting relationship with this hypothesis which showed that addictive behaviours of the workforce are positively mediating between risky cybersecurity behaviour practices and IS countermeasures.

Mishra *et al*. (2014) stated that personal innovativeness such as self-efficacy and urgency in computers can be very beneficial to address security threats. The researchers stated that employees' level of understanding is directly related to their risky cybersecurity behaviour practices and addictive behaviours. Supporting the above discussion, Safa *et al.* (2015) specified that the willingness of individuals is very significant to successfully incorporate the information security countermeasures. The researchers helped understand that employees must understand the impact of the security threats so that it is easier for them to follows the security guidelines which are provided by commercial establishments. On the other hand, the researchers also stated that human behaviour is the biggest IT security threat and it can be resolved only with the help of cybersecurity behaviour practices. Hence, employee knowledge as well as employee behaviour are strongly related to each other and users' addictive behaviours play a huge role in identifying the exact information security countermeasures required to address the risky cybersecurity behaviour practices. Literature in the literature review differed, for example, the discussions of Safa *et al.* (2015) do not match the result which was obtained from the hypothesis; however, the discussions of other researchers such as Mishra *et al*. (2014) and Cheng, Zhai and Smyth (2014) do align with the results obtained from the hypothesis.

The results obtained from the final hypothesis help in understanding that security awareness countermeasures are positively related to the users' addictive behaviours. Considering the theory of planned behaviour as discussed by Sheeran and Rivis (2017), it can be suggested that security awareness countermeasures depend upon numerous factors such as employee age, religion, marital status and gender. The researchers stated that security awareness countermeasures are very significant across public organisations as they add value to the business. Business challenges such as security risks and the resistance coming from employees can be addressed with the help of security awareness. Engagement of the employees, which is greatly required for the growth of a business, is also supported by the security awareness; the literature also helps in understanding that the security awareness of the employees is very significant to counter the threat coming from the security risks. Hence, it can be said that the discussions in the literature show the same results which were obtained from this hypothesis testing which indicated that higher levels of security awareness countermeasures have an influence on the users' addictive behaviours.

Renowned scholars such as Safa *et al.* (2015) highlighted that employees must understand the impact of security attacks on both the organisation and on their personal career. They stated that employees must behave in systemised modus in the workplace as it can help them to gain appreciation from the management team and also help them to deal with the IS threats. The researchers stated that the employees of public organisations must understand different types of security awareness countermeasures before following them. Safa *et al.* (2015) focused hugely on the interest of the employees to address the users' addictive behaviours, as the researchers believe that employee interest is very closely associated with users' addictive behaviours. Considering the reasoned action model which was proposed by Fishbien and Ajzen,

it can be said that the behavioural practices depend upon subjective norms such as motivation and normative beliefs; on the other hand, behavioural beliefs can also play a leading role to determine the attitude of an employee. Based on this model, it can be said that users' addictive behaviours are very closely related to each other and can help to improve the security awareness countermeasures. Hence, the discussions of this article also show the same results as obtained in the hypothesis testing.

7.8 Conclusion

This chapter of this thesis has helped the researcher to identify all the answers to the research questions created in the first chapter. From the literature review, it can be understood that user behaviour can influence the IS countermeasures. It can be concluded that the addictive behaviour of the workforce can have an influence on both attitudes towards cybersecurity and awareness countermeasures. From the frequency discussion, it can be concluded that most of the workforce comply with the security policies of their business environments, and the authority instructs them to follow the organisation's IS polices. The frequency distribution was also helpful to understand that most of the workforce practise the IS countermeasures when it is properly communicated to them. Having control over their feelings is very significant to resolve most of the data security challenges. It can be concluded that there is a moderate positive association between IS countermeasures and risky cybersecurity behaviour practices. There is a moderate positive relationship between attitudes towards cybersecurity countermeasures and users' addictive behaviour. There is a positive correlation between awareness countermeasures and the impulsivity IS countermeasures; at the same time, it can also be concluded that there is a positive correlation between risky cybersecurity behaviour practices and users' addictive behaviour. The regression analysis helps in understanding that IS countermeasures have an

influence on the behaviour of the workforce towards IS. It can be concluded that the intention of the workforce can have an influence on the behaviour of the workforce as well. IS countermeasures influence workplace behaviours and behavioural practices have an influence on the IS countermeasures. From the moderation, it can be concluded that the addictive behaviour of the workforce positively mediates between IS countermeasures and behavioural practices.

CHAPTER 8: CONCLUSION AND RECOMMENDATIONS

8.1 Research Overview

Employees in any public or private organisation play a very important role in ensuring the security of the organisation's information system. Although there are technological approaches to securing information systems, the approaches can be termed as vague if the employees are not well conversant with how to implement and observe the security measures. Security of information is a vital key in any organisation. Due to advances in technology, the means of storing, transferring, processing and fetching data have really been transformed. Despite this advancement being of great importance to organisations, it is also an avenue for cyber criminals to attack the information systems. Therefore, it is important for public and private organisations to explore all the possible vulnerabilities that can cause breaches of information security.

8.2 Meeting the Aim and Objectives of this Thesis

The researcher of this thesis developed research objectives to help in exploring cybersecurity threats in relations to employees' social practices. The developed objectives are describing in the following sections;

8.2.1 To examine the mediating effect of the users' addictive behaviours on the relationships between information security countermeasures and risky cybersecurity practices

Security of information systems can only be managed if the possible threats have been assessed and evaluated. Threat appraisal involves identifying the threat and its origin, how it happens and the impact it can cause to the organisation. Once the threat has been assessed

thoroughly, procedures to mitigate it should then be established. This can be to ignore the threat if it has no impact, to contain and eliminate it while the organisation continues with normal operations, or to shut down the entire system if the threat will have a massive impact. Public organisations in the UAE should come up with well-stated algorithms for threat appraisal and coping appraisal. Understanding common sources of threats is the easiest way to combat the threats.

8.2.2 To define the link between risky cybersecurity practices and countermeasures of information security

With the protection motivation theoretical model in place, organisations will be able to come up with programmes that will motivate employees to secure the information systems in public organisations in the UAE. Normally, humans tend to think positively when they are motivated. In this case, motivated employees will eventually develop positive attitudes towards IS countermeasures (Alshboul and Streff, 2017). This model will enable the public organisations to formulate ways that will motivate employees to exercise self-information security responsibility rather than depending on system experts to enforce security.

8.2.3 To identify countermeasures for information security that affects risky cybersecurity practices

It is normal for organisations to establish information security measures to combat threats to information systems. Despite these measures, the workforce also has its own personal informed ways of handling cybersecurity. In order to ensure maximum information security, the security measures set by the organisation and the personal cybersecurity approaches of the employees have to be integrated. The integration should be carried out on the employees' current approaches and behaviours and not the expected future approaches. This is because information

security threats keep on changing with technology and hence the approaches and behaviours applied now may not be applicable in the future. Current operations of the workforce are likely able to influence the future behaviours.

8.2.4 To recognise employees' risky behaviour practices that can affect public sector information security

Most employees in public organisations view information threats as hacking or other technical operations. However, this is not the case. An information threat can be a simple activity such as not shutting down computers or sharing of passwords. It is the duty of the organisation to come up with security awareness programmes to help employees change their perspective on information threats (Okae *et al*., 2019). The employees often think that security actions have to be implemented by the organisation's IT team. However, proper awareness will make them understand it is the duty of every stakeholder to enforce information security. Through frequent security awareness, the employees will have a deeper understanding of information threats and measures to mitigate them at the employee level.

8.3 Key Findings of this Thesis

The section is very beneficial for the readers of this research study to understand whether the results obtained from the hypothesis testing are similar to the discussions. The research divided the independent variable (information security countermeasures) into two sections, attitudes towards cybersecurity countermeasures and security awareness countermeasures. Then it set out to test the direct relationship between information security countermeasures (ISC-IB) and risky cybersecurity behaviour practices (RScB) as defined by Harlington (2017). The summary of the hypotheses is shown in Table 7.1. The RScB instrument was grouped into three main constructs, digital trust, risky behaviours and mitigation measures. Similarly, the ATC-IB

instrument was clustered into attitude and self-efficacy while the security awareness countermeasures (SA-IB) instrument was clustered into administrative countermeasures, managerial countermeasures and support countermeasures. The results showed that nine hypotheses were supported. However, digital_trust <--- manag_meas and mitigating_behav <--- manag_meas direct relationship are not supported. This suggests that participants thought that managerial countermeasures are not important determinates for assessing employees' vulnerability to cyber-attacks.

Table 8. 1: The direct relationship between ISC-IB and RScB

Indirect Path: Hypothesis			P	Status
digital_trust	<---	Attidue	***	Supported
digital_trust	<---	manag_meas	,109	Rejected
digital_trust	<---	supp_meas	,026	Supported
digital_trust	<---	admin_meas	,002	Supported
Riskybehaviour	<---	Attidue	***	Supported
Riskybehaviour	<---	Selfefficay	,020	Supported
mitigating_behav	<---	manag_meas	,095	Rejected
Riskybehaviour	<---	manag_meas	,005	Supported
mitigating_behav	<---	Selfefficay	***	Supported
Riskybehaviour	<---	digital_trust	***	Supported
mitigating_behav	<---	digital_trust	,056	Partial
mitigating_behav	<---	admin_meas	,010	Supported
mitigating_behav	<---	Attidue	,059	Partial

Users' addictive behaviours in the UAE are positively mediating between IS countermeasures and the risky cybersecurity behaviour practices. The model is very successful to predict the dependent variable of the hypothesis which is risky cybersecurity behaviour practices towards the IS countermeasures of the public organisations' workers.

Based on the data obtained from the first hypothesis, it can be stated that attitudes towards cybersecurity countermeasures are positively related to the risky cybersecurity

behaviour practices. Results obtained from the second hypothesis suggest that security awareness countermeasures are positively related to the risky cybersecurity behaviour practices.

Through data collected from the hypothesis it was understood that users' addictive behaviours are positively related to the risky cybersecurity behaviour practices. Based on the results obtained from the fourth hypothesis, it can be comprehended that attitudes towards cybersecurity countermeasures are positively related to the users' addictive behaviours. The results obtained from the fifth hypothesis suggest that users' addictive behaviours are positively mediating between the risky cybersecurity behaviour practices and information security countermeasures.

The results obtained from the final hypothesis help in understanding that security awareness countermeasures are positively related to the users' addictive behaviours.

8.4 Research Novelty and Contribution to Knowledge

This research study contributes to knowledge of information security by a demonstration of the critical as well as important role of the human factors in the development of an information security countermeasures system (Siponen *et al*., 2014). The contribution of this particular study is a practical as well as a theoretical basis for the security of information in recommendations of the objective framework to assess, develop and model the human behaviour information security countermeasures approaches in public organisations. One of the main contributions of this particular research study is to make changes to the holistic management of the information security in order to establish the information security countermeasures. There is a lack of research as well on the impact of the public organisational cultural dimensions on the information security countermeasures (Pearlson *et al.*, 2016). Information security needs to

focus on the human behaviour. There is indication of an information security culture which reduces the risks to the informational assets with reduced rates of human errors and misbehaviour.

This particular thesis expanded our understanding in the following ways:

1. It reviews current materials which are related to the information security breaches, research as well as mechanisms along with published findings.
2. It looks into the significance of the human elements in security assurance.
3. It proposes further research with the use of non-standard information security assurance mechanisms that are applied in a number of fields as well as highlights the implications.
4. It proposes a different way of establishing information security countermeasures relating to specific cultures.

The thesis looked into published information security data breaches and moved on to define assurance as well as identify the current assurance methods adopted by public organisations. It then progressed to the human factors pertaining to the information security assurance and they are related to the human behaviour which underpins the research study. Then the thesis moved on to the mechanisms to measure as well as assess use outside of the cybersecurity field.

8.5 Research Implications

Research on cybersecurity is greatly influenced by this thesis in various ways. The first contribution of the thesis is the conceptual model proposed, which integrates the information security countermeasures of an organisation with the motivation theory on information

protection (Fielder *et al.*, 2016). This model explains the relationship between employees, cues to action and the experience of employees due to previous encounters with cyber-attacks. The research demonstrates that the cues to action of employees whenever there is an information security breach are enhanced by the behaviour of their peers. The research also implies that employees are motivated to take part in security training by the cues to action. Through the training, the experience of employees in handling information security is boosted. As their experience of security increases, they are able to understand the severity of cyber-attacks and how to respond efficiently to various kinds of information security attacks. This improves the behaviour of employees towards cybersecurity compliance as they will be able to identify barriers that limit them from complying with cybersecurity behaviours.

For employees to comply with the organisation's policies on cybersecurity, they need to be motivated by certain factors. This thesis describes some of the factors that motivate them. Motivated employees will always be at the forefront of identifying security risks and mitigating them, hence reducing the frequency with which information attacks on the organisation occur (Burns *et al.*, 2017). This finding opposes results from previous research, for example NG and Xu (2007), who state that the behaviour of employees towards cybersecurity is not influenced by their higher levels to cues to action

Another contribution of this thesis to cybersecurity research is that it has illustrated the relationship between the awareness of employees regarding cybersecurity and the organisation's IS countermeasures, strategies to combat the attacks, and the security compliance behaviour. The conclusion on this provides a new way in which the compliance behaviour of employees relating to information security can be evaluated. This finding adds some content to the previous research on employees' and organisation's belief factors Fielder *et al*. (2016). From the research,

it was identified that employees will do all they can to combat cybersecurity attacks when they are informed of the organisation's information system's security countermeasures (ISSC).

8.6 Implications for Research/Theory

There are complications and concerns which are directly associated with the social behaviour of the employees towards IS countermeasures across the UAE's public organisations. The social behaviours of employees are in terms of addictive practices, their attitude, and their risky operations that can affect information security. These practices and behaviours play a major role in securing an organisation's information system. The information is likely to be compromised when employees have a negative attitude towards IS countermeasures, negative addictive behaviours such as leaving the computers without shutting them down, and risky practices such as installing software from unverified sources. The research discussions were very beneficial to conclude that there are numerous errors in security awareness training, such as human errors and communication issues, and these errors might have an impact on both the behaviour of the employees and on the progress of the public organisations. The differences in employees' cultural dimensions may have an impact on their behaviour as well. Therefore, organisations should enhance awareness concerning information security countermeasures in order to ensure the employees maintain professional behaviours. The security of the information system in an organisation mainly depends on the routing practices of the workforce. This should work hand in hand with technological remedies such as data encryption and access controls to help the UAE's public organisations to address the IS security threats. From the discussions of this research, it can be concluded that the IS security awareness of the UAE's public organisations has to be emphasised regularly so that the threats coming from both inside and outside the work environment can be addressed.

Aligning the theory of reasoned action with the topic of discussion, it can be concluded that the employees must understand the significance of the IS training schedule in the first place and the training schedule must not have any sort of communication gap among the resources working across the UAE's public organisations. Based on this theory, it can be said that the pre-existing attitude of the employees has to be checked prior to the training schedules to obtain the desired results. Aligning the theory of planned behaviour with the discussions of this research, it can be stated that the behaviour of the employees has to be managed in the first place, to address the security risks of the public organisations. Self-efficacy of the employees is strongly associated with their attitude and behaviour. From the protection motivation theory, it was determined that the intention of an employee is based on the level of security threats and the ability of the employees to cope with those threats. From the general deterrence theory, it can be concluded that employees of public organisations in the UAE must be certain about their actions; they must understand the clarity of the entire procedure to address the security threats. All the factors which have an impact on the intention of the employees can be identified and decisive steps can be taken using this theory. Based on the technology acceptance model, the attitude of the employees of the public organisations in the UAE can depend hugely on the perceived usefulness of the technologies which can address the security threats; and, at the same time, on the perceived ease of use of those technologies as well.

From the research, it can be concluded that the negative experience with IS security threats must not have any effect on the behaviour of the employees working across the UAE's public organisations. The IT governance framework can be incorporated across the UAE's public organisations as it can help them to understand the significance of the IS training schedules which can help the change their attitude towards IS countermeasures and risky

practices, which will help in addressing the security threats. Lack of IS awareness, motivation and knowledge can have a huge influence on the routine practices of the workforces working in the UAE's public organisations. At the same time, it can be concluded that the threats coming from inside an organisation are mainly due to the inappropriate behaviour of the employees, such as providing their password to an unauthorised person and being unaware of the IS policies. It can also be understood that the creation of an IS security culture can be very beneficial for a public organisation to manage the behaviour of its employees as this culture has a big influence on the intentions of the workforce as well. An IS security policy can help to enhance the behaviour of the employees of the UAE's public organisations.

8.7 Implications for Practice/Managers

The findings from the larger section of the population which was considered in the data collection procedure are concluded below:

8.7.1 Hypothesis 1: Attitudes towards cybersecurity countermeasures are positively related to the risky cybersecurity behaviour practices.

The results obtained from the participants help in understanding that the attitudes towards cybersecurity countermeasures are positively related to the risky cybersecurity behaviour practices. In this hypothesis, the independent variable is the attitudes towards cybersecurity countermeasures and the dependent variable is the risky cybersecurity behaviour practices, and the independent variable is able to predict 37% of the dependent variable. Attitudes towards cybersecurity countermeasures have the highest influence on the risky cybersecurity behaviour practices (0.684). At the same time, it can be determined that attitudes towards cybersecurity countermeasures are positively related to the risky cybersecurity

behaviour practices as p=0.000.The data analysis conducted by the researcher agrees with the discussions of Chen and Tung (2014), who stated that the risky cybersecurity behaviour practices depend hugely on the attitudes towards cybersecurity countermeasures, and this concept was also supported by Mullan *et al*. (2015), when they stated that the workplace practices have a huge influence on the risky cybersecurity behaviour practices. Hence, it can be understood that attitudes towards cybersecurity countermeasures are positively related to the risky cybersecurity behaviour practices.

8.7.2 Hypothesis 2: Security awareness countermeasures are positively related to the risky cybersecurity behaviour practices.

On the basis of the analysis and results obtained from the survey participants, it can be said that security awareness countermeasures are positively related to risky cybersecurity behaviour practices. The dependent variable of this hypothesis is risky cybersecurity behaviour practices and the independent variable of the hypothesis is the security awareness countermeasures. From the results, it can be concluded that 37.3% of the risky cybersecurity behaviour practices can be predicted from the security awareness countermeasures. It can also be concluded that security awareness countermeasures have a huge influence on the risky cybersecurity behaviour practices (0.479). At the same time, it can also be said that the security awareness countermeasures are positively related to the risky cybersecurity behaviour practices as p=0.000. The data analysis conducted by the researcher agrees with the discussions of Pearlson *et al*. (2016), who stated that security awareness countermeasures in a commercial environment can play a leading role to address security risks such as cyber-attacks. At the same time, Heckmann, Comes and Nickel (2015) highlighted that risks coming from inside an organisation can be solved if appropriate security awareness countermeasures are maintained.

The researchers stated that cybersecurity benefits from the maintenance of good security awareness countermeasures as well in public organisations. Hence, it can be understood that security awareness countermeasures are positively related to risky cybersecurity behaviour practices.

8.7.3 Hypothesis 3: Users' addictive behaviours are positively related to the risky cybersecurity behaviour practices.

The results obtained from the opinion of most of the participants suggest that the users' addictive behaviours are positively related to the risky cybersecurity behaviour practices. The dependent variable of this hypothesis is the risky cybersecurity behaviour practices and the independent variable of the hypothesis is the users' addictive behaviours. The independent variable of the hypothesis is able is to predict 37.4% of the dependent variable. From the results obtained, it can also be concluded that the users' addictive behaviours have a huge influence on the risky cybersecurity behaviour practices of the employees (0.547). At the same time, it can also be understood that the users' addictive behaviours are positively related to the risky cybersecurity behaviour practices as p=0.000. The results of this data analysis agree with the discussions in the literature where Humphries (2017) stated that the users' addictive behaviours are closely associated with the risky cybersecurity behaviour practices. Humphries stated that the addictive behaviours and the attitude behaviour of an employee are very closely associated with each other and both of them are closely associated with the risky cybersecurity behaviour practices as well. On the other hand, the significance of linking the action and the users' addictive behaviours was discussed by Martins *et al*. (2014), when they stated about the theory of reason action. Malekian *et al*. (2017) stated a different opinion about the topic: they highlighted that the technical expertise of the employees sometimes directs their risky

cybersecurity behaviour practices towards IS. The researchers stated that employees of public organisations must understand the key reasons behind the occurrence of the security attacks and the ways in which they must be addressed. Moreover, Kautonen *et al*. (2015) stated that the plan of action of each employee determined their addictive behaviours. From their discussions, it can be concluded that new employees are not always aware of the IS countermeasures guidelines; for those employees, it cannot be said that their addictive behaviours are not associated with their risky cybersecurity behaviour practices. However, from the perspective of a senior employee, it can be said that the risky cybersecurity behaviour practices and addictive behaviours of the employees are strongly associated with each other. Hence, on the basis of hypothesis testing and the scholars' discussions, it was understood that users' addictive behaviours are positively related to the risky cybersecurity behaviour practices.

8.7.4 Hypothesis 4: Attitudes towards cybersecurity countermeasures are positively related to the users' addictive behaviours.

The results obtained from the survey which was conducted on 124 samples indicated that attitudes towards cybersecurity countermeasures are positive related to the users' addictive behaviours in the public organisations. The independent variable of this hypothesis is the attitudes towards cybersecurity countermeasures, whereas the users' addictive behaviours are the dependent variable. The independent variable of this hypothesis is able to predict 7.6% variability of the users' addictive behaviours. The hypothesis test is also very useful as it provided a detailed description of the relationship among the two variables, and based on the analysis it can be said that the two parts of the hypothesis are very influential on each other (0.365). The statistical significance of this hypothesis testing (0.002) helps in understanding that attitudes towards cybersecurity countermeasures are positively related to the addictive

behaviours of users working in the public organisations. Attitudes towards cybersecurity countermeasures are positively related to the users' addictive behaviours as p=0.002. The results of this data analysis are also in agreement with the discussions of Cheng, Zhai and Smyth (2014), who stated that addictive behaviours of users working in public organisations are influenced by external factors such as job satisfaction ad workplace motivation. The researchers stated that each of these factors is greatly responsible for the attitudes towards cybersecurity countermeasures which are adopted by the organisations to address the security threats. Supporting the above discussion, Siponen *et al*. (2014) helped in understanding that workforces must not perform any illegal activity. The article helped the readers of this thesis to understand that employees must be able to understand where they are going wrong, as it can help them to create the positive attitude required to understand the usefulness of the IS countermeasures. Hence, it was determined that attitudes towards cybersecurity countermeasures are positively associated with the addictive behaviours of the users working across the UAE's public organisations.

8.7.5 Hypothesis 5: Users' addictive behaviours are positively mediating between the risky cybersecurity behaviour practices and information security countermeasures.

Based on the data obtained from the survey respondents, it was understood that users' addictive behaviours are positively mediating between IS countermeasures and risky cybersecurity behaviour practices. The results obtained from analysing this data show a supporting relation with this hypothesis. The mediator of this hypothesis is the addictive behaviours of the users working in the UAE's public organisations. Based on the discussions, it can be said that the impact of the users' addictive behaviours is 0.393, whereas the impact on the IS countermeasures is found to be 0. 063.The study also helps in understanding that

employees' attitude towards IS countermeasures can predict 30.8% of the dependent variable of this hypothesis. Cheng, Zhai and Smyth (2014) said that users' addictive behaviours such as impulsivity, premeditation and urgency are very beneficial for the improvement of workplace behaviours. The researchers stated that the employees' addictive behaviours are very significant to understand the information security countermeasures and the risky cybersecurity behaviour practices of the employees can play a key role in their IS practices. On the other hand, Mishra *et al*. (2014) critically evaluated the role of users' addictive behaviours in both IS countermeasures and risky cybersecurity behaviour practices, as they suggested that personal innovativeness such as security awareness, self-efficacy and attitude towards cybersecurity can be useful to address the security threats. Thus, it can be stated that users' addictive behaviours are positively mediating between risky cybersecurity behaviour practices and the IS countermeasures.

8.7.6 Hypothesis 6: Security awareness countermeasures are positively related to the users' addictive behaviours.

The results obtained from analysing the data collected from the 124 respondents indicated that the security awareness countermeasures are positively related to the users' addictive behaviours. The dependent variable of this hypothesis is the addictive behaviours of users working across the UAE's public organisations and the independent variable of this hypothesis is the security awareness countermeasures. Based on the calculations, it can be concluded that 7.6% variability of the independent variable of this hypothesis can be predicted by the dependent variable of the hypothesis, which is the users' addictive behaviours. It can be determined that the users' security awareness countermeasures have the highest impact on the users' addictive behaviours across the UAE's public organisations. It can also be concluded that

the security awareness countermeasures are positively related to the users' addictive behaviours as p=0.002.

From the calculations, it can be understood that the security awareness countermeasures of the users in the public organisations have a huge influence on the users' addictive behaviours (0.365). The results of this data analysis are in agreement with the discussions of Sheeran and Rivis (2017), who stated that employee attitude depends upon factors such as exposure and social upbringing. The investigators of this journal article stated that there are numerous factors which might influence the security awareness countermeasures, such as the administrative countermeasures, managerial countermeasures and support countermeasures. Supporting the above discussion, Safa *et al.* (2015) also helped in highlighting that employees must understand the impact of the security risks before working with the organisation and that can be done by informing them of the security awareness countermeasures. Hence, it can be concluded that the security awareness countermeasures of public organisations are related to the users' addictive behaviours.

8.8 Research Limitations

There are different research limitations which affect the structure of this examination to consider alongside the nature of the investigation. As indicated by Clark and Creswell (2014), an exploratory work is restricted to a few research limitations which are normal. The following are the thesis limitations:

Time constraint: the scheduled time to perform this particular research study along with examining the mediating effect of the users' addictive behaviours on the relationships between

information security countermeasures and risky cybersecurity practices was limited. Because of the research limitations, the researcher was required to conduct a cross-sectional study. This particular study was limited in conducting a detailed analysis along with evaluating the hidden details of the selected topic. Because of the time limitation, the researcher conducted this research study based on the UAE's public organisations only and the research study is mainly based on primary data. The researcher tried to end the research study within the scheduled time so that there was no such possibility of any deadline being missed or any kind of delays in the project.

Data reliability: the data were collected from the employees of public organisations in the UAE in the form of an online questionnaire administered through use of a survey. To lead the information for this examination. Each piece of data is to be kept in a confidential place so that no unauthorised person can access it. Therefore, each piece of data is kept on a password-protected database system.

Budget limitations: spending on this research study was constrained, which led to the confined extent of this examination. In the tight research spending plan, the researcher was restricted to an investigation into the UAE's public organisations just to investigate the human behaviour risks in information security countermeasures. The researcher likewise limited the investigations' budget to meet the university requirements.

8.9 Future Research Recommendations

Business conditions of the public organisations change constantly; at the same time, the needs and expectations of the employees also change. The recommendations for future research are as follows:

- The data obtained for this research were collected in a short time span; hence, it can be said that collection of data over years can provide more insights into the opinions collected from the employees of public organisations in the UAE.
- Employee behaviour can be studied over a longer period of time using a longitudinal study. Repeated observations from the same variables which were considered in this thesis can help to identify more useful and relevant information about the behaviour of the employees towards IS countermeasures.

Personal interview as the data collection procedure can also help to classify the factors which have a direct influence on employee behaviour. Detailed information on personal feelings can be obtained from this data collection procedure.

The list of recommendations considering all the factors which have an influence on the behaviour of the workforces of the UAE's public organisations are as follows:

- Based on the study, it was found that security awareness countermeasures are positively related to the users' addictive behaviours. Hence, it can be recommended that the UAE's public organisations must be looking forward to maintain and adjust their methods of awareness and professional work culture, as this would help to enhance the positive addictive behaviour of the employees towards IS.

- The study indicated that security awareness countermeasures are directly related to the risky cybersecurity behaviours. Hence, it can be recommended that the UAE's public organisations must maintain a good organisational awareness such as open communication. Open-ended communications can be very beneficial for the employees to understand the significance of the IS countermeasures. At the same time, discussion about the business's values can also be very useful to enable employees to develop a positive attitude as far as IS countermeasures are concerned. This can help in enforcing security in the organisation.
- Based on the study, it was found that attitudes towards cybersecurity countermeasures are positively related to the risky cybersecurity behaviours. Hence, it can be recommended that the UAE's public organisations must aim to have an influence over their employees' intentions.
- The study helped in understanding that IS countermeasures are positively related to the users' addictive behaviours. Hence, it can be recommended that public organisations must be stating the significance of IS countermeasures in the first place. Technology-based training sessions can be provided to the employees of these organisations as this would help them to understand the significance of IS countermeasures and enhance their addictive behaviours.
- Based on the study, it was understood that the behavioural practices are positively related to the IS countermeasures. Hence, it can be recommended that public organisations in the UAE must monitor the behavioural practices of their employees on a regular basis. A behavioural analytics tool is strongly recommended for the organisations as it will help them help to reveal the actions taken by their employees.

- Based on the study, it was found that the addictive behaviours of the employees are positively related to their risky behavioural practices towards IS. Hence, it can be recommended that the UAE's public organisations must aim to educating the employees on addictive behaviours that can put the security of information at risk.

When all these recommendations are carried out accordingly, the organisations are less likely to experience information security threats from both within and outside.

REFERENCES

A'ang Subiyakto, A., Ahlan, R., Kartiwi, M., Hakiem, N., Huda, M. Q., and Susanto, A. (2018) 'The information system project profiles among universities in Indonesia', *Indonesian Journal of Electrical Engineering and Computer Science*, 12(2), pp.865-872.

Ab Rahman, N. H. and Choo, K. K. R. (2015) 'A survey of information security incident handling in the cloud', *Computers and Security*, 49, pp. 45–69. doi: 10.1016/J.COSE.2014.11.006.

Abbas, J., Aman, J., Nurunnabi, M., and Bano, S. (2019) 'The impact of social media on learning behavior for sustainable education: Evidence of students from selected universities in Pakistan', *Sustainability*, 11(6), p.1683. doi: 10.3390/su11061683.

Abbasi, A., Sarker, S. and Chiang, R. H. L. (2016) 'Big data research in information systems: Toward an inclusive research agenda', *Journal of the Association for Information Systems*, 17(2), p. 3. doi: 10.17705/1jais.00423.

Adam, A., Yuniarsih, T., Ahman, E., and Kusnendi, K. (2020) 'The mediation effect of organizational commitment in the relation of organization culture and employee performance', *In 3rd Global Conference on Business, Management, and Entrepreneurship (GCBME 2018)*, pp.260-264. Atlantis Press. Available at: https://www.atlantis-press.com/proceedings/gcbme-18/125933720 (Accessed: 27 November 2021).

Ahmad, Z., Ong, T. S., Liew, T. H., and Norhashim, M. (2019) 'Security monitoring and information security assurance behaviour among employees: An empirical analysis', *Information and Computer Security*, 27(2), pp. 165–188. doi: 10.1108/ICS-10-2017-0073/FULL/HTML.

Al-Daeef, M. M., Basir, N., and Saudi, M. M. (2017) 'Security awareness training: A review ', *Lecture Notes in Engineering and Computer Science* . Available at: https://oarep.usim.edu.my/jspui/handle/123456789/1880 (Accessed: 24 October 2018).

Albarracin, D. and Shavitt, S. (2017) 'Attitudes and attitude change', *Annual Review of Psychology*, 69, pp.299-327. doi: 10.1146/annurev-psych-122216.

Aldahmash, A. H., Alamri, N. M., and Aljallal, M. A. (2019) 'Saudi Arabian science and mathematics teachers' attitudes toward integrating STEM in teaching before and after

participating in a professional development program', *Cogent Education*, 6(1). doi: 10.1080/2331186X.2019.1580852.

Aldawood, H. and Skinner, G. (2019) 'Reviewing cyber security social engineering training and awareness programs—Pitfalls and ongoing issues', *Future Internet*, Vol. 11, Page 73, 11(3), p. 73. doi: 10.3390/FI11030073.

Alexander, D. (2014) 'Social media in disaster risk reduction and crisis management', *Science and Engineering Ethics*, 20(3), pp.717-733. doi: 10.1007/s11948-013-9502-z.

Alhosani, K. E. H. A., Khalid, S. K. A., Samsudin, N. A., Jamel, S., and bin Mohamad, K. M. (2019) 'A policy driven, human oriented information security model: A case study in UAE banking sector', *In 2019 IEEE Conference on Application, Information and Network Security (AINS)*, pp.12-17. IEEE. Available at: https://ieeexplore.ieee.org/abstract/document/8968705/ (Accessed: 27 June 2020).

Alshare, K. A., Lane, P. L. and Lane, M. R. (2018) 'Information security policy compliance: A higher education case study', *Information and Computer Security*, 26(1), pp. 91–108. doi: 10.1108/ICS-09-2016-0073/FULL/HTML.

Ameen, N., Tarhini, A., Shah, M. H., Madichie, N., Paul, J., and Choudrie, J. (2021) 'Keeping customers' data secure: A cross-cultural study of cybersecurity compliance among the Gen-Mobile workforce', *Computers in Human Behavior*, 114. doi: 10.1016/j.chb.2020.106531.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., and Xu, L. (2017) 'Gender difference and employees' cybersecurity behaviors', *Computers in Human Behaviour*, 69, pp. 437–443. doi: 10.1016/j.chb.2016.12.040.

Argyriou, E., Um, M., Carron, C., and Cyders, M. A. (2018) 'Age and impulsive behavior in drug addiction: A review of past research and future directions', *Pharmacology Biochemistry and Behavior*, 164, pp. 106–117. doi: 10.1016/J.PBB.2017.07.013.

Arnott, D., Lizama, F. and Song, Y. (2017) 'Patterns of business intelligence systems use in organizations', *Decision Support Systems*, 97, pp. 58–68. doi: 10.1016/J.DSS.2017.03.005.

Asadi, S., Nilashi, M., Safaei, M., Abdullah, R., Saeed, F., Yadegaridehkordi, E., and Samad, S. (2019) 'Investigating factors influencing decision-makers' intention to adopt

green IT in Malaysian manufacturing industry', *Resources, Conservation and Recycling*, 148, pp. 36–54. doi: 10.1016/j.resconrec.2019.04.028.

Asrar-ul-Haq, M. and Kuchinke, P. (2016) 'Impact of leadership styles on employees' attitude towards their leader and performance: Empirical evidence from Pakistani banks', *Future Business Journal*, 2(1), pp. 54–64. doi: 10.1016/j.fbj.2016.05.002.

Attig, C., Wessel, D. and Franke, T. (2017) 'Assessing personality differences in human-technology interaction: An overview of key self-report scales to predict successful interaction', *International Conference on Human-Computer Interaction*, pp. 19–29. doi: 10.1007/978-3-319-58750-9_3.

Awang, Z., Afthanorhan, A., and Mamat, M. (2016) 'The likert scale analysis using parametric based structural equation modeling (SEM)', *Computational Methods in Social Sciences*, 4(1), p.13 . Available at: https://www.researchgate.net/profile/Ali-Al-Allaq/post/Can_we_use_6_point_Likert_Scale_while_using_SEM_I_am_wandering_how_it_would_be_to_analyze/attachment/628bfd70f20e03378c4b75ff/AS%3A1159012628344838%401653341552115/download/Likert+Scale.pdf (Accessed: 27 July 2017).

Bae, S., Han, S. M. and Moura, S. (2019) 'Modeling & control of human actuated systems', *IFAC-Papers on Line*, 51(34), pp.40-46. doi: 10.1016/j.ifacol.2019.01.016.

Barratt, E.S and Felthous, A.R. (2003) 'Impulsive versus premeditated aggression: Implications for mens rea decisions', *Behavioral Science & the Law*, 21(5), pp. 619–630. doi: 10.1002/bsl.555.

Battleday, R. M., Peterson, J. C. and Griffiths, T. L. (2017) 'Modeling human categorization of natural images using deep feature representations', *ArXiv Preprint* ArXiv:1711.04855. Available at: http://arxiv.org/abs/1711.04855 (Accessed: 27 October 2019).

Beauchaine, T. P., Zisner, A. R., and Sauder, C. L. (2017) 'Trait impulsivity and the externalizing spectrum', *Annual Review of Clinical Psychology*, 13, pp. 343–368. doi: 10.1146/annurev-clinpsy-021815-093253.

Bhatti, N. B., Siyal, A. A., Qureshi, A. L., and Bhatti, I. A. (2019) 'Socio-economic impact assessment of small dams based on t-paired sample test using SPSS software', *Civil Engineering Journal*, 5(1), pp.153-164. doi: 10.28991/cej-2019-03091233.

Birkel, H. S., Veile, J. W., Müller, J. M., Hartmann, E., and Voigt, K. I. (2019) 'Development of a risk framework for industry 4.0 in the context of sustainability for established manufacturers', *Sustainability (Switzerland)*, 11(2), p. 384. doi: 10.3390/su11020384.

Bloomberg, L. and Volpe, M. (2018) 'Completing your qualitative dissertation: A road map from beginning to end,' California. *Sage Publications*. Available at: https://books.google.com/books?hl=ar&lr=&id=v_pyDwAAQBAJ&oi=fnd&pg=PP1&ots=UMl_MOk2Uj&sig=hz_aW5cF7Wxodpewe5UkD6wd57M (Accessed: 27 February 2019).

Böhme, R., Kirchner, M., Katzenbeisser, S., and Petitcolas, F. (2016) 'Media forensics. In information hiding', *Artech House*, pp.231-259.

Broady, T., Chan, A., and Caputi, P. (2010) 'Comparison of older and younger adults' attitudes towards and abilities with computers: Implications for training and learning', *British Journal of Educational Technology*, pp. 473–485. doi: 10.1111/j.1467-8535.2008.00914.x.

Bujang, M. A. and Baharum, N. (2016) 'Sample size guideline for correlation analysis', *World, 3(1)*, pp.37-46. doi: 10.22158/wjssr.v3n1p37.

Burns, A. J., Posey, C., Roberts, T. L., and Lowry, P. B. (2017) 'Examining the relationship of organizational insiders' psychological capital with information security threat and coping appraisals', *Computers in Human Behavior*, 68, pp. 190–209. doi: 10.1016/J.CHB.2016.11.018.

Cain, A. A., Edwards, M. E. and Still, J. D. (2018) 'An exploratory study of cyber hygiene behaviors and knowledge', *Journal of Information Security and Applications*, 42, pp. 36–45. doi: 10.1016/j.jisa.2018.08.002.

Chen, M. F. and Tung, P. J. (2014) 'Developing an extended theory of planned behavior model to predict consumers' intention to visit green hotels', *International Journal of Hospitality management*, 36, pp.221-230. Available at: https://www.sciencedirect.com/science/article/pii/S0278431913001266 (Accessed: 27 December 2016).

Cheng, L., Li, W., Zhai, Q., and Smyth, R. (2014) 'Understanding personal use of the internet at work: An integrated model of neutralization techniques and general deterrence theory', *Computers in Human Behavior*, 38, pp. 220–228. doi: 10.1016/j.chb.2014.05.043.

Chin, J., Jiang, B. C., Mufidah, I., Persada, S. F., and Noer, B. A. (2018) 'The investigation of consumers' behavior intention in using green skincare products: A pro-environmental behavior model approach', *Sustainability*, 10(11), p.3922. doi: 10.3390/su10113922.

Chu, A. M. and So, M. K. (2020) 'Organisational information security management for sustainable information systems: An unethical employee information security behavior perspective', *Sustainability*, 12(8), p.3163.

Clark, V. P. and Creswell, J. (2014) 'Understanding research: A consumer's guide ,' New York. *Pearson Higher Education.* Available at: https://repository.vnu.edu.vn/handle/VNU_123/90019 (Accessed: 28 March 2017).

Cobb, W. (2021) 'Biometric cybersecurity and workflow management ', *US Patent Application*. 17/068. Google Patents . Available at: https://patents.google.com/patent/US20210044583A1/en (Accessed: 27 January 2022).

Conner, M. and Norman, P. (2015) 'EBOOK: Predicting and changing health behaviour: Research and practice with social cognition models ', Berkshire (UK). *McGraw-Hill Education*. Available at: https://www.google.com/books?hl=ar&lr=&id=pMkvEAAAQBAJ&oi=fnd&pg=PR3&ots=eW1Dy7ilLx&sig=wZzZhlPJEy0PMc2rnjxphs0E80E (Accessed: 27 April 2017).

Connolly, L. Y., Lang, M., Gathegi, J., and Tygar, D. J. (2017) 'Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study', *Information & Computer Security*, 25(2), pp.118-136.

Coutlee, C. G., Politzer, C. S., Hoyle, R. H., and Huettel, S. A. (2014) 'An abbreviated impulsiveness scale constructed through confirmatory factor analysis of the barratt impulsiveness scale version 11 ', *Archives of Scientific Psychology*, pp. 1–12. doi: 10.1037/arc0000005.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. (2013) 'Future directions for behavioral information security research', . *Computers & Security*, 32, pp.90-101. doi: 10.1016/j.cose.2012.09.010.

Crossler, R. E., Long, J. H., Loraas, T. M., and Trinkle, B. S. (2014) 'Understanding compliance with bring your own device policies utilizing protection motivation theory: Bridging the intention-behavior gap', *Journal of Information Systems*, 28(1), pp.209-226. Available at: https://meridian.allenpress.com/jis/article-abstract/28/1/209/75873 (Accessed: 27 May 2018).

D'Arcy, J. and Teh, P. L. (2019) 'Predicting employee information security policy compliance on a daily basis: The interplay of security-related stress, emotions, and neutralization', *Information and Management*, 56(7), p. 103151. doi: 10.1016/j.im.2019.02.006.

Dahbur, K., Bashabsheh, Z. and Bashabsheh, D., (2017) 'Assessment of security awareness: A qualitative and quantitative study', *International Management Review*, 13(1), p.37. Available at: https://search.proquest.com/openview/ba98a8bc4cf71224c96295ee6eeea0fe/1?pq-origsite=gscholar&cbl=28202 (Accessed: 27 July 2019).

Dall'Arno, M. and Scarani, V. (2020) 'Worst-case quantum hypothesis testing with separable measurements', *Quantum, 4*, p.320. doi: 10.22331/Q-2020-09-11-320.

Daniel, W. and Cross, C. (2018) 'Biostatistics: a foundation for analysis in the health sciences ,' Hoboken, NJ. *Wiley*. Available at: https://www.google.com/books?hl=ar&lr=&id=PON1DwAAQBAJ&oi=fnd&pg=PA3&dq=daniel+ww+(1999).+biostatistics+a+foundation+for+analysis+in+the+health+sciences&ots=a7YAeWmrRw&sig=aqzn0f2Tj5ZcrtnJ4E30fVyT39w (Accessed: 21 August 2019).

Darlington, R. and Hayes, A. (2016) 'Regression analysis and linear models: Concepts, applications, and implementation ,' New York. *Guilford Publications.* Available at: https://www.google.com/books?hl=ar&lr=&id=YDgoDAAAQBAJ&oi=fnd&pg=PP1&ots=8hKZzSjAxE&sig=FLiyi3OLXwPuodLYRQ3FJ83FFmY (Accessed: 27 January 2017).

David, D. P., Keupp, M. M., and Mermoud, A. (2020) 'Knowledge absorption for cyber-security: The role of human beliefs', *Computers in Human Behavior*, 106, p.106255. doi: 10.1016/j.chb.2020.106255.

De Leeuw, A., Valois, P., Ajzen, I., and Schmidt, P. (2015) 'Using the theory of planned behavior to identify key beliefs underlying pro-environmental behavior in high-school students: Implications for educational intervention', *Journal of Environmental Psychology*, 42, pp.128-138. doi: 10.1016/j.jenvp.2015.03.005.

Dennis, A. R. and Minas, R. K. (2018) 'Security on autopilot: Why current security theories hijack our thinking and lead us astray', *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 49(SI), pp.15-38.

Derevensky, J. L., Hayman, V. and Gilbeau, L. (2019) 'Behavioral addictions: excessive gambling, gaming, internet, and smartphone use among children and adolescents', *Pediatric Clinics of North America. W.B. Saunders*, pp. 1163–1182. doi: 10.1016/j.pcl.2019.08.008.

Dhillon, G., Abdul Talib, Y. Y. and Picoto, W. N. (2020) 'The mediating role of psychological empowerment in information security compliance intentions', *Journal of the Association for Information Systems*, 21(1), p.5.

Disman, D., Ali, M. and Barliana, M.S. (2017) 'The use of quantitative research method and statistical data analysis in dissertation: An evaluation study', *International Journal of Education*, 10(1), pp.46-52 . Available at: https://ejournal.upi.edu/index.php/ije/article/view/5566 (Accessed: 27 November 2018).

Dougherty, M. R., Slevc, L. R. and Grand, J. A. (2019) 'Making research evaluation more transparent: Aligning research philosophy, institutional values, and reporting', *Perspectives on Psychological Science*, 14(3), pp. 361–375. doi: 10.1177/1745691618810693.

Dwivedi, Y. K., Rana, N. P., Jeyaraj, A., Clement, M., and Williams, M. D. (2019) 'Re-examining the unified theory of acceptance and use of technology (UTAUT): Towards a revised theoretical model', *Information Systems Frontiers*, 21(3), pp. 719–734. doi: 10.1007/s10796-017-9774-y.

Edson, M., Henning, P. and Sankaran, S. (2016) 'A guide to systems research: Philosophy, processes and practice ', (Vol. 10) Singapore. *Springer*. Available at: https://link.springer.com/content/pdf/10.1007/978-981-10-0263-2.pdf (Accessed: 27 February 2017).

Evans, M., He, Y., Maglaras, L., and Janicke, H. (2019) 'HEART-IS: A novel technique for evaluating human error-related information security incidents', *Computers & Security*, 80, pp.74-89.

Fetters, M. D. and Molina-Azorin, J. F. (2019) 'Rebuttal—Conceptualizing integration during both the data collection and data interpretation phases: A response to David Morgan', *Journal of Mixed Methods Research*, 13(1), pp. 12–14. doi: 10.1177/1558689818780596A.

Fielder, A., Panaousis, E., Malacaria, P., Hankin, C., and Smeraldi, F. (2016) 'Decision support approaches for cyber security investment', *Decision Support Systems*, 86, pp. 13–23. doi: 10.1016/j.dss.2016.02.012.

Fimin, M. (2017) ‘Are employees part of the ransomware problem?’, *Computer Fraud & Security*, 2017(8), pp. 15–17. doi: 10.1016/S1361-3723(17)30072-6.

Fine, S. and Edward, M. (2017) ‘Breaking the rules, not the law: The potential risks of counterproductive work behaviors among overqualified employees’, *International Journal of Selection and Assessment*, 25(4), pp. 401–405. doi: 10.1111/IJSA.12194.

Fletcher, A. J. (2016) ‘Applying critical realism in qualitative research: Methodology meets method’, *International Journal of Social Research Methodology*, 20(2), pp. 181–194. doi: 10.1080/13645579.2016.1144401.

Flick, U. (2015) ‘Introducing research methodology: A beginner’s guide to doing a research project ’, California. *Sage Publications.* Available at: https://www.google.com/books?hl=ar&lr=&id=jcOICwAAQBAJ&oi=fnd&pg=PP1&ots=rsTxe_8481&sig=rHSk1B7TNQ7RGZFsXNXZgtZvfCA (Accessed: 27 September 2016).

Friese, S. (2019) ‘Qualitative data analysis with ATLAS. Ti’, California. *Sage Publications*. Available at: https://www.google.com/books?hl=ar&lr=&id=QauMDwAAQBAJ&oi=fnd&pg=PP1&ots=HQeCm8qpNa&sig=vxUCYWV2EsqJ6SNJeGtxYZpD590 (Accessed: 27 October 2020).

Fuentes, A. (2017) ‘Human niche, human behaviour, human nature’, *Interface Focus*, 7(5), p.20160136. doi: 10.1098/rsfs.2016.0136.

Galletta, M., Portoghese, I., Melis, P., Gonzalez, C. I. A., Finco, G., D’Aloja, E., and Campagna, M. (2019) ‘The role of collective affective commitment in the relationship between work-family conflict and emotional exhaustion among nurses: A multilevel modeling approach’, *BMC Nursing*, 18(1), pp. 1–9. doi: 10.1186/s12912-019-0329-z.

Gates, M., Elliott, S. A., Johnson, C., Thomson, D., Williams, K., Fernandes, R. M., and Hartling, L. (2018) ‘A descriptive analysis of non-Cochrane child-relevant systematic reviews published in 2014’, *BMC Medical Research Methodology*, 18(1), pp.1-10. doi: 10.1186/s12874-018-0562-2.

George, D. and Mallery, P. (2016) ‘Frequencies’, In IBM SPSS statistics 23 step by step, pp. 115–125, New York. *Routledge.* doi: 10.4324/9781315545899-12.

Gerber, N., McDermott, R., Volkamer, M., and Vogt, J. (2016) ‘Understanding information security Compliance-Why goal setting and rewards might be a bad idea’, *In HAISA*, pp.145-

155 . Available at: https://download.hrz.tu-darmstadt.de/pub/FB20/Dekanat/Publikationen/SECUSO/7_Understanding_information_security_compliance__Why_goal_setting_and_rewards_might_be_a_bad_idea.pdf (Accessed: 27 June 2020).

Gjertsen, E. G. B., Gjære, E. A., Bartnes, M., and Flores, W. R. (2017), February 'Gamification of information security awareness and training', *In ICISSP*, pp.59-70.

Glanz, K., Rimer, B. K. and Viswanath, K. (2008) 'Health behavior and health education: theory, Research, and practice', Hoboken, NJ. *John Wiley & Sons*. Available at: https://www.google.com/books?hl=ar&lr=&id=1xuGErZCfbsC&oi=fnd&pg=PT12&dq=Health+Behaviour+and+Health+Education:+Theory,+Research+and+Practice&ots=-q7a8J560r&sig=D1vYqN8uuRJwdDNcoe-_NCMdXBo (Accessed: 26 October 2016).

González, J. (2019) 'Building information security awareness and training for older adults', (Doctoral dissertation, *Utica College*). Available at: https://search.proquest.com/openview/c4e2bab1f2d4897618e660731b1cac40/1?pq-origsite=gscholar&cbl=18750&diss=y (Accessed: 27 May 2020).

Gotsis, M. and Jordan-Marsh, M. (2018) 'Calling HCI professionals into health research: Patient safety and health equity at Stake', *In Proceedings of the 22nd Pan-Hellenic Conference on Informatics*, pp. 213–218. doi: 10.1145/3291533.3291562.

Gray, D. E. (2019) 'Doing research in the business world', California. *Sage Publications*. Available at: https://www.torrossa.com/gs/resourceProxy?an=5017980&publisher=FZ7200 (Accessed: 27 July 2021).

Green, S. and Salkind, N. (2013) 'Using SPSS for Windows and Macintosh', books a la carte. New York. *Pearson Higher Education.* Available at: https://dl.acm.org/doi/abs/10.5555/2563627 (Accessed: 28 December 2016).

Grey, I., Daly, R., Thomas, J., and Marassas, W. (2018) 'The relationship between shame and guilt: Cultural comparisons between Ireland and the United Arab Emirates', *Mental Health, Religion and Culture*, 21(3), pp. 221–230. doi: 10.1080/13674676.2018.1455651.

Gritzalis, D., Kandias, M., Stavrou, V., and Mitrou, L. (2014) 'History of information: The case of privacy and security in social media', *In Proceedings of the History of Information Conference*, pp.283-310 . Available at: https://www.infosec.aueb.gr/Publications/INFOHIST-2014 Legal Publications.pdf (Accessed: 28 April 2017).

Guhr, N., Lebek, B. and Breitner, M. H. (2019) 'The impact of leadership on employees' intended information security behaviour: An examination of the full-range leadership theory', *Information Systems Journal*, 29(2), pp. 340–362. doi: 10.1111/ISJ.12202.

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. doi: 10.1016/j.heliyon.2017.e00346.

Hadlington, L. and Murphy, K. (2018) 'Is media multitasking good for cybersecurity? Exploring the relationship between media multitasking and everyday cognitive failures on self-reported risky', *Cyberpsychology, Behavior, and Social Networking*, 21(3), pp. 168–172. doi: 10.1089/cyber.2017.0524.

Hajli, N. and Lin, X. (2016) 'Exploring the security of information sharing on social networking sites: The role of perceived control of information', *Journal of Business Ethics*, 133(1), pp. 111–123. doi: 10.1007/S10551-014-2346-X.

Hall, L., Hume, C. and Tazzyman, S. (2016) 'Five degrees of happiness: Effective smiley face likert scales for evaluating with children', *In Proceedings of the 15th International Conference on Interaction Design and Children*, pp. 311–321. doi: 10.1145/2930674.2930719.

Hanus, B. and Wu, Y. A. (2016) 'Impact of users' security awareness on desktop security behavior: A protection motivation theory perspective', *Information Systems Management*, 33(1), pp.2-16.

Hayes, A. F. (2017) 'Introduction to mediation, moderation, and conditional process analysis: A regression-based approach', New York. *Guilford publications.*

Hayes, A. F. and Montoya, A. K. (2017) 'A tutorial on testing, visualizing, and probing an interaction involving a multicategorical variable in linear regression analysis', *Communication Methods and Measures*, 11(1), pp.1-30.

He, D., Zeadally, S., Kumar, N., and Lee, J. H. (2016) 'Anonymous authentication for wireless body area networks with provable security', *IEEE Systems Journal*, 11(4), pp.2590-2601. Available at: https://ieeexplore.ieee.org/abstract/document/7458160/ (Accessed: 28 May 2018).

Heckmann, I., Comes, T., and Nickel, S. (2015) ‘A critical review on supply chain risk–Definition, measure and modeling ’, *Omega*, pp. 119–132. doi: 10.1016/j.omega.2014.10.004.

Hina, S., Panneer Selvam, D. D. D. and Lowry, P. B. (2019) ‘Institutional governance and protection motivation: Theoretical insights into shaping employees’ security compliance behavior in higher education institutions in the developing world’, *Computers and Security*, 87, p. 101594. doi: 10.1016/j.cose.2019.101594.

Howard, D. (2018) ‘Development of the cybersecurity attitudes scale and modeling cybersecurity behavior and its antecedents’, (Master dissertation, *University of South Florida*). Available at: https://search.proquest.com/openview/3dc3023a78987b7a73a7bd6c5dd0796d/1?pq-origsite=gscholar&cbl=18750 (Accessed: 28 November 2020).

Hsu, J. S. C., Shih, S. P., Hung, Y. W., and Lowry, P. B. (2015) ‘The role of extra-role behaviors and social controls in information security policy effectiveness’, *Information Systems Research*, 26(2), pp. 282–300. doi: 10.1287/ISRE.2015.0569.

Humphries, B. (2017) ‘Re-thinking social research: Anti-discriminatory approaches in research methodology’, New York. *Taylor & Francis*. Available at: https://www.google.com/books?hl=ar&lr=&id=6EQrDwAAQBAJ&oi=fnd&pg=PR2&ots=yCo7cT2J28&sig=0FRJCAvTutSOzUWRFFFGSUKxSx4 (Accessed: 28 July 2018).

Ifinedo, P. (2014) ‘Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition’, *Information & Management*, pp. 69–79. doi: 10.1016/j.im.2013.10.001.

Jacobi, C., Atteveldt, W. and Welbers, K. (2016) ‘Quantitative analysis of large amounts of journalistic texts using topic modelling ’, *Digital Journalism*, 4 (1), pp. 89–106. doi: 10.1080/21670811.2015.1093271.

Jahromi, A. A., Kemmeugne, A., Kundur, D., and Haddadi, A. (2019) ‘Cyber-physical attacks targeting communication-assisted protection schemes ’, *IEEE Transactions on Power Systems*, 35(1), pp. 440–450. doi: 10.1109/tpwrs.2019.2924441.

Jeeragal, R. (2018) ‘Experimental investigation on control of NOx emission in hydrogen fueled spark ignition engines’, (Doctoral Dissertation, I*ndian Institute of Technology Delhi*). Available at: http://103.27.10.17/bitstream/handle/12345678/7723/TH-5643.pdf?sequence=2&isAllowed=y (Accessed: 28 January 2019).

Jeong, C. Y., Lee, S. Y. T. and Lim, J. H. (2019) 'Information security breaches and IT security investments: Impacts on competitors', *Information and Management*, 56(5), pp. 681–695. doi: 10.1016/j.im.2018.11.003.

Józsa, K. and, Morgan, G. (2017) 'Reversed items in Likert scales: Filtering out invalid responders ', *Journal of Psychological and Educational Research*, 25(1), pp. 7–25. Available at: http://publicatio.bibl.u-szeged.hu/24130/1/reverseditem.pdf (Accessed: 28 March 2018).

Kampas, S. R., Tarkowski, A. R., Portell, C. M., and Bhatti, N. (2016) 'System and method for cloud enterprise services', Washington, U.S. *Accenture Global Services Ltd*, Patent 9,235,442. Google Patents . Available at: https://patents.google.com/patent/US9235442B2/en (Accessed: 28 September 2017).

Karjalainen, M., Sarker, S. and Siponen, M. (2019) 'Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective', *Information Systems Research*, 30(2), pp.687-704.

Kautonen, T., Gelderen, M. and Fink, M. (2015) 'Robustness of the theory of planned behavior in predicting entrepreneurial intentions and actions', *Entrepreneurship Theory and Practice*, 39(3), pp.655-674 . Available at: https://journals.sagepub.com/doi/abs/10.1111/etap.12056 (Accessed: 28 June 2016).

Kessler, S. R., Pindek, S., Kleinman, G., Andel, S. A., and Spector, P. E. (2020) 'Information security climate and the assessment of information security risk among healthcare employees', *Health Informatics Journal*, 26(1), pp. 461–473. doi: 10.1177/1460458219832048.

Khando, K., Gao, S., Islam, S. M., and Salman, A. (2021) 'Enhancing employees information security awareness in private and public organisations: A systematic literature review', *Computers & Security*, 106, p.102267.

Kim, S. H., Yang, K. H. and Park, S. (2014) 'An integrative behavioral model of information security policy compliance', *The Scientific World Journal*, 2014. doi: 10.1155/2014/463870.

Kogut, C. S., Cotta de Mello, R. D. and da Rocha, A. (2020) 'International expansion for knowledge acquisition or knowledge acquisition for international expansion?', *Multinational Business Review*, 28(2), pp. 177–200. doi: 10.1108/MBR-11-2018-0084/FULL/HTML.

Kokolakis, S. (2017) 'Privacy attitudes and privacy behaviour: A review of current research on the privacy paradox phenomenon', *Computers & Security*, 64, pp. 122–134. doi: 10.1016/j.cose.2015.07.002.

Kumar, R. (2018) 'Research methodology: A step-by-step guide for beginners', California. *Sage Publications*. Available at: https://www.google.com/books?hl=ar&lr=&id=J2J7DwAAQBAJ&oi=fnd&pg=PP1&ots=cvrkEzQCii&sig=u1RMREd2y-v5KxT6JW-rUxhjMu0 (Accessed: 28 September 2019).

Lajoie, B. (2016) 'Computational approaches for the analysis of chromosome conformation capture data and their application to study long-range gene regulation', (Doctoral Dissertation, *UMass Chan*) . Available at: https://escholarship.umassmed.edu/gsbs_diss/833/ (Accessed: 28 October 2017).

Layton, T. (2016) 'Information security: Design, implementation, measurement, and compliance ', Boca Raton. *CRC Press*. Available at: https://www.taylorfrancis.com/books/mono/10.1201/9781420013412/information-security-timothy-layton (Accessed: 28 February 2017).

Lazar, J., Feng, J. and Hochheiser, H. (2017) 'Research methods in human-computer interaction ', Boston. *Morgan Kaufmann*. Available at: https://www.google.com/books?hl=ar&lr=&id=hbkxDQAAQBAJ&oi=fnd&pg=PP1&ots=Sq735a245P&sig=xefqI__8AqyaxpeaDJ-_u5j0ryM (Accessed: 28 April 2018).

Leavy, P. (2017) 'Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches', New York. *Patricia Leavy*. Available at: https://www.google.com/books?hl=ar&lr=&id=hxyDDgAAQBAJ&oi=fnd&pg=PP1&ots=T59Z3Sq8h9&sig=xpmUxU_xjhzL7GyLA0XviYuouxE (Accessed: 28 November 2018).

Lewis, J. (2016) 'Using ATLAS. ti to facilitate data analysis for a systematic review of leadership competencies in the completion of a doctoral dissertation', (Doctoral Dissertation, *Salve Regina University*) . Available at: https://core.ac.uk/download/pdf/56512753.pdf (Accessed: 28 January 2017).

Lewis, S. (2015) 'Qualitative inquiry and research design: Choosing among five approaches', *Health Promotion Practice*, 16(4), pp. 473–475. doi: 10.1177/1524839915580941.

Li, L., Xu, L., He, W., Chen, Y., and Chen, H. (2016) 'Cyber security awareness and its impact on employee's behavior', *In International Conference on Research and Practical Issues of Enterprise Information Systems*, 268, pp. 103–111. doi: 10.1007/978-3-319-49944-4_8.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., and Yuan, X. (2019) 'Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behaviour', *International Journal of Information Management*, 45, pp.13-24.

List, J. A., Shaikh, A. M. and Xu, Y. (2016) 'Multiple hypothesis testing in experimental economics ', *Experimental Economics*, 22(4), pp.773-793. Available at: https://asset-pdf.scinapse.io/prod/2281690356/2281690356.pdf (Accessed: 28 May 2017).

Litz, D. and Scott, S. (2017) 'Transformational leadership in the educational system of the United Arab Emirates', *Educational Management Administration and Leadership*, 45(4), pp. 566–587. doi: 10.1177/1741143216636112.

Maass, W., Parsons, J., Purao, S., Storey, V. C., and Woo, C. (2018) 'Data-driven meets theory-driven research in the era of big data: Opportunities and challenges for information systems research', *Journal of the Association for Information Systems*. *Association for Information Systems*, pp. 1253–1273. doi: 10.17705/1jais.00526.

Magazzeni, D., Mcburney, P. and Nash, W. (2017) 'Validation and verification of smart contracts: A research agenda', *Computer*, 50(9), pp. 50–57. doi: 10.1109/MC.2017.3571045.

Mahapatra, S. (2019) 'Smartphone addiction and associated consequences: Role of loneliness and self-regulation', *Behaviour and Information Technology*, 38(8), pp. 833–844. doi: 10.1080/0144929X.2018.1560499.

Malekian, A., Hayati, D., and Aarts, N. (2017) 'Conceptualizations of water security in the agricultural sector: Perceptions, practices, and paradigms ', *Journal of Hydrology*, 544, pp.224-232 . Available at: https://www.sciencedirect.com/science/article/pii/S0022169416307326 (Accessed: 28 May 2018).

Mamonov, S. and Benbunan-Fich, R. (2018) 'The impact of information security threat awareness on privacy-protective behaviors', *Computers in Human Behavior*, 83, pp. 32–44. doi: 10.1016/j.chb.2018.01.028.

Martins, C., Oliveira, T. and Popovič, A. (2014) 'Understanding the internet banking adoption: A unified theory of acceptance and use of technology and perceived risk application', *International Journal of Information Management*, 34(1), pp. 1–13. doi: 10.1016/J.IJINFOMGT.2013.06.002.

Mathew, S. and Perreault, C. (2016) 'Cultural history, not ecological environment, is the main determinant of human behaviour', *Proceedings of the Royal Society B: Biological Sciences*, 283(1826). doi: 10.1098/rspb.2016.0177.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., and Pattinson, M. (2017) 'Individual differences and information security awareness', *Computers in Human Behaviour,* 69, pp.151-156.

McCusker, K. and Perfusion, S. (2015) 'Research using qualitative, quantitative or mixed methods and choice based on the research ', *Perfusion,* 30(7), pp. 537–542. doi: 10.1177/0267659114559116.

Mellenbergh, G. J. (2019) 'Null hypothesis testing', *In Counteracting Methodological Errors in Behavioral Research*, pp. 179–218. doi: 10.1007/978-3-030-12272-0_12.

Menard, P., Warkentin, M., and Lowry, P. B. (2018) 'The impact of collectivism and psychological ownership on protection motivation: A cross-cultural examination ', *Computers and Security*, 75, pp.147–166 . Available at: https://www.sciencedirect.com/science/article/pii/S0167404818300488 (Accessed: 28 May 2019).

Meoli, A., Fini, R., Sobrero, M., and Wiklund, J. (2020) 'How entrepreneurial intentions influence entrepreneurial career choices: The moderating influence of social context', *Journal of Business Venturing*, 35(3), p. 105982. doi: 10.1016/j.jbusvent.2019.105982.

Merhi, M. I. and Ahluwalia, P. (2019) 'Examining the impact of deterrence factors and norms on resistance to information systems security', *Computers in Human Behavior*, 92, pp. 37–46. doi: 10.1016/j.chb.2018.10.031.

Mi, H., Huang, X., Muruganujan, A., Tang, H., Mills, C., Kang, D., and Thomas, P. D. (2017) 'Panther version 11: Expanded annotation data from gene ontology and reactome pathways, and data analysis tool enhancements', *Nucleic Acids Research,* 45(D1), pp. 183–189. doi: 10.1093/nar/gkw1138.

Mikalef, P., Pappas, I. O., Krogstie, J., and Giannakos, M. (2018) 'Big data analytics capabilities: A systematic literature review and research agenda', *Information Systems and E-Business Management*, 16(3), pp. 547–578. doi: 10.1007/s10257-017-0362-y.

Milková, E. and Ambrožová, P. (2018) 'internet use and abuse: Connection with internet addiction', *Journal on Efficiency and Responsibility in Education and Science*, 11(2), pp. 22–28. doi: 10.7160/eriesj.2018.110201.

Mishra, D., Akman, I., and Mishra, A. (2014) 'Theory of reasoned action application for green information technology acceptance', C*omputers in Human Behavio*r, 36, pp. 29–40. doi: 10.1016/j.chb.2014.03.030.

Montano, D. E. and Kasprzyk, D. (2015) 'Theory of reasoned action, theory of planned behaviour, and the integrated behavioural model', In Glanz, K., Rimer, B K. and Viswanath K. (Eds) 'Health behaviour and health education: Theory, research and practice (5th ed)', pp.95-124. San Francisco, CA: *Jossey-Bass*.

Moody, G. D., Siponen, M. and Pahnila, S. (2018) 'Toward a unified model of information security policy compliance', *MIS Quarterly: Management Information Systems*, 42(1), pp. 285–311. doi: 10.25300/MISQ/2018/13853.

Nelson, L. D., Simmons, J. and Simonsohn, U. (2018) 'Psychology's Renaissance', *Annual Review of Psychology*, 69(2018), pp. 511–545. doi: 10.1146/annurev-psych-122216.

Neneh, B. N. (2019) 'From entrepreneurial intentions to behavior: The role of anticipated regret and proactive personality', *Journal of Vocational Behavior*, 112, pp. 311–324. doi: 10.1016/J.JVB.2019.04.005.

Newhouse, W., Keith, S., Scribner, B., and Witte, G. (2017) 'National initiative for cybersecurity education (NICE) cybersecurity workforce framework ', *NIST Special Publication*, 800(2017), p.181. doi: 10.6028/NIST.SP.800-181.

Nudy, M., Chinchilli, V. M., and Foy, A. J. (2019) 'A systematic review and meta-regression analysis to examine the "Timing Hypothesis" of hormone replacement therapy on mortality, coronary heart disease and stroke', *IJC Heart & Vasculature*, 22, pp.123-131. Available at: https://www.sciencedirect.com/science/article/pii/S2352906718301957 (Accessed: 28 February 2020).

Palau-Saumell, R., Forgas-Coll, S., Sánchez-García, J., and Robres, E. (2019) 'User acceptance of mobile apps for restaurants: An expanded and extended UTAUT-2', *Sustainability*, 11(4), p. 1210. doi: 10.3390/su11041210.

Parker, A. and Brown, I. (2019) 'Skills requirements for cyber security professionals: A content analysis of job descriptions in South Africa', *Communications in Computer and Information Science*, 973, pp. 176–192. doi: 10.1007/978-3-030-11407-7_13/COVER.

Patiño, S. and Yoo, S. G. (2018) 'Study of the maturity of information security in public organizations of Ecuador', *Communications in Computer and Information Science*, 883, pp. 99–109. doi: 10.1007/978-3-030-00940-3_8.

Paul, J., Modi, A., and Patel, J. (2016) 'Predicting green product consumption using theory of planned behavior and reasoned action', *Journal of Retailing and Consumer Services*, 29, pp. 123–134. doi: 10.1016/j.jretconser.2015.11.006.

Paulus, T. and Bennett, A. (2015) 'I have a love–hate relationship with ATLAS. ti'TM: Integrating qualitative data analysis software into a graduate research methods course', *International Journal of Research & Method in Education*, 40(1), pp. 19–35. doi: 10.1080/1743727X.2015.1056137.

Peacock, D. and Irons, A. (2017) 'Gender inequalities in cybersecurity: Exploring the gender gap in opportunities and progression', *International Journal of Gender, Science and Technology*, 9(1), pp.25-44. Available at: https://scholar.archive.org/work/mumtcjx7svbwlj4zlup5s542de/access/wayback/http://genderandset.open.ac.uk/index.php/genderandset/article/viewFile/449/824 (Accessed: 28 September 2018).

Pearce, J. L. (2017) 'Toward an organizational behavior of contract laborers: Their psychological involvement and effects on employee co-workers', *Academy of Management Journal*, 36(5). https://doi.org/10.5465/256646, 36(5), pp. 1082–1096. doi: 10.5465/256646.

Pearlson, K., Saunders, C. and Galletta, D. (2016) 'Managing and using information systems: A strategic approach', Hoboken. NJ. *John Wiley & Sons*. Available at: https://www.google.com/books?hl=ar&lr=&id=kpAgCwAAQBAJ&oi=fnd&pg=PR4&dq=Managing+and+using+information+systems&ots=gK1_95KuPl&sig=XEqKwBztYWo3qhPYIzvDveVqinY (Accessed: 28 November 2017).

Peltier, T. (2016) ‘Information security policies, procedures, and standards: Guidelines for effective information security management ’, Boca Raton. *CRC Press.* Available at: https://www.google.com/books?hl=ar&lr=&id=mM_LsS-W4f4C&oi=fnd&pg=PP1&ots=WhV-p0bBik&sig=_Thsnw1cj87bftf-UsL9Nr0qEkc (Accessed: 28 January 2021).

Pencheva, D., Hallett, J. and Rashid, A. (2019) ‘Bringing cyber to school: Integrating cyber security into secondary school education’, *IEEE Security & Privacy,* 18(2), pp.68-74. Available at: https://www.cybok.org/media/downloads/IEEE_SP_Bringing_Cyber_to_School_-_Oct_19.pdf (Accessed: 28 April 2020).

Perera, S. and Samaraweera, G. (2019) ‘Impacts of social media addiction on employee performance of services sector in Sri Lanka’, *In Sri Lanka Economic Research Conference (SLERC) 2019*, p. 24 . Available at: http://www.sljer.org/images/SLFUE_2019_WUSL/proceedings/Proceedings-2019.pdf#page=47 (Accessed: 28 June 2020).

Pickering, J. B., Engen, V. and Walland, P. (2017) ‘July. The interplay between human and machine agency’, *In International Conference on Human-Computer Interaction,* pp.47-59. Springer, Cham.

Proctor, W. R. and Capstone, A. (2016) ‘Investigating the efficacy of cybersecurity awareness training programs’, (Doctoral Dissertation, *Utica College*).

Qi, J., Cao, Y., Niu, Z., Li, C., Yi, Y., and Cai, Z. (2019) ‘Effect of internet addiction on college students’ mental health level based on fuzzy neural network’, *5 th International Workshop on Education, Development and Social Sciences*. doi: 10.25236/iwedss.2019.087.

Queirós, A., Faria, D., and Almeida, F. (2017) ‘Strengths and limitations of qualitative and quantitative research methods’, *European Journal of Education Studies*, 3(9), pp.369-387. doi: 10.5281/zenodo.887089.

Rogers, R. W. (1975) ‘A protection motivation theory of fear appeals and attitude change’, *The Journal of Psychology,* 91(1), pp. 93–114. doi: 10.1080/00223980.1975.9915803.

Ruggieri, M., Hsu, T.T. and Ali, M.L. (2019) ‘Security considerations for the development of secure software systems’, *In 2019 IEEE 10th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON),* pp.1187-1193. IEEE.

Ryan, G. (2018) 'Introduction to positivism, interpretivism and critical theory', *Nurse Researcher*, 25(4), pp.41-49. Available at: https://pubmed.ncbi.nlm.nih.gov/29546962/ (Accessed: 26 October 2019).

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T. (2015) 'Information security conscious care behaviour formation in organizations', *Computers & Security*, 53, pp.65-78. doi: 10.1016/j.cose.2015.05.012.

Safa, N. S., Maple, C., Watson, T., and Von Solms, R. (2018) 'Motivation and opportunity based model to reduce information security insider threats in organisations', *Journal of Information Security and Applications*, 40, pp. 247–257. doi: 10.1016/j.jisa.2017.11.001.

Safa, N., Von Solms, R. and Furnell, S. (2016) 'Information security policy compliance model in organizations', *Computers and Security*, 56, pp. 1–13. doi: 10.1016/j.cose.2015.10.006.

Sahay, A. (2016) 'Peeling Saunder's research onion', *Research Gate*, Art, pp.1-5. Available at: https://www.researchgate.net/profile/Arunaditya-Sahay/publication/309488459_Peeling_Saunder's_Research_Onion/links/5813283508aedc7d89609ea8/Peeling-Saunders-Research-Onion.pdf (Accessed: 28 February 2017).

San Martin, A., Sinaceur, M., Madi, A., Tompson, S., Maddux, W. W., and Kitayama, S. (2018) 'Self-assertive interdependence in Arab culture', *Nature Human Behaviour*, 2(11), pp.830-837. doi: 10.1038/s41562-018-0435-z.

Schmitt, F., Bieg, H. J., Manstetten, D., Herman, M., and Stiefelhagen, R. (2016) 'Exact maximum entropy inverse optimal control for modeling human attention switching and control', *In 2016 IEEE International Conference on Systems, Man, and Cybernetics, SMC - Conference Proceedings*, pp. 2807–2813. doi: 10.1109/SMC.2016.7844664.

Scholl, M. C., Fuhrmann, F. and Scholl, L. R. (2018) 'Scientific knowledge of the human side of information security as a basis for sustainable trainings in organisational practices', *Proceedings of the 51st Hawaii International Conference on System Sciences*, pp.2235-2244.

Senyo, P. K., Addae, E. and Boateng, R. (2018) 'Cloud computing research: A review of research themes, frameworks, methods and future research directions', *International Journal of Information Management*, 38(1), pp. 128–139. doi: 10.1016/J.IJINFOMGT.2017.07.007.

Sheeran, P. and Rivis, A. (2017) 'Descriptive norms as an additional predictor in the theory of planned behavior: A meta-analysis', *In Planned Behavior: The Relationship between Human Thought and Action*, pp. 43–62. doi: 10.4324/9781315126449-4/DESCRIPTIVE-NORMS-ADDITIONAL-PREDICTOR-THEORY-PLANNED-BEHAVIOR-META-ANALYSIS-AMANDA-RIVIS-PASCHAL-SHEERAN.

Shields, P. M. (2017) 'Strategies for successfully completing a dissertation: Lowering anxiety, managing a project, creating theory and thinking about football'.

Si, H., Shi, J. G., Tang, D., Wu, G., and Lan, J. (2020) 'Understanding intention and behavior toward sustainable usage of bike sharing by extending the theory of planned behavior', *Resources, Conservation and Recycling*, 152, p. 104513. doi: 10.1016/j.resconrec.2019.104513.

Simonsohn, U., Nelson, L. and Simmons, J. (2017) 'Research methodology, design, and analysis', *Annual Review of Psychology*, 1(69).

Sinha, A. (2015) 'Cloud based mobile device security and policy enforcement', *US Patent 9*, 119,017 Google Patents . Available at: https://patents.google.com/patent/US9119017B2/en (Accessed: 28 March 2019).

Siponen, M., Mahmood, M. A., and Pahnila, S. (2014) 'Employees' adherence to information security policies: An exploratory field study', *Information & Management*, 51(2), pp.217-224. doi: 10.1016/j.im.2013.08.006.

Smith, J. A. (2015) 'Qualitative psychology: A practical guide to research methods', *Qualitative Psychology*, pp.1-312.

Snitsarenko, P., Zahorka, O., Koretskyi, A., Sarychev, Y., and Tkachenko, V. (2020) 'Expert methods application to assess information security threats impact in the military sphere', *In 2020 IEEE 15th International Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (TCSET)*, pp.41-45. IEEE. Available at: https://ieeexplore.ieee.org/abstract/document/9088703/ (Accessed: 28 November 2021).

Soomro, Z. A., Shah, M. H., and Ahmed, J. (2016) 'Information security management needs more holistic approach: A literature review', *International Journal of Information Management*, 36(2), pp.215-225. doi: 10.1016/j.ijinfomgt.2015.11.009.

Soska, K. and Christin, N. (2015) 'Measuring the longitudinal evolution of the online anonymous marketplace ecosystem', *In USENIX Security Symposium*, pp.33-48. Available at: http://www.andrew.cmu.edu/user/nicolasc/publications/SC-USENIXSec15.pdf (Accessed: 28 July 2018).

Stewart, H. and Jürjens, J. (2017) 'Information security management and the human aspect in organizations', *Information & AMP; Computer Security*, 25(5), pp. 494–534. doi: 10.1108/ICS-07-2016-0054.

Stieglitz, S., Mirbabaie, M., Ross, B., and Neuberger, C. (2018) 'Social media analytics–Challenges in topic discovery, data collection, and data preparation', *International Journal of Information Management*, 39, pp.156-168. doi: 10.1016/j.ijinfomgt.2017.12.002.

Sunarta, E. A., Sulaeman, E. S., and Budihastuti, U. R. (2019) 'Path analysis on the determinants of visual inspection acetic acid utilization on early detection of cervical cancer: Application of health belief model theory', *Journal of Health Promotion and Behavior*, 4(1), pp.32-42. doi: 10.26911/thejhpb.2019.04.01.04.

Taherdoost, A. (2022) 'Measurement and scaling techniques in research methodology; Survey/questionnaire development ', *International Journal of Academic Research in Management*, 6(1), pp.1-5. Available at: http://elvedit.com/journals/IJARM/wp-content/uploads/Measurement-and-Scaling-Techniques-in-Research-Methodology-Survey-and-Questionnaire-Development.pdf (Accessed: 28 September 2022).

Tam, K. and Jones, K. (2018) 'Maritime cyber-security policy: The scope and impact of evolving technology on international shipping', *Journal of Cyber Policy*, 3(2), pp.147-164. doi: 10.1080/23738871.2018.1513053.

Tamilmani, K., Rana, N. P., Wamba, S. F., and Dwivedi, R. (2021) 'The extended unified theory of acceptance and use of technology (UTAUT2): A systematic literature review and theory evaluation', *International Journal of Information Management*, 57, p. 102269. doi: 10.1016/J.IJINFOMGT.2020.102269.

Tang, M. and Zhang, T. (2016) 'The impacts of organisational culture on information security culture: A case study', *Information Technology and Management*, 17(2), pp.179-186.

Taylor, B. and Bean, H. (2017) 'Conceptualizing multicultural discourses of security: Introduction to the special issue', *Journal of Multicultural Discourses*, 12(4), pp.312-331. doi: 10.1080/17447143.2017.1366497.

Taylor, R. W., Caeti, T. J., Loper, D. K., Fritsch, E. J., and Liederbach, J. (2007) 'Digital crime and digital terrorism (3ed.)', Upper Saddle River, NJ: *Prentice Hall Press*. Available at: http://www.jissec.org/Contents/V3/N1/V3N1-Lapke-p64.pdf (Accessed: 28 June 2020).

Taylor, S., Bogdan, R. and DeVault, M. (2015) 'Introduction to qualitative research methods: A guidebook and resource', New York. *John Wiley & Sons*. Available at: https://www.google.com/books?hl=ar&lr=&id=pONoCgAAQBAJ&oi=fnd&pg=PR11&ots=Qiyhdy6v-P&sig=nwq6v7aGVfzkP3s82urA3Bwx8bg (Accessed: 28 June 2017).

Teh, P. L., Ahmed, P. K. and D'Arcy, J. (2015) 'What drives information security policy violations among banking employees? Insights from neutralization and social exchange theory', *Journal of Global Information Management*, 23(1), pp. 44–64. doi: 10.4018/JGIM.2015010103.

Thompson, E. C. (2017) 'Selecting security measures', *In building a HIPAA-compliant cybersecurity program*, pp.27-51. New York. *Springer Science*.

Tittle, C. R. (2018) 'Control balance: Toward a general theory of deviance', New York. *Routledge*. doi: 10.4324/9780429501326/CONTROL-BALANCE-CHARLES-TITTLE.

Topping, C. (2017) 'The role of awareness in adoption of government cyber security initiatives: A study of SMEs in the UK', (Master Dissertation, *Lulea University*). doi: 10.13140/RG.2.2.33896.08964.

Torten, R., Reaiche, C. and Boyle, S. (2018) 'The impact of security awarness on information technology professionals' behaviour', *Computers and Security*, 79, pp.68–79.

Tsai, H. Y. S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N. J., and Cotten, S. R. (2016) 'Understanding online safety behaviors: A protection motivation theory perspective', *Computers and Security*, 59, pp. 138–150. doi: 10.1016/J.COSE.2016.02.009.

Tu, C. Z., Yuan, Y., Archer, N., and Connelly, C. E. (2018) 'Strategic value alignment for information security management: A critical success factor analysis', *Information and Computer Security*, 26(2), pp. 150–170. doi: 10.1108/ICS-06-2017-0042.

Tuffour, I. (2017) 'A critical overview of interpretative phenomenological analysis: A contemporary qualitative research approach', *Journal of Healthcare Communications*, 2(4), p.52. Available at: http://repository.uwl.ac.uk/id/eprint/4082/ (Accessed: 28 April 2019).

Tunc-Aksan, A. and Akbay, S. E. (2020) ‘Smartphone addiction, fear of missing out, and perceived competence as predictors of social media addiction of adolescents’, *European Journal of Educational Research*, 8(2), pp.559-566 . Available at: https://dergipark.org.tr/en/pub/eujer/article/554248 (Accessed: 28 January 2022).

Vaioleti, T. M. (2006) ‘Talanoa research methodology: A developing position on pacific research ’, *Waikato Journal of Education*, 12. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.888.7702&rep=rep1&type=pdf (Accessed: 28 April 2017).

Valizadeh, N., Bijani, M., Hayati, D., and Fallah Haghighi, N. (2019) ‘Social-cognitive conceptualization of Iranian farmers’ water conservation behavior’, *Hydrogeology Journal*, 27(4), pp. 1131–1142. doi: 10.1007/s10040-018-01915-8.

Van Bavel, R., Rodríguez-Priego, N., Vila, J., and Briggs, P. (2019) ‘Using protection motivation theory in the design of nudges to improve online security behavior’, *International Journal of Human Computer Studies*, 123, pp. 29–39. doi: 10.1016/j.ijhcs.2018.11.003.

Vance, A., Anderson, B. B., Kirwan, C. B., and Eargle, D. (2014) ‘Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG)’, *Journal of the Association for Information Systems*, 15(10), p.2. Available at: https://core.ac.uk/download/pdf/301380653.pdf (Accessed: 28 July 2017).

Varnum, M. E. W. and Grossmann, I. (2016) ‘Pathogen prevalence is associated with cultural changes in gender equality ’, *Nature Human Behaviour*, 1(1), pp.1-4 . doi: 10.1038/s41562-016-0003.

Venkatesh, V., Thong, J. Y. L. and Xu, X. (2016) ‘Unified theory of acceptance and use of technology: A synthesis and the road ahead’, *Journal of the Association for Information Systems*, 17(5), pp.328-376 . Available at: https://scholar.archive.org/work/wyplyuuz6bacjj5mxvkzvecf3i/access/wayback/https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1743&context=jais (Accessed: 28 March 2019).

Vilceanu, M. and Johnson, K. (2018) ‘Gender and cybersecurity: Consumer awareness, experience and trust’, *Association of Marketing Theory and Practice Proceedings 2018*, 46. Available at: https://digitalcommons.georgiasouthern.edu/amtp-proceedings_2018/46 (Accessed: 28 October 2020).

Visvizi, A., Lytras, M. D. and Daniela, L. (2018) 'Chapter 19 education, innovation and the prospect of sustainable growth and development', *In The Future of Innovation and Technology in Education: Policies and Practices for Teaching and Learning Excellence*, pp. 297–305. doi: 10.1108/978-1-78756-555-520181015.

Viswanadham, N. (2018) 'Performance analysis and design of competitive business models', *International Journal of Production Research*, 56(1–2), pp. 983–999. doi: 10.1080/00207543.2017.1406171.

Wang, C. and Zhang, X. (2019) 'An empirical study of the effect of phonetic teaching on the listening ability of Marine college students—Based on SPSS Software', *In 2019 International Conference on Advanced Education, Service and Managemen*t, 3, pp.755-758. doi: 10.35532/JSSS.V3.168.

Watson, J., Lacey, D., Kerr, D., Salmon, P., and Goode, N. (2019) 'Understanding the effects of compromise and misuse of personal details on older people', *Australasian Journal of Information Systems*, 23. Avilable at: https://doi.org/10.3127/ajis.v23i0.1721

Webster, M. D. (2018) 'Philosophy of technology assumptions in educational technology leadership', *Journal of Educational Technology & Society*, 20(1), pp.25-36. Available at: https://www.researchgate.net/profile/Mark-Webster-6/publication/324454574_Philosophy_of_Technology_Assumptions_in_Educational_Technology_Leadership_Questioning_Technological_Determinism/links/5ace5c2baca2723a33437c03/Philosophy-of-Technology-Assumptions-i (Accessed: 28 January 2019).

Williams, M. D., Rana, N. P. and Dwivedi, Y. K. (2015) 'The unified theory of acceptance and use of technology (UTAUT): A literature review', *Journal of Enterprise Information Management*, 28(3), pp.443-488 . Available at: https://core.ac.uk/download/pdf/78854435.pdf (Accessed: 28 May 2017).

Wong, W. P., Tan, H. C., Tan, K. H., and Tseng, M. L. (2019) 'Human factors in information leakage: Mitigation strategies for information sharing integrity', *Industrial Management and Data Systems*, 119(6), pp. 1242–1267. doi: 10.1108/IMDS-12-2018-0546/FULL/.

Workforce in the UAE - *The Official Portal of the UAE Government* (2020). Available at: https://u.ae/en/information-and-services/jobs/uae-workforce (Accessed: 21 August 2021).

Wu, D. (2020) 'Empirical study of knowledge withholding in cyberspace: Integrating protection motivation theory and theory of reasoned behavior', *Computers in Human Behavior*, 105, p. 106229. doi: 10.1016/J.CHB.2019.106229.

Yazdanmehr, A., Wang, J. and Yang, Z. (2020) ‘Peers matter: The moderating role of social influence on information security policy compliance’, *Information Systems Journal*, 30(5), pp. 791–844. doi: 10.1111/isj.12271.

Yu, L., Li, H., He, W., Wang, F. K., and Jiao, S. (2020) ‘A meta-analysis to explore privacy cognition and information disclosure of internet users’, *International Journal of Information Management*, 51, p. 102015. doi: 10.1016/j.ijinfomgt.2019.09.011.

Zafar, H., Randolph, A. B., and Martin, N. (2017) ‘Toward a more secure HRIS: The role of HCI and unconscious behavior’, *AIS Transactions on Human-Computer Interaction*, 9(1), pp.59-74. doi: 10.17705/1thci.00089.

Zhang, T., Tao, D., Qu, X., Zhang, X., Lin, R., and Zhang, W. (2019) ‘The roles of initial trust and perceived risk in public’s acceptance of automated vehicles’, *Transportation Research Part C: Emerging Technologies*, 98, pp. 207–220. doi: 10.1016/j.trc.2018.11.018. Available at: https://www.sciencedirect.com/science/article/pii/S0968090X18308398 (Accessed: 28 December 2020).

Žukauskas, P., Vveinhardt, J. and Andriukaitienė, R. (2018) ‘Philosophy and paradigm of scientific research’, *In management culture and corporate social responsibility. London. IntechOpen*. doi: 10.5772/65483.