INTEGRATED SEM-NEURAL NETWORK APPROACH TO IMPROVE CYBERSECURITY BEHAVIOUR THROUGH CYBER HYGIENE AMONG EMPLOYEES OF SOFTWARE DEVELOPMENT SMALL AND MEDIUM-SIZED ENTERPRISES (SMES)

SHADAB KALHORO

DOCTOR OF PHILOSOPHY
(COMPUTER SCIENCE)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TUNKU ABDUL RAHMAN
MARCH 2024

INTEGRATED SEM-NEURAL NETWORK APPROACH TO IMPROVE CYBERSECURITY BEHAVIOUR THROUGH CYBER HYGIENE AMONG EMPLOYEES OF SOFTWARE DEVELOPMENT SMALL AND MEDIUM-SIZED ENTERPRISES (SMES)

By

SHADAB KALHORO

A thesis submitted to the
Faculty of Information and Communication Technology,
Universiti Tunku Abdul Rahman,
in partial fulfillment of the requirements for the degree of
Doctor of Philosophy in Computer Science
March 2024

DEDICATION

I dedicate this thesis to my parents, my father, "Al Nawaz Kalhoro," and my mother, "Mrs. Zainab Khatoon," whose enduring love, continuous encouragement, and unwavering support have guided me throughout my educational pursuit. I hope that this achievement fulfills the dreams they have envisioned for me.

I extend this dedication to my husband, "Mr. Junaid Ur Rehman Abbasi," for his patience, support, and love during this journey. I also dedicate it to my beloved daughter, Khadijah Abbasi, whose presence brings immense joy to our lives.

Each of you is the reason I persist. You are what motivates me every single day.

ABSTRACT

INTEGRATED SEM-NEURAL NETWORK APPROACH TO IMPROVE CYBERSECURITY BEHAVIOUR THROUGH CYBER HYGIENE AMONG EMPLOYEES OF SOFTWARE DEVELOPMENT SMALL AND MEDIUM-SIZED ENTERPRISES (SMES)

Shadab Kalhoro

In today's digital landscape, organizations heavily rely on information technology to enhance their services, yet this reliance also exposes them to cybersecurity threats. The Fourth Industrial Revolution (IR 4.0) has ushered in opportunities but also challenges, notably the rise of cybercrime. Cyberattacks are escalating globally, affecting diverse sectors, and placing industries at risk. According to recent statistic of Malaysia Computer Emergency Response Team (MyCERT- 2023): 62% of cyber incidents are online fraud, 8.6% is Malicious code, 14% intrusion detection, and 10 % is content related. Taking a deeper dive into the issues Cyber Security Malaysia provided a statistical report in 2023 and observed that a substantial 85.23% of the threat feeds related to Malaysia are occupied by malware concerns. Conversely, the remaining 14.77% encompasses phishing-related elements, including phishing URLs, IP addresses, and domains. Malaysia's Cyber Security Strategy 2020–2024 warns of potential losses amounting to RM 51 billion due to cybersecurity incidents, although the actual figures might be higher due to underreported incidents.

Small and Medium-sized Enterprises (SMEs), particularly in software development, are prime targets for cybercriminals. Human behaviour within these organizations often becomes a vulnerability, as employees' lack of awareness and negligence lead to security breaches. Many SMEs lack sufficient investment in cybersecurity, awareness, and robust policies, making them susceptible to attacks. To overcome this issue, good cyber hygiene behaviour and practices can assist in reducing the threats and improve cybersecurity.

This research explores the cyber hygiene behaviour of employees in Malaysian software development SMEs and providing the best cyber hygiene practices to keep safe their passwords, information, and defenses against cyberattacks.

Utilizing the Theory of Planned Behaviour (TPB), the study investigates the relationship of knowledge sharing, attitudes, subjective norms, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived value, cyber trust, personality traits, and intention concerning cyber hygiene behaviour. Hypothetical relationship is developed in this thesis to comprehensively explore cyber hygiene behaviour. As used in this thesis, TPB was supposed to give sufficient information and understanding about end users' intentions towards cyber hygiene.

The research adopts a two-step approach, combining Structural Equation Modelling (SEM) and Neural Network (NN) analysis, to analyze the factors shaping cyber hygiene behaviour.

The study's quantitative research approach targets Malaysian software development SMEs, focusing on Selangor, Kuala Lumpur, Johor, Perak, and Penang. Data were gathered from employees of SME software enterprises in these regions and analyzed using Smart-PLS and SPSS software.

Results indicate that subjective norm, perceived behavioural control, and cyber hygiene knowledge do not significantly impact cyber hygiene intention. However, threat appraisal, perceived cyber hygiene value, cyber trust, and personality traits play significant roles in shaping employees' cyber hygiene intentions, providing comprehensive insights into cyber hygiene behaviour.

This study holds critical implications for software development SMEs, emphasizing the need for enhanced knowledge, awareness and behaviour change among employees of Malaysian software development SMEs to mitigate cybersecurity risks.

This research has the global COVID-19 pandemic posed challenges in physically collecting data from respondents The limitation of this research involved the difficulty and time-consuming nature of finding suitable respondents during the online data collection process. The absence of physical presence led to challenges in tracking genuine responses, particularly as

respondents tend to overlook questionnaires on online platforms this impacting overall data collection efficiency.

ACKNOWLEDGEMENT

All gratitude to ALLAH, the ALMIGHTY the supreme authority, who possesses profound knowledge of the universe's ultimate truths and is the origin of all wisdom. He is who empowered me, showering countless blessings upon me. He is who granted me the strength, opportunity, and endurance to successfully accomplish this research work.

I express my sincere gratitude to my supervisor, Dr. Ramesh Kumar Ayyasamy, for his invaluable guidance, patience, and unwavering encouragement during my PhD journey. His advice, support and feedback helped me at all times through the process of research and writing of this thesis.

I also would like to thank Dr Abdulkarim Kanaan Jebna for his support and guidance.

I would also like to extend my thanks to my other co-supervisor, Dr. Mobashar Rehman, for his invaluable support and guidance throughout my PhD. His expertise in the field has greatly contributed to the success of my work.

I would like to express my sincere appreciation to the Faculty of Information and Communication Technology (FICT) at the Universiti Tunku Abdul Rahman (UTAR) for providing me the opportunity to pursue a PhD degree in the Department of Computer Science.

Also, I would like to thank my colleagues and friends at Universiti Tunku Abdul Rahman (UTAR) who made this a fun learning space.

I want to convey my deep appreciation to my parents (Ali Nawaz Kalhoro and Mrs. Zainab Khatoon) for their unwavering love, guidance, and support that helped me navigate through challenging moments in my life.

Most importantly, I would like to thank my husband Mr Junaid Ur Rehman Abbasi who has been there for me throughout my PhD journey providing encouragement, inspiration, and unwavering support.

I extend my gratitude to my daughter, Khadijah Abbasi, whose arrival during the period when I was working on my thesis brought immense joy and fulfillment into our lives.

I want to thank My father in law (Mr. Akram Ali Abbasi) and My mother in law (Mrs. Jamal Khatoon) for the unwavering and unconditional support they have provided to me all the times.

I express my gratitude to my elder sister Dr. Maryam Kalhoro for providing me with unfailing support, continuous encouragement and expertise have been a constant source of motivation at every step of my PhD.

I am grateful to my younger sisters (Dr. Nayab Kalhoro), (Ms. Anam Kalhoro), (Dr. Bakhtawar Kalhoro), as well as my younger brothers (Engineer Shahbaz Ali) and (Dr. Shehzad Ali) for their unwavering support, enabling me to concentrate on my career.

Words cannot express my appreciation to each one of you.

"This research was supported by the Universiti Tunku Abdul Rahman, Kampar, Malaysia. Under the UTAR Research Fund, IPSR/RMC/UTARRF/2020-C1/M04,."

APPROVAL SHEET

This thesis entitled **"INTEGRATED SEM-NEURAL NETWORK APPROACH TO IMPROVE CYBERSECURITY BEHAVIOUR THROUGH CYBER HYGIENE AMONG EMPLOYEES OF SOFTWARE DEVELOPMENT SMALL AND MEDIUM-SIZED ENTERPRISES (SMES)"** was prepared by SHADAB KALHORO and submitted as partial fulfilment of the requirement for the degree of Doctor of Philosophy (Computer Science) at Universiti Tunku Abdul Rahman.

Approved by

(Dr. Ramesh Kumar Ayyasamy) Date: 04/03/2024
Main Supervisor
Faculty of Information and Communication Technology
Universiti Tunku Abdul Rahman

Date: 05/03/2024

(Dr Abdulkarim Kanaan Jebna)
Co- Supervisor
Faculty of Information and Communication Technology
Universiti Tunku Abdul Rahman

(Dr. Mobashar Rehman) Date: 05/03/2024
External Co-Supervisor)
Department of Management Leadership & Organisations
Middlesex University London.

SUBMISSION SHEET

FACULTY OF IFORMATION AND COMMUNICATION

TECHNOLOGY

UNIVERSITI TUNKU ABDUL RAHMAN

Dated: 04 March 2024

SUBMISSION OF THESIS

It is hereby certified that ***SHADAB KALHORO*** **ID No:** ***20ACD06698*** has completed this dissertation entitled **"INTEGRATED SEM-NEURAL NETWORK APPROACH TO IMPROVE CYBERSECURITY BEHAVIOUR THROUGH CYBER HYGIENE AMONG EMPLOYEES OF SOFTWARE DEVELOPMENT SMALL AND MEDIUM SIZED ENTERPRISES (SMES)"** under the supervision of **Dr. Ramesh Kumar Ayyasamy** (Main Supervisor) from the Department of Information Systems, Faculty of Information and Communication Technology**, Dr Abdulkarim Kanaan Jebna** (Co-Supervisor) Department of Information Systems, Faculty of Information and Communication Technology. **Dr. Mobashar Rehman** (External Co-Supervisor) Business School, Middlesex University London.

I understand that the University will upload softcopy of my dissertation in PDF format into UTAR Institutional Repository, which may be made accessible to UTAR community and public.

Yours truly,

_____

(SHADAB KALHORO)

DECLARATION

I hereby declare that the thesis is based on my original work except for the quotations and citations which have been duly acknowledged. I also declare that it has not been previously or concurrently submitted for any other degree at UTAR or other institutions.

_____

Name: Shadab Kalhoro

Student ID: 20ACD06698

Date: 04 March 2024

TABLE OF CONTENTS

LIST OF FIGURES

Figures **Page**

LIST OF TABLES

Table **Page**

LIST OF ABBREVIATIONS

ANN	Artificial Neural Networks
AT	Attitude
COVID-19	Coronavirus disease-2019
GDP	Gross Domestic Product
IT	Information Technologies
INT	Intention
MCMC	Malaysian Communications and Multimedia Commission
MSME	Malaysian Small and Medium Size enterprise
MyCERT	Malaysia Computer Emergency Response Team
SEM	Structural Equation Modeling
SME	Small and Medium Size enterprise
SN	Subjective Norms
SLR	systematic literature review
SPSS	Statistical Package for Social Science
PLS-SEM	Partial Least Squares Structural Equation Modeling
TRA	Theory of Reasoned Action
TPB	Theory of Planned Behaviour
PBC	Perceived Behavioural Control
RMSE	Root Mean Square Error

CHAPTER ONE

INTRODUCTION

1.1.Overview

Chapter one offers an overview of this study, outlining background, addressing problem statement, identifying research gaps, formulating research questions and objectives, and highlighting the study's significance. This chapter sets out the research context for understanding cyber hygiene, cyber hygiene behaviour, and the platforms used for cyber hygiene behaviour. It starts by examining how cyber hygiene affects employees working in software development SMEs in Malaysia. The factors influencing the cyber hygiene behaviour for employees of software development SMEs in Malaysia were investigated using the model of theory of planned behaviour TPB. In addition, thesis investigates the relation among the factors namely the cyber hygiene attitude, subjective norm, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits. Cyber hygiene intention is the mediator whereas cyber hygiene behaviour is the dependent variable. The research scope is thoroughly examined to establish the boundaries of the research. Lastly, this chapter concludes with highlighting the importance of investigating employees cyber hygiene behaviour in SMEs and providing a comprehensive summary of the rest of the thesis.

1.2.Research Background

As technology continues to advance, it has develop an integral aspect of everyday life, with a growing number of individuals utilizing mobile devices

for daily activities such as shopping, banking, and entertainment. Effective information sharing through communication technology is used to handle all of these services. Organizations are utilizing communication technology increasingly to boost productivity and provide customers with quick and efficient services [1] [2].

The crimes related to technology are growing in conjunction with technology's advancement. Information theft is done through a variety of techniques. When computer networks are exploited to conduct criminal activities, such activities are called cybercrime [3].

Both commercial and governmental organizations now face new information security concerns due to the complexity and expansion of technology settings [4]. These difficulties are frequently linked to an increased risk of security breaches. Yossuf et al. (2022) stated that information systems, as well as data, are crucial resources in the majority of contemporary organizations. These resources are utilized in operational, managerial, and executive decision-making, creating new business opportunities across several industries [5].

Malaysia undoubtedly has many societal challenges, which is consistent with the rise in internet usage. The Malaysian government is presently facing serious risks from cybercrime [6]. People must be aware to protect their private information to tackle the problem of cybercrime in Malaysia.

The rapid digital transformation globally has forced businesses, including SMEs, to adapt their technology usage rapidly and significantly. Despite being the backbone of economies worldwide, small, and medium-sized firms (SMEs) also suffer from far tighter resource limits while dealing with similar cyber

threats. In accordance with the report of Department of Statistics Malaysia's (DOSM 2021), SMEs accounted for 38.2 percent of Malaysia's GDP in 2020, generating a value-added of RM 512.8 billion. However, by 2024, Malaysia expects digital SMEs to significantly contribute between RM 79 billion and RM 99 billion to the country's GDP [7]. The changes have, however, increased cybercrime threats and posed a danger to the internal security of almost all firms. Organizations are depending more and more on communication technology. Hence the data shared must be protected from misuse. Regarding cybersecurity risks and assaults in the past, huge businesses were the main targets since they offered the greatest financial benefits for attackers [8]. Inadequate monitoring and security procedures against unauthorized modification affect most local enterprises, leading to unauthorized exposure. SMEs face more development challenges and worries related to cybersecurity than bigger organizations since they lack the IT expertise and resources to establish the cybersecurity system using technical instruments.

Cybercrime is the fastest-growing form of illegal activity in both the U.S. and globally [9]. Almost every businesses altered their work processes during the COVID-19 worldwide pandemic, most companies started allowing employees to work from home, and about half of all small enterprises experienced cyberattacks [10]. Based on information from the world economic forum, it is projected that the losses from cybercrime over the next five years, increasing from $8.44 trillion in 2022, surpassing to about $11 trillion in 2023, and possibly reaching around $24 trillion by 2027 [11]. Hacking has accounted for over 4 billion stolen records including financial data, login passwords, and

personal data during the past ten years with the majority from larger organizations [12].

In 2023, author Neri stated that larger organizations have embraced frameworks such as the International Organization for Standardization (ISO), Control Objectives for Information and Related Technologies (COBIT), National Institute of Standards and Technology (NIST), and similar ones in response to the digital landscape [13]. However, SMEs often struggle with the complexity and cost associated with adopting and implementing these frameworks.

The World Economic Forum's Global Risk Reports 2021 ranks cybersecurity failure as the eighth most important global risk. Myanmar has lowest cybersecurity ranking, whereas Denmark leads in cyber safety, giving to the Global Cyber Safety Index 2020 [1], [14]. In 2020, email phishing and pharming constituted approximately 33% of all reported cybercrimes, as indicated in the National Cybersecurity Index [15]. These risks are frequently reported by US customers online. Extortion, through methods like ransomware, ranks as the third most prevalent cybercrime, involving accessing data and devices before demanding payment in Bitcoin or other forms.

Based on the 2023 research conducted by the Statista Department, Malaysia experienced over 28 thousand recorded cyberattacks in 2022. Rendering to data provided by the Royal Malaysian Police (PDRM) in 2021,[16] there were 14,229 reported cybercrime incidents, marking an increase from 11,875 in 2019. These incidents led to total losses amounting to RM 413 million. Many SMEs in Malaysia have become targets due to their lack of expertise in implementing adequate cybersecurity protocols [1]. Giving to the Malaysia Computer

Emergency Response Team (MyCERT) [2] the number of cyber incidents reported to Cyber999 increased from 6,512 in 2020 to 10,016 in 2021. These incidents primarily involved fraud, infiltration attempts, and malicious software.

In addition, almost 85% of Malaysian SMEs have experienced several cyberattacks [17]. Adleena Huzaizi in 2021, estimates Malaysia's potential economic loss was US$12.2 billion. from cyberattack [18].

Human behaviour is frequently the cause for the majority of cybersecurity vulnerabilities. The study also found that in Malaysia, 48% of online problems were the result of human mistakes, 40% of firms reported client file leaks, and ransomware assaults and phishing emails harmed 35%. Human behaviour is seen as the weakest link in information systems, making it more crucial than ever to understand the interactions between information systems and humans [19]. Effective information security goes beyond technological solutions since human elements and an organization's security culture must also be considered [20]. The most popular kind of cyberattack is social engineering scam because it relies on identifying and exploiting a potential victim's human flaws. Malaysia Cyber Security Strategy 2020-2024 revealed that Malaysia could lose RM 51 billion because of cybersecurity occurrences [21].

A logging and alerting system is often used by SMEs, but employees awareness training is not given as much priority [22]. According to a recent survey lack of employee awareness continues to be the leading cause of security mishaps. Employee awareness is lacking, which leads to cyberattacks against Malaysian SME's engaged in software development [23]. In the meanwhile, Fikry et al. (2023) did research and found that the main reason because of which

user were the target of fraud and social media hacks was a lack of cyber hygiene practices [6]. While failing to implement effective security procedures in a company might lead to financial losses and privacy violations.

One way to enhance this security process is to increase training and awareness, which covers the security measures, so that people may employ to secure information and raise their knowledge of possible risks. Businesses experience cyberattack events more frequently despite when their employees have received security training and have access to various security policies, processes, and technology solutions [24]. Additionally, this training has to be expanded from corporate settings to personal settings and from PCs and networks to the pervasive mobile phone. Organizations should increase their resistance to cyberattacks to ensure their operations can improve swiftly. This is necessary because they must be capable of responding quickly and effectively when a cyberattack happens [25].

According to the "Malaysian Communications and Multimedia Commission" (MCMC) report from 2020, the internet usage is increasing in Malaysia [26]. The investigations demonstrated the urgent need for attention to the cyber hygiene behaviour among employees of Malaysian SMEs engaged in software development. Although many studies have been done on cyber hygiene behaviour, there is still a requirement for more investigation to completely understand the variables that influence cyber hygiene behaviour among employees of SMEs that specialize in software development [27], [28]. To address the challenges, there is a requirement to examine the variables that affect cyber hygiene behaviour among employees of software development SMEs. Therefore, the study aims is to conduct comprehensive inquiry about

cyber hygiene behaviour and benefit employees of software development SMEs by providing good cyber hygiene practices to overcome the recognized cybersecurity issues and challenges.

In summary, understanding and addressing cyber hygiene and related behaviours among software development SMEs in Malaysia is essential for combating the complex challenges posed by cyber threats. Enhancing cyber hygiene practices among employees can strengthen SMEs' ability to protect their operations and contribute to the complete resilience of the digital ecosystem.

Exploring cyber hygiene and related behaviors is crucial for understanding the impact of technology on organizations, especially SMEs, as they face unique challenges in cybersecurity due to limited resources. Despite their substantial role in the economy, SMEs often lack the essential infrastructure to effectively combat cyber risks, making them susceptible to cybercriminals. The rising instances of cyberattacks, such as phishing scams and ransomware, highlight the urgent need for improved cyber hygiene practices among SMEs, particularly those involved in software development.

This study aims to address gaps in existing literature by investigating the factors influencing cyber hygiene behavior among employees of software development SMEs in Malaysia. By conducting a thorough examination of cyber hygiene behavior, the study seeks to offer valuable insights and practical recommendations to assist SMEs in effectively mitigating cybersecurity risks.

1.3.Cybersecurity Situation for SMEs

Cyber threats do not discriminate based on the size of organizations, indicating that SMEs and large both corporations are susceptible to similar threats [29]. Larger enterprises often have the financial and human resources to implement controls, even though they have more personnel and devices, which increases their attack surface. The specialized cybersecurity employees at larger businesses often have suitable levels of education [30]. SMEs make fewer investments in cybersecurity, but when it comes to the expenses related to successful cyberattacks, they bear a greater amount of cost than large companies [31]. Cybersecurity challenges faced by small businesses need to be addressed as a matter of national security.

Since SMEs are supposed to be fundamentally more susceptible, they are being targeted by cyber threats more frequently [32]. SMEs are often the victims of attacks by new and inexperienced cybercriminals [33]. The authors in [34] stated that, SMEs who planned their IT security under the assumption that their networks and information were already secure are to blame for this inadequate security. Author from [35] stated in his study that every firm, regardless of size, industry, or sector, was reportedly a victim of the attacks. Based on academic and industry reports, SMEs commonly encounter various types of cyberattacks, including social engineering (like phishing), hacking (involving stolen credentials and data theft), malware (such as ransomware), misuse (such as malicious insider activities), web-based attacks, and supply chain attacks in e-commerce. [36].

1.4.Impact of cyber threats on SMEs

The challenges posed by cyber threats will have a wide range of effects on SMEs. Landscape of cyber threats gets more complicated as technology dependence is important for the business to continue and remain applicable now and the future. Though, SMEs may quickly become targets of incursion attacks, data breaches, and ransomware attacks if they do not practice for appropriate protection and are not aware of cyberattacks.

Sukumar et al. (2023) stated that there are several different sorts of cybercriminal operations that target SMEs. For instance, the competing company may gain unauthorized access to an organization's network in order to harm the system and leak crucial documents that might result in data breaches and steal the intellectual property (IP) [37].

One of the immediate outcome of cyberattacks targeting SMEs is their financial consequences. Cybercriminals can inflict substantial financial harm through diverse methods, such as ransom demands, theft of sensitive financial information, and the expenses linked to investigating and rectifying the breach. Furthermore, cyberattacks can lead to operational disruptions that impede the day-to-day functioning of SMEs, resulting in downtime, diminished productivity, and missed business prospects [38].

The effects of a cyberattack go beyond financial and operational setbacks; they also stain the reputation of SMEs. Clients and collaborators, who previously trusted the SME with their information and transactions, may doubt its capability to protect sensitive data. This loss of trust might prompt clients to switch to other providers, collaborators to reconsider their partnerships, and

inflict lasting damage on the SME's brand image, requiring significant time and resources to repair [39].

Cybercriminals frequently deploy malware threats to harm SMEs. In the NIST publication guide, Barker et al. (2022), stated that the aim of malware attacks is to compromise an organization's confidentiality, integrity, and availability, resulting in operational harm, financial losses, and reputational damage [40].

Almansoori et al. (2023), explained their report on a data breach that cybercriminals use malware attacks to launch sophisticated attacks [41]. Ransomware is a severe risk might temporarily or permanently shut down a firm in which in which a system or program fails to operate. Whether a firm is a large multinational or an SME, these cyber threats can consequence in substantial losses.

1.5.Security Risks posed by SME Employees

Different organizations are impacted by the threats to cybersecurity caused by human error. Kobis (2020), stated that the human factor is the primary source of sensitive information [42]. Human factors are crucial variables that impact the information security practices of SMEs and are frequently undervalued and ignored [43], [44]. Many different kinds of employees mistakes ultimately allow unauthorized access to confidential data and other corporate assets, leading to security breaches. Errors made by employees put businesses at risk. Employees could utilize storage devices infected by a virus [45]. Workers could unintentionally click on unfamiliar links on a website or click links that go to websites that collect sensitive data. Data breaches are increasingly happening due to unauthorized disclosure of personal data [46].

Another scenario occurs when individuals open malicious attachments in fake emails out of curiosity, carelessness, or lack of awareness. These files are crafted to automatically install themselves upon opening. Certain attitudes, behaviours, and actions that encourage unprotected connections impact employee mistakes. Certain user attitudes contribute to recurring mistakes, such as when a user says, It won't happen to me. [47]. These careless behaviours provide opportunistic attackers access to valuable, sensitive corporate data and resources. To invade privacy, criminals hijack secure sessions [48]. Cybercriminals compromise data security standards such as data confidentiality, availability, and integrity when they seize control. Authorized users have access to data at all times. Any negligent user behaviour could potentially expose the system and its data to attackers, compromising the principle and leading to poor service and delayed decision-making [49].

Furthermore, users may inadvertently embed malware into commonly used programs. The malicious installation package is often available on websites designed to deceive inexperienced users. Consequently, users unknowingly download and install software from untrustworthy sources. Other users act as an interface for criminals by using their credentials carelessly. Such behaviour may be caused by a poor capability to memorize the suitable characters for password requirements, a lack of personnel, or workers who are overloaded with work demand. A lack of assistance or instruction can occasionally worsen inappropriate user behaviour [42].

Human-related factors such as social engineering, malware, phishing, worms, and spyware have an impact on cybersecurity principles [50]. Alexei and Alexei (2023)’s study, a harmful programs, risks associated with spoofing,

and access to unauthorized data might result in data theft. Given the foregoing, employee behaviour may impact the fundamentals of information security, threatening [51].

Human behavior plays an important part in cybersecurity, as the actions of employees can significantly impact an organization's security measures. It is imperative for SMEs to assign resources towards cybersecurity training initiatives aimed at equipping staff with up-to-date knowledge on emerging threats, best practices for online safety, and familiarity with the organization's specific cybersecurity protocols [52]. By actively involving employees in discussions regarding cybersecurity where they feel encouraged to report any suspicious activities or incidents, SMEs can introduce a sense of responsibility among their workforce towards safeguarding the organization's security [53]. These training programs empower employees to identify and report potential threats promptly, thereby enhancing the overall cybersecurity resilience of the organization.

1.6.Research Problem

In today's cybersecurity landscape, there is a continuous cycle of individuals enhancing their security measures and receiving training to defend against harmful attacks, while attackers constantly seek new methods to penetrate networks. Growing digital technologies are giving rise to new enterprises and opening up huge markets for SMEs, but they are also making those firms more susceptible to cybersecurity attacks. Furthermore, Rajaretnam, (2020) emphasized the issue of privacy and cybersecurity risk, and the author said that data security is essential for companies in the digital era since it significantly influences businesses, customer confidence, and trust [54]. When everything is

interconnected, possibility of data hacking and alteration for malicious purposes can have significant financial repercussions. consequences. According to study released by Microsoft in collaboration with (Microsoft Malaysia News Centre, 2021), the potential cost of economic harm from cybersecurity incidents in Malaysia might reach US$12.2 billion [55].

Due to a lack of awareness, SMEs have grown increasingly appealing and susceptible to social engineering attacks in recent years. Almost two-thirds of SMEs experienced cyberattacks this year [27]. Social engineering attacks were used by hackers against businesses, notably SMEs, during the Covid-19 outbreak. It is challenging to distinguish between social engineering attacks, though, as they tend to vary from one another. A successful attack might result in a system breach, generating significant losses for SMEs [56].

Because of their restricted resources and lack of awareness about cyber threats, the majority of SMEs are still inadequately equipped to safeguard their digital systems. Many SME firms struggle to recover after an attack [57]. Like most organizations, SME lack of necessary planning, skill, and experience for various potential situations. In the annual global study on "Cyber Resilient Organizations" conducted by IBM and the Ponemon Institute [58], it was discovered that 77% of the 3600 security and IT professionals worldwide lacked a cybersecurity incident response plan, rendering them unprepared to effectively manage such incidents.

Despite increased investment by companies in security awareness training programs, as well as various policies, procedures, and technological solutions, incidents continue to happen more commonly in organizations that offer such

training [27]. Although most employees assert that they are familiar with the company's standards and practices, this is insufficient.

A recent investigation in Malaysia revealed that nearly half of all cyber incidents, totaling 48%, resulted from human error, with consumer data being the most commonly compromised information. Additionally, 40% of businesses reported incidents involving the leakage of customer files, while 35% fell victim to ransomware attacks and malicious email phishing links [59].

Additionally, cyberattacks are growing more complex as cybercriminals exhibit profound technical proficiency and novel specializations in using technology and social tools [56]. Several studies conducted within the Malaysian context indicate that software development enterprises among SMEs in Malaysia encounter significant challenges [59]. According to information from Cyber Security Malaysia's Computer Emergency Response Team, there have been 178 data breaches so far, an increase of about 200% from the 63 attacks reported the previous year. Although many occurrences were unreported, a cybersecurity expert thinks the actual number is likely far higher [18].

Thus, many individuals believe that the main cause of these mishaps is because they do not understand how to safeguard their online system or the consequences of protection [60]. To effectively combat these cyberattacks, appropriate preparation and strategy are therefore essential. Malaysian SMEs must reevaluate their cybersecurity procedures and develop plans to secure their information and workers against the risks of cybersecurity breaches, cybercrimes, and cyberterrorism to maintain some level of data security. It is

essential to conduct a study on the employees of software development SMEs to address this issue.

1.7.Research Gap

Mutalib et al. (2021), in their research work noted that infected end users' computers, particularly home users, and SME organizations, readily vulnerable due to lack of cybersecurity knowledge and cyber defenses [58]. Recent information from the Malaysia SME Cyber Preparedness Report [61] indicated that 84% of Malaysian SMEs had encountered cyber incidents. According to the report, ransomware attacks affected 35% of the event. Every year, the rising trend in new malware demonstrates how serious and concerning this issue is, necessitating a plan to reduce and eliminate these online threats.

According to reports, many SMEs are hesitant to notify law enforcement authorities about incidences of cybercrime for various reasons, including their poor public image or desire to avoid regulatory repercussions in some nations [41]. Since law enforcement may collaborate with both domestic and international counterparts to halt these crimes, it is crucial to inform SMEs that reporting crimes to them can assist in minimizing the number of cyberattacks that SMEs experience [62]. Small and medium-sized businesses (SMEs) can better defend themselves from attacks by quickly identifying and responding to such cyberattacks [63].

In recent years, the issue of cyberattacks against SMEs engaged in software development has gained more attention. Nevertheless, a significant research gap exists in investigating cyber hygiene practices among the employees of Malaysian software development SMEs [64], [65].

It is widely acknowledged that SMEs contribute positively to the world economy, but it is also well acknowledged that they are more susceptible to cyberattacks than large corporations. Weak corporate cybersecurity might contribute to increased attacks on SMEs [66]. Small firms keep records of information such as client names, phone numbers, addresses, and credit card numbers [41]. Due to all of this information, fraudsters greatly value small firms. Cybersecurity vulnerabilities have been linked to behaviour by humans [67]. Cyberattacks against SME software development occur due to lack of employees' knowledge [68].

Meanwhile, Hadlington et al. (2021), performed the study and found that users were vulnerable to fraud and social media attacks because of a lack of cyber hygiene practices [69]. The author advises software development SMEs to focus on security awareness, which might help their employees and organizations in recognizing the risks. The authors Kalhoro et al. (2021), have demonstrated that even trained users with high-security awareness and training behave similarly to unskilled users. Therefore, information awareness and a change in employee attitude are required for successful cybersecurity practices [70]. Kalhoro et al. (2021) also highlighted that people need more information to modify their behaviour and enhance cybersecurity. It was also noted that 81% of participants had received cybersecurity hygiene training. However, neither their behaviour nor their understanding was said to have improved [70]. According to the researchers ' findings, it should offer all users the most efficient training [62] .

On the contrary, another study show that employee ignorance is frequently used as an entrance point for cybercrime [47]. According to Tamjidyamcholo et

al. (2013), cyberattacks may be developed both within and outside of an organization, making workers the most vulnerable threat. The majority of cyberattacks are caused by human acts, which have the potential to expose organizations [71]. Employee negligence is associated with decisions that degrade an organization's information security [34].

Meanwhile, Alharbi et al. (2021) revealed that professional personnel with better cybersecurity expertise tend to practice bad cyber hygiene, particularly when losing an organization's sensitive data [28]. Abu-Amara et al. (2021), claims that knowledge may be a double-edged sword since it allows workers to influence an organization's cybersecurity policy or even participate in fraudulent cybersecurity activity [72]. Despite organizational personnel's knowledge regarding cybersecurity, no action is made to practice good cyber hygiene [56]. Establishing rewards and penalties is necessary to ensure employees practice proper cyber hygiene [25].

Considering this, the current body of study has shown a research gap, requiring additional research based on a strong theoretical framework and sample that can be generalized to demonstrate the existing research gap better.

Researchers have looked at cyber hygiene behaviour from a variety of perspectives, focusing on knowledge sharing, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, personality traits, and other TBP factors i.e., attitude, subjective norm, perceived behavioural control. In the present corpus of research, no single study has focused on all of the relevant components linked with cyber hygiene behaviours while also having a strong theoretical foundation. Additionally, it's crucial to highlight that none of the studies employed the Structural Equation Modeling-Artificial Neural

Network Approach (SEM-ANN) technique concerning cyber hygiene behaviour. Hence, there is a practical need to enhance awareness about cyber hygiene and change the behaviour of employees in Malaysian software development SMEs.

1.8.Research Objectives

Main research question of this study is: To examine cyber hygiene behaviour for employees of Malaysian software development SMEs, integrating the theory of planned behaviour [73]. Cyber hygiene behaviour among employees of software development SMEs is impacted by factors such as knowledge sharing, cyber hygiene attitude, subjective norm, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits. The following objectives are outlined to accomplish the purpose of this research:

RO1. To identify the factors impacting cybersecurity behaviour among employees of software development SMEs.

RO2. To determine the impact of individual factors such as knowledge sharing, cyber hygiene attitude, subjective norm, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits on cyber hygiene intention among employees of software development SMEs.

RO3. To examine the SEM-Neural network approach in improving cybersecurity behaviour through cyber hygiene among the employees of software development SMEs.

1.9.Research Questions

The following are the derived research questions from the review of literature:

RQ1. What factors influence cybersecurity behaviour among employees in software development SMEs?

RQ2. How do individual factors such as knowledge sharing, cyber hygiene attitude, subjective norm, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits influence the intention to practice cyber hygiene among employees in software development SMEs?

RQ3. How does the SEM-Neural network approach enhance cybersecurity behaviour and promote cyber hygiene among employees in software development SMEs?

1.10. Research Hypotheses

Following hypotheses have been formulated as follows to address the research questions:

H1: Knowledge sharing positively influences attitude to perform cyber hygiene intention.

H2: Cyber hygiene attitude will have a positive impact on cyber hygiene intention.

H3: Cyber hygiene subjective norms will have positive influences on cyber hygiene intention.

H4: Cyber hygiene perceived behavioural control will have a positive influence on cyber hygiene intention.

H5: Threat Appraisal will have a positive influence on cyber hygiene intention.

H6: Cyber hygiene knowledge will have a positive influence towards cyber hygiene intention.

H7: Perceived cyber hygiene value will have a positive impact on the cyber hygiene intention.

H8: Cyber trust will have a positive influence on cyber hygiene intention.

H9: Personality traits will have a positive influence on the cyber hygiene intention.

H10: Cyber hygiene intention has a positive and substantial impact on cyber hygiene behaviour.

1.11. Research Scope

Organizations become completely integrated with various types of ICTs as technology becomes more prevalent. The dependance on technology has also increased, this has given rise to issues such as cyberattacks. Employee negligence may cost and harm an organization in terms of money as well as the loss of critical knowledge [74]. Thus, it is necessary to detect employee cybersecurity behaviour because in many cases cyberattacks occur due to a lack of awareness among employees.

To comprehensively explore the cyber hygiene behaviour, the hypothetical relationships developed for this research. To gain deeper insights in cyber hygiene behaviour a quantitative research approach is used for software development SMEs using employees as respondents. Given the dispersed distribution of questionnaire, it is necessary to establish a representative population [75]. The study was concerned with SMEs located in five states of

Malaysia, namely Selangor, Kuala Lumpur, Johor, Perak, Penang. Consequently, data was collected from employees of software development SMEs located in these five Malaysian states. The justification behind choosing these states is that these are considered a business hub in Malaysia with a great part of SMEs are situated [76]. According to the SME Corp Malaysia (2021), about 61 percent or 1226494 of SMEs are in these five states [77]. These states possess modern facilities, including high-speed internet connections and sophisticated telecommunication systems, fostering notable advancements where the largest concentrations of knowledge workers and learning specialists thrive [76]. The study's approach seeks to offer a complete knowledge on the employee's cyber hygiene behaviour.

As a result, the focus of this research is centered on cyber hygiene behaviour among employees of Malaysian software development SMEs.

1.12. Theoretical Significance of the Study

This research offering a conceptual model based on Theory of Planned behaviour (TPB) [73], [78] to predict cyber hygiene behaviour among employees of software development SMEs in Malaysia.

In addition to employees, software development SMEs, and the Malaysian government will know what to consider when developing a strategy to prevent cyberattacks. This study looks into the elements that motivate employees to practice cyber hygiene. Unlike the conventional method of focusing on only a few variables, this research attempts to bridge the gap by analyzing a wide range of variables including knowledge sharing, cyber hygiene attitude, subjective norm, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits.

As a result, this research can help academics, policymakers, employees, governments, and software companies understand the possible factors that push software development SMEs to participate in cyber hygiene behaviour.

In this research, a self-administered survey is utilized for quantitative research. The study employs a comprehensive two-step analytical approach, incorporating both structural equation modeling (SEM) in the initial phase and artificial neural network (ANN) analysis in the subsequent phase. This two-step multi-analytical method enhances accuracy, exploring both linear and nonlinear connections among variables. The outcomes provide valuable insights into the factors influencing cyber hygiene behaviours among employees in software development SMEs, aiding researchers in gaining a deeper understanding of these behaviours.

1.13. Practical Significance of the Study

The practical significance is centered on actual consequences on the cybersecurity landscape of SMEs as well as the entire digital ecosystem. The outcomes of the research may be utilized to establish cyber hygiene practices and programs aimed at minimizing cyberattack incidences in Malaysian software development SMEs. Here are some of the most important characteristics of practical significance:

1. **Strengthening Cybersecurity Practices**

The practical significance of the study can help SMEs to establish more effective cybersecurity measures, reduce vulnerabilities, and mitigate possible risk of cyber threats.

2. **Risk Mitigation and Threat Prevention**

The research can assist SMEs in dealing with possible hazards and risks proactively. Practical advice based on the study's results can enable SMEs to adopt preventive actions, lowering the chance of cyber events that can disrupt the corporate operations.

3. Employee Training and Awareness

SMEs should provide employee training programs and awareness campaigns to address particular weaknesses emphasized in the research. SMEs may create training materials that resonate with employees and improve their knowledge of cybersecurity best practices. Furthermore, this study helps workers understand the significance of their activities in protecting security, which may lead to a collaborative effort to secure their digital assets and information.

4. Policy and Regulatory Alignment

This study can help policymakers in developing the rules and regulations that consider the particular demands and problems that Malaysian software development SMEs encounter.

The practical significance of studying the cybersecurity behaviour among the employees of software development SMEs in Malaysia lies in its potential to strengthen cyber hygiene practices. Ultimately, the study's outcomes can lead to real-world improvements in cybersecurity and digital resilience within SMEs.

1.14. Sustainable Development Goals

Cybersecurity behaviour in software development SMEs in Malaysia is closely linked to several Sustainable Development Goals (SDGs) due to its impact on economic growth, technological advancement, and the establishment of secure digital environments. By determining the factors that contribute to

cyber hygiene behaviour, the research seeks to increase awareness, reduce cyberattacks, and create a safer online environment for SMEs. Here's an explanation of how cybersecurity behaviour aligns with specific SDGs.

SDG - 8: Decent Work and Economic Growth

Cybersecurity practices may aid in creating a secure place of employment for SME employees while also protecting them from cyber threats; this helps economic growth, decent work opportunities, and the development of resilient business ecosystems, as specified in SDG 8.

SDG - 9: Industry, innovation, and infrastructure

Effective cybersecurity practices may assist in protecting against cyberattacks and avoid data breaches, which can result in financial losses and reputational harm. This, in turn, can help to expand digital industries and inventions. Sustainable development goal (SDG 9) emphasizes a robust infrastructure, industrialization, innovation, and software development. SMEs contribute to economic diversification and innovation by securing their digital assets.

SDG - 16: Peace, Justice, and strong institution

Cybersecurity behaviour strengthens institutions by protecting them from cyberattacks, data breaches, and problems that threaten stability. Software development SMEs that focus on cybersecurity help to construct effective, responsible, and transparent institutions, as proposed in SDG 16.

Cybersecurity behaviour in software development SMEs in Malaysia are integrally tied to various SDGs. By prioritizing cybersecurity practices, these SMEs contribute to economic growth, innovation, the building of safe digital

environments, and the attainment of the SDGs' many sustainable development goals.

1.15. Operational Definitions of the Variables

The variables which are independent for this research study are knowledge sharing, cyber hygiene attitude, subjective norm, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits, whereas mediating variable is cyber hygiene intention, whereas variable cyber hygiene behaviour is the dependent. Table 1.1. presents the variables definitions used for this investigation.

Table 1. 1: Definitions of the Variables

	Variables	Description	Ref
1	Knowledge Sharing	The practice of exchanging information, ideas, expertise, and experiences among individuals, groups, or organizations to improve collective understanding and decision-making is referred to as knowledge sharing. It is the voluntary sharing of knowledge, ideas, and best practices within a community or network to enable learning, cooperation, and innovation.	[79]
2	Attitude	Attitude refers to both positive as well as negative feelings about carrying out a specific behaviour. It is based on people's ideas, consequences, and concerns about a certain behaviour.	[78]
3	Subjective Norm	Subjective norms refer to what others (relatives, close friends, coworkers, or business partners) believe about an	[78]

		individual when they are performing a specific task.	
4	Perceived Behavioural Control	PBC refers to the perceived comfort or difficulty of managing and displaying an attitude towards specific behaviours and demands to do behaviour.	[78]
5	Threat Appraisal	The cognitive process through which individuals or organizations evaluate and analyze the seriousness, probability, and possible effect of a given threat or risk is referred to as threat appraisal.	[80]
6	Cyber Hygiene Knowledge	Knowledge refers to the attention put on what an employee understands. Cyber hygiene knowledge is centered on an employee's awareness of how to respond in particular scenarios.	[81]
7	Perceived cyber hygiene value	The subjective evaluation of an individual's or organization's relevance and advantages associated with practicing effective cyber hygiene is referred to as perceived cyber hygiene value.	[82]
8	Cyber trust	Cyber trust refers to the confidence in the reliability, dependability, rationality, and effectiveness of a person or entity in the digital realm.	[83]
9	Personality Traits	Positive and intrinsic motivation to the service based on past practices and the company's track record of service quality.	[84]

10	Cyber hygiene intention	A deliberate and planned desire of an individual or organization to engage in practices that promote good cyber hygiene is referred to as cyber hygiene intention. It entails making a conscious decision to adopt cybersecurity behaviours and processes that help in the prevention of cyberattacks, the safeguarding of sensitive information, and the maintenance of a secure digital environment.	[73]
11	Cyber hygiene behaviour	The collection of proactive and preventative acts, practices, and habits that individuals and organizations take to maintain a secure and safe digital environment is referred to as cyber hygiene behaviour. These actions are intended to safeguard sensitive information, digital assets, and systems from cyber threats, attacks, and vulnerabilities.	[85]

1.16. Summary

The first chapter presents an overview of the study, which attempts to determine the factors that impact cyber hygiene behaviour among employees of Malaysian software development SMEs. It describes the background, research gap, problem statement, theoretical and practical significance. This chapter also describes the scope of the research study as well as the research objectives and hypotheses, summarizes in table 1.2. The next chapter encompasses a literature review related to the research subject.

Table 1.2 Summary of Research Questions, Objectives, and Hypothesis

Research Question	Research Objective	Hypothesis
RQ.1 What factors influence cybersecurity behaviour among employees in software development SMEs***?***	**RO1**. To identify the factors impacting cybersecurity behaviour among employees of software development SMEs.	A systematic literature review (SLR) was performed to extract factors that influence cybersecurity behaviour among employees of software development SMEs. The extracted factors have been classified as knowledge sharing, cyber hygiene attitude, cyber hygiene subjective norm, cyber hygiene perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, personality traits. Hence, below are the hypothesis: *H1: Knowledge sharing positively influences attitude to perform intention.* *H2: Cyber hygiene attitude will have a positive impact on intention.* *H3: Cyber hygiene subjective norms will have positive influences on cyber hygiene intention.* *H4: Cyber hygiene perceived behavioural control will have a positive impact on cyber hygiene intention.* *H5: Threat Appraisal will have a positive effect on cyber hygiene intention.* *H6: Cyber hygiene knowledge will have a*
RQ.2 How do individual factors such as knowledge sharing, cyber hygiene attitude, subjective norm, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits influence the intention to practice cyber hygiene among employees in software development SMEs?	**RO2**. To determine the impact of individual factors such as knowledge sharing, cyber hygiene attitude, subjective norm, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits on cyber hygiene intention among employees of software development SMEs.	
RQ.3 How does the SEM-Neural network approach enhance cybersecurity behaviour and promote cyber hygiene among employees in software development SMEs?	**RO3.** To examine the SEM-Neural network approach in improving cybersecurity behaviour through cyber hygiene among the employees of software development SMEs.	

		positive influence towards cyber hygiene intention. *H7: Perceived cyber hygiene value will have a positive effect on the cyber hygiene intention.* *H8: Cyber trust will have a positive effect on cyber hygiene intention.* *H9: Personality traits will have a positive impact on the intention.* *H10: Cyber hygiene intention has a positive and substantial impact on cyber hygiene behaviour.*

CHAPTER TWO

LITERATURE REVIEW

2.1. Introduction

This chapter offers a thorough exploration of cyber hygiene and cyber hygiene behaviours. Its significance to the thesis lies in establishing the foundation for research hypotheses, theoretical foundations, and the conceptual research framework. The researcher examines and establishes connections between various variables related to cyber hygiene behaviour, encompassing elements such as knowledge sharing, cyber hygiene attitude, cyber hygiene subjective norm, cyber hygiene perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived value, cyber trust, personality traits, and intention. This examination is conducted by referencing existing literature and previous studies by other researchers. Utilizing the collected data, a conceptual framework is constructed, incorporating appropriate theories and phenomena. This framework helps in shaping methodological research designs. The primary objective of this chapter is to compile existing research on cyber hygiene among employees of Malaysian software development SMEs.

2.2.Cyber Hygiene

Deora and Chudasama (2021), affirms that with the increasing growth in cyberattacks, cybercrime cannot be eliminated it may be reduced by cyber hygiene practices [86]. Cyber hygiene has been recognized as an important factor in reducing cybersecurity breaches. The rise in data breaches is due to humans failing to practice cyber hygiene. Most people do not employ firewall protection since they have not been educated; certain people are more inclined

to participate in unsafe behaviours such as password sharing. Neigel et al. 2020 stated that cyber hygiene practices preserve the security and confidentiality of online users' private data on their internet-connected devices from being compromised in a cyberattack [87].

To improve the understanding of the topic, it is necessary to investigate various definitions of cyber hygiene that are currently in use. Table 2.1. present a summary of the operational definitions of cyber hygiene by different researchers.

Table 2.1: Cyber Hygiene Definitions

Definitions of Cyber Hygiene	Reference
Cyber hygiene is an adaptive behaviour used to reduce risky online behaviours that can threaten a person's data.	[6]
Cyber hygiene is the practice of taking steps and putting policies into place to enhance cybersecurity and preserve system health while reducing the possibility of being the victim of a cyberattack.	[87]
According to the author, cyber hygiene is the precautions computer users take to secure confidential information from theft and cyberattacks.	[27]
Procedures that Internet users should adhere to protect their devices and private data online. is known as cyber hygiene.	[88]
The cybersecurity procedures that online users should take to guard the confidentiality and integrity of their information on devices with internet access from being compromised by a cyberattack.	[89]
Awareness of the concept, awareness of risks, and understanding end-user behaviour are all components of cyber hygiene. It teaches people how to protect themselves against cyberattacks that result in cyberattacks.	[90]

Cyber hygiene refers to employee security practices that significantly decrease the risk of cyberattacks. These practices include upgrading systems, employing firewalls, scanning computers for infections, using strong passwords, and more.	[70]

Cyber hygiene states to a flexible set of skills and practices designed to prevent individuals from engaging in risky online behaviours, thereby safeguarding their social, financial, and sensitive data [91]. This practice is essential for people to adopt as it help in protecting their identity and other vulnerable information from potential compromise or theft. Cyber hygiene is a widely acknowledged method for mitigating cybersecurity risks, helping in the anticipation of problems like information breaches, and cyberattacks [92]. Analogous to personal hygiene, cyber hygiene emphasizes the importance of individuals taking proactive measures and cultivating healthy habits to shield sensitive information from cyber threats.

Good cyber hygiene is necessary for maintaining cybersecurity. Everyone must practice good cyber hygiene to shield themselves from online risks, including people and organizations. Maintenance and security are the two benefits of routinely practicing good cyber hygiene. Maintaining a well-structured system reduces the likelihood of hacker attacks. While anticipating threats can be difficult, being prepared and averting them is possible through sensible cyber hygiene practices [93].

Organizations are susceptible to cyberattacks and incur significant costs due to security breaches. To defend against cyberattacks, employees become the first line of defense [94]. Businesses may improve security measures and secure digital potential hazards by implementing strong cyber hygiene practices. It is

important to secure individual and organizational security by protecting employees via cyber hygiene.

In recent times, numerous data breaches have occurred due to various factors such as malware, insider threats, lost devices, and inadvertent disclosures, underscoring the critical importance of cybersecurity [95]. Unfortunately, SMEs face budgetary limitations and have restricted access to IT resources [96]. Nevertheless, fostering good cyber hygiene practices can substantially enhance cybersecurity without imposing significant additional costs, primarily through raising employee awareness.

Many employees have poor online behaviour and lack fundamental knowledge and training in this area. They readily reveal their personal information on social networks and openly share their passwords, which are also saved automatically. End users are aware of the risks but cannot adopt the recommended practices to safeguard their personal and organizational information. Small firms are vulnerable to fraud because they have a lack of employees with security expertise and a sizable budget for cybersecurity investments. In that situation, employees are more susceptible to cyberattacks, which might harm the company and force its closure [97].

Employees can adopt effective cyber hygiene by updating software, utilizing antivirus programs, generating unique passwords, enabling two-factor authentication, and following similar protocols. Engaging in proper cyber hygiene not only encourages responsible behaviour but also safeguards against potential threats [70].

The cyber hygiene practices of employees can be influenced by their job title and the type of organization they work for. These factors may impact the

specific cyber hygiene practices which need to be familiar [89]. Cyber hygiene places a lot of emphasis on how well-informed users are about various security measures. In addition, the author argues that concentrating on the degree of knowledge of certain cyber hygiene practices offers some benefits. The first benefit is that awareness always comes before behaviour, that is why the majority of campaigns initiates to concentrate on raising awareness before promoting behavioural change [98].

Thus, evaluating awareness enables us to address the fundamental causes of the cyber hygiene issue. Fikry et al. 2023, stated that the frequency of people's cyber behaviours depends on the device, the application, the service, or the operating system [6]. For instance, individuals may modify their privacy settings on social media platforms whenever they submit material online because the platform enables them and facilitates such modifications.

2.3.Cyber Hygiene Behaviour

A recurring issue in research literature has been the absence of seriousness of SMEs in handling cybersecurity threats. The literature has often expressed worry about how lightly SMEs approach cybersecurity issues. As demonstrated by Alahmari and Duncan (2020) SMEs do not seem concerned about the normative pressure from the cybersecurity community [15]. As a result, authorized individuals frequently participate in harmful behaviours without realizing them, endangering the organization's data, security, and existing technical preventative measures [99]. In the present day, numerous businesses face challenges in adhering to cybersecurity policies. The underlying issue lies not in employees' knowledge and awareness, but in their unfavorable cybersecurity attitudes and behaviours [100]. User commitment and behaviour

are essential components to maintain the security and safety of the company's technology and resources .

Many cybersecurity vulnerabilities in SMEs might be attributed to employee behaviour. For instance, violating organizational regulations, corporate policies, and information rules might pose several cybersecurity threats. While education and training are vital for changing behaviour, in some circumstances, even knowledge cannot ensure proper behaviour [101]. According to a prior study, employee behaviour during awareness campaigns and training sessions was adequately reported at 85%; however, actual behaviour was lower than 54% [7]. Kok et al. (2020), explained users' actions and attitudes were substantially associated with cybersecurity awareness, but their knowledge did not have a significant connection [81].

Employees' cybersecurity behaviour can often demonstrate careless behaviour, such as using weak passwords, sharing login credentials, leaving devices vulnerable online, accessing company systems over unsafe networks, and managing organizational data casually [24].

Another research highlighted that most cybersecurity experts believe the security practices currently employed by SMEs might hinder efficiency. This is primarily because SMEs lack interaction with the research community and miss out on insights derived from large enterprise environments [102]. The suggestion has been made that elevating training efforts could boost knowledge. However, this knowledge might not necessarily result in practical and effective cybersecurity practices [103]. Therefore, If substantial changes in practices and policies are not implemented to tackle this problem, SMEs will continue to be a prime target for individuals seeking to exploit cybercrimes [104] .

Employees of SMEs having risk to their device software and was readily hacked by attackers if they don't practice proper cyber hygiene [105]. When an attacker possesses device-level software access privileges, they engage in various technical and fraudulent activities to gain control over the data within the system. These activities include malware insertion, denial of service, misidentification, and privilege escalation [106].

Insufficient cyber hygiene practices create vulnerabilities and make businesses susceptible to threats and attacks. A prominent example is the WannaCry Ransomware attack, which specifically aimed at individuals using operating systems of Microsoft, including versions 8, 2003, and XP [91]. Individuals who failed to update their software's security version fell victim to this attack. Outdated software becomes an easy target for various attacks and malicious malware. If software is not regularly updated, businesses remain exposed to recent threats. Computers operating on unlicensed Windows software are particularly at risk [107]. Poor cyber hygiene practices can lead to diverse data losses for individuals.

When it comes to data system security, passwords are vulnerable to network attacks, making them a major risk factor. Despite extensive government initiatives aimed at promoting safe online practices, numerous individuals continue to partake in risky password behaviors. These behaviors encompass sharing passwords, utilizing identical passwords across various platforms, and selecting easily predictable passwords [108]. The survey conducted in Malaysia found that bank account passwords and social media passwords were the next most often transferred credentials after emails [109]. Such actions may have

negative consequences for people, like identity theft, bank account loss, fraud, and others.

Phishing is one of the twenty-first century's most prevalent and well-organized crimes because of a lack of cyber hygiene behaviour. When someone sends fraudulent emails to gain personal information, this is known as phishing [110].

In conclusion, employees lack the necessary knowledge regarding effective cyber hygiene practices that can safeguard them from online threats. This study focuses on analyzing the cyber hygiene behaviour of employees within Malaysian software development SMEs. The aim is to assess whether individuals with a solid grasp of cyber hygiene concepts demonstrate suitable cyber hygiene behaviour in their everyday activities. Understanding that individuals are more susceptible to cyber threats than computer systems, it becomes crucial to enhance employees' comprehension of good cyber hygiene practices.

Consequently, this research applies theory of planned behaviour (TPB) to elucidate a novel framework and reevaluate previously established significant findings. The TPB provides a well-established psychological framework, making it suitable for understanding individual intentions and strengthening cybersecurity measures within organizations, particularly in software development SMEs. The justification for using TPB is that it is widely recognized and validated in the field of information systems and security, it effectively predicts and clarifies human behavior. TPB also applicable in explaining knowledge-sharing behaviors based on attitude, subjective norm, and perceived behavioral control. According to Ajzen's report in [111] that TPB

can be integrated with other factors to account for variations in people intentions or behaviors. TPB offering a structured approach to data collection and analysis, TPB enables researchers to systematically evaluate and scrutinize key constructs such as attitude, subjective norm, and perceived behavioral control, facilitating thorough investigations into the factors impacting cybersecurity behaviors [112].

2.4.Factors of Cyber Hygiene Behaviour

A Systematic Literature Review (SLR) was conducted in order to disclose the factors that influence to cyber hygiene behaviour among employees of Malaysian software development SMEs. Based on their nature, relevance, and discussion context in the literature the identified factors were subsequently sorted as: Knowledge sharing, cyber hygiene attitude, cyber hygiene subjective norm, cyber hygiene perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived value, cyber trust, personality traits and cyber hygiene intention. The overview of these respective factors, thereby contributing to a better understanding of the factors that underlie employees cyber hygiene for Malaysian software development SMEs. Below is an in-depth discussion of the factors.

2.4.1. Knowledge Sharing

Knowledge sharing discusses to the act when someone shares their knowledge with another person. Knowledge is a fundamental prerequisite to taking the proper action in every scenario. Knowledge is necessary to perform appropriately in a certain situation [113]. In a small or medium-sized firm, it entails enabling the flow of knowledge to improve learning, problem-solving,

innovation, and decision-making. Collaborations and training that improve knowledge sharing among employees positively impact their attitudes and user awareness [114].

Knowledge sharing empowers individuals to identify and respond to cyber threats effectively. Kok et al. (2020), explain that in order to comprehend cyberattacks and their associated risks, individuals must initially grasp and be conscious of how to safeguard themselves against such attacks[115]. This entails knowing the possible effects and what may be done to mitigate them. The author further explained that information's confidentiality, integrity, and availability increase when users are well-informed about knowledge and awareness and can prevent threats and attacks.

Knowledge sharing as a factor of cyber hygiene behaviour promotes a collective understanding of cybersecurity, enhances awareness, and encourages the spread of best practices within communities and organizations.

2.4.2. Cyber Hygiene Attitude

A key factor attitude, which describes how someone feels about engaging in a certain behaviour and can be either good or negative. A positive or negative expression of employees towards an object is called an attitude. An attitude is developed based on a person's ideas, values, experiences, and emotions related to the behaviour [116]. Attitude is one of the most important psychological elements that affects an employee's desire to engage in secure behaviour [117]. When attempting to understand behaviour, attitude is considered as a crucial component. It includes the person's overall favourable or negative assessment within the cybersecurity behaviour.

In SMEs, attitude shows how employees see and assess engaging in a certain behaviour, such as implementing cyber hygiene practices. According to Etezady, (2019), if an employee has a bad attitude towards cybersecurity practices, it may be because they feel that these procedures are time-consuming, difficult to understand, or not important [118]. Also, Etezady explain that an employee's attitude is whether or not they plan to follow company policies on cybersecurity. Kaur and Mustafa, (2013), studied how user behaviour and attitude are crucially related to cybersecurity knowledge and awareness [113].

A favorable attitude signifies a positive perception of cybersecurity measures, such as employing robust passwords, activating two-factor authentication, and consistently updating software. This factor is often linked to a willingness to adopt and adhere to these practices.

2.4.3. Cyber Hygiene Subjective Norm

Cyber hygiene subjective norm is another factor related to cyber hygiene behaviour which indicates the social pressure around adopting a specific behaviour. It expresses the expectations, viewpoints, and acceptance or disapproval of the behaviour expressed by colleagues, managers, and other essential persons or groups. In other words, subjective norms are people's opinions of certain behavioural patterns that are important to them. Employees may experience a good subjective norm if they believe their coworkers and managers actively encourage and approve cyber hygiene security knowledge. On the other hand, the subjective norm can be less favourable if employees think that their coworkers are uninterested in or adverse towards such security knowledge [80].

Johnson (2017) explained that an employee may have a stronger intention to carry out a behaviour if they feel there is a significant societal expectation or pressure [119]. Subjective norm was utilized in the study [120] to examine the usage of home computers for personal use and the implementation of security-related measures. The researcher further elaborates the findings and demonstrated that subjective norms impacted the adoption of security measures on home computers, but this impact did not extend to the intention to adopt measures for online security.

Understanding the effect of subjective norms in SMEs requires designing interventions that consider the social environment and encourage employees behaviour that are align with the subjective norms inside the organization. Positive subjective norms imply encouragement and approval from others, creating social motivation to follow cybersecurity protocols. Social support and influence from one's social circles significantly impact an individual's decision to engage in cyber hygiene behaviours.

2.4.4. Cyber Hygiene Perceived Behavioural Control

This is another factor for cyber hygiene behaviour [121]. It represents the person's assessment of their ability to carry out their behaviour effectively while taking external as well as internal factors into account. Specifically in SMEs, perceived behavioural control (PBC) states to an employee's perception of how much control they have over acquiring a particular security behaviour, such as practicing cyber hygiene. Perceived behavioural control is also described as ease or difficulty in doing security behaviour [122]. Worker's PBC would be high if they feel they have the abilities, resources, and knowledge to practice cyber hygiene properly . On the other hand, their PBC may be lower if they

perceive difficulties such as a lack of time or insufficient training. Employees are inclined to participate in a behavior when they perceive themselves as capable of doing so, thereby reinforcing their intention [98].

Understanding perceived behavioural control in the context of SMEs is important in designing interventions that remove perceived obstacles, improve employee skills and resources, and ultimately encourage the adoption of desirable behaviours. In order to increase the chance of effective behaviour change, it helps in identifying areas where resources and assistance may be offered. High perceived behavioural control indicates self-confidence in practicing cybersecurity behaviours despite obstacles. Therefore, this factor influences an individual's intention to adopt cyber hygiene measures and their ability to overcome barriers hindering those practices.

2.4.5. Threat Appraisal

Threat describes the likelihood and intensity of risk. It could be the possibility of losing something valuable. Value might include social status, financial success, good physical and mental health, and confidential or commercial knowledge. The term "Threat Appraisal" in the context of cyber hygiene behaviour refers to a person's desire to participate in a certain security behaviour. It indicates the person's evaluation and perception of the seriousness and sensitivity of a prospective danger or risk. It entails assessing the possible drawbacks of not engaging in particular behaviours, such as maintaining good cyber hygiene in relation to cybersecurity [80].

If employees perceive high levels of threat they may be more motivated to adopt behaviours that reduces those risks. Designing interventions that address workers' perceptions of cybersecurity risks and the possible effect of those risks

requires an understanding of threat appraisal within the context of cyber hygiene behaviour for SMEs. Organizations may improve employee intentions to engage in behaviours that lead to a more secure digital environment by appropriately analyzing and managing threat perceptions [123].

Higher threat appraisal leads to increased vigilance and motivation to adopt cyber hygiene practices as protective measures. Understanding the severity of potential threats prompts individuals to take preventive actions, making threat appraisal a critical factor in cybersecurity behaviour.

2.4.6. Cyber Hygiene Knowledge

The term cyber hygiene knowledge describes a psychological aspect that affects a person's desire to engage in cybersecurity-related behaviours, particularly those linked to upholding a secure digital environment. An person's knowledge, awareness, and familiarity with key cybersecurity ideas and practices are all included in their cyber hygiene knowledge. It impacts a person's capacity to weigh the advantages and disadvantages of engaging in cyber hygiene behaviours, which in turn affects their intention to perform cybersecurity behaviour [124]. Cyber hygiene knowledge pertains to a person's comprehension of the measures required to protect themselves from cyberattacks. Significant disparities persist between professionals and non-professionals concerning basic cyber hygiene practices such as software updates and backups. Their attitude may change if they are more knowledgeable about cyber hygiene [125].

It was discovered that employees with high knowledge of phishing threat mitigation may prevented more from phishing attempts. If employees want to improve cyber hygiene behaviours they first have to understand the existence

of cyberthreats and how they may be avoided. The majority of individuals are aware that they are vulnerable to cyberattacks, but they lack the knowledge necessary to practice basic cyber hygiene, such as protecting passwords. Antunes et al. (2021) underscores the importance of integrating knowledge with suitable attitudes and mindful behaviours to safeguard sensitive information in both enterprises and communities. The author asserts that despite increased awareness of security breaches, many users fail to adopt proper cybersecurity practices to secure their data [126].

Cyber hygiene knowledge empowers individuals to make informed decisions, recognize potential risks, and take proactive actions. It forms the foundation for adopting and maintaining effective cybersecurity practices, including recognizing phishing attempts, identifying malware, and securing personal information.

2.4.7. Perceived Cyber Hygiene Value

Perceived value refers to the assessment of users' when comparing benefits against the cost. It indicates a psychological element that affects a person's desire to engage in cybersecurity-related behaviours within organization [127]. The relevance, advantages, and significance of adopting cyber hygiene behaviours within an organizational environment, such as upholding good cyber hygiene practices, are referred to as perceived cyber hygiene value. It acts as a motivating factor that affects a person's attitude and decision-making process, eventually determining whether they want to engage in cybersecurity behaviours. Employees are more motivated to take proactive measures to safeguard their digital environment, sensitive data, and the security of the

organization when they are aware of the benefits and significance of good security practices [128].

Recognizing the value of cybersecurity practices motivates individuals to adopt and adhere to these behaviours. When individuals perceive the tangible benefits, such as protecting sensitive data or avoiding financial losses, they are more likely to participate in cyber hygiene practices.

2.4.8. Cyber Trust

Trust is a desire to feel secure in relying on someone or something [83]. This can be credited to interpersonal connections and stands as a fundamental element of a social structure. Trust affects relationships both among and within social entities, such as those among friends, families, organizations, communities, businesses, and nations.

The term cyber trust describes the degree of certainty, faith, and belief that stakeholders and workers have in the company's ability to sustain a safe and reliable digital environment. It includes confidence in the organization's cybersecurity procedures, technologies, and techniques designed to preserve private data and protecting against cyber threats [129].

High levels of cyber trust indicate a belief that digital interactions and data are secure, fostering a sense of safety and assurance. Trust in online security influences one's willingness to engage in various online activities, including adopting and adhering to cybersecurity practices.

2.4.9. Personality Traits

Personality traits are persistent and consistent characteristics of a person's behaviour, cognition, and emotions that effect how they perceive and react to diverse circumstances. It can affect a person's views, intentions, and actions,

including their participation in actions linked to cybersecurity in SMEs. According to the commonly used big five paradigm, there are five primary personality traits: agreeableness, conscientiousness, neuroticism, openness, and extraversion [84]. Cooperative traits are measured by agreeableness, dependable and organized traits by conscientiousness, insecure and anxious traits by neuroticism, sometimes referred to as emotional stability, creative and intellectual traits by openness, and enthusiastic and extroverted traits by extraversion [130].

Although personality is a topic that receives much attention in psychological literature, little research has examined the connection between personality factors and security behaviours. The majority of research on personality factors has focused on phishing vulnerability. Lopez-Aguilar and Solanas (2021) stated that there is an association between phishing vulnerability and a high level of neuroticism in females and between openness and lax privacy settings [131]. High openness and extraversion were linked to a lower sensitivity to phishing [132]. A low awareness of security risk when purchasing online has been linked to high extraversion [133]. In the case of SMEs, including personality traits in the context of cyber hygiene behaviour enables a more thorough knowledge of the elements that influence cybersecurity practices.

Personality traits, like as conscientiousness (organized, responsible) and openness (willingness to try new things), could influence an individual's inclination to follow cybersecurity best practices. Personality trait factor shape attitudes, intentions, and behaviours related to cyber hygiene.

2.4.10. Cyber Hygiene Intention

Psychology defines human behaviour as founded on an individual's beliefs, goals, and intentions. An intention is a state of mind that expresses a commitment to carry out a certain activity now or in the future [134]. Planning and mental effort are involved in intention in order to accomplish a goal. An individual's desire to practice cyber hygiene demonstrates their readiness and commitment to participate in cybersecurity behaviours [135]. A crucial predictor of cyber hygiene behaviour is cyber hygiene intention, affected by several variables that determine how motivated a person is to adopt good cyber hygiene practices. Employees' desire to engage in cybersecurity behaviours, such as good cyber hygiene, safe online behaviour, and adherence to organizational cybersecurity standards, is their cyber hygiene intention [136].

Intention serves as an important factor of cyber hygiene behaviour. It indicates the likelihood of individuals engaging in security practices in the future. A strong intention to adopt cyber hygiene measures often translates into consistent and proactive cybersecurity behaviour.

The intention based model is the foundation of most prior security research utilizing cyber hygiene behaviour. Security intentions may or may not transform into actual security behaviour; however, there is evidence that behaviour does correspond to intentions [120]. Therefore, intention has a higher impact on security behaviour in an organizational setting.

This factor is used to investigate and predict the intention of security behaviour among the employees of Malaysian software development SMEs.

Understanding these factors comprehensively is essential for designing targeted interventions, educational programs, and policies aimed at promoting

good cyber hygiene behaviours among individuals and organizations, thereby enhancing overall cybersecurity.

2.5.The Underpinning Theories

The concept of intention has become prominent in literature of behavioural sciences. Given the complexity of human behavior, predicting it requires taking into account multiple factors [73]. Previous research has employed various theoretical frameworks to anticipate individuals' behavioral intentions regarding specific activities. Theoretical foundation of the study involves the TPB the idea taken from the theory of reasoned action (TRA) [78]. In this study TPB is used to predict the cyber hygiene behaviour among employees of software development SMEs. Researchers have applied TPB to predicts an individual's behaviour through intention, attitude, subjective norms, and PBC.

2.5.1. TPB and Cyber Hygiene Behaviour

Theory of planned behaviour (TPB) aims to enlighten and anticipate human behaviour using a person's intentions. In various studies, TPB has been used to elucidate the relationship between beliefs, attitude, behavioural intentions, and behaviour. TPB, initially developed based on Ajzen's theory of reasoned action (TRA), is significant for understanding how individuals make behavioural decisions. The TPB is frequently used to comprehend and examine behavioural intentions and their relation to actual behaviour in various domains, including psychology, the social sciences, and health promotion [116], [137]. TPB considers possible elements that could indirectly influence behaviour through behavioural intention. And behavioural intention is exaggerated by attitude toward the behaviour (AT), subjective norms (SN), and perceived behavioural control (PBC) [119].

A person's level of favorable and unfavorable evaluation for a particular behaviour is their attitude towards the behaviour [117]. Subjective norms are the social pressures that impose on people to act in a certain way, including expectations from friends, family, and other significant referents [138]. A person's difficulty in engaging in a certain behaviour is known as perceived behavioural control [139]. Also, Hiranrat et al. (2021), explored the intention that indicates how hard individuals are ready to achieve the behaviour [121]. In other words, intention may be a good interpreter of actual behaviour, although the link among intention and behaviour is not perfect [136]. Numerous researchers confirmed the possibility of using TPB to describe how cybersecurity behaviour forms [140], [141], [142].

With the context to SMEs, the TPB may support the design of interventions to encourage desirable behaviours by the explanation and prediction of intents and behaviours linked to cybersecurity practices and information sharing. According to studies, attitudes, subjective norms, and PBC all have a role in deciding whether or not a person involves in cyber hygiene behaviour among employees of Malaysian software development SMEs [143], [144]. Results of the research suggest the TPB can offer useful insights into the root causes and possible solutions for cyber hygiene. The TPB, a theoretical framework for understanding human behaviour, is depicted in Figure 2.1.

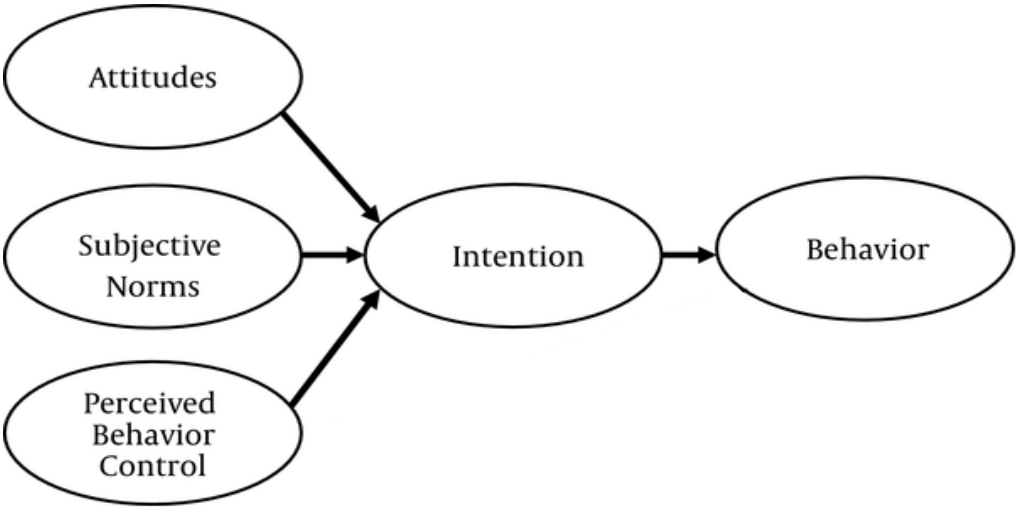

Figure 2.1 Theory of Planned Behaviour [145]

2.6.Research Framework of Study

Evidence-based on the literature study revealed that various factors influence the attitude that affects the behaviour to practice cyber hygiene. The study aims to examine the underlying factors and motives that impacts cyber hygiene behaviour among employees of software development SMEs in Malaysia using TPB as the rational choice framework [73], [145] . Figure 2.2 demonstrates the proposed model for this investigation. The model finds independent variables such as knowledge sharing, cyber hygiene attitude, cyber hygiene subjective norms, cyber hygiene perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, personality traits significantly associated with the cyber hygiene intention to use cyber hygiene behaviour.

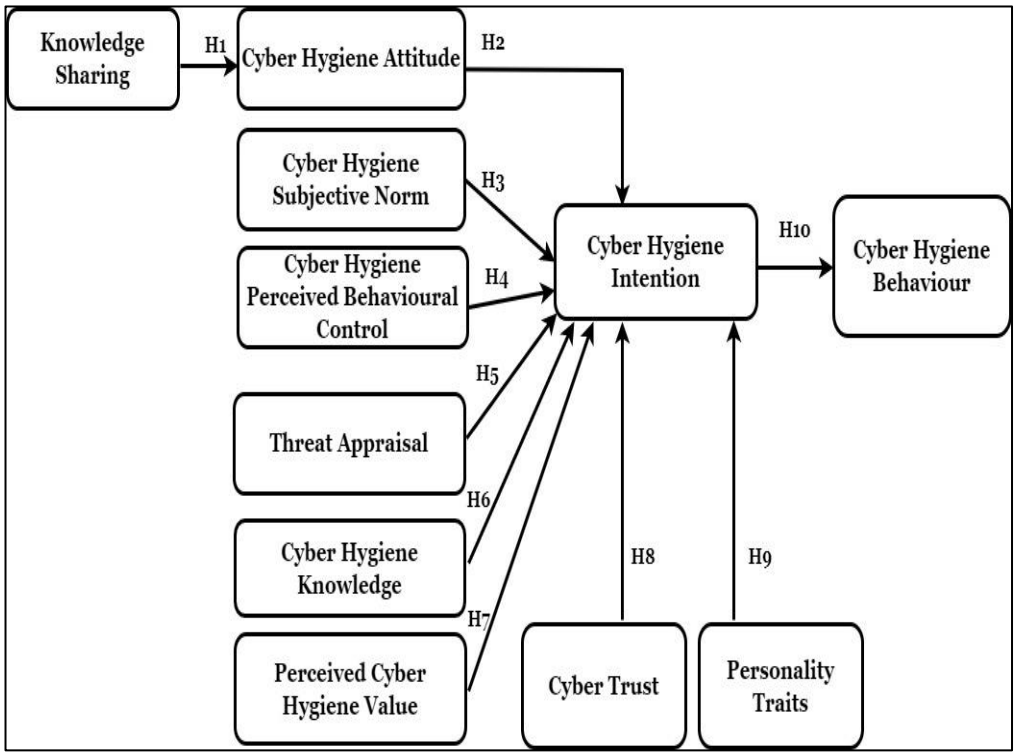

Figure 2.2 Research Framework

2.7.Study Variables And Hypothesis Development

This segment of thesis presents an overview of the variables involved in current study and afford a comprehensive review of the relevant literature. Additionally, this section will outline the hypothesis development of the study. The TPB variables include subjective norms, PBC, attitude, intention, and behaviour. Other factors are knowledge sharing, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, personality traits are independent variable constructs, while mediating variable is cyber hygiene intention. Following are in-depth critical analyses of the variables:

2.7.1. Knowledge Sharing and Cyber Hygiene Attitude

Gaining knowledge is the initial step toward transforming one's behaviour. Sharing of knowledge is characterized by the willingness of individuals, groups

to impart or disseminate information to others [146]. Cain et al. (2018), also described knowledge sharing as a related behaviour in which individuals seek out the knowledge from others [90]. Sharing knowledge improves people's understanding of cyber hygiene in the context of this study. Employees may cooperate on cyber information risks in the workplace through knowledge sharing, allowing them to generate ideas and exchange security-related information [79].

A person's tendency to respond positively or negatively to an item or a concept is called their attitude [147]. Attitude is an important consideration in knowledge-sharing activities because a person's ability to solve issues might impact their value to employers [148]. Employees will actively participate in knowledge-sharing initiatives if they believe they are significant and helpful for their company [149]. On the other side, employees will refrain from sharing their expertise with competitors if a person experiences a loss of influence or resources in the sharing knowledge or producing knowledge [150].

Behaviour has the power to affect attitude, and attitude has the power to affect intention. Hence, an individual's inclination to share knowledge is shaped by their attitude, which influences their behavioural intention to engage in knowledge sharing [151]. These interactions among these three knowledge exchange, attitude, and behaviour occur dynamically and sometimes reciprocally [152], [153], [154]. Consequently, the first hypothesis of this study states:

H1: Knowledge sharing positively influences attitude to perform cyber hygiene intention.

2.7.2. Cyber Hygiene Attitude and Cyber Hygiene Intention

A person's attitude is the point of view which can affect an individual's behaviour [115]. Attitude has captured the interest of numerous specialists in several fields, due to its capacity to characterize a person's behaviour. A individual's attitude towards a behaviour is influenced by the set of ideas that person holds about that behaviour [84]. Negative attitudes may decrease a target behaviour and conversely, Positive attitudes encourage favourable behaviour [155]. Even if a person is an expert on cybersecurity threats, they still need to be able to describe how cyber hygiene practices have evolved. Therefore, in light of this, it is anticipated that employees who have a favourable attitude towards cyber hygiene would feel fewer incentives to comply with bad cyber hygiene practices.

The literature from behavioural research suggest that attitudes play a major role in elucidating cyber hygiene behaviour [126]. The association among attitude and behavioural intention has been studied by numerous studies in information security[156], [157]. Most of the investigations focuses on attitude-behavioural intention relationship and are carried out in an organizational context. There are several researches like [158], [159] demonstrate a favourable correlation between attitude towards security, and behavioural intention. Additionally, Alotaibi and Aloud (2023); and Matlala (2023), found that employees have a positive attitude towards cybersecurity practices and intention to follow those practices [160] and [161]. Hadlington, (2017), once employees are at work, they no longer consider cybersecurity to be a major issue [147]. Tischer et al. (2016), revealed a negative change in user attitudes and cybersecurity intention [162]. Therefore, it is necessary to evaluate the

correlation between attitude and CH intention. Therefore, it is hypothesized that:

H2: Cyber hygiene attitude will have a positive impact on cyber hygiene intention.

2.7.3. Cyber Hygiene Subjective norm and Cyber Hygiene Intention

Subjective norms is the impact of how others observe about a specific behaviour [119]. The societal pressure on employees to involve in or prevent them from involving in a certain behaviour is demonstrated by subjective norms [120]. This pressure can be placed by department heads, managers, supervisors, or even coworkers who view cybersecurity as an effective and practical approach that improves cyber hygiene behaviour and reduces the threat of cybersecurity breaches [163]. When examining employee compliance with cybersecurity, discovered that subjective norms play an important role in establishing an atmosphere where employees comply with cybersecurity practices [164].

Ismail (2022) stated that the employees' intentions to maintain security are substantially predicted by subjective norms [165]. In the research of [166], [167], authors found that subjective norms positively impacted employees' cybersecurity behaviour and played an important and essential role in performing the cybersecurity behaviour. In the study of Abet (2023), subjective norms were not discovered to be significantly influential for the intention among the employees of organization [168]. According to a recent study [122], [147], [169], subjective norm does not influence actual security behaviour. Therefore, this research will provide a prospect to evaluate and find the association between subjective norms and cyber hygiene intention. Consequently, it is hypothesized that:

H3: Cyber hygiene subjective norms will have positive influences on cyber hygiene intention.

2.7.4. Cyber Hygiene Perceived Behavioural Control and Cyber Hygiene Intention

Hiranrat et al. (2021), perceived behavioural control (PBC) has the capability of an individual to carry out a specific behaviour [121]. A person may or may not be able to carry out the desired behaviour, and this affects how person belief about their intentions and behaviour [136]. As noted in the findings of Abdul et al. (2020), their study demonstrates that sharing ability and willingness are two critical elements that influence cybersecurity behaviour [170]. When it comes to cyber hygiene PBC may be significant in predicting a person's intention to participate in specific behaviour. If an individual perceives control over their behaviour and believe in engaging cyber hygiene practices, those individuals may be more likely to plan to engage in cyber hygiene behaviour [171], [172].

On the other hand, people could be less likely to intend to participate in this behaviour if people feel they have no control over their actions or think it is challenging to practice good cyber hygiene [169], [173], [174]. Adisty et al. (2023), identified users' participation and cybersecurity experience as the significant aspect that influences their opinions of practicing cyber hygiene behaviour [175]. Among employees of the organizations, researcher of [116], [176] have also discovered a high correlation between PBC and cybersecurity. Based on the aforementioned conflict in the literature we considered this below hypotheses in this research:

H4: Cyber hygiene perceived behavioural control will have a positive influence on cyber hygiene intention.

2.7.5. Threat Appraisal and Cyber Hygiene Intention

Threat appraisal addresses how individuals perceive the seriousness of cybersecurity risks and the possibility that these threats might affect either of them individually or the entire organization [177]. The threat is the deliberate exploitation of uncertainty. The threat is not simply limited to a potential loss of money or even identity; it also encompasses the disclosure of private information [178]. Threat appraisal refers to the user's evaluation of the risk posed by a potentially harmful occurrence [179]. Threat appraisal has been identified as a crucial element that influences how people perceive and act in relation to adherence with security regulations in the organization [180]. Wong et al. (2022) stated that an employees have high threat appraisal towards cybersecurity practices [181].

When customers encounter difficulties managing the illegal distribution or misuse of their company or private data, they lose trust and become increasingly apprehensive. This fosters a sense of uncertainty, causing them to hesitate and be reluctant to share personal information [182].

Employees' threat appraisals would be high, if they consider cybersecurity risks to be extremely serious and think there is a chance they would be attacked [183]. On the other hand, employees' threat appraisal may be lower, if employees underestimate the severity of threats or believe they are unlikely to be targeted [165], [167]. Alzahrani and Seth (2021) revealed that threat appraisal significantly influences employees' with the cybersecurity intention [184]. In view of this, fifth hypothesis of the study is formulated as under:

H5: Threat Appraisal will have a positive influence on cyber hygiene intention.

2.7.6. Cyber Hygiene Knowledge and Cyber Hygiene Intention

At present, the majority of existing cybersecurity expertise focuses on securing the intricate digital networks of large corporate entities. The in-depth knowledge and skills required for employees to secure data of small company systems are not given much attention [90]. The state to which a person intends to engage in this cyber hygiene practice is significantly influenced by their level of expertise in cyber hygiene knowledge [70]. As observed by Abawajy, a basic understanding of cybersecurity knowledge may not transfer into adequate cybersecurity countermeasures to reduce cyber threats [114]. Further from the results the researcher recommended for enhancing the knowledge of cybersecurity through cybersecurity training programs that used theoretical lectures and simulators to offer experience to cybersecurity safety technologies.

For example, the 'Phishing Simulator' is a common training tool intended to improve awareness of fraudulent emails sent by hackers, which often lead to the unauthorized disclosure of sensitive information [185]. As indicated in a research conducted by Conetta (2019), users tend to exhibit enhanced cybersecurity behaviour with an increase in their knowledge about cybersecurity [125]. The researcher also suggests that cyber hygiene knowledge has an important impact on users' intentions to use cyberspace securely. Cain et al. (2018) explored the extent of cyber knowledge among individuals. Their research specifically examined how employees uphold system integrity and utilize online security tools such as firewalls and antivirus software [90]. Recent studies have also discovered a high correlation between cyber hygiene knowledge and security behaviour among SMEs employees [150]. A study by

Cain et al.(2018) found that cyber hygiene knowledge were positively related to cybersecurity behaviour among the employees.

According to the author's research in [134], [186], self-identified professionals had less cyber hygiene knowledge than self-identified non-experts. Therefore, these surprising outcomes suggest a need for increased efforts in obtaining essential cybersecurity knowledge. Hence, sixth hypothesis of the study is formulated as under:

H6: Cyber hygiene knowledge will have a positive influence towards cyber hygiene intention.

2.7.7. Perceived Cyber Hygiene Value and Cyber Hygiene Intention

Organizations must understand and promote perceived cyber hygiene value to emphasize the relevance of cybersecurity behaviours and motivate workers to adopt responsible practices that boost the organization's overall security and resilience against cyber threats [187]. Employees may be more motivated to engage in cybersecurity behaviour if they perceive highly valued in practicing good cybersecurity [128]. The importance of perceived value in influencing people's intentions to adopt cybersecurity behaviours has been addressed in several research [188]. The idea of perceived cyber hygiene value is closely related to the concept of perceived advantages, which has been extensively discussed in the literature on technology adoption and behaviour change [189]. In the context of technology adoption, the author Lutfi (2022), established the idea of perceived usefulness, emphasizing that people are more persuaded to accept new technologies if they perceive them as beneficial and boosting their productivity [190]. This idea aligns with the results of (Lutfi et al., 2022), according to which staff members are more inclined to practice good cyber

hygiene if they believe it will safeguard their personal and professional interests [191].

Al-Okaily et al. (2023), provides their study on information privacy behaviours emphasized that people are more possible to participate in protective behaviours if they perceive that doing so will protect personal information and prevent undesirable outcomes [192]. Perceived value affects the intention to engage in a behaviour as well as the maintenance of long-term relationships between users [193]. It is clear from the literature on cybersecurity and privacy that people are more motivated to intent the behaviours when they perceive the value for cybersecurity. Thus, it can be hypothesized that:

H7: Perceived cyber hygiene value will have a positive impact on the cyber hygiene intention.

2.7.8. Cyber Trust and Cyber Hygiene Intention

Trust is a belief that someone or something is sincere, trustworthy, morally upright, and efficient. According to the author trust is the commitment to play a necessary part in developing interpersonal connections that encourage information exchange [83]. Authors Apau and Koranteng (2019) believed that information sharing is a kind of cooperation in business organizations and that this collaboration cannot occur without trust between various parties [129]. In a study of Chen et al. (2014), researcher emphasized trust's critical role in young people's exposure to personal information during online interactions [194].

Information security administrations refrain from sharing information to prevent attackers from exploiting shared data. In such scenarios, trust plays a vital role in cybersecurity [129].

For SMEs to create an organizational culture where workers feel confident about cybersecurity, they must comprehend and promote cyber trust. Akman and Mishra (2010), if employees have confidence in the organization's cybersecurity policies and procedures, they may be more likely to adopt cyber-hygiene practices since they will feel safer and more secure [195]. Businesses prioritizing building and sustaining confidence in their digital practices foster an atmosphere where employees are more likely to practice good cyber hygiene practices that improve overall organizational security and resilience to cyberattacks.

Abdul et al. (2020) in their research asserted that the sharing of knowledge and the disclosure of private information by employees during online communication is the core elements of cyber trust [170]. However, research by [196], [197] revealed that cyber trust plays a key part in the field of exchanging cybersecurity. As from literature, findings are diverse and inconsistent. As a result, it is essential to evaluate the association among cyber trust and intention for cyber hygiene intention. Therefore, eight hypothesis of the study is formulated as:

H8: Cyber trust will have a positive influence towards cyber hygiene intention.

2.7.9. Personality Traits and Cyber Hygiene Intention

Understanding an employee's personality traits in the context of SMEs and cybersecurity can help in designing interventions and communication approaches to encourage cyber hygiene behaviours effectively [198]. There are several applications for personality constructs, including cybersecurity [84]. Frauenstein and Flowerday (2020), explained socioeconomic factors, personality traits, and product consumption all influence how successful

attitudes change behaviour [132]. To better understand the adoption and usage of cybersecurity software, personality traits were employed in this study.

Carvalho et al. (2020), explained that conscientiousness and agreeableness were shown to be the two personality traits that have the most effects on organizations [133]. Additionally, earlier research has demonstrated that conscientiousness and agreeableness are stronger indicators of employees' compliance with policies and standards when behaviour is not observed. Several behavioural investigations have shown a substantial inverse association between conscientiousness and security conduct [199]. Although agreeableness and security conduct have been significantly correlated, people with greater relational orientations are more likely to agree to practice cybersecurity behaviours [200]. Research has mostly concentrated on people and their psychological attributes that make them susceptible to cyberattacks.

Results, meanwhile, are not conclusive. conscientiousness, extraversion, openness to new experiences, and agreeableness were personality qualities that made people more vulnerable to cyberattacks [201]. However, research from [198], [202] found that conscientiousness, agreeability, and openness to experience were associated with reduced risk-taking and greater information security awareness. Therefore, it may be argued that personality traits do affect the frequency of increasing or decreasing cyberattacks, which in turn affects a person's cyber hygiene. Thus, it can be hypothesized that:

H9: Personality traits will have a positive effect on the cyber hygiene intention.

2.7.10. Cyber Hygiene Intention and Cyber Hygiene Behaviour

One of the key part of the TPB, which has been utilized extensively in research on information security behaviour, is intention [148]. The intent is to

follow organizational policies about data security, implement data security practices, and share knowledge regarding information security [203]. A person's intention to involve in a particular behaviour can serve as a predictor for the actual behaviour they plan to exhibit in the future [140]. Stronger intentions rise the likelihood of a person continuously engaging in behaviours to carry out those intentions [180]. Intention captures an individual's readiness to take practical steps to protect sensitive information, avoid cyber threats, and contribute to a secure digital environment within the SME [71].

Understanding and supporting cyber hygiene intention is essential for SMEs to successfully urge staff members to follow responsible cyber hygiene practices. Organizations might build interventions to encourage a culture of cyber hygiene awareness and inspire workers to take an active role in behaviours that support overall cybersecurity resilience [176]. The concept of intended behaviour defines intention as the inclination to engage in a specific behaviour, rather than the actual execution of the behavior itself [136]. According to Ajzen, intentions reflect a person’s resolve to engage in a specific behaviour. Intention is the most reliable predictor of whether an activity will occur [73]. This means that an person's decision to engage in cyber hygiene is solely based on their own will.

According to studies [71], [115], [204], that persons with a positive intention towards a particular act are more likely to perform that act. Additionally, the author discovered that behaviour is a direct outcome of intention, and that intention is the best predictor of behaviour [205]. In this research, it is hypothesize that the intention has a substantial impact on cyber hygiene behaviour based on the TPB:

H10: Cyber hygiene intention has a positive and substantial impact on cyber hygiene behaviour.

2.8.Summary

Literature on cyber hygiene is thoroughly reviewed in Chapter 2, which also includes an overview of Ajzen's theory of planned behaviour (TPB). This research developed the conceptual framework, which incorporates this theories and their relevant variables, are also presented. The research introduces its hypothesis and outlines the proposed conceptual framework, establishing the basis for the research.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1.Introduction

Chapter delve into the methodology and research design employed in the investigation, offering insights into the research method, problem statement, and research objectives. It begins by outlining the research purpose, philosophy and design utilized. The chapter discusses the questionnaire method approach, the targeted population, the sampling procedure, pilot testing, data collection processes, and the analysis methodology. Reliability, and validity of study are also evaluated in this chapter.

Preceding chapters extensively explored the research background, presenting the problem statement, research objectives, and literature review to underpin this study. This chapter elucidates how the research objectives were attained, involving problem identification, and addressing research questions using diverse techniques and approaches. The study employed various methods such as founding the research paradigm, research methodology, and data collection techniques. It also involved identifying an appropriate and sizable target population, selecting statistical tools, and employing interpretation methods to assess the presented hypotheses.

This study focuses on factors like knowledge sharing, cyber hygiene attitudes, cyber hygiene subjective norms, cyber hygiene perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, personality traits, and cyber hygiene intention to utilize cyber

hygiene behaviour among employees of Malaysian software development SMEs. Detailed approaches are outlined below.

3.2.Research Purpose

This study is closely related to the hypothesis. As a result, there are many uncertainties and illusions replicated in the interpretation of the research's objective and significance. There has been inadequate research on the problem of cyber hygiene behaviours among Malaysian employees of software development SMEs. This research will close a knowledge gap by putting theories from the behavioural sciences to the test and delivering results and suggestions.

Furthermore, study employed the research fundamentals proposed by Creswell [206]. The research purpose is defined, followed by the research philosophies and assumptions, research design, and the appropriate methodology for this research.

3.3.Research Philosophy

Research philosophy includes assumptions, practices, and beliefs regarding how the researcher views the world. These assumptions and ideas are the foundation for research strategy and methodology for performing research within a specific field. When addressing research philosophy, the two fundamental concepts are ontology and epistemology. Ontology delves into the essence of reality, while epistemology examines the methods by which researchers attain knowledge and understanding about that realism [207] . In practice, epistemological research entails spending time in the field and developing relationships with participants. This research preferred the concept of epistemology.

It represents a common perspective that shapes the whole research process, from the design of research questions to the interpretation of findings. Through this researcher's perspective on reality, knowledge, and the nature of the research process. They impact the research methods used to conduct research, data-collecting procedures, and the criteria used to establish the validity and reliability of study findings.

This study adopts a quantitative and positivist approach. In deductive research, procedures are initially hypothesized and then tested against observations, while inductive research seeks to identify new patterns based on exact explanations. Deductive reasoning elucidates cause-and-effect associations among variables and concepts and facilitates the evaluation of quantitative data. It also follows a logical progression, starting with theory and leading to the development of new hypotheses [208].

The research adopts an epistemological perspective characterized by objectivity rather than subjectivity, as it utilizes closed-ended questionnaires among employees of software development SMEs in Malaysia. Objectivism highlights the existence of objects and social norms unaffected by social factors, focusing exclusively on objects and structure. As a result, this study adheres to a positivism philosophy to attain the research objectives using survey questionnaires. For this study, a closed-ended questionnaire was created and distributed to employees of software development SMEs in Malaysia.

3.4.Research Approach

This study utilized a quantitative research design to explore the connections among the variables. The chosen research design was based on surveys. Because of the availability of data, quantitative research has taken precedence. More

crucially, current technological advancement and social changes, it offers interesting novel research possibilities [209].

In this study, the deductive approach was employed, wherein investigators start with general theories and assume specific concepts from the observations gathered towards the conclusion. The most common perspective of the nature of theory and research is deductive reasoning. The deductive method is utilized to build a framework based on existing literature, aiming to address the research gap. The theory is the starting point for the deductive process, and hypotheses are developed from the theory. The hypothesis testing research technique is related to deductive reasoning [210].

Data is collected after formulating hypotheses based on the theory, followed by analysis. The discussions in deductive reasoning proceed from principles to specific cases. However, this method is best suited for producing quantitative data from big samples. According to Holden and Lynch, a deductive method can help in removing uncertainty during research [211], Therefore, a deductive method is most appropriate because this study relies on previous researches in the field and employs a conceptual model established from the literature review. The overall research approach adopted for this research is presented in Table 3.1.

Table 3.1: Overall Research Approach the Study

Strategy	**Quantitative/Survey**
Research Philosophy	Positivism
Research Approach	Quantitative /Deductive Approach
Time Horizon	Cross-Sectional setting
Data Collection	Survey (self-administrated questionnaire)

Sampling Strategy	Non-Probability Sampling
Data Analysis	Multi-Analytical Approach using SEM-ANN

3.5.Research Design of this Study

A systematic strategy specifying how a research study will be conducted. It includes the entire approach for gathering and analyzing the data to answer research questions or hypotheses. A well-designed research study helps to guarantee that the data acquired is reliable, valid, and appropriate to the objectives of the research. It gives an essential long-term plan to support and guide the researcher [206] and [212].

The primary goal of research is to recognize the factors that affect cybersecurity behaviour among employees in software development SMEs. This proposed research used a quantitative approach to test hypotheses and model the relationship between various factors, such as knowledge sharing, attitudes, subjective norms, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived value, cyber trust, personality traits, and intention. Questionnaire which closed-ended is designed and modified from prior research and pre-tested to determine its validity and reliability. A self-administered questionnaire was used to collect data from employees of software development SMEs form the five state of Malaysia (i.e., Selangor, Kuala Lumpur, Johor, Perak, and Penang). The researcher employed Smart-PLS and the latest version of SPSS software for data analysis.

3.6.Sampling Strategy

This research study employed the non-probability sampling approach. This sampling approach does not give equal chances for each sample element [213]. Because of COVID-19 [214], the majority of legitimate responses were readily

acquired by sending an electronic questionnaire to individuals whose e-mail addresses were accessible, as well as other alternative sources such as friends, colleagues, and relatives/officials residing in areas. The specifics of the study's sampling are elaborated below.

3.6.1. Targeted Population

According to the SME Corp. Malaysia (2021), Malaysia has 1226494 SMEs; corresponding with this report, 16% are medium, 19.8% are small, and 78.6% are micro-organizations [77]. This study select five states of Malaysia namely Selangor, Kuala Lumpur, Johor, Perak, and Penang since they represent 61% of Malaysia's total number of SMEs. As a result, the software development SMEs in these five locations were the study's target population. The SME list was acquired from the Small and Medium Industries Development Corporation (SMIDEC) website of Malaysia (www.smidec.gov.my) [77]. Using this list, details of software development SMEs situated within these states were gathered. Table 3.2 displays the count of SMEs in Malaysian states.

Table 3.2: Number of SMEs in Malaysian States

S. No	States	No of SMEs	Percentage
1.	Selangor	179271	19.8
2.	Kuala Lumpur	133703	14.7
3.	Johor	98190	10.8
4.	Perak	75140	8.3
5.	Penang	66921	7.4
6.	Sarawak	61036	6.7
7.	Sabah	55702	6.2
8.	Kedah	48894	5.4
9.	Kelantan	46618	5.1
10.	Pahang	37573	4.1
11.	Negeri Sembilan	32721	3.6
12.	Malacca	31361	3.5
13.	Terengganu	29324	3.2
14.	Perlis	6808	0.8
15.	Labuan	2567	0.3
16.	Putrajaya	1236	0.1

3.6.2. Sampling Location and Sampling Frame

Malaysia has a total of sixteen states and the sampling location of this study comprises of software development SMEs located in the five states in of Malaysia, namely Selangor, Kuala Lumpur, Johor, Perak, Penang. The sampling for this investigation aligns with the target population that is employees of software development SMEs. This research specifically targets technical employees as respondents because they are directly involved in digital operations and are thus better positioned to recognize current cybercrimes and cybersecurity practices.

3.6.3. Sample Size

The sample size in a research study refers to the total number of participants involved. It is a subset of the larger population from which the researcher derives his or her conclusions [215]. It should be noted that sample size is an important part of the research methodology. In quantitative research, researchers frequently employ formulae that consider the desired level of confidence, margin of error, and population size [216]. A small sample size might provide statistically insignificant results, whereas a higher sample size produces more reliable results [212].

Various scholars have anticipated varying smallest sample sizes reliant on factors such as the study question, type of analysis, and the population under investigation. Beckett et al. (2017), for example, advised a sample size of between 200 and 400 participants for SEM [217], but author in [218] recommended a minimum of 200 responders for sophisticated SEM models. Meanwhile, researcher Harris proposed that the minimal sample size for robust

SEM be 200 in [219]. Author Hair et al. (2019), recommended that 100 respondents are the " minimum sample size" when using SEM [220]

.

The sample size in the current research was obtained using the Krejcie and Morgan (1970) formula, which is commonly employed for estimating sample size in limited populations [221].

According to the SME Corp. Malaysia (2021), there are 1226494 SMEs established in Malaysia, while the number of employees in SMEs are unknown [77]. A 95% confidence level and a 5% margin of error were utilized to compute the suitable sample size for this study, and population estimated size for Malaysian SMEs personnel was 1 million. The least sample size required by the Krejcie and Morgan formula was 384 [221].

Hence, the sample size of 529 is acceptable for present research. It fits the sample size criterion in determining the factors that motivate employees of Malaysian software development SMEs to practice cyber hygiene behaviour. The sample size allows for an accurate estimate and relevant statistical analysis. The researcher used the Krejcie and Morgan formula to guarantee that the sample size was acceptable for the finite population of employees of software development SMEs in Malaysia. Table 3.3 illustrates the sample size required for a confidence interval based on the population, calculated using Kreije and Morgan's (1970) formula.

Table 3.3: Sample Size in a Large Population

	Confidence Interval=95%			**Confidence Level=99%**		
	Margin of Error			**Margin of Error**		
Population size	5%	2.5%	1%	5%	2.5%	1%

100	80	94	99	87	96	99
500	217	377	475	285	421	485
1000	278	606	906	399	727	943
10000	370	1,332	4,899	622	2,098	6,239
100000	383	1,513	8,762	659	2,585	14,227
500000	384	1,532	9,423	663	2,640	16,055
1000000	384	1,534	9,512	663	2,647	16,317

Source: [221]

3.6.4. Sampling Technique

A sampling technique denotes to a method employed by researchers to choose a subgroup of persons or items from a larger population, enabling data collection and the drawing of conclusions about the population as a whole [222]. The selection of a sampling technique relies on factors such as the research inquiry, population attributes, resource availability, and the degree of representativeness required, all of which inform the chosen sampling approach. Researchers must carefully assess the strengths and limits of each technique to ensure that their selected approach matches their research aims and generates reliable outcomes [223].

This research employs a non-probability sampling method [224]. The rationale for employing this sampling method is twofold: in certain instances, the population lacks clear definition, and in some research contexts, making interpretations from the sample to the broader population is not necessary. Moreover, the population size is vast. To obtain a substantial sample size, the researcher needs to access ultimate respondents through acquaintances in a specific area. Another justification for is that it is non probability method of sampling and are more cost-effective and simpler to employ compared to alternative methods [225].

As the target population are Malaysian software development SMEs scattered across various geographical states. Therefore, select top five geographical states on frequency of available SMEs based on the SME Corp Malaysia (2021). The top five states with the highest number of SMEs were selected, namely Selangor, Kuala Lumpur , Johor, Perak, and Penang. These states were chosen because they cover a major share of the target population and provide a diversified sample of Malaysian SMEs. Following the selection of five geographical states, a list of all SMEs was generated, followed by identifying software development SMEs from those five geographical states.

Once the software development SMEs have been identified, the respondents (employees) from each software development SME must be identified to gather data. Convenience sampling is employed to identify respondents at this stage. The data was gathered during the COVID-19 pandemic, which needed physical distance measures; a convenience sample approach was utilized in this research to gather data from employees of software development SMEs. Convenient sampling is a non-probability strategy in which the participant is easily accessible to the researcher [223]. This sampling method is justified for situations where the population lacks clear definition or when there is limited understanding about the individuals involved. In such cases, researchers choose a convenient sample to ensure immediate access. Moreover, when dealing with a vast population, the researcher need to obtain a substantial sample size necessitates to reaching out with the help of friends in specific regions. Another justification is that non-probability convenient sampling methods are preferred for their cost-effectiveness and simplicity in comparison to other methods. [224].

A closed-ended questionnaire is being designed and disseminated among employees of Malaysian software development SMEs.

3.7.Time Horizon

In research, the time horizon states to the time span during which a research is carried out, or the precise time range within which data is gathered, analyzed, and evaluated. There are two basic time horizon options: longitudinal studies and cross-sectional studies [226]. A cross-sectional research is carried out at a particular moment in time to collect quantitative data and to identify the research variables and their relationships [227]. The longitudinal study, on the other hand, collects data over an extended period of time, allowing researchers to monitor changes and advancements in variables over time. Longitudinal studies provide insights into trends, patterns, and causal relationships that emerge and evolve over time [210].

This research employs a cross-sectional approach because it aims to examine the factors related with cyber hygiene behaviour among employees of software development SMEs at a specific point in time. Cross-sectional studies can provide insights faster than longitudinal research and are less expensive since they do not require lengthy data-collecting periods [209]. A cross-sectional time horizon facilitates the collection of organizational data, making it the best option for this study.

3.8.Research Instrument Development

Research instrument development is the systematic method of producing tools, instruments, or measurements that are used to gather data in a research study. These tools are intended to collect reliable, accurate, and valid data from

participants or sources related to the study's objectives. The construction of research instruments is a significant component in the research process since the quality of the instruments directly influences the quality and integrity of the collected data and the validity of research conclusions [209].

The researcher developed a questionnaire for this quantitative investigation to obtain data from actual respondents. The instrument was created in order to accomplish the objectives of this research.

3.8.1. Measurement Instrument

The instrument was divided into two sections: one for gathering demographic and background information from participants, and the other for assessing cyber hygiene behaviours among employees of software development SMEs. The instrument included a five-point Likert scale to evaluate cyber hygiene behaviors, ranging from 1 to 5 (from strongly disagree to strongly agree) [228].

3.8.2. Research Instrument

A closed-ended electronic questionnaire was developed centered on research's framework content to speed up the data gathering process. The final questionnaire contains 132 questions, with different items assessing each component. Each item's measurement was adapted from previous research to fit the context of cyber hygiene behaviour intention.

The questionnaire consisted of two sections. Section A included of eight questions, which gathered demographic material about the respondents, including gender, age, ethnicity, education level, occupation, and experience.

Part B measured respondents' perceptions of cyber hygiene behaviour-related factors using a five-point Likert scale (1– Strongly disagree; 2; Disagree;

3 –Neither Agree or Disagree; 4- Agree; 5 – Strongly Agree). The questionnaire underwent review by a panel of researchers with expertise in cyber hygiene behaviour, and modifications were implemented based on their feedback. The instrument underwent pilot testing with 45 participants from Software Development SMEs in Malaysia, revealing no significant issues. The scale demonstrated good reliability, with an overall Cronbach's alpha of 0.813. Demographic data collected from respondents are presented in Table 3.4.

Table 3.4: Demographic Questions of the Respondents

S.No	Measure	Items
1	Gender	
		Male
		Female
2	Age	
		21 to 30 years
		31 to 40 years
		41 to 50 years
		51 years to above
3	Ethnicity	
		Malay
		Chinese
		Indian
		Others
4	Education Level	
		Bachelors
		Postgraduate
		Diploma/Certification
5	Occupation	
		Software Developer
		Software Programmer
		Software Engineer
6	Software Development Experience	
		1-5 years
		6-10 Years
		11-15 Years

7	How frequently do you utilize third-party services (such as USB drives, smartphones, tablets, Dropbox, Google Docs) for storing or processing work-related documents? • I actively use different third-party services for work purposes. • I use third-party services from time to time for work purposes. • I seldom use third party services for work purposes. • I do not use any third-party services for work purposes.
8	How often do you bring your own device (BYOD) for storing or processing work related documents? • I actively bring my own device for work purposes. • I bring my own device from time to time for work purposes. • I seldom bring my own device for work purpose. • I do not bring my own device for work purposes.

The specifics of the variables and their corresponding items are provided and discussed in the subsequent sections below.

3.8.2.1. Knowledge Sharing Items

The first independent variable in this research towards cyber hygiene attitude is knowledge sharing. Five items in total were occupied from the research conducted by [83]. Table 3.5 shows the item labels and codes used in measuring the knowledge sharing variable. Each item is assessed on a 5-point Likert scale, ranging from strongly disagree to strongly agree.

Table 3.5: Measurement items for Knowledge Sharing

Dimension	Code	Measurement Items	Author
Knowledge Sharing	**KS 1**	Sharing knowledge within the organization holds significant value.	[83]
	KS 2	Sharing knowledge with colleagues within the organization is advantageous.	
	KS 3	I regularly share my knowledge at work to mitigate security risks.	

	KS 4	I believe knowledge sharing enhances my comprehension of the effectiveness of cybersecurity policies within my organization.
	KS 5	Sharing knowledge motivates me to adhere to cybersecurity policies and procedures.

3.8.2.2. Cyber Hygiene Attitude Items

People's ideas about any entity determine their attitude towards the behaviour, impacting their behavioural intention [69]. Cyber hygiene attitude measurement scale items are used to assess an individual's attitudes toward cyber hygiene behaviour. Cyber hygiene attitude is a second independent variable towards cyber hygiene intention. Table 3.6 displayed the items employed in this study were drawn from [119]; [135].

Table 3.6: Measurement items for Cyber Hygiene Attitude

Dimension	Code	Measurement Items	Author
Cyber Hygiene Attitude	**AT1**	Adhering to organizational cyber hygiene policies is crucial.	[119]; [135]
	AT2	Practicing cyber hygiene significantly reduces the risk of information security breaches.	
	AT3	Engaging in cyber hygiene is a prudent practice that minimizes the risk of information security incidents.	
	AT4	Demonstrating cyber hygiene behaviour is a valuable asset within the organization.	
	AT 5	Implementing cyber hygiene serves as a beneficial behavioural tool to protect the organization's information assets.	

3.8.2.3. Cyber Hygiene Subjective Norms Measurement Items

The scale items for measuring subjective norms in this study were borrowed from [83] and are displayed in Table 3.7. Subjective norms relate to the belief of others (relatives, close friends, coworkers, or business partners) toward a person when they act in a particular manner [120]. The subjective norm, the third independent variable, reflects individuals' inclination towards cyber hygiene when influenced by social considerations.

Table 3.7: Measurement items for Cyber Hygiene Subjective Norms

Dimension	Code	Measurement Items	Author
Subjective Norms	**SN1**	My colleagues think that we should share our cyber hygiene knowledge.	[83]
	SN2	The head of the department regards cyber hygiene as a cultural value.	
	SN3	Senior staff members in my company hold a positive perspective on cyber hygiene.	
	SN4	My office friends motivate me to share my cyber hygiene knowledge.	
	SN5	Both my family and friends encourage me to share knowledge about cyber hygiene.	

3.8.2.4. Cyber Hygiene Perceived Behavioural Control Measurement Items

Perceived behavioural control (PBC) correlates to a person's perspective of how simple or complicated it is to do a given task [171]. PBC is a fourth independent variable towards cyber hygiene intention. Table 3.8 outlined the PBC measurement scale utilized in this study comprises five items adapted from [83].

Table 3.8: Measurement items for Cyber Hygiene Perceived Behavioural Control

Dimension	Code	Measurement Items	Author
Perceived Behavioural Control	**PBC1**	I possess sufficient knowledge about cyber hygiene to educate other staff members.	[83], [229]
	PBC2	I am capable of sharing cyber hygiene knowledge to reduce the risk of cybersecurity breaches.	
	PBC3	Cyber hygiene tasks are straightforward and enjoyable for me.	
	PBC4	I have valuable resources to impart cyber hygiene knowledge to fellow employees.	
	PBC5	I refrain from sharing my personal information on social platforms.	

3.8.2.5. Threat Appraisal Measurement Items

The fifth independent variable of this research is threat appraisal. Measurement scale items for threat appraisal are used to assess a person's intention to engage in cyber hygiene behaviour. Table 3.9 showed a total of 7 items used in this were adapted from the study of [230].

Table 3.9: Measurement items for Threat Appraisal

Dimension	Code	Measurement Items	Author
Threat Appraisal	**TA 1**	Safeguarding my organization's information is crucial.	[230]
	TA 2	Security threats to my organization's information pose significant risks.	
	TA 3	I perceive cybersecurity attacks on my organization as detrimental.	
	TA 4	At work, unauthorized access to my confidential information is a grave concern for me.	
	TA 5	Data loss due to hacking deeply concerns me.	

	TA 6	I recognize that my organization could be at risk of security breaches if I do not follow its cyber hygiene policy.
	TA 7	I could be susceptible to malicious attacks if I neglect my organization's cyber hygiene policy.

3.8.2.6. Cyber Hygiene Knowledge Measurement Items

Cyber Hygiene Knowledge is the sixth independent variable of this study towards cyber hygiene intention, used to assess an individual's cyber hygiene behaviour. Seven items relating to cyber hygiene knowledge, adapted from [83] and are presented in Table 3.10.

Table 3.10: Measurement items for Cyber Hygiene Knowledge

Dimension	Code	Measurement Items	Author
Cyber Hygiene Knowledge	**CHK 1**	I am well-versed in the organization's cybersecurity policies and my duties to safeguard organizational resources.	[83]
	CHK 2	I comprehend the necessity of creating and using robust passwords.	
	CHK 3	I am knowledgeable about defending against 'social engineering,' 'phishing,' and 'cybercrime.'	
	CHK 4	I exercise caution to avoid discussing sensitive information in public spaces.	
	CHK 5	While browsing or downloading from the Internet, I exclusively visit trustworthy and reputable websites.	
	CHK 6	When downloading software, I adhere to all license and copyright regulations.	
	CHK 7	I exercise prudence when opening email attachments and clicking on links.	

3.8.2.7. Perceived Cyber Hygiene Value Measurement Items

Perceived cyber hygiene value is the seventh independent variable of this study, used to evaluate an individual's cyber hygiene behaviour. A total of five items used for perceived cyber hygiene value were adapted from Gratian et al. (2018) and are stated in Table 3.11.

Table 3.11: Measurement for Perceived Cyber Hygiene Value

Dimension	Code	Measurement Items	Author
Perceived Cyber Hygiene Value	**PCHV 1**	I am satisfied with the cybersecurity awareness campaign conducted in our organization.	(Gratian et. al, 2018)
	PCHV 2	Our organization has well-documented cybersecurity policies that are readily available if needed.	
	PCHV 3	The perceived level of cybersecurity service matches the ideal standard.	
	PCHV 4	I am pleased that cyber hygiene is a top priority for everyone in the organization.	
	PCHV 5	The perceived performance in cyber hygiene exceeds expectations.	

3.8.2.8. Cyber Trust Measurement Items

The eighth independent variable of this study is cyber trust, used to measure cyber hygiene behaviour of an individual. Table no 3.12 presented total of five items used for cyber trust were adapted from [83].

Table 3.12: Measurement items for Cyber Trust

Dimension	Code	Measurement Items	Author
Cyber Trust	**CT 1**	I trust in the reliability of my colleague's knowledge about cyber hygiene.	

CT 2	I have confidence in the effectiveness of my colleague's cyber hygiene knowledge.	[83]
CT 3	I believe my colleague's understanding of cyber hygiene reduces the risk of cybersecurity breaches.	
CT 4	I find my colleague's cyber hygiene knowledge valuable.	
CT 5	I trust that my colleagues would not misuse the cyber hygiene knowledge we share.	

3.8.2.9. Personality Traits Measurement Items

Personality traits manifest in the consistent patterns of thoughts, emotions, and actions displayed by individuals [84]. The ninth independent variable of this study personality traits towards cyber hygiene intention, used to assess an individual's cyber hygiene behaviour. A total of 50 items used for personality traits were adapted from the study of [231], [232] and are presented in Table 3.13.

Table 3.13: Measurement items for Personality Traits

Dimension	Code	Items	Author
Personality Traits	**PT 1**	I feel comfortable around people.	
(Extraversion)	**PT 2**	I make friends easily.	
	PT 3	I excel in handling social situations.	[231], [232]
	PT 4	I am the center of attention at gatherings.	
	PT 5	I know how to engage people.	
	PT 6	I am not very talkative.	

	PT 7	I prefer to stay in the background
	PT 8	I would describe my experiences as somewhat dull.
	PT 9	I don't like drawing attention to myself.
	PT 10	I am reserved in my speech.
(Agreeableness)	**PT 11**	I speak positively about others.
	PT 12	I believe in the good intentions of others.
	PT 13	I hold others in high regard.
	PT 14	I accept people as they are.
	PT 15	I put others at ease.
	PT 16	I have a sharp tongue.
	PT 17	I cut others to pieces.
	PT 18	I suspect hidden motives in others.
	PT 19	I get back at others.
	PT 20	I insult people.
(C**onscientiousness)**	**PT 21**	I am always prepared.
	PT 22	I pay attention to details.
	PT 23	I get chores done right away.
	PT 24	I carry out my plans.
	PT 25	I make plans and stick to them.
	PT 26	I waste my time.
	PT 27	I find it difficult to get down to work.
	PT 28	I do just enough work to get by.
	PT 29	I don't see things through.
	PT 30	I avoid my responsibilities.
(Neuroticism)	**PT 31**	I frequently feel sad.
	PT 32	I have a negative view of myself.
	PT 33	I often feel low.

	PT 34	I experience mood swings.
	PT 35	I easily become anxious.
	PT 36	I rarely get annoyed.
	PT 37	I seldom feel down.
	PT 38	I am comfortable with who I am.
	PT 39	I am not easily bothered by things.
	PT 40	I am content with myself.
(Openness to experience)	**PT 41**	I value the importance of art.
	PT 42	I have a vivid imagination.
	PT 43	I tend to vote for liberal candidates.
	PT 44	I carry the conversation to a higher level.
	PT 45	I enjoy hearing new ideas.
	PT 46	I am not interested in abstract ideas.
	PT 47	I do not like art.
	PT 48	I avoid philosophical discussions.
	PT 49	I do not enjoy going to art museums.
	PT 50	I tend to vote for conservative candidates.

3.8.2.10. Cyber Hygiene Intention Measurement Items

According to the theory of [145], intention is the mediating variable to cyber hygiene behaviour. Table no 3.14 stated behavioural intention items which are adopted from the study of [83].

Table 3.14: Measurement items for Cyber Hygiene Intention

Dimension	Code	Measurement Items	Author
	CH (Int) 1	I am intend to share my knowledge of cyber hygiene to minimize risks.	

Cyber Hygiene Intention	**CH(Int) 2**	I intend to share my cyber hygiene experiences with colleagues to enhance their awareness.	[83]
	CH(Int) 3	I will inform fellow staff about new methods and software that can mitigate cyber hygiene risks.	
	CH(Int) 4	I will share reports on cyber hygiene incidents with others to mitigate risks.	
	CH(Int) 5	I consistently review privacy settings to minimize cyber hygiene issues.	

3.8.2.11. Cyber Hygiene Behaviour Measurement Items

The degree to which a person's adopts various cybersecurity measures to protect themselves from specific cyber threats they are susceptible to. Cyber hygiene behavior, the dependent variable in this study, illustrates the real and consistent adoption of cyber hygiene practices by employees in software development SMEs. Thirty three items are adopted from the study of [117]. Those items are presented in table 3.15.

Table 3.15: Measurement items for Cyber Hygiene Behaviour

Dimension	Code	Measurement Items	Author
Cyber Hygiene Behaviour	**CHB 1**	I have installed anti-virus software, firewall, and anti-spyware on my computer.	[117]
	CHB 2	I consistently update the anti-virus software I have installed.	
	CHB 3	I become suspicious if my computer slows down significantly.	

CHB 4	I avoid downloading free anti-virus software from unknown sources.
CHB 5	I disable the anti-virus on my work computer to download information from websites.
CHB 6	I scan removable drives before using them on my personal computer.
CHB 7	I download data and materials from websites on my work computer without verifying their authenticity.
CHB 8	I bring my own USB to work to transfer data.
CHB 9	I create passwords that are not very complex, often using family names and birthdates.
CHB 10	I share passwords with friends and colleagues.
CHB 11	I use different passwords for various applications.
CHB 12	I include lowercase, uppercase, numbers, and special characters in my passwords.
CHB 13	I use passwords longer than 8 characters.
CHB 14	I rarely change my passwords.
CHB 15	I sometimes use the "Remember my password" option.

CHB 16	I occasionally write down passwords.
CHB 17	I do not use password hints to recover forgotten passwords.
CHB 18	I educate myself about phishing by reading materials on the topic.
CHB 19	I avoid providing confidential information in any type of email.
CHB 20	I do not open email attachments from strangers.
CHB 21	I avoid clicking hyperlinks in email messages.
CHB 22	I am cautious about email messages announcing contests/prizes.
CHB 23	I prefer typing URLs in a new browser rather than clicking hyperlinks.
CHB 24	I click on links contained in emails from trusted friends or colleagues.
CHB 25	I refrain from clicking links in unsolicited emails from unknown sources.
CHB 26	I do not establish trusted online relationships with strangers.
CHB 27	I ignore SMS messages announcing contests involving large sums of money.

CHB 28	I do not send personal information to strangers over the Internet.	
CHB 29	I do not enter payment information on websites lacking clear security information.	
CHB 30	I check URL spellings before any transactions.	
CHB 31	I never accept any amount of money for services offered by online sites.	
CHB 32	I am aware of and can identify the latest online scams.	
CHB 33	I do not accept parcels and gifts from Internet friends.	

3.9.Pretesting

Pre-testing is the preliminary evaluation of a questionnaire with a set of respondents to discover flaws in the questionnaire. It is a procedure that involves determining the validity and reliability of questionnaire items to verify that they effectively measure the defined variables [233].

Four expert in the field of cybersecurity were requested to review each item of the questionnaire to ensure that they properly measured the intended variables. The items were evaluated by the experts based on their knowledge and expertise. Experts offered helpful and valuable input on the questions' language, structure, and sequencing to ensure that they accurately assessed the relevant variables.

The instrument was also distributed to eight employees of software development SMEs in order to examine and analyze the clarity, relevance, and

ease of understanding of each item. Their input was also utilized to modify and improve the instrument to be clear and simple.

The feedback from experts and employees was utilized to enhance and improve the instrument in order to guarantee that it accurately measured the intended variables.

3.10. Pilot Study

Pilot testing assesses the reliability and validity of an instrument to determine its suitability for data collection. It helps researchers avoid misallocation of resources such as time, effort, and money by ensuring that the chosen approach is appropriate. Pilot testing is an efficient method for identifying any ambiguities or problems with the instrument [216] and [234]. The researchers can modify and improve the instrument's validity and accuracy by undertaking a small-scale rehearsal of actual data collection.

In this study, the researcher conducted a pilot survey by distributing an online questionnaire to employees of software development SMEs in Malaysia. To enhance the instrument's reliability, the present study conducted the pilot testing on 45 respondents, which is a larger sample size than the minimum recommended by author [235]. The respondents were employees of software development SME of Malaysia.

3.11. Reliability of the Instrument

The tests of reliability and validity play an essential role in determining the quality of research. The reliability of the measurement is concerned with consistency, whereas the validation process is concerned with finding the extent to which theory support the interpretations of test scores anticipated by the suggested use of tests.

As defined by Sekaran and Bougie, Cronbach's alpha is a test for inter-item consistency that quantifies the internal consistency of items in a scale or survey [236], [237]. According to Krejcie and Morgans, the minimum acceptable range for Cronbach's alpha is 0.6 [221].

Table 3.16: Case Processing Summary

		N	%	N of Items
Cases	Valid	45	100.0	
	Excluded	0	.0	
	Total	45	100.0	132

Note. Listwise deletion based on all variables in the process.

The data obtained from the participants during the pilot study phase was analyzed using IBM-SPSS software. This analysis included conducting internal consistency tests and Cronbach's alpha tests. A total of 45 cases were processed using SPSS-Version-22-0, as illustrated in Table 3.16. The resulting Cronbach's alpha values for the variables are presented in Table 3.17. These values serve as evidence that the measurement items employed in this study exhibit reliability. These outcomes substantiate that the questionnaire maintains internal consistency and is suitable for gauging the constructs of interest within the study. In summary, table 3.17 present the total reliability of alpha was 0.8570.

Table 3.17: Pilot-testing Results of Reliability

Variables	Cronbach's Alpha
Cyber Hygiene Attitude	**0.813**
Cyber Hygiene Behaviour	**0.783**
Cyber Hygiene Knowledge	**0.888**
Cyber Hygiene Perceived Behavioural Control	**0.853**
Cyber Trust	**0.844**
Cyber Hygiene Intention	**0.884**
Knowledge Sharing	**0.863**
Perceived Cyber Hygiene Value	**0.796**
Personality Traits	**0.927**
Cyber Hygiene Subjective Norm	**0.84**
Threat appraisal	**0.871**
Total	**8.570**

Note. Pilot testing results of study using SPSS.

3.11.1. Validity of the Instrument

Validity plays a pivotal role in the development of research instruments as it measures how accurately the instrument captures the intended concept [238]. In this study, validity is evaluated through three commonly employed approaches: content, convergent, and discriminant validity. To guarantee content validity, research instrument undergoes a meticulous examination by experts in the respective field.

Convergent validity scrutinizes whether the research instrument correlates with other measurements of the same construct [239]. This is determined by assessing the factor loadings within each dimension via factor analysis. Confirmatory factor analysis is a frequently employed technique for assessing

convergent validity. Farrell (2009) has advocated for factor loading as a means to establish convergent validity [240].

In contrast, discriminant validity pertains to how distinct latent variables' measurements remain unique from one another [241]. This is achieved by analyzing the correlations between the measurements and other variables using correlation analysis. Analysis of correlation is observe the discriminant validity of each component have been utilized in the study of [242].

The researcher has employed content, convergent, and discriminant validity to appraise the validity of the developed research instrument. The outcomes of these evaluations are presented in Chapter 4.

3.12. Data Collection

This research adopts the primary data gathering approach, involving the use of a structured questionnaire to gather data. Ensuring the accuracy and reliability of collected data is a critical step in any research endeavor. To obtain primary data, the study first identified the target population, which consists of employees working in software development SMEs.

For this research, a questionnaire specifically designed for the study was employed to gather data. The initially paper-based closed-ended questionnaire has been transformed into a digital format using Google Forms. This digital questionnaire was then distributed using a convenient sample among employees working in software development SMEs located in the top five states in Malaysia with the highest concentration of such SMEs: Selangor, Kuala Lumpur, Johor, Perak, and Penang.

Stringent measures were implemented throughout the data gathering process to guarantee the integrity and reliability of data. The resulting sample size proved to be substantial, enabling a robust and comprehensive analysis.

3.13. Data Screening

This study conducted data screening to examine for missing data, outliers, and potential errors that could impact the validity and reliability of the findings. Data screening is an important research step involving the examination and preparation of collected data for subsequent analysis. It provide assistance to researchers in detecting and resolving issues like missing values, outliers, inconsistencies, and errors that may compromise the validity and reliability of the analysis results [243]. Various approaches, including univariate, bivariate, and multivariate methods, were employed to detect outliers [244].

The collected data underwent screening using diverse techniques such as descriptive statistics, frequency distributions, and histograms. Missing data and outliers were identified and managed through imputation or removal. To enhance data accuracy, responses were cross-referenced with the original questionnaires, and any disparities were rectified. Additionally, the data was scrutinized for violations of assumptions necessary for statistical analysis, such as normality and homogeneity of variance.

3.14. Data Analysis

Data analysis is a critical phase in the research process. During this phase, responses to the questionnaire items were gathered and prepared for analysis. Quality checks were performed to ensure data accuracy. The data underwent screening, and outliers were eliminated to enhance reliability. Incomplete questionnaires were excluded from the analysis, and no missing values were

found in the dataset. Moreover, appropriate data analysis methods were chosen in accordance with the research objectives, and several measures were taken to ensure the validity and reliability of the data.

To examine and authenticate the suggested framework, a two-step multi-analytical strategy integrating Structural Equation Modeling (SEM) and Artificial Neural Network (ANN) analysis was utilized. SEM was utilized in the initial step, followed by ANN analysis in the subsequent step. Given the complexity of cyber hygiene behaviour adoption, it is significant to comprehend the factors that affect employees in software development SMEs to engage in cyber hygiene practices. SEM is a robust method for hypothesis testing and framework validation [245]. However, it simplifies decision-making complexities by relying on statistical modeling for linear relationships [246].

To achieve a balanced approach, the first step involved SEM analysis [247] to identify relationships among variables and test hypotheses that significantly influence employees' cyber hygiene behaviour. In the second step, ANN was employed to detect non-linear relationships and make more precise predictions than traditional regression techniques. The significant variables supported by SEM were used as inputs for the ANN analysis to predict factors influencing employees in software development SMEs more accurately. The Root Mean Square Error (RMSE) was used to evaluate the performance of the ANN model [248].

Notably, this study stands out as one of the first to integrate SEM and Artificial Neural Networks to uncover the precursors of cyber hygiene behaviour. Previous studies have predominantly relied on SEM alone for behaviour prediction.

The data collected from the participants was analyzed using descriptive and inferential statistics. Descriptive statistics, generated with Statistical Package for Social Science (SPSS) Version 28, offered an overview of the participants' profiles. Demographic characteristics were analyzed using descriptive statistics, enabling numerical comparisons of variables [249]. Demographic data were presented through frequency and percentage to quantify specific quantities. Mean and standard deviation of each construct within the data collection instrument were highlighted to describe central tendencies and data dispersion.

For hypothesis testing and data analysis, the SmartPLS 3.0 software was used for PLS-SEM, while SPSS 28 was employed for ANN analysis.

3.15. Summary

This chapter provides a complete description of the research methodology utilized in this research. The chapter begins by outlining the research philosophy, approach, and strategy employed for the investigation. Positivism serves as the chosen research philosophy, prioritizing objectivity, measurement, and observation. The research approach followed a deductive, while the research strategy involved conducting survey research..

Data collection involved administering an online survey, employing a convenience sampling approach. The survey instrument was thoroughly developed by drawing from items found in previously validated scales. The development process involved pre-testing and conducting a pilot investigation to improve quality of the questionnaire. Subsequently, collected survey data underwent coding and analysis. This chapter also provides a detailed explanation of the data analysis approaches used in the study. The chosen approach, a multi-analytical method known as SEM-ANN, was deemed the

most suitable for the data analysis process. This method was chosen because it can identify relationships between variables, test hypotheses, and uncover both linear and non-linear connections among the study's variables.

CHAPTER FOUR

DATA ANALYSIS AND RESULTS

4.1.Introduction

Findings and outcomes of data collection method are explained in this chapter. This section examines demographic information, PLS algorithms, and bootstrapping results using and SmartPLS and version 22.0 of SPSS to explore the effects of variables. This chapter provides the survey findings, reliability analysis, and path analysis results obtained from the SEM. The SEM outcomes were derived following data screening and validation of the relationships between the variables. PLS-SEM (Partial Least Square, Structural Equation Modelling) also covered the findings of the hypotheses and model fitness. The findings and their significance within the study context are thoroughly analyzed in this discussion. In the following section, the data was examined using the SEM-ANN approach, and the outcomes are detailed in this chapter. Lastly, a summary of the study's outcomes is provided.

4.2.Survey Findings

Data was gathered via an online survey consisting of 132 items designed within a conceptual framework to assess the cybersecurity behaviours of employees in software development SMEs. Demographic information was also gathered to enhance the understanding of the sample population.

4.2.1. Demographic Analysis

Comprehensive demographic data provided by participants, including information on gender, age, ethnicity, education level, occupation, and

professional background are presented in table 4.1 . Demographic data was also gathered to determine if a person was eligible to participate in the survey. It was also mentioned in a literature study that gender has an impact on cybersecurity behaviour. Male and female behaviour varies in various ways, and these gender changes can take many distinct forms [130], [195]. Significant gender and behavioural differences have been found in the research of Cain in [90]. He asserted that men possessed more knowledge about internet hygiene compared to women. In the case of Malaysia, 410 (77.50%) of the 529 respondents are men, and the remaining respondents are women.

Moreover, a significant portion of the respondents in the population sample fell within the 21–30 and 31-40 age brackets, constituting 55.95% (296) and 28.54% (151) of the participants, respectively. Research conducted by Ugwu presents descriptive insights into users' knowledge and practices related to cyber hygiene. It is widely acknowledged that age plays a role in the behaviours related to cyber hygiene [27].

Giving to the Malaysian Statistics Department (2021), over fifty percent of the nation's population belongs to the Malay ethnicity, resulting in the majority of respondents being Malay at 55.38%. Chinese respondents make up 24.19%, Indians account for 10.77%, and others represent 9.64% [77]. Table 4.1 shows that out of the total sample size of 529 respondents, 293 were Malaysian, and the remaining participants were foreign residents.

In terms of educational qualifications, Table 4.1 indicates that 68.80% (364) of the total sample population held a bachelor’s degree, 20.22% (107)

had completed their postgraduate studies, and 10.96% (58) possessed a diploma degree.

Regarding occupation, the report revealed that most respondents are software developers 27.41% followed by software programmers, software engineers and software designer with 22.11%, 16.44% and 12.09. The percentage for software requirement engineer was 8.5% and for software analyst it was 6.42%. Software tester with 4.15% whereas software project manager have percentage of 2.83%.

Most respondents have 1-5 years of experience in software development SME 54.25%, followed by 6-10 and 11-15 years with 28.54% and 8.88%, on the other hand respondents who have 16-20 years of experience was 5.29% and respondents from more than 20 years have 3.02%.

Regarding cyber hygiene behaviour question for third party services, 43.66 % respondents are actively using different third party services for storing or processing work related documents (for example: USB drives, smartphones, tablets, drop box, google docs) work purpose, 20.2 % use time to time third party services, respondents who uses seldom third party services were 19.09 %, whereas 17.01 respondents do not use any 3rd party services for work purpose. Respondents also asked about how often you bring you own device for storing or processing work related documents [250]. 56.89 % of respondents replied that they bring their own device for work purposes, 20.60 % of respondents bring time to time, 14.36 % seldom brin their own device whereas 8.12 % respondents do not bring their devices for work purpose.

Overall, the respondents' demographics illustrates that sample is diverse and representative of the Malaysian population, with comparable distributions across a range of demographic factors.

Table 4.1: Demographic Results

S.No	Measure	Items	Percentage	Frequency
1	Gender			
		Male	77.50	410
		Female	22.49	119
2	Age			
		21-30 years	55.95	296
		31-40 years	28.54	151
		41-50 years	10.01	53
		51 years to above	5.48	29
3	Ethnicity			
		Malay	55.38	293
		Chinese	24.19	128
		Indian	10.77	57
		Others	9.64	51
4	Education Level			
		Bachelors	68.80	364
		Postgraduate	20.22	107
		Diploma/Certification	10.96	58
5	Occupation			
		Software Developer	27.41	145
		Software Programmer	22.11	117
		Software Engineer	16.44	87
		Software Designer	12.09	64
		Software Requirement Engineer	8.5	45
		Software Analyst	6.42	34
		Software Tester	4.15	22
		Software Project ınager	2.83	15
6	Software Development Experience			
		1-5 years	54.25	287
		6-10 Years	28.54	151
		11-15 Years	8.88	47

		16-20 Years	5.29	28
		More than 20 Years	3.02	16
7	How frequently do you utilize third-party services (such as USB drives, smartphones, tablets, Dropbox, Google Docs) for storing or processing work-related documents?	I actively use different third-party services for work purposes.	43.66	231
		I use third-party services from time to time for work purpose.	20.22	106
		I seldom use third party services for work purposes.	19.09	101
		I do not use any third-party services for work purposes.	17.01	90
8	How often do you bring your own device (BYOD) for storing or processing work related documents?	I actively bring my own device for work purposes.	56.89	301
		I bring my own device from time to time for work purposes.	20.60	109
		I seldom bring my own device for work purpose.	14.36	76
		I do not bring my own device for work purposes.	8.12	43

4.2.2. Response rate

The survey's data were gathered from Malaysian software development SMEs. The survey form was distributed online. The study only included questionnaires that were fully completed.

In this research, 720 questionnaires were distributed, and 552 respondents met the qualifications to participate, constituting an acceptable sample size for the study. Twenty three survey questions were deleted because the respondents didn't fit the requirements. After these outliers were eliminated, 529 survey

questions were discovered to be full and included in the survey for analysis. The response rate is displayed in table 4.2.

Table 4.2: Survey Response Rate

Surveys	Frequency	Percentage
Distributed	720	100%
Returned	552	76.66 %
Useable	529	73.47

4.3.Measurement Model Analysis

The measurement model is important in confirming validity and reliability of the questionnaire used in research to assess intended constructs. This analysis aids researchers in assessing how closely indicators or items matches the latent variables or underlying construct they are trying to measure. It assists researchers in improving both the accuracy and reliability of their measuring techniques [139]. It is essential to meet this fundamental premise for the correct use of structural models for hypothesis testing since it ensures the consistency and applicability of both the data and the data-gathering tool [251].

Several tests, including composite reliability, convergent and discriminant validity, R square, and model fitness of the research model, are used to develop a viable measurement model.

This investigation employed partial least squares structural equation modeling (PLS-SEM) analysis methods to assess the relationships among variables and to provide more advanced and contemporary approaches [121]. The data analysis conducted by SmartPLS comprises Cronbach's alpha is greater than 0.70, composite reliability CR is greater than 0.70,and average

variance extracted AVE greater than 0.50, and the structural consequence of the model to confirm the hypotheses [221] and [246].

As per Hair et al. (2013), Smart PLS is utilized in two main stages: confirmatory factor and path analysis. These phases are employed to explore measurement models and structural models, aiming to comprehend the value and associations between the aspects [242].

The analysis model is employed in this work is shown in Figure 4.1, and its validity and reliability were determined using the tests stated above. Therefore, assessing the model supports in gauging the quality standards of constructs, starting with an investigation of the factor loadings and proceeding to assess construct reliability and validity.

4.3.1. Construct Reliability

A statistical measure called construct reliability, also known as internal consistency reliability, is employed in research and measurement to evaluate the dependability and consistency of a latent construct that is measured by several items inside a measurement instrument, like a questionnaire or survey. It assesses to what extent various items or questions consistently measure the same underlying notion [238].

Cronbach's alpha and composite reliability are commonly employed statistical metrics for assessing the reliability of constructs. It is widely used measure of internal consistency and is considered an indicator of scale reliability. The overall amount of variance compared to the total scale variance is represented by composite reliability, which assesses the internal consistency of scale items alike to Cronbach's alpha [220].

If each construct meets or exceeds the threshold value of 0.70, the measurement model is deemed to have adequate internal consistency. As per Hair et al. (2014), the composite reliability should be 0.70 or above [242]. Table 4.3 presents the results of Cronbach's alpha and composite reliability in the current study. According to the PLS Algorithm test results, all hypotheses encounter the cutoff values of 0.70 for Cronbach-Alpha and CR [241].

The variables, i.e., cyber hygiene attitude, cyber hygiene intention, perceived behavioural control, subjective norm, cyber hygiene behaviour, cyber hygiene knowledge, cyber trust, knowledge sharing, perceived cyber hygiene value (PCHV), personality traits, and threat appraisal have values with 0.878, 0.911, 0.929, 0.947, 0.980, 0.906, 0.926, 0.918, 0.935, 0.993, and 0.889 respectively. Similarly, the (CR) are also affirmative that is 0.885, 0.912, 0.930, 0.949, 0.981, 0.908, 0.929, 0.921, 0.901, 0.993, and 0.890 respectively. The measurement model is internally consistent and reliable, as demonstrated in the table below. Thus, it may be inferred that construct reliability has been achieved for the current investigation.

Table 4.3: Reliability and Construct Validity

Constructs	Cronbach's Alpha	Composite Reliability
CH Attitude	0.878	0.885
CH Intention	0.911	0.912
CH PBC	0.929	0.930
CH SN	0.947	0.949
CH Behaviour	0.980	0.981
CH Knowledge	0.906	0.908
Cyber Trust	0.926	0.929
Knowledge Sharing	0.918	0.921
PCHV	0.935	0.901
Personality Traits	0.993	0.993
Threat Appraisal	0.889	0.890

** Note: CH = Cyber Hygiene*

4.3.2. Construct Validity

The construct validity is an essential aspect of measuring instrument development and evaluation. It describes the degree to which a measuring tool (such as a test, questionnaire, or scale) properly evaluates the particular construct. In short, construct validity measures whether the instrument measures the intended outcomes [220].

Researchers frequently use tests like convergent and discriminant validity to determine construct validity. If several construct indicators are assessing the same underlying concept, the construct is said to have convergent validity. On the contrary, discriminant validity evaluates if the construct of the model are unique from one another and does not evaluate the similar underlying construct [238].

4.3.2.1.Convergent Validity (Average Variance Extracted AVE)

Convergent validity, a subset of construct validity, used in measurement and research to evaluate how well results of measuring instrument correlate with those scores from other instruments or measures that are conceptually connected to the same construct. Convergent validity offers empirical proof that a measurement tool is capturing a particular construct in a way that is in line with accepted theories and prior studies [220]. It increases the instrument overall validity by demonstrating that it generates results that associate with what is expected for the targeted construct. The average variance extracted (AVE) is a commonly employed metric for assessing convergent validity. It quantifies the proportion of shared variance among latent constructs relative to measurement error. AVE values are between 0 and 1, with higher values showing greater convergent validity [252]. Authors Hair et. al (2014) and Fornell and Larcker

(1981), provided that an AVE of 0.50 or higher is satisfactory [246] and [253]. Table 4.4 shows AVE for all latent, i.e., cyber hygiene attitude, cyber hygiene intention, perceived behavioural control, subjective norm, cyber hygiene behaviour, cyber hygiene knowledge, cyber trust, knowledge sharing, PCHV, personality traits, and threat appraisal, display the robust values of AVE that is 0.734, 0.738, 0.778, 0.825, 0.616, 0.681, 0.772, 0.754, 0.882, 0.745, and 0.603. The AVE results indicate that items within each construct converge, with values exceeding 0.50 for all constructs. Thus, the convergent validity is deemed acceptable.

Table 4.4: Convergent Validity (AVE)

Constructs	Average Variance Extracted
CH Attitude	0.734
CH Intention	0.738
CH PBC	0.778
CH SN	0.825
CH Behaviour	0.616
CH Knowledge	0.681
Cyber Trust	0.772
Knowledge Sharing	0.754
PCHV	0.882
Personality Traits	0.745
Threat Appraisal	0.603

** Note: CH = Cyber Hygiene*

4.3.2.2.Discriminant Validity

The goal of discriminant validity is to show that the measuring instrument is able to differentiate between the construct it is intended to assess and other constructs that are conceptually or theoretically distinct. Discriminant validity must be established for the instrument to give different and useful evaluations of desired construct [241].

Discriminant validity underscores the importance of ensuring a reflective construct maintains a meaningful relationship with its items in the PLS model noted by [246].

Researchers often utilize the Fornell-Larcker criteria and the heterotrait-monotrait ratio (HTMT) to evaluate discriminant validity. The Fornell and Larcker criteria are commonly employed for this purpose, examining whether each construct evaluates a distinct phenomenon from others in the research. The heterotrait-monotrait ratio can also determine if constructs are distinct and measure different phenomena from each other [19]. Discriminant validity, which is required to determine a relationship between variables, is shown in Table 4.5. Diagonal values are positive for all latent variables.

i. ***The Fornell-Larcker criterion***

It is the shared variance between two constructs is less than the variance of each individual construct. [241]. Fornell and Larcker's (1981) criterion defines a ratio utilized to estimate the discriminant validity of a construct, indicating it is achieved when the square root of the Average Variance Extracted (AVE) is higher than its correlation with all other constructs [253]. The results of the Fornell-Larcker criteria, presented in Table 4.5, indicate that discriminant validity is achieved when the square root of the AVE for each construct (highlighted) exceeds the inter-construct correlations. (Tolah et al., 2021).

ii. The Heterotrait Monotrait Criterion (HTMT)

The HTMT ratio estimates the degree to which the correlation between two construct is stronger than the correlation with itself [241]. An HTMT ratio of less than 0.85 is a frequently employed criterion for discriminant validity [218]. If the HTMT value is less than one, it indicates that there is a difference in

correlation between the two constructs. Findings of the HTMT ratio are shown in Table 4.6, and the values below the cutoff of 0.85 demonstrating that discriminant validity has also been attained.

Table 4.5: Fornell and Larcker Criterion (Discriminant Validity)

Constructs	AT	CH(Int)	CH(PBC)	CH(SN)	CHB	CHK	CT	KS	PCHV	PT	TA
AT	**0.857**										
CH(Int)	0.337	**0.859**									
CH(PBC)	0.326	0.583	**0.882**								
CH(SN)	0.416	0.678	0.738	**0.908**							
CHB	0.379	0.877	0.622	0.736	**0.785**						
CHK	0.479	0.725	0.567	0.726	0.803	**0.825**					
CT	0.313	0.852	0.564	0.683	0.887	0.709	**0.878**				
KS	0.460	0.725	0.562	0.696	0.799	0.898	0.706	**0.868**			
PCHV	0.412	0.098	0.074	0.197	0.127	0.178	0.172	0.188	**0.939**		
PT	0.337	0.812	0.609	0.689	0.877	0.730	0.798	0.745	0.146	**0.863**	
TA	0.295	0.705	0.556	0.614	0.708	0.714	0.645	0.727	0.162	0.697	**0.776**

Note. AT=Attitude, CH(Int)= Cyber Hygiene Intention, CH(PBC)= Cyber Hygiene Perceived Behavioural Control, CH(SN)= Cyber Hygiene Subjective Norms, CHB= Cyber Hygiene Behaviour, CHK= Cyber Hygiene Knowledge, CT= Cyber Trust, KS= Knowledge Sharing, PCHV= Perceived Cyber Hygiene Value, PT= Personality Traits, TA= Threat Appraisal.

Table 4.6: HTMT Criterion (Discriminant Validity)

Constructs	AT	CH(Int)	CH(PBC)	CH(SN)	CHB	CHK	CT	KS	PCHV	PT	TA
AT											
CH(Int)	0.369										
CH(PBC)	0.357	0.632									
CH(SN)	0.452	0.727	0.788								
CHB	0.402	0.926	0.649	0.761							
CHK	0.532	0.797	0.618	0.783	0.852						
CT	0.336	0.920	0.604	0.723	0.927	0.770					
KS	0.503	0.792	0.605	0.744	0.842	0.831	0.761				
PCHV	0.457	0.099	0.078	0.206	0.125	0.189	0.182	0.195			
PT	0.357	0.856	0.634	0.712	0.892	0.773	0.832	0.782	0.145		
TA	0.326	0.782	0.609	0.664	0.752	0.792	0.702	0.799	0.170	0.739	

Note. AT=Attitude, CH(Int)= Cyber Hygiene Intention, CH(PBC)= Cyber Hygiene Perceived Behavioural Control, CH(SN)= Cyber Hygiene Subjective Norms, CHB= Cyber Hygiene Behaviour, CHK= Cyber Hygiene Knowledge, CT= Cyber Trust, KS= Knowledge Sharing, PCHV= Perceived Cyber Hygiene Value, PT= Personality Traits, TA= Threat Appraisal.

4.3.2.3.Cross Loading

Cross-loadings are a concept employed in factor analysis, to concurrently estimate the association between several latent factors and observed variables. Cross loadings show the strength and direction of the linear relationships between each latent factor and each observable variable. It comprises indicators that illustrate why latent variables are loaded within their own construct rather than others and the extent of their relationship with each other [220]. Therefore, discriminant validity can be achieved through cross-loading analysis. A measurement model is considered reliable when each loading of item evaluations exceed 0.5–0.7 [246]. All values are crucial at 0.5, ranging from a minimum of 0.7 to a maximum of 0.927. Table 4.7 detailed the cross loading of all loadings.

Table 4.7: Cross Loadings

	AT	CH(Int)	CH(PBC)	CH(SN)	CHB(	CHK	CT	KS	PCHV	PT	TA
AT1	**0.771**	0.320	0.310	0.350	0.363	0.440	0.294	0.423	0.211	0.367	0.285
AT3	**0.923**	0.312	0.294	0.381	0.342	0.426	0.292	0.422	0.438	0.302	0.266
AT4	**0.885**	0.281	0.260	0.378	0.321	0.400	0.269	0.386	0.380	0.256	0.244
AT5	**0.839**	0.221	0.235	0.301	0.252	0.357	0.198	0.321	0.395	0.200	0.199
CH(Int)1	0.322	**0.882**	0.517	0.609	0.804	0.655	0.820	0.646	0.086	0.706	0.586
CH(Int)2	0.335	**0.863**	0.492	0.574	0.772	0.631	0.796	0.628	0.103	0.693	0.548
CH(Int)3	0.307	**0.849**	0.529	0.614	0.754	0.642	0.740	0.649	0.103	0.673	0.579
CH(Int)4	0.251	**0.863**	0.497	0.562	0.720	0.586	0.660	0.585	0.060	0.700	0.668
CH(Int)5	0.226	**0.838**	0.470	0.550	0.714	0.597	0.634	0.604	0.065	0.715	0.653

CH(PBC)1	0.330	0.465	**0.879**	0.660	0.514	0.509	0.466	0.481	0.097	0.512	0.458
CH(PBC)2	0.281	0.521	**0.895**	0.664	0.566	0.483	0.503	0.507	0.056	0.549	0.512
CH(PBC)3	0.256	0.511	**0.864**	0.589	0.536	0.434	0.500	0.429	0.030	0.506	0.447
CH(PBC)4	0.277	0.511	**0.897**	0.665	0.534	0.525	0.486	0.499	0.053	0.533	0.508
CH(PBC)5	0.295	0.556	**0.873**	0.675	0.584	0.546	0.527	0.557	0.092	0.579	0.520
CH(SN)1	0.372	0.564	0.682	**0.882**	0.599	0.600	0.547	0.577	0.169	0.566	0.510
CH(SN)2	0.388	0.608	0.677	**0.925**	0.677	0.664	0.626	0.635	0.178	0.629	0.562
CH(SN)3	0.385	0.642	0.666	**0.935**	0.706	0.683	0.664	0.667	0.190	0.670	0.569
CH(SN)4	0.382	0.598	0.673	**0.900**	0.655	0.656	0.615	0.633	0.182	0.621	0.566
CH(SN)5	0.364	0.658	0.660	**0.898**	0.696	0.689	0.641	0.643	0.175	0.639	0.574
CHB(Online scm1)	0.245	0.731	0.557	0.618	**0.801**	0.645	0.715	0.660	0.082	0.735	0.643
CHB(Online scm2)	0.223	0.710	0.557	0.582	**0.792**	0.613	0.673	0.612	0.016	0.722	0.602
CHB(Online scm3)	0.235	0.708	0.567	0.603	**0.796**	0.622	0.705	0.614	0.083	0.712	0.573
CHB(Online scm4)	0.193	0.681	0.545	0.601	**0.781**	0.611	0.709	0.618	0.075	0.702	0.588
CHB(Online scm5)	0.289	0.655	0.465	0.544	**0.762**	0.597	0.677	0.587	0.078	0.674	0.450
CHB(Online scm6)	0.262	0.643	0.426	0.496	**0.740**	0.560	0.639	0.539	0.064	0.646	0.420
CHB(Online scm7)	0.325	0.645	0.464	0.555	**0.773**	0.612	0.653	0.595	0.107	0.667	0.458
CHB(Online scm8)	0.265	0.657	0.446	0.541	**0.758**	0.595	0.666	0.566	0.087	0.683	0.470
CHB(Psd1)	0.212	0.688	0.433	0.540	**0.772**	0.585	0.677	0.580	0.041	0.675	0.516
CHB(Psd2)	0.200	0.668	0.403	0.500	**0.768**	0.556	0.690	0.549	0.048	0.651	0.503
CHB(Psd3)	0.325	0.712	0.466	0.571	**0.799**	0.642	0.743	0.653	0.097	0.683	0.571
CHB(Psd4)	0.357	0.655	0.472	0.590	**0.779**	0.685	0.682	0.659	0.144	0.678	0.538
CHB(Psd5)	0.297	0.696	0.505	0.589	**0.824**	0.620	0.719	0.613	0.131	0.707	0.516
CHB(Psd6)	0.283	0.696	0.500	0.591	**0.826**	0.604	0.715	0.594	0.106	0.705	0.509
CHB(Psd7)	0.214	0.681	0.466	0.550	**0.789**	0.562	0.724	0.574	0.078	0.685	0.505

CHB(Psd8)	0.309	0.706	0.466	0.574	**0.801**	0.676	0.725	0.663	0.102	0.690	0.544
CHB(Psd9)	0.377	0.718	0.506	0.620	**0.828**	0.681	0.730	0.708	0.126	0.688	0.586
CHB(Pshing1)	0.392	0.685	0.536	0.631	**0.803**	0.685	0.705	0.707	0.161	0.672	0.533
CHB(Pshing2)	0.344	0.696	0.469	0.591	**0.810**	0.674	0.710	0.691	0.126	0.704	0.572
CHB(Pshing3)	0.408	0.723	0.531	0.640	**0.818**	0.699	0.749	0.686	0.171	0.706	0.589
CHB(Pshing4)	0.461	0.729	0.553	0.645	**0.807**	0.702	0.715	0.714	0.164	0.705	0.640
CHB(Pshing5)	0.425	0.721	0.511	0.644	**0.816**	0.697	0.757	0.674	0.155	0.696	0.591
CHB(Pshing6)	0.404	0.717	0.524	0.640	**0.816**	0.709	0.741	0.694	0.173	0.686	0.606
CHB(Pshing7)	0.388	0.696	0.533	0.667	**0.796**	0.698	0.733	0.689	0.145	0.693	0.617
CHB(Pshing8)	0.245	0.726	0.563	0.592	**0.796**	0.616	0.686	0.612	0.065	0.708	0.612
CHB(ml1)	0.452	0.651	0.483	0.624	**0.778**	0.715	0.694	0.716	0.129	0.704	0.593
CHB(ml2)	0.270	0.668	0.453	0.580	**0.764**	0.606	0.679	0.611	0.099	0.681	0.511
CHB(ml3)	0.239	0.638	0.407	0.491	**0.745**	0.552	0.653	0.566	0.087	0.670	0.497
CHB(ml4)	0.225	0.639	0.438	0.475	**0.725**	0.561	0.609	0.549	0.025	0.676	0.549
CHB(ml5)	0.233	0.635	0.454	0.526	**0.747**	0.611	0.659	0.596	0.101	0.648	0.572
CHB(ml6)	0.238	0.607	0.445	0.484	**0.692**	0.538	0.601	0.546	0.084	0.651	0.509
CHB(ml7)	0.254	0.718	0.460	0.568	**0.788**	0.634	0.688	0.629	0.069	0.671	0.672
CHB(ml8)	0.213	0.778	0.465	0.545	**0.784**	0.601	0.720	0.600	0.050	0.718	0.618
CHK1	0.353	0.547	0.450	0.538	0.597	**0.741**	0.547	0.627	0.140	0.545	0.560
CHK2	0.413	0.595	0.475	0.628	0.645	**0.790**	0.582	0.657	0.202	0.579	0.517
CHK3	0.399	0.572	0.426	0.566	0.647	**0.814**	0.559	0.691	0.196	0.605	0.587
CHK5	0.380	0.615	0.458	0.601	0.691	**0.849**	0.605	0.783	0.118	0.627	0.622
CHK6	0.409	0.625	0.502	0.642	0.693	**0.873**	0.621	0.813	0.119	0.623	0.620
CHK7	0.415	0.631	0.496	0.616	0.697	**0.876**	0.597	0.859	0.114	0.630	0.627
CT1	0.235	0.694	0.454	0.556	0.743	0.566	**0.885**	0.571	0.177	0.681	0.538

CT2	0.217	0.704	0.468	0.564	0.746	0.556	**0.887**	0.549	0.150	0.667	0.508
CT3	0.231	0.709	0.472	0.558	0.762	0.603	**0.876**	0.611	0.200	0.698	0.556
CT4	0.337	0.810	0.538	0.651	0.816	0.671	**0.871**	0.673	0.113	0.733	0.599
CT5	0.336	0.807	0.533	0.654	0.816	0.698	**0.874**	0.680	0.123	0.716	0.617
KS1	0.382	0.644	0.482	0.591	0.702	0.808	0.603	**0.882**	0.146	0.656	0.617
KS2	0.360	0.604	0.434	0.574	0.664	0.778	0.589	**0.866**	0.152	0.600	0.643
KS3	0.388	0.613	0.463	0.599	0.697	0.731	0.624	**0.797**	0.177	0.639	0.547
KS4	0.438	0.644	0.529	0.623	0.702	0.814	0.620	**0.885**	0.142	0.670	0.674
KS5	0.419	0.640	0.521	0.628	0.701	0.767	0.627	**0.907**	0.199	0.662	0.669
PCHV3	0.362	0.072	0.052	0.145	0.085	0.122	0.141	0.129	**0.929**	0.099	0.110
PCHV4	0.390	0.068	0.074	0.198	0.100	0.167	0.152	0.168	**0.926**	0.120	0.156
PCHV5	0.404	0.118	0.078	0.204	0.152	0.197	0.181	0.213	**0.962**	0.173	0.177
PT1	0.265	0.734	0.563	0.602	0.798	0.658	0.721	0.657	0.108	**0.919**	0.654
PT10	0.246	0.717	0.517	0.592	0.768	0.633	0.707	0.634	0.127	**0.910**	0.609
PT11	0.273	0.715	0.527	0.610	0.780	0.644	0.711	0.663	0.117	**0.921**	0.619
PT12	0.291	0.741	0.578	0.645	0.800	0.675	0.724	0.676	0.117	**0.916**	0.641
PT13	0.295	0.710	0.545	0.595	0.774	0.634	0.718	0.645	0.146	**0.909**	0.587
PT14	0.265	0.702	0.527	0.591	0.748	0.618	0.694	0.623	0.116	**0.906**	0.589
PT15	0.288	0.719	0.531	0.600	0.771	0.632	0.713	0.643	0.127	**0.920**	0.606
PT16	0.295	0.737	0.550	0.614	0.795	0.652	0.734	0.666	0.129	**0.929**	0.636
PT17	0.296	0.758	0.543	0.620	0.808	0.691	0.731	0.694	0.107	**0.929**	0.656
PT18	0.275	0.739	0.555	0.628	0.787	0.674	0.722	0.682	0.110	**0.916**	0.652
PT19	0.297	0.728	0.521	0.595	0.783	0.646	0.711	0.662	0.142	**0.916**	0.609
PT2	0.276	0.747	0.585	0.642	0.795	0.675	0.731	0.667	0.110	**0.909**	0.688
PT20	0.320	0.733	0.552	0.610	0.782	0.667	0.717	0.679	0.156	**0.916**	0.649

PT21	0.274	0.751	0.574	0.643	0.816	0.670	0.739	0.682	0.112	**0.927**	0.653
PT22	0.291	0.717	0.527	0.601	0.786	0.624	0.712	0.647	0.132	**0.908**	0.608
PT23	0.264	0.738	0.574	0.638	0.812	0.660	0.741	0.670	0.129	**0.928**	0.636
PT24	0.273	0.720	0.541	0.632	0.787	0.648	0.708	0.668	0.105	**0.914**	0.621
PT25	0.292	0.725	0.552	0.601	0.804	0.651	0.734	0.673	0.139	**0.926**	0.638
PT26	0.299	0.708	0.554	0.616	0.782	0.653	0.703	0.671	0.136	**0.913**	0.622
PT27	0.306	0.710	0.551	0.608	0.779	0.641	0.707	0.665	0.149	**0.922**	0.642
PT28	0.286	0.704	0.539	0.602	0.770	0.624	0.705	0.639	0.121	**0.918**	0.606
PT29	0.251	0.733	0.518	0.598	0.776	0.628	0.704	0.649	0.086	**0.894**	0.626
PT3	0.293	0.741	0.564	0.623	0.802	0.673	0.727	0.682	0.132	**0.913**	0.675
PT30	0.259	0.667	0.529	0.581	0.746	0.600	0.667	0.623	0.103	**0.867**	0.577
PT31	0.262	0.679	0.498	0.549	0.732	0.601	0.662	0.610	0.109	**0.884**	0.587
PT32	0.254	0.682	0.511	0.568	0.744	0.604	0.654	0.617	0.091	**0.880**	0.579
PT33	0.239	0.613	0.407	0.447	0.603	0.486	0.520	0.510	0.084	**0.723**	0.516
PT34	0.292	0.743	0.563	0.628	0.789	0.667	0.724	0.675	0.131	**0.918**	0.670
PT35	0.338	0.731	0.587	0.645	0.809	0.670	0.732	0.681	0.169	**0.917**	0.665
PT36	0.280	0.721	0.548	0.611	0.776	0.656	0.716	0.667	0.134	**0.917**	0.638
PT37	0.314	0.715	0.536	0.607	0.792	0.656	0.710	0.670	0.140	**0.921**	0.644
PT38	0.358	0.593	0.449	0.567	0.634	0.562	0.596	0.579	0.166	**0.637**	0.473
PT39	0.353	0.597	0.444	0.532	0.642	0.547	0.594	0.581	0.174	**0.618**	0.500
PT4	0.292	0.707	0.559	0.602	0.763	0.634	0.690	0.631	0.118	**0.903**	0.598
PT40	0.352	0.576	0.422	0.519	0.626	0.543	0.565	0.574	0.151	**0.613**	0.470
PT41	0.335	0.595	0.473	0.537	0.672	0.582	0.607	0.600	0.142	**0.668**	0.491
PT42	0.342	0.568	0.452	0.504	0.629	0.546	0.578	0.558	0.120	**0.635**	0.420
PT43	0.362	0.599	0.453	0.555	0.681	0.598	0.619	0.615	0.118	**0.650**	0.470

PT44	0.339	0.609	0.461	0.548	0.675	0.581	0.607	0.585	0.146	**0.665**	0.486
PT45	0.324	0.613	0.478	0.537	0.644	0.533	0.592	0.570	0.097	**0.631**	0.449
PT46	0.315	0.724	0.532	0.610	0.789	0.667	0.715	0.665	0.166	**0.894**	0.640
PT47	0.253	0.693	0.497	0.580	0.732	0.597	0.664	0.609	0.087	**0.851**	0.568
PT48	0.258	0.631	0.417	0.500	0.642	0.519	0.566	0.525	0.122	**0.728**	0.513
PT49	0.272	0.724	0.533	0.603	0.772	0.614	0.697	0.643	0.125	**0.896**	0.614
PT5	0.335	0.721	0.576	0.641	0.795	0.667	0.716	0.674	0.146	**0.919**	0.658
PT50	0.217	0.649	0.413	0.536	0.660	0.548	0.590	0.562	0.100	**0.718**	0.542
PT6	0.283	0.746	0.566	0.628	0.802	0.679	0.739	0.684	0.134	**0.931**	0.657
PT7	0.283	0.761	0.534	0.629	0.811	0.686	0.758	0.693	0.100	**0.923**	0.642
PT8	0.291	0.742	0.568	0.636	0.803	0.663	0.750	0.689	0.155	**0.924**	0.649
PT9	0.305	0.743	0.558	0.646	0.803	0.691	0.728	0.698	0.152	**0.924**	0.652
TA1	0.372	0.568	0.431	0.558	0.617	0.688	0.538	0.815	0.168	0.567	**0.676**
TA2	0.199	0.570	0.431	0.465	0.582	0.507	0.542	0.539	0.150	0.600	**0.786**
TA3	0.297	0.573	0.419	0.488	0.570	0.595	0.522	0.575	0.197	0.578	**0.831**
TA4	0.169	0.528	0.484	0.467	0.499	0.503	0.468	0.511	0.107	0.525	**0.809**
TA5	0.160	0.554	0.414	0.492	0.560	0.539	0.507	0.487	0.081	0.525	**0.759**
TA6	0.198	0.472	0.392	0.381	0.452	0.491	0.403	0.474	0.089	0.448	**0.773**
TA7	0.194	0.543	0.440	0.459	0.538	0.533	0.497	0.522	0.075	0.519	**0.790**

Note. AT=Attitude, CH(Int)= Cyber Hygiene Intention, CH(PBC)= Cyber Hygiene Perceived Behavioural Control, CH(SN)= Cyber Hygiene Subjective Norms, CHB= Cyber Hygiene Behaviour, CHK= Cyber Hygiene Knowledge, CT= Cyber Trust, KS= Knowledge Sharing, PCHV= Perceived Cyber Hygiene Value, PT= Personality Traits, TA= Threat Appraisal.

4.3.2.4.Factor Loading

Factor loadings is a statistical approach used in research and measurement to evaluates a set of observable variables (indicators or items) and the relationship between latent factors or constructs [254]. They aid in the analysis and comprehension of complicated datasets by assisting researchers in determining which variables are most closely associated with each factor while offering insightful information about the underlying structure of the data [240]. In this study, none of the items had a factorloading below 0.50, meeting the recommended threshold as suggested by Hair et al. (2019) [220]. This indicates the reliability and validity of all indicators as representations of the construct, confirming a strong connection between each indicator and the fundamental factor. Furthermore, none of the items were eliminated based on factor loading. Table 4.8 presented the factor loading values for all indicators.

Table 4.8: Factor Loadings

	AT	CH(Int)	CH(PBC)	CH(SN)	CHB(	CHK	CT	KS	PCHV	PT	TA
AT1	0.771										
AT3	0.923										
AT4	0.885										
AT5	0.839										
CH(Int)1		0.882									
CH(Int)2		0.863									
CH(Int)3		0.849									

CH(Int)4	0.863			
CH(Int)5	0.838			
CH(PBC)1		0.879		
CH(PBC)2		0.895		
CH(PBC)3		0.864		
CH(PBC)4		0.897		
CH(PBC)5		0.873		
CH(SN)1			0.882	
CH(SN)2			0.925	
CH(SN)3			0.935	
CH(SN)4			0.900	
CH(SN)5			0.898	
CHB(Online scm1)				0.801
CHB(Online scm2)				0.792
CHB(Online scm3)				0.796
CHB(Online scm4)				0.781
CHB(Online scm5)				0.762
CHB(Online scm6)				0.740
CHB(Online scm7)				0.773
CHB(Online scm8)				0.758
CHB(Psd1)				0.772
CHB(Psd2)				0.768
CHB(Psd3)				0.799
CHB(Psd4)				0.779
CHB(Psd5)				0.824

CHB(Psd6)	0.826	
CHB(Psd7)	0.789	
CHB(Psd8)	0.801	
CHB(Psd9)	0.828	
CHB(Pshing1)	0.803	
CHB(Pshing2)	0.810	
CHB(Pshing3)	0.818	
CHB(Pshing4)	0.807	
CHB(Pshing5)	0.816	
CHB(Pshing6)	0.816	
CHB(Pshing7)	0.796	
CHB(Pshing8)	0.796	
CHB(ml1)	0.778	
CHB(ml2)	0.764	
CHB(ml3)	0.745	
CHB(ml4)	0.725	
CHB(ml5)	0.747	
CHB(ml6)	0.692	
CHB(ml7)	0.788	
CHB(ml8)	0.784	
CHK1		0.741
CHK2		0.790
CHK3		0.814
CHK5		0.849
CHK6		0.873

CHK7	0.876				
CT1		0.885			
CT2		0.887			
CT3		0.876			
CT4		0.871			
CT5		0.874			
KS1			0.882		
KS2			0.866		
KS3			0.797		
KS4			0.885		
KS5			0.907		
PCHV3				0.929	
PCHV4				0.926	
PCHV5				0.962	
PT1					0.919
PT10					0.910
PT11					0.921
PT12					0.916
PT13					0.909
PT14					0.906
PT15					0.920
PT16					0.929
PT17					0.929
PT18					0.916
PT19					0.916

PT2	0.909
PT20	0.916
PT21	0.927
PT22	0.908
PT23	0.928
PT24	0.914
PT25	0.926
PT26	0.913
PT27	0.922
PT28	0.918
PT29	0.894
PT3	0.913
PT30	0.867
PT31	0.884
PT32	0.880
PT33	0.723
PT34	0.918
PT35	0.917
PT36	0.917
PT37	0.921
PT38	0.637
PT39	0.618
PT4	0.903
PT40	0.613
PT41	0.668

PT42	0.635	
PT43	0.650	
PT44	0.665	
PT45	0.631	
PT46	0.894	
PT47	0.851	
PT48	0.728	
PT49	0.896	
PT5	0.919	
PT50	0.718	
PT6	0.931	
PT7	0.923	
PT8	0.924	
PT9	0.924	
TA1		0.676
TA2		0.786
TA3		0.831
TA4		0.809
TA5		0.759
TA6		0.773
TA7		0.790

Note. AT=Attitude, CH(Int)= Cyber Hygiene Intention, CH(PBC)= Cyber Hygiene Perceived Behavioural Control, CH(SN)= Cyber Hygiene Subjective Norms, CHB= Cyber Hygiene Behaviour, CHK= Cyber Hygiene Knowledge, CT= Cyber Trust, KS= Knowledge Sharing, PCHV= Perceived Cyber Hygiene Value, PT= Personality Traits, TA= Threat Appraisal

4.3.2.5.Explanation of Variance

In quantitative research, the explanation of variance is essential. It describes the variability within the data values and is crucial for determining its quality. Higher variance rates are often preferable before hypothesis testing, since good predictions need high-quality data evaluated through variance,.

Akossou and Palm suggest that the R-squared value indicates the extent to which independent variables account for variability [255]. R-squared represents the proportion of variation in the dependent variable explained by the independent variable. A higher R-squared value signifies a stronger relationship between the independent and dependent variables and the capacity to explain a larger portion of the variance.

As presented in table 4.9, the model in this study attained satisfactory statistics of R-squared of all endogenic variables, surpassing the threshold value of 0.10 [256]. The research reveals an R-squared value of 0.770 for CHB, indicating that 77% of the variance in CHB can be explained by AT, CH(PBC), CH(SN), CHK, KA, PCHV, CT, PT, and TA. Whereas other endogenous variables, such as AT and CH(Int), have (R2) values of 0.211 and 0.799. Therefore, it can be concluded that the current study has sufficiently explained the variance, and the data are suitable for further hypothesis testing.

Table 4.9 Values of R square

Constructs	R Square	R Square Adjusted
AT	0.211	0.210
CH(Int)	0.799	0.796
CHB	0.770	0.769

4.3.2.6.Model Fitness

Evaluation of the model fitness for any research project is important since it helps to establish if the information gathered, and the instruments utilized to gather the information are appropriate for further analysis. Degree to which the hypothesis on the regression line matches the data gathered through surveys is known as model fitness [256].

There are several statistical and mathematical procedures available to evaluate model fitness. The Standardized Root Mean Square Residual (SRMR) statistical test was employed in the present research to evaluate the model's fitness. One of the most popular model fitness tests PLS-SEM researchers use is SRMR.

It may establish the global fitness of a research model in PLS and prevent model misspecification [246]. According to Hwang and Lee (2016) SRMR is the root mean square difference among observed and model correlations [183]. Hong & Furnell (2019) stated that PLS is better suited with an SRMR value of less than 0.08 [140]. The model in this study matches the data, as shown by the SRMR of 0.050 (<0.08). The results of the SRMR are presented in Table 4.9. This indicates that the information gathered, and the instrument utilized in this study are appropriate for further analysis and hypothesis testing.

Table 4.10 The Model Fitness

	Saturated Model	Estimated Model
SRMR	0.050	0.078

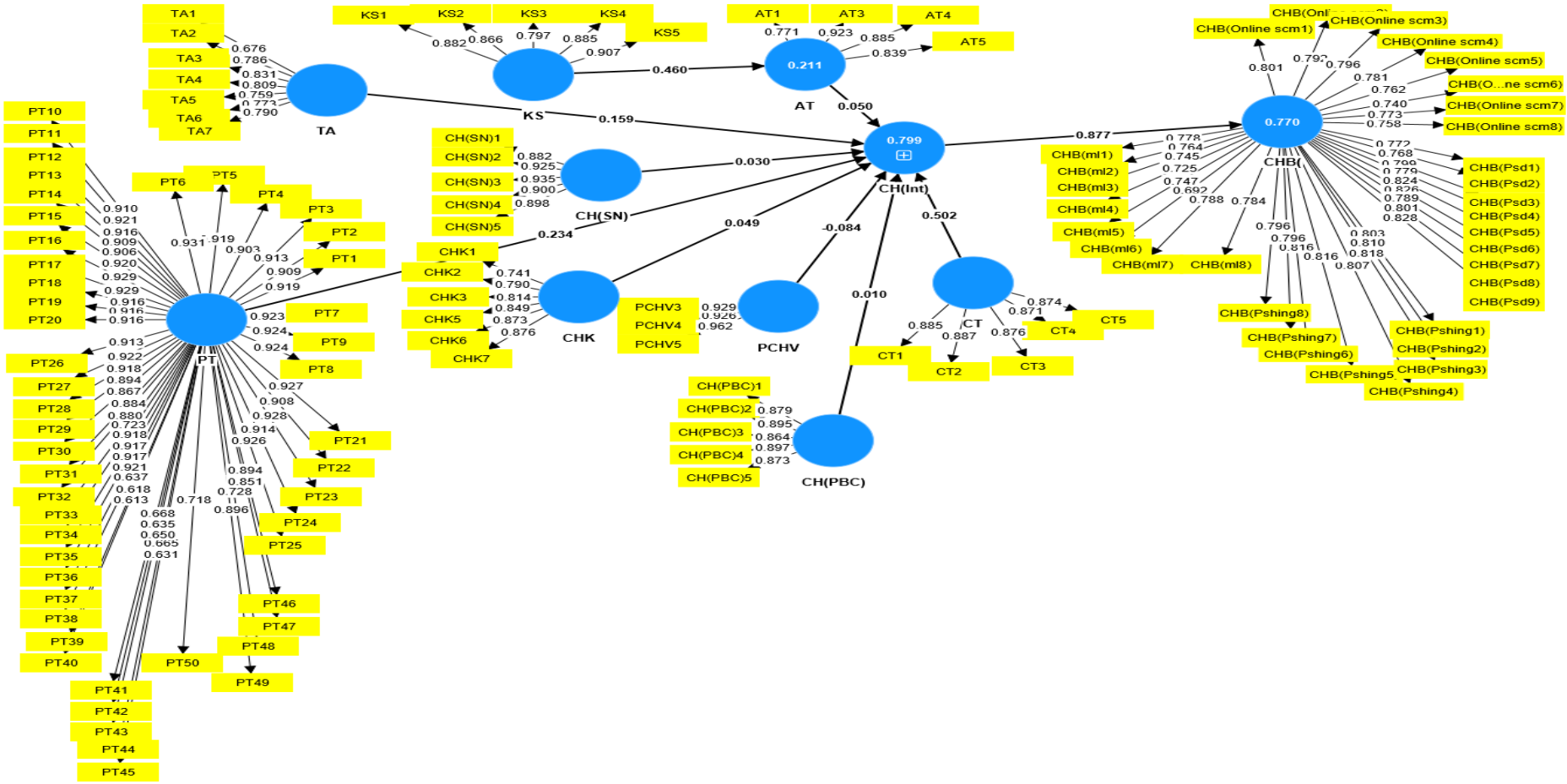

Figure 4.1 Structural Equation Modeling (PLS Algorithm)

4.4.The Structural Model

The Structural model is used to explain and examine the associations between variables. It offers a theoretical illustration of how several elements or variables interact and have an impact with one another.

A highly efficient method for examining the relationship between variables and determining if the data supports the hypothesis is structural equation modeling (SEM) [257]. When SEM examines the conceptual model and analyses the association among the variables, it is regarded as a reliable evaluation [147].

To validate the proposed hypotheses, the subsequent step in structuralequation modeling entails assessing the hypothesized relationships.

4.4.1. Hypotheses Testing

A statistical technique referred to as hypothesis testing is used in the study and analysis of data to make decisions or infer correlations between variables or population based on sample data.

T-statistics are utilized to evaluate hypotheses. Hypotheses are considered as accepted if the t-statistics result exceeds or equals the threshold of 1.96 [220].

The study produced several ideas on the influence of various factors on cyber hygiene behaviour. To ascertain the importance of the findings, statistical analysis was utilized to evaluate the hypotheses, including computing path coefficients, and performing t-tests. Table no 4.12 presented results hypothesis indicating value of t and beta coefficients.

Study found that knowledge sharing, attitude, threat appraisal, perceived cyber hygiene behaviour, cyber trust and personality traits are engaging employees into cyber hygiene intention and provides a holistic view in

contributing to the cyber hygiene behaviour. On the other hand, variable subjective norm, perceived behavioural control and cyber hygiene knowledge are not affecting the cyber hygiene intention to perform cyber hygiene behaviour.

H1. Knowledge sharing positively influences attitude to perform cyber hygiene intention.

The first hypothesis estimates that knowledge sharing positively impacts cyber hygiene attitude. The findings revealed that the path from knowledge sharing *(β =0.460, T=12.700, P value= 0.000)* positively and significantly impacted cyber hygiene attitude to perform cyber hygiene intention. Therefore, hypothesis one is **supported.**

H2. The CH attitude is significantly connected to the cyber hygiene intention.

The second hypothesis examines a positive cyber hygiene (CH) attitude has an effect on the intention to practice cyber hygiene. The consequences indicate that the path from the cyber hygiene attitude *(β =0.050, T=2.059, P value= 0.040)* significantly impacts cyber hygiene intention. Thus, the outcomes indicate that hypothesis two is **supported**.

H3. Subjective norms have a substantial influence on cyber hygiene intention.

In this study, a hypothesis was formulated suggesting that Subjective Norms positively and significantly influence cyber hygiene intention. However, the findings indicate that the subjective norm has a minimal and non-significant effect on cyber hygiene intention, with values of *(β = 0.030, T = 0.813, P value = 0.416)*. Hence, hypothesis three is **not supported.**

H4. Perceived behavioural control have a significant effect on cyber hygiene intention.

The present research developed a hypothesis that Perceived behavioural control has a positive and substantial impact on cyber hygiene intention. The hypothesis has been rejected based on the values *(β =0.010, T=0.326, P value= 0.744).* It is concluded that hypothesis four is **not supported.**

H5. The threat appraisal will have a positive influence on cyber hygiene intention.

The fifth hypothesis estimates that threat appraisal positively influences cyber hygiene intention. Results revealed that threat appraisal *(β =0.159, T=4.826, P value= 0.000)* positively and significantly affects cyber hygiene intention. Therefore, hypothesis five is **supported.**

H6. Cyber hygiene knowledge will have a positive influence towards cyber hygiene intention.

Hypothesis six estimates that the level of cyber hygiene knowledge significantly influences the intention to practice cyber hygiene. However, the findings revealed no substantial connection between cyber hygiene knowledge and intention to adopt cyber hygiene practices i.e., (*β =0.049, T=1.309, ρ=0.191*). Hence hypothesis six is **not supported.**

H7. Perceived cyber hygiene value will have a positive impact on the cyber hygiene intention.

Hypothesis seven assesses that cyber hygiene perceived value has a substantial and positive influence on cyber hygiene intention. The outcome also supported that cyber hygiene perceived value significantly impacts cyber

hygiene intention based on the values, i.e., (*β =-0.084, T=4.140, ρ = 0.000)*. Therefore, hypothesis seven is **supported.**

H8: Cyber trust will have a positive influence on cyber hygiene intention.

Hypotheses eight of this study evaluate that cyber trust positively and significantly impact cyber hygiene intention. The result revealed that cyber trust have a significant effect on cyber hygiene intention. As a result, the path from cyber trust based on the vales i.e., (*β =-0.502, T=12.603, ρ = 0.000)*. Therefore, hypothesis eight is **supported.**

H9. Personality traits have a positive impact on cyber hygiene intention.

Hypothesis nine estimates that personality traits have significant effect on cyber hygiene intention. The results showed that personality traits have positive and significant association with cyber hygiene intention with the values i.e., (*β =0.234, T=5.424, ρ=0.000*). Hence hypothesis nine **supported.**

H10. Cyber hygiene intention has a positive and substantial impact on CH behaviour.

Hypotheses ten of this research evaluate that cyber hygiene intention positively and significantly impact cyber hygiene (CH) behaviour. The result revealed that cyber hygiene intention have significant impact on cyber hygiene behaviour. As a result, the path from cyber hygiene intention values are (*β =-0.877, T=9.852 ρ = 0.000)*. Therefore, hypothesis ten is **supported.**

Table 4.11: Hypothesis Testing

HYPOTHESES		Path Coefficient	Sample mean (M)	T statistics	P values	Decision
H 1	(KS) -> (AT)	0.460	0.463	12.700	0.000	Supported

H 2	AT -> CH(Int)	0.050	0.048	2.059	0.040	Supported
H 3	CH(SN) -> CH(Int)	0.030	0.029	0.813	0.416	**Not Supported**
H 4	CH(PBC) -> CH(Int)	0.010	0.012	0.326	0.744	**Not Supported**
H 5	TA -> CH(Int)	0.159	0.160	4.826	0.000	Supported
H 6	CHK -> CH(Int)	0.049	0.051	1.309	0.191	**Not Supported**
H 7	PCHV -> CH(Int)	-0.084	-0.082	4.140	0.000	Supported
H 8	CT -> CH(Int)	0.502	0.497	12.603	0.000	Supported
H 9	PT -> CH(Int)	0.234	0.235	5.424	0.000	Supported
H 10	CH(Int) -> CHB	0.877	0.878	9.852	0.000	Supported

Note: KS= Knowledge Sharing, AT= Attitude, CH(INT)= Cyber Hygiene Intention, CH(SN)= Cyber Hygiene Subjective Norm, CH(PBC)= Cyber Hygiene Perceived Behavioural Control, TA= Threat Appraisal, CHK= Cyber Hygiene Knowledge, PCHV= Perceived Cyber Hygiene Value, CT= Cyber Trust, PT= Personality Traits, CHB= Cyber Hygiene Behaviour.

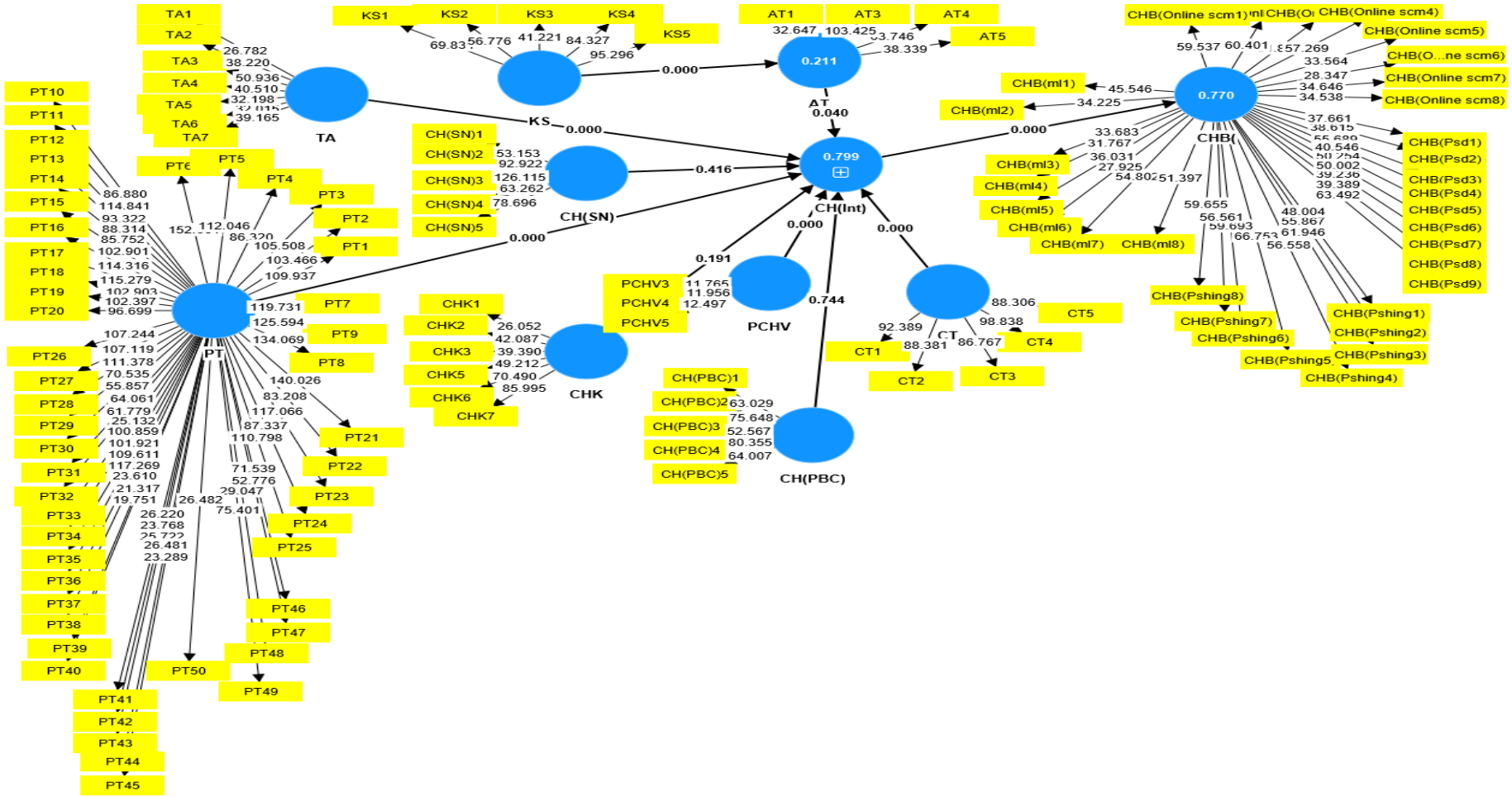

Figure 4.1 Structural Equation Modeling (Bootstrapping)

4.5.Analysis Results of Artificial Neural Network

This study takes a multidisciplinary approach by combining SEM with neural network analysis, which is considered as one of the key techniques for performing artificial intelligence. Complex decision-making processes can be streamlined by using a standard statistical technique like SEM, which can only detect linear associations [258]. A suggested artificial neural network model (ANN) that could imply nonlinear relationships. The adoption outcomes as well as linear and nonlinear correlations may be captured by the ANN algorithm. Additionally, the ANN can offer greater optimistic accuracy than linear models. Also, the ANN model is robust to noise, deviations, and use small-size samples [259].

As a result, this study uses a two-stage methodology similar to that of [258], Initially, SEM is utilized to evaluate the study model and find the substantial hypothesized predictors. Subsequently, these significant predictors serve as inputs for the neural network model to determine the relative significance of each predictor variable [260]. The feedback propagation multilayer perception (MLP) neural network, one of the utmost broadly used neural networks, was employed in this study. This network uses a neural network to transport signals from the input to the output layer. The data is subsequently saved in input and output on the network. The count of input neurons matches the quantity of independent predictors [261].

In contrast, depending on the neural network model, the output layer neurons are equal to the structure. Mehedintu and Soava (2022) stated that the quantity of neurons in the hidden layer significantly impacts the reliability of results. Results might be generalized if there are too many neurons, which could

lead to overload [262]. The neural network module for IBM's SPSS was used in this study for conducting ANN analysis.

4.5.1. ANN Model summary (Root mean Square Error (RMSE))

The ANN Model for cyber hygiene behaviours is graphically presented in fig. 4.3. For inputs and hidden layers, multilayer perceptron have been utilized [5]. Multiple learning cycles can reduce errors and enhance prediction accuracy. [263]. To boost efficiency, the ANN model's output is often conducted at grade [0, 1]. To mitigate the risk of overload, the neural network model underwent ten-fold cross-validation, partitioning the data into 90% for training and 10% for testing [264]. The sample size for testing and training (multilayer perceptron) is shown in Table 4.12.

This research used a ten-fold cross-validating approach and measured the root mean square of errors (RMSE) to avoid the risk of overfitting. For the purpose of evaluating the accuracy level attained by the model. Table 3 shows the model summary (Root Mean Square of Error (RMSE)) for all ten NN models for training and testing data sets. In Table 4.13, the RMSE average values for the training and testing processes are shown. These values are comparatively low (0.195 for training and 0.187 for testing), which demonstrates a high level of accuracy in predicting variability in cyber hygiene behaviour.

Table 4.12: Multilayer Perceptron (Sample Size for Training & Testing)

	Sample size (Training)(InT)	Sample size (Testing)(InT)	Total sample size
1	**467**	**62**	**529**
2	**475**	**54**	**529**
3	**469**	**60**	**529**
4	**464**	**65**	**529**

5	**471**	**58**	**529**
6	**475**	**54**	**529**
7	**470**	**59**	**529**
8	**478**	**51**	**529**
9	**470**	**59**	**529**
10	**475**	**54**	**529**

Note. InT= Intention

The graphical output of the model summary is shown in Figure 4.4, and it demonstrates that the root mean square errors for the ANN model are relatively small, which denotes a good model fit [258]. Therefore, this research confirms that there is an excellent model fit.

In conclusion, the statistical validation of the ANN model has been accomplished using the RMSE values. The findings imply that the models' input variables are reliable indicators of cyber hygiene behaviour.

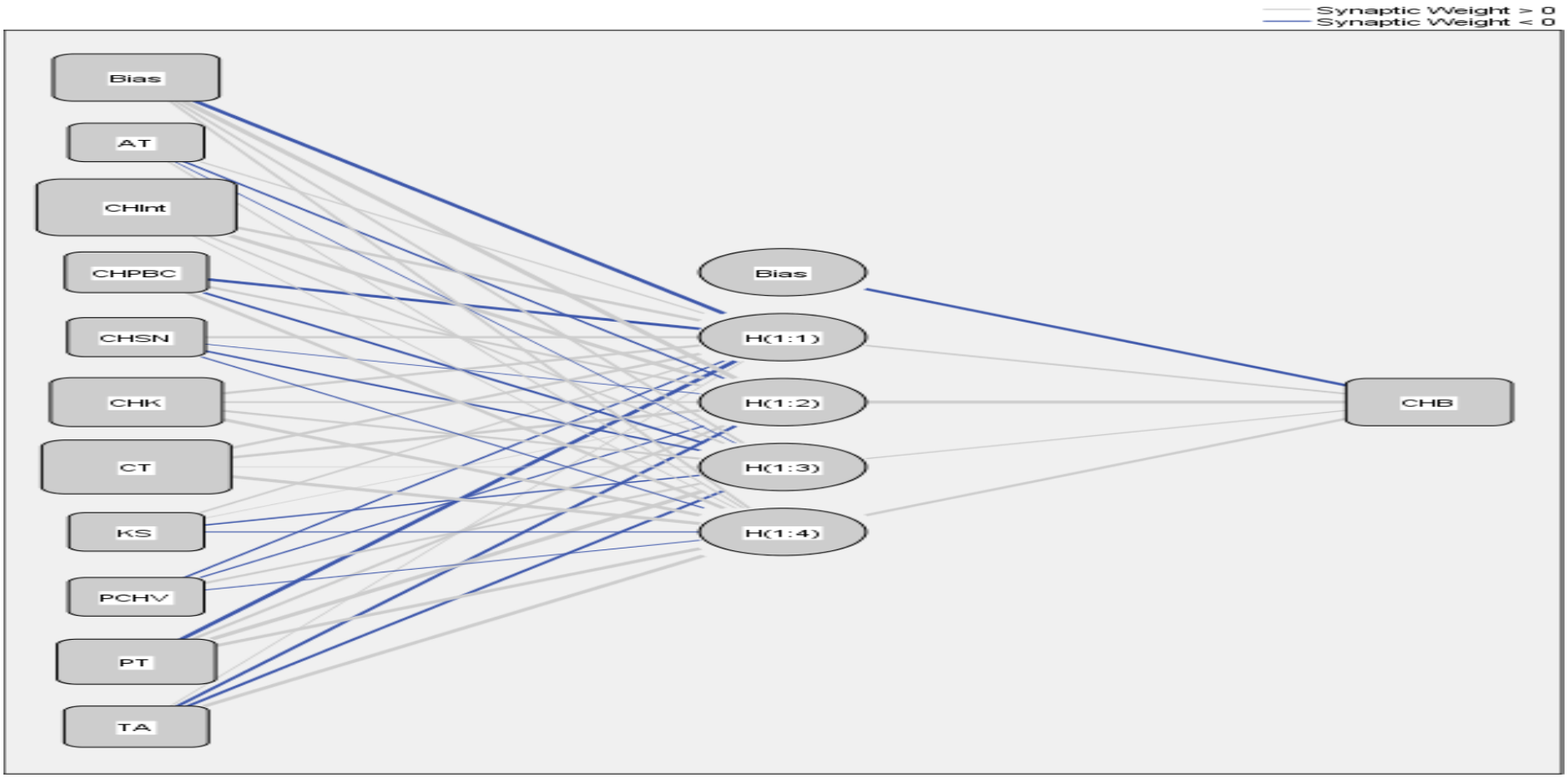

Figure 4.2 ANN Model - Cyber Hygiene Behaviour

Table 4.13: Model Summary (RMSE Values)

#	Sum of square error (Training) (InT)	Sum of square error (Testing) (InT)	RMSE (Training) (InT)	RMSE (Testing) (InT)	RMSE(Training)(InT)-RMSE (Testing) (InT)
1	17.412	2.409	0.193	0.197	0.004
2	18.049	1.862	0.195	0.186	0.009
3	20.424	1.639	0.209	0.165	0.043
4	16.124	1.575	0.186	0.156	0.031
5	15.528	1.622	0.182	0.167	0.014
6	21.495	2.102	0.213	0.197	0.015
7	19.907	2.053	0.206	0.187	0.019
8	18.237	1.958	0.195	0.196	0.001
9	16.691	2.644	0.188	0.212	0.023
10	16.012	2.245	0.184	0.204	0.020
Total Average	**17.988**	**2.011**	**0.195**	**0.187**	**0.008**
Standard deviation	**2.039**	**.354**	**0.011**	**0.018**	**0.008**

Note. RMSE= Root Mean Square Error, InT= Intention

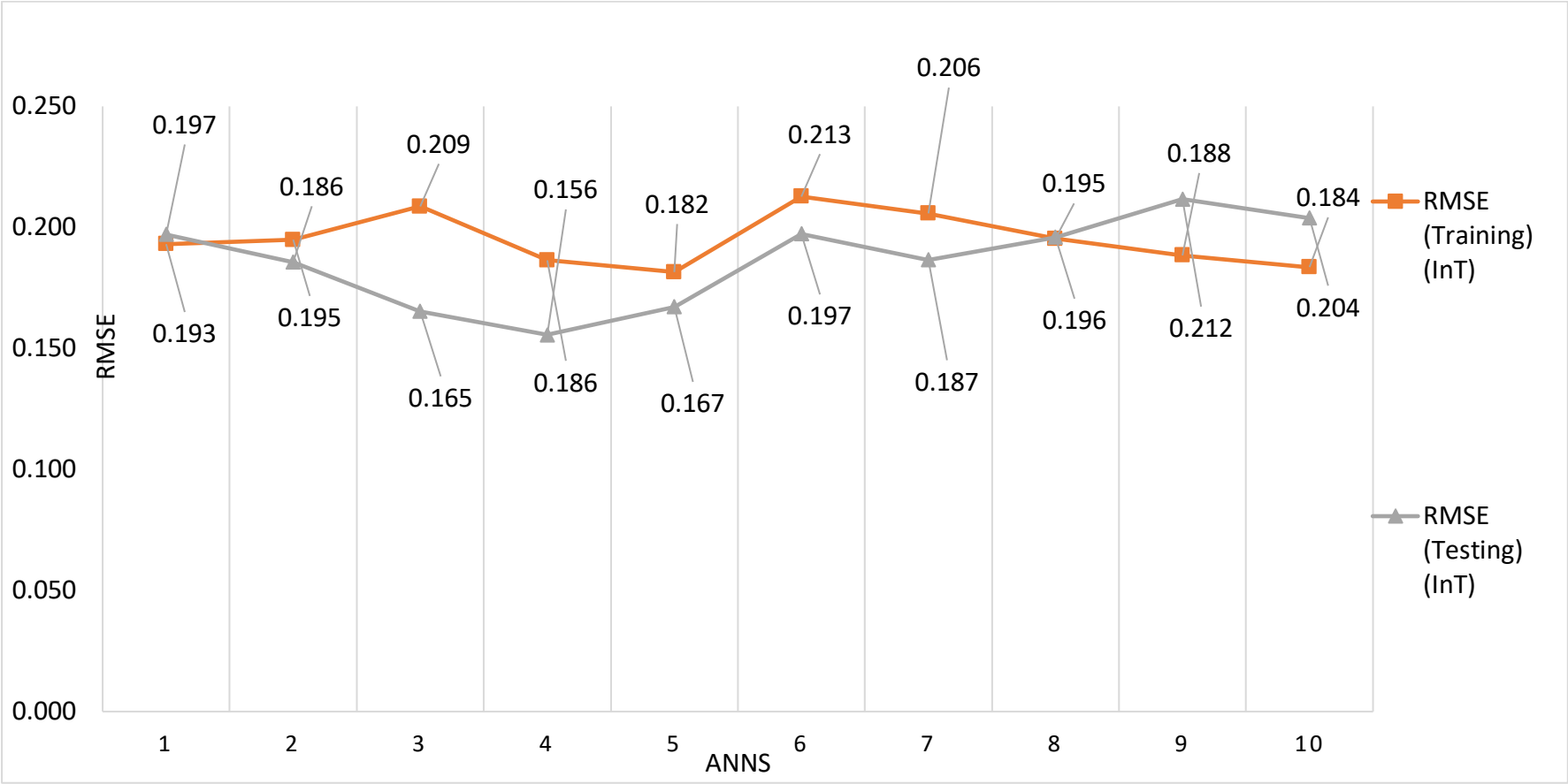

Figure 4.3 Graphical Output of Model Summary

4.5.2. ANN-Sensitivity Analysis

Sensitivity analysis is the procedure of determining how changes to the neural network's input variables or parameters impact the model's output or performance [263]. This made it easier in understanding the ANN's sensitivity or reactivity to changes in its inputs or configurations [265]. Sensitivity analysis has been used in the relevant ANN models to find the relative significance of independent factors on the dependent variable [248] and [260]

Table 4.14. shows the sensitivity analysis. This study conducted sensitivity analysis to determine the normalized importance of the neurons, calculated by dividing their relative importance by the maximum importance and expressing it as a percentage [266] [264]. This enabled us to measure the predictive strength of each input neuron.

For ANN Model, where cyber hygiene behaviour is used as the output variable. The findings specify that four independent variables have a substantial impact on cyber hygiene behaviour, namely Cyber trust, cyber hygiene intention, cyber hygiene knowledge and personality traits. The sensitivity analysis further reveals that cyber trust is the most crucial input in predicting cyber hygiene behaviour as output, with a relative importance of 100 %. Cyber hygiene intention is the second most crucial predictor with a percentage of 85 %. followed by cyber hygiene knowledge and personality traits, which have relative importance with 52.4 % and 44.5 %, respectively. The results of sensitivity analysis are displayed in table 4.14 below.

Table 4.14: Independent Variable Importance (Sensitivity Analysis)

Neural Network (NN)	AT	CH(INT)	CH(PBC)	CH(SN)	CHK	CT	KS	PCHV	PT	TA
NN(i)	0.04	1.00	0.15	0.07	0.59	0.85	0.03	0.04	0.39	0.17
NN(ii)	0.08	0.50	0.06	0.24	0.45	1.00	0.16	0.09	0.42	0.12
NN(iii)	0.10	0.70	0.22	0.13	0.65	1.00	0.29	0.08	0.47	0.41
NN(iv)	0.15	0.75	0.10	0.07	0.56	1.00	0.13	0.04	0.50	0.18
NN(v)	0.09	0.66	0.18	0.10	0.38	1.00	0.23	0.10	0.23	0.14
NN(vi)	0.11	1.00	0.25	0.31	0.45	0.70	0.44	0.09	0.28	0.43
NN(vii)	0.05	0.45	0.08	0.22	0.44	1.00	0.20	0.06	0.55	0.24
NN(viii)	0.09	1.00	0.17	0.43	0.41	0.87	0.19	0.10	0.53	0.27
NN(ix)	0.12	1.00	0.03	0.16	0.43	0.92	0.19	0.08	0.27	0.17
NN(x)	0.08	0.87	0.13	0.16	0.52	1.00	0.20	0.07	0.53	0.16
Overall	**0.09**	**0.79**	**0.14**	**0.19**	**0.49**	**0.93**	**0.21**	**0.08**	**0.42**	**0.23**
Average Importance (%)	**39.8%**	**85.0%**	**14.8%**	**20.2%**	**52.2%**	**100%**	**22.1%**	**8.0%**	**44.5%**	**24.5%**

Note. AT=Attitude, CH(Int)= Cyber Hygiene Intention, CH(PBC)= Cyber Hygiene Perceived Behavioural Control, CH(SN)= Cyber Hygiene Subjective Norms, CHB= Cyber Hygiene Behaviour, CHK= Cyber Hygiene Knowledge, CT= Cyber Trust, KS= Knowledge Sharing, PCHV= Perceived Cyber Hygiene Value, PT= Personality Traits, TA= Threat Appraisal

.

4.6.Summary

The research data analysis and outcomes are presented in Chapter 4. Data gathering and analysis using SEM-ANN are both covered in the description of the data analysis procedure. Measures taken to ensure data validity and reliability are discussed, as well as limitations of the data set. The findings of the research are presented next, including results of SEM-ANN analysis. Significant relationships among variables are also presented.

From the findings and discussion, it is determined that the variable subjective norm, perceived behavioural control and cyber hygiene knowledge are not affecting the cyber hygiene intention to perform cyber hygiene behaviour. Organizations should launch training programs aimed at improving employees' comprehension and awareness of cyber hygiene practices. This endeavor can foster a culture of cybersecurity awareness and accountability throughout the organization. Moreover, SMEs should ensure that cyber hygiene knowledge is an important factor to consider. While educating employees is the primary approach, organizations must also strategize on how to reshape their attitudes and behaviours regarding cyber hygiene.

The research findings suggest a positive correlation between knowledge sharing and cyber hygiene attitude with cyber hygiene intention. This study emphasizes how attitude and knowledge sharing play crucial roles in shaping behavioral intentions, consistent with prior research results. Hence, the recommendation is to focus on a resilient mindset to empower individuals in cybersecurity, shifting them from vulnerability to resilience.

Conversely, this study also found that threat appraisal, perceived cyber hygiene behaviour, and cyber trust significantly influence cyber hygiene

behaviour. It is advisable for organizations to invest in initiatives that enhance employees' capacity to evaluate and address cyber threats adeptly. Additionally, building trust in cybersecurity protocols and systems can motivate employees to embrace and uphold cyber hygiene practices. Personality traits engaging employees into cyber hygiene intention and provides a holistic view in contributing to the cyber hygiene behaviour. These findings are similar to the past results. Therefore, acknowledging the impact of personality traits on cyber hygiene intention can assist organizations in customizing their cybersecurity training and awareness initiatives to suit various personality profiles.

This research further highlights the significance of cyber hygiene intention in influencing cyber hygiene behaviour. The study reveals a notable correlation between cyber hygiene intention and behaviour, emphasizing the importance of enhancing employees' cyber hygiene practices to foster a stronger intention towards cyber hygiene behaviour. Consequently, this investigation delves into the diverse factors contributing to cyber hygiene behaviour, addressing an existing gap in the literature, and offering valuable understandings to enhance the cyber hygiene practices of software development employees.

CHAPTER FIVE

DISCUSSION AND IMPLICATIONS

5.1.Introduction

In the upcoming chapter, a detailed examination of the outcomes obtained from the data analysis is undertaken. The aim is to thoroughly investigate the factors influencing cyber hygiene behaviour in employees of software development SMEs. This section provides a comprehensive explanation of the research models' findings, outlining their practical and theoretical implications. Additionally, the chapter concludes by addressing the research restrictions and offering recommendations for future research efforts.

5.2.Discussion of Key findings

The objective of this research was to investigate the factor influencing cyber hygiene behaviour among employees of software development SMEs in Malaysia. To achieve this objective, a two-stage SEM-ANN approach was employed to analyze and validate a model grounded in the TPB.

Subsequently, research questions that were developed to achieve the study's objectives, providing corresponding research findings that align with both the objectives and questions are discussed below.

Research Question 1. *What factors influence cybersecurity behaviour among employees in software development SMEs?*

Research Objective 1. *To identify the factors impacting cybersecurity behaviour among employees of software development SMEs.*

For the first objective a systematic literature review (SLR) was performed to extract factors that impact cybersecurity behaviour among employees of software development SMEs. The extracted factors have been classified as knowledge sharing, cyber hygiene attitude, cyber hygiene subjective norm, cyber hygiene perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, personality traits. Hence, researchers deduce that these factors collectively influence the desire toward cybersecurity behaviour and act as a constraint against cyberattacks.

Research Question 2. *How do individual factors such as knowledge sharing, cyber hygiene attitude, subjective norm, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits influence the intention to practice cyber hygiene among employees in software development SMEs?*

Research Objective 2. *To determine the impact of individual factors such as knowledge sharing, cyber hygiene attitude, subjective norm, perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits on cyber hygiene intention among employees of software development SMEs.*

In this research the author clearly found the factors affecting cyber hygiene behaviour. Only three association are not supported, i.e., cyber hygiene subjective norm, cyber hygiene perceived behavioural control and cyber hygiene knowledge as indicated in Table 5.1. The remaining associations, such as knowledge sharing, cyber hygiene attitude, threat appraisal, perceived cyber hygiene value, cyber trust, and personality traits, establish a statistically

significant association with the intention to engage in cyber hygiene behaviour. These results contribute valuable insights to researchers' understanding of the factors influencing employees' cyber hygiene behaviour.

Table 5.1: Hypotheses Test Results

S.No	Hypothesis	Result
H_1	Knowledge Sharing (KS) -> Attitude (AT)	Supported
H_2	Attitude -> Cyber Hygiene Intention CH(Int)	Supported
H_3	Cyber Hygiene Subjective Norm CH(SN) -> Cyber Hygiene Intention CH(Int)	Not Supported
H_4	Cyber Hygiene Perceived Behavioural Control CH(PBC) -> Cyber Hygiene Intention CH(Int)	Not Supported
H_5	Threat Appraisal TA -> Cyber Hygiene Intention CH(Int)	Supported
H_6	Cyber Hygiene Knowledge CHK -> Cyber Hygiene Intention CH(Int)	Not Supported
H_7	Perceived Cyber Hygiene Value PCHV -> Cyber Hygiene Intention CH(Int)	Supported
H_8	Cyber Trust CT -> Cyber Hygiene Intention CH(Int)	Supported
H_9	Personality Traits PT -> Cyber Hygiene Intention CH(Int)	Supported
H_{10}	Cyber Hygiene Intention CH(Int) -> Cyber Hygiene Behaviour CHB	Supported

Research Question 3. *How does the SEM-Neural network approach enhance cybersecurity behaviour and promote cyber hygiene among employees in software development SMEs?*

Research Objective 3*. To examine the SEM-Neural network approach in improving cybersecurity behaviour through cyber hygiene among the employees of software development SMEs.*

In the context of the Neural Network approach, the outcomes indicate that four independent variables exert a significant influence on cyber hygiene behaviour. These variables include cyber trust, cyber hygiene intention, cyber hygiene knowledge, and personality traits. Notably, the findings underscore the paramount importance of cyber trust as it emerges as the most critical input for predicting cyber hygiene behaviour, with a relative importance of 100%. Subsequently, cyber hygiene intention, cyber hygiene knowledge, and personality traits exhibit relative importance values of 85%, 52.4%, and 44.5%, respectively.

These results effectively convey that the input variables utilized in the models serve as potent predictors of cyber hygiene behaviour. The comprehensive outcomes of the neural network analysis can be found in Table 5.2

Table 5. 2: Neural Network Results

Variables	Relative importance
Cyber trust	100%
Cyber Hygiene Intention	85%
Cyber Hygiene Knowledge	52.2%
Personality Traits	44.5%
Attitude	39.8%
Threat Appraisal	24.5%
Knowledge sharing	22.1%
Cyber Hygiene Subjective Norm	20.2%
Cyber Hygiene Perceived Behavioural Control	14.8%
Perceived Cyber Hygiene Value	8.0%

5.2.1. Knowledge sharing positively influences attitude to perform cyber hygiene intention.

In Chapter 4, the data reveals a substantial positive correlation between knowledge sharing and cyber hygiene attitude, as proved by a t value of 12.700 and p value of 0.000. Path coefficient, which stands at 0.460, falls within the recommended range of 0.1 to 1. Consequently, the first hypothesis is deemed valid and accepted.

These findings are in concurrence with previous research, highlighting a strong correlation between knowledge sharing and attitude [267]. Previous research has consistently shown that knowledge sharing positively influences one's attitude toward engaging in cyber hygiene intention [268] and [154]. It is well-established that possessing enough knowledge fosters a positive attitude, which, in turn, can drive behavioural change [269] and [270]. Individuals who hold knowledge sharing in high regard and maintain a positive attitude are more motivated to participate in good cyber hygiene practices. Therefore, the hypothesis positing a significant relationship between knowledge sharing, CH attitude, and the intention to engage in CH practices is supported in this current research.

5.2.2. Cyber hygiene attitude will have a positive impact on cyber hygiene intention.

The outcomes of the study reveal a considerable positive correlation among CH attitude and intentions. This is evidenced by a path coefficient of 0.050, a t-statistic of 2.059, and a p-value of 0.040. This observation is substantiated by

path coefficient falling in the range of 0.1 to 1, the t value 1.96, and value of p being below the alpha value of 0.05.

These research outcomes align with prior studies, providing robust support for the relationship under scrutiny. For instance, according to the TPB developed by Ajzen and Fishbein (1975) in [148], attitudes toward a particular behaviour reflect an individual's comprehensive evaluation of engaging in that behaviour [271]. Attitudes are modeled by expectancy beliefs regarding the likelihood of certain consequences resulting from the behaviour and the perceived desirability of those consequences [73] (Ajzen, 1991)). In the context of this study, attitudes proved to be a robust predictor of an individual's intention to adopt cybersecurity practices. The scales employed to measure attitude exhibited a commendable level of internal consistency, affirming their suitability for measurement [272]. The strong and positive association observed between attitudes and behavioural intentions underscores that cultivating a more favorable association enhances the likelihood of implementing cybersecurity practices. Past studies have consistently demonstrated a positive connection between attitudes and intentions [273], [274], [275]. In summary, the hypothesis claiming a substantial association among cyber hygiene attitude and intention is confirmed within the context of this current study.

5.2.3. Cyber hygiene subjective norms will have positive influences on cyber hygiene intention.

The path analysis, employing Bootstrapping, revealed no substantial relationship among cyber hygiene subjective norm and cyber hygiene intention. This conclusion is assisted by a t= 0.813, which is below the accepted threshold of 1.96, and an associated value of p =0.416, exceeding the alpha value of 0.05.

Consequently, hypothesis suggesting a connection among cyber hygiene subjective norm and cyber hygiene intention is rejected based on the unfavorable t-statistic and p-value.

These research findings deviate from those of previous studies. As defined by Ajzen (1991) [73], subjective norms encompass the external pressures people perceive when contemplating whether to act. Generally, individuals are more inclined to adhere to the expectations of significant organizations or influential figures. However, this study's results indicate that employees who perceive higher levels of subjective norm and expectations regarding cyber hygiene intention do not necessarily hold a positive relation toward cyber hygiene behaviour. This stands conflict to prior studies, which often reported a robust positive correlation between subjective norms and behaviour, signifying that people are more likely to involve in cybersecurity practices [271], [276].

However, the findings of [147], [277], [278] suggests that subjective norms do not significantly influence the intention to practice cybersecurity. In the context of this research, it becomes evident that subjective norms exert no discernible impact on the cyber hygiene behaviour among employees of Malaysian software development SMEs.

The results indicate that employees do not experience societal pressure to engage in cyber hygiene behaviour. Additionally, investigations by [119], [169], [279] have all reported weak and negative predictive relationships between subjective norms and behavioural intentions. Therefore, this study aligns with these findings and also rejects the assumption supporting a important association between subjective norms and CH intention.

5.2.4. Cyber hygiene perceived behavioural control will have a positive impact on cyber hygiene intention.

The results revealed a lack of substantial connection between cyber hygiene perceived behavioural control and cyber hygiene intention. This was evident from the t-statistic value of 0.326, which fell below the accepted threshold of 1.96, and the corresponding p-value of 0.744, surpassing the alpha value of 0.05. Therefore, the hypothesis suggesting an association among cyber hygiene perceived behavioural control and cyber hygiene intention is dismissed due to the unfavorable t-statistic and p-value.

This study sought to explore the impact of perceived behavioural control on cyber hygiene behaviour among employees of software development SMEs. Perceived behavioural control, as defined by Ajzen, 1991 in [73] affects to an individual's perceived level of ability and control when engaging in a particular behaviour. Previous research often indicated that employees who believed they had greater control over their behaviour were more inclined to have an intention to engage in cyber hygiene practices [122], [271]. However, the outcomes of this study do not align with these prior research findings, which suggested that perceived control is not a robust predictor of cyber hygiene intention. There is a divergence in research outcomes, with some studies, such as [116], [136], [176] implying that perceived behavioural control significantly impacts cybersecurity behaviours. Conversely, other studies, including [204], [280], [281], have found a negative association between perceived behavioural control with intention.

In the context of this research, it becomes apparent that perceived behavioural control does not exert a noticeable impact on the cyber hygiene

behaviour of employees in software development SMEs in Malaysia. The findings propose that employees lack confidence in their ability to engage in cyber hygiene behaviour. Additionally, studies by researcher Arpaci & Baloɨlu and other authors Tsai et al. (2016) in [173], [174], and have also indicated that perceived behavioural control does not significantly influence intentions. Therefore, this study aligns with these findings and also rejects the assumption supporting a substantial association among perceived behavioural control and cyber hygiene intention.

5.2.5. Threat appraisal will have a positive influence on cyber hygiene intention.

The results illustrate a significant link between threat appraisal and cyber hygiene intention. This is supported by a value of 4.826 t-statistic, which surpasses the accepted threshold of 1.96, and a corresponding of 0.000 p-value, falling below the alpha value of 0.05. Therefore, the hypothesis suggesting a substantial connection between threat appraisal and cyber hygiene intention is confirmed and validated.

Threat appraisal encompasses an individual's or organization's perception and evaluation of cybersecurity threats and risks within the digital environment. This perception entails their comprehension of potential hazards, vulnerabilities, and the likelihood of encountering cyber threats [278]. Importantly, these research findings align agreeably with previous studies.

Earlier research consistently establishes a statistically substantial positive association between threat appraisal and cyber hygiene intention. As elucidated in prior studies [282], when individuals or organizations perceive a higher level of threat and risk in the digital realm, it positively influences their intention to

engage in cyber hygiene practices. This perspective is supported by the author in [283] and [284] that threat appraisal serves as a motivating factor for both individuals and organizations to embrace and sustain effective cyber hygiene practices as a protective measure.

Moreover, previous authors in [177], [179] have emphasized that substantial cybersecurity threats act as catalysts, prompting individuals and organizations to demonstrate intent in practicing cybersecurity measures, such as using robust passwords, regularly updating software, and being cautious online. Therefore, this study concurs with and validates the premise supporting the relationship between threat appraisal and CH intention.

5.2.6. CH knowledge will have a positive influence towards cyber hygiene intention.

The results do not indicate a significant correlation among cyber hygiene (CH) knowledge and cyber hygiene intention. This conclusion is assisted by a p-value of 0.191, surpassing the value of alpha = 0.05. Additionally, the path coefficient is 0.049, and the T stands at 1.309, falling below the threshold of 1.96. Therefore, there is no substantial link among cyber hygiene knowledge and cyber hygiene intention.

These findings diverge from those of previous research. Earlier studies consistently revealed robust correlations between knowledge and intention, as well as knowledge and cyber hygiene behaviour, thereby affirming the association among knowledge, attitude, and the practice of cybersecurity threat prevention. Conversely, authors such as [27], [124], [285] have revealed a crucial and beneficial connection between knowledge and cyber hygiene

intention. However, in contrast, researchers [84], [286], [287] have investigated scenarios in which employees who share their knowledge exhibit a high level of knowledge awareness, yet their behaviours do not significantly differ from those of untrained users.

In the context of this study, it becomes evident that cyber hygiene knowledge does not exert a discernible impact on the cyber hygiene behaviour of employees in software development SMEs in Malaysia. Consequently, this research also rejects the assumption that supports a significant association between perceived behavioural control and CH intention.

5.2.7. Perceived cyber hygiene value will have a positive influence on the cyber hygiene intention.

Hypothesis seven suggest that the perceived cyber hygiene value significantly affects CH intention. The outcomes, with a beta coefficient (β) of -0.084, a t = 4.140, and (ρ) of 0.000, explicitly indicate the significant influence of perceived cyber hygiene value on cyber hygiene intention. Therefore, hypothesis seven have strong support.

These results are associated agreeably with previous research. For instance, as suggested by an author in [127], when individuals or organizations perceive a higher value in adhering to cyber hygiene practices (such as utilizing strong passwords, regularly updating software etc.,) they exhibit a heightened inclination to intend to engage in these practices.

The concept of cyber hygiene perceived value assesses the degree to which individuals or organizations recognize the significance of practicing good cyber hygiene. It essentially measure the perception that maintaining secure and safe

digital practices is both beneficial and imperative [187]. This positive impact underscores the notion that the perceived value of cyber hygiene serves as a motivating force, encouraging employees or organizations to proactively enhance their cybersecurity measures [128].

Furthermore, other researchers in [288], [289] suggests that emphasizing the importance and advantages associated with perceived cyber hygiene value can serve as an effective strategy for promoting improved cybersecurity practices among individuals or organizations. Thus, the hypothesis proposing a notable connection between perceived cyber hygiene value and cyber hygiene intention is strongly substantiated in this present study.

5.2.8. Cyber trust will have a positive influence towards cyber hygiene intention.

Hypothesis eight in this study examines the positive and substantial impact of cyber trust on cyber hygiene intention. The results clearly demonstrate that cyber trust has a substantial impact on cyber hygiene intention, with path coefficients represented by values of T statistic (T) of 12.603, and a p-value (ρ) of 0.000. Therefore, hypothesis eight is supported.

These research findings correspond with prior studies. For instance, cyber trust plays a substantial role in fostering connections that facilitate the sharing of cybersecurity awareness among employees, as evidenced by the work of [290] [98]. This variable essentially encapsulates the level of trust or confidence that individuals or organizations place in the security measures, systems, and practices within the digital or online environment [261]. It signifies their belief that their digital interactions and data remain protected and secure [71]. Further

support from other studies, including those conducted by [67], [162], underscores the significant role of cyber trust in the domain of cybersecurity.

The findings of [129] and [291] suggest that as the level of cyber trust rises, corresponding to higher confidence in online security, there will be a positive impact on the intention to practice cyber hygiene.

Researchers in their work [292] elucidate that employees or organizations who exhibit trust in the security of digital environments are more inclined to engage in cybersecurity practices, such as utilizing robust passwords, keeping updated software.

As a result, cyber trust exerts an influence on the cyber hygiene behaviour of employees in software development SMEs in Malaysia. Therefore, this study accept the assumption that supports the association between cyber trust and cyber hygiene intention.

5.2.9. Personality traits will have a positive impact on the cyber hygiene intention.

The findings of hypothesis nine indicate a significant association between personality traits and cyber hygiene attitude, as reflected in a p-value of 0.000, which is lower than the alpha value of 0.05, a T statistic of 5.424, surpassing the threshold of 1.96, and a path coefficient of 0.234. Consequently, personality traits are indeed significantly linked to cyber hygiene intention.

Personality traits are recognized for their capacity to shape how individuals perceive and respond to various situations and challenges. They encompass enduring characteristics and behavioural tendencies that define an individual's personality, encompassing factors like openness, conscientiousness, extroversion, agreeableness, and neuroticism. These findings align with prior

research, where personality traits have been identified as predictors of security behaviours, including adherence to rules and procedures when behaviour is not monitored [293], [294].

In this study, a substantial and positive association is established between specific personality traits and cyber hygiene intention. As mentioned in [84], personality traits may exert a positive influence on an individual's intention to practice cyber hygiene. Additionally, researchers in [133] [130] noted that traits such as conscientiousness and agreeableness significantly impact individual concerns regarding information security and privacy.

Personality traits consistently emerge as factors related to intentions and behaviours in various studies. In [198] [131] researcher further elucidated that personality traits can be valuable when designing cybersecurity awareness and training programs, as tailoring strategies to individuals with different personality profiles may encourage better to improve cyber hygiene practices. Another researcher in their study [199] explained that individuals with higher levels of conscientiousness, characterized by traits like organization, responsibility, and attention to detail, tend to be more inclined to follow cybersecurity best practices. Therefore, this study affirms the assumption supporting the relationship between personality traits and CH intention.

5.2.10. CH intention has a positive and significant impact on cyber hygiene behaviour.

The results detailed in Chapter 4 indicate a significant and positive relationship among cyber hygiene intention and cyber hygiene behaviour. This association is confirmed by a (β)= 0.6877, a t= 9.852, which exceeds the threshold of 1.96, and p= 0.000.

This outcome aligns agreeably with prior research findings. As noted by author in [84], [274], [115] behaviour becomes more predictable when intentions are considered. In many instances, individuals' intentions serve as a reasonably accurate predictor of their subsequent behaviour [170], [293] [267]. It is noted that behavioural intention can explain a significant portion of forthcoming behavioural changes, on average [203].

On the contrary, the study emphasizes a notable and positive correlation between the intention for cyber hygiene and the behaviour of employees in software development SMEs. This suggests that individuals with a stronger intention to engage in cyber hygiene practices are more inclined to manifest these behaviours.

These findings support existing research on this subject, such as the studies conducted by [140], [200], [273], [278], which have likewise reported that individuals with a high level of intention to adopt cyber hygiene practices are more likely to follow the cyber hygiene behaviour. Consequently, the results of this study underscore the pivotal role played by cyber hygiene intention in shaping the behaviour of employees within software development SMEs. Thus, the hypothesis suggesting a important connection among cyber hygiene intention and cyber hygiene behaviour, as developed by the researchers, is supported, and accepted.

5.3.Theoretical Implications

Theoretical implications regarding cybersecurity behaviour through cyber hygiene among employees of small and medium-sized enterprises (SMEs) in software development refer to the valuable insights and contributions that research in this area can provide to the broader theoretical understanding of

cybersecurity practices. This advancement enhances knowledge and theories concerning how employees in SMEs engage in cyber hygiene behaviours to safeguard digital assets and information.

The present study establishes a comprehensive theoretical framework by applying a well-established behavioural theory, the theory of planned behaviour (TPB) [73], to comprehend the cybersecurity behaviours of employees within SMEs. This theory serves as the primary theoretical foundation (underpinnings) of the study, helping in the identification of key aspects of cyber hygiene practices and their relationship to employee intentions [25].

Furthermore, integrating additional factors such as knowledge sharing, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits into our research model that is (TPB) which has introduced a novel theoretical contribution to software development processes in shaping cyber hygiene behaviours. This theoretical discovery lays the foundation for imminent research on cyber hygiene behaviours.

This study can validate the TPB model in explaining and predicting cybersecurity behaviour among employees of Malaysian software development SMEs. It can evaluate whether factors such as knowledge sharing, cyber hygiene attitudes, cyber hygiene subjective norms, cyber hygiene perceived behavioural control, threat appraisal, cyber hygiene knowledge, perceived cyber hygiene value, cyber trust, and personality traits align with cyber hygiene intention to perfume cyber hygiene behaviour. The research explores how employees perceive the risks associated with their software development SMEs and how these perceptions impact their behaviour.

The study emphasizes the need for a profound comprehension of employee attitudes and behaviours regarding cyber hygiene. Challenges such as insufficient awareness, internal threats, vulnerable passwords and authentication underscore the importance of addressing employee behaviour and awareness to counter cybersecurity attacks effectively.

Additionally, this study unveiled new relationships, including those between personality traits and cyber hygiene intention, perceived cyber hygiene value, cyber trust, and cyber hygiene intention. While their effects on information security have been studied previously, their impacts on cyber hygiene intention remained unexplored [295]. These newly identified relationships provide novel foundations for future researcher to expand the existing literature [296].

In contrast to existing related studies utilizing linear models, this research employs a two-staged SEM-ANN methodology, encompassing both linear and PLS models and non-linear ANN models.

This novel approach overcomes the limitations of linear models by incorporating a non-linear model. In linear models, a reduction in one predictor might be balanced out by an increase in another predictor [297]. By utilizing a non-linear Artificial Neural Network (ANN) model, researchers have effectively tackled the shortcomings of linear models, and thus offered a new theoretical contribution to the existing literature.

Overall, the theoretical implications of this study enhance an improved understanding of the factors impacting cyber hygiene behaviour and can guide the development of effective interventions to address this issue among software development SMEs in Malaysia.

5.4.Practical Implications

In addition to its theoretical implications, current research holds significant practical implications for various stakeholders in Malaysia, including the government, organizations, employees, policymakers, and small and medium-sized enterprises (SMEs) operating in digital landscape. By investigating the factors influencing cyber hygiene behaviour among employees in Malaysian software development SMEs, this research aligns with Malaysia's national goals concerning Sustainable Development (specifically, Goals #8, #9, and #16). The findings offer valuable insights to the Malaysian government and relevant authorities, aiding in the formulation of strategies and policies to combat cyberattacks. Moreover, the results serve as guidance for employees of SMEs to creäte a healthy atmosphere wherever it is tough for Malaysian SMEs to engage in cyber hygiene behaviour.

An important finding is that SMEs face susceptibility to cyber threats because of their comparatively limited security measures and awareness. This puts their online accounts and other critical data, such as business financial information and transactions, at risk [298]. The study emphasizes the significant impact of the theory of planned behaviour (TPB) on cyber hygiene behaviour, suggesting that raising awareness, imparting better cyber knowledge, and offering enhanced cyber support can substantially enhance cyber hygiene behaviour among employees at a minimal cost.

Moreover, the research underscores the need for small businesses to recognize their susceptibility to cyberattacks, urging the involvement of cyber practitioners and legislators in creating awareness that cybercriminals can attack not only big organizations but also small businesses.

SMEs should prioritize employee cybersecurity training through frequent programs, encompassing workshops, online courses, and simulations to raise awareness of cybersecurity issues and endorse good cyber hygiene practices. SMEs can elaborate practical approaches to constantly increase employee awareness of cybersecurity. This can involve sending regular reminders and updates about cybersecurity threats, best practices, and policy changes. Moreover, performing simulated phishing exercises can evaluate employees' capacity to identify phishing attempts. Subsequently, targeted training can be provided to those who succumb to the simulated attacks [293].

In terms of technical measures, SMEs should implement robust security practices such as data encryption techniques, procedures, policies, and advanced authentication methods like Multi-Factor Authentication (MFA) across various systems and applications used within the organization. This can substantially improve security by requiring multiple forms of verification for access [299]. SMEs should give clear and user-friendly guidelines to employees on how to set up and utilize MFA. Clear instructions and support for MFA setup are essential. Furthermore, automating software updates and patches can ensure that all systems are equipped with the latest security fixes. Developing incident response plans outlining clear steps during cyber incidents is imperative.

This study advocates a proactive approach to cybersecurity for SMEs, emphasizing employee training and awareness, strong policies, and technical controls to mitigate cybersecurity risks in Malaysian software development SMEs.

This study also sheds light on the enhancement of security culture within organizations. Rather than creating a new culture, the first step towards a

successful security culture is to understand and evaluate the existing cultural norms among employees. This can facilitate the development of more relatable messaging and robust training for security culture [300].

Policymakers can utilize the study's results to develop policies and regulations to address cyber hygiene behaviours for SMEs in Malaysia. Policymakers should craft clear and concise cybersecurity policies and guidelines for SMEs that outline cyber hygiene practices, ensuring that these documents are easily available and understandable by all employees [287]. Regular policy reviews and revisions are essential to adapt to evolving threats and technologies.

For the Malaysian government, the study highlights the need for policies and regulations to address cyber hygiene practices in the country. The government must develop effective interventions to prevent cyberattacks. By addressing cyber hygiene practices, the government can contribute to creating a secure and more respectful online environment for all Malaysians SMEs. At the national level, the research urges the government to take proactive measures to secure the digital environment.

Practical implication of this study influences to the national agenda of Malaysia on “Sustainable Development Goals” by assessing different cyber hygiene behaviour aspects related the employees of Malaysian software development SMEs.

Offering insights that can facilitate collaborative efforts among SMEs, employees, policymakers, and the government. Implementing good cyber hygiene practices. This will ultimately contribute to creating a safer and more respectful online environment for SMEs in Malaysia.

5.5.Recommendations

Addressing cyber hygiene in Malaysian software development SMEs is a serious concern, demanding immediate action. To foster a secure and more productive learning environment, a set of recommendations has been devised. These suggested recommendation offer actionable strategies to tackle the identified challenges and enhance cybersecurity practices within SMEs. The following are the study's recommendations:

1. **Establish training initiatives focused on cybersecurity awareness and conduct regular evaluations of security awareness:**

In light of the research outcomes, design training programs emphasizing cybersecurity awareness consistently highlight the significance of cyber hygiene practices to all employees within software development SMEs. Ensure these programs encompass important cyber hygiene practices and are easily accessible to all staff members. Implementation strategies may involve regular reminders, email notifications, and internal campaigns. Additionally, SMEs are encouraged to conduct periodic assessments of security awareness among employees to evaluate their understanding and adherence to cyber hygiene practices. Utilize the assessment outcomes to pinpoint areas requiring enhancement.

2. **Establish transparent cybersecurity policies and guidelines:**

Small and medium-sized enterprises (SMEs) ought to create and disseminate clear cybersecurity policies and guidelines delineating the anticipated behaviour and responsibilities of their employees. Guarantee that these policies are straightforward, easily comprehensible, and readily available.

3. **Enforce Multi-factor authentication (MFA) and develop an incident response strategy:**

Encourage SMEs to employ MFA across their systems and applications to enhance security measure. Offer clear instructions on MFA setup and help employees throughout the process. Additionally, SMEs should establish a detailed incident response plan, specifying sequential actions to take during a cyber incident. Ensure this plan is routinely reviewed and revised to align with evolving threats.

4. **Allocate Adequate Funds for Cybersecurity:**

It is advisable for SMEs to dedicate sufficient budget and resources to cybersecurity initiatives. Position cybersecurity as a strategic investment rather than merely a cost.

5. **Stay informed on emerging threats:**

Advise SMEs to stay informed about the most recent cybersecurity threats and vulnerabilities pertinent to their industry. Encourage active participation in industry-specific cybersecurity forums and networks for sharing valuable information.

6. **Promote partnerships with academic institutions and invest in research and development:**

Facilitate partnerships between SMEs and specialized academic institutions in the field of cybersecurity, fostering research collaborations and providing access to cutting-edge cybersecurity knowledge. Encourage SMEs to invest in continuous research and development initiatives focused on cybersecurity. This entails exploring innovative technologies and strategies to enhance cyber hygiene practices.

7. **Frequently update software and systems, and perform post-incident analysis:**

Highlight the significance of regularly updating software, systems, and applications to address known vulnerabilities. Implement a structured process to ensure timely updates. Following a cybersecurity incident, advise SMEs to conduct a detailed post-incident analysis to recognize root causes and areas needing improvement. Utilize this analysis to strengthen future security protocols.

These recommendations offer a holistic guide for SMEs in the software development sector to enhance their cybersecurity perspective and encourage improved cyber hygiene practices among their employees.

5.6.Study's Limitations

There are numerous limitations in this research that must be acknowledged. Researchers faced several constraints during the research process. However, it is significant to note that these limitations do not diminish the consequence of the findings, which will be valuable for future research efforts.

One limitation lies in the online surveys conducted, where authenticity of responses cannot be guaranteed. Utilizing a quantitative method for data collection. The feasible timeframe for administering a quantitative investigation is constrained to only a limited months. This timeframe was insufficient to gather a comprehensive dataset encompassing diverse behavioural variations.

Additionally, the global COVID-19 pandemic posed challenges in physically collecting data from residents in Malaysian cities. Convenience sampling was introduced.

Respondents might swiftly skim through the question, their minds automatically leaning towards agree or neutral. Consequently, individuals hurrying to complete tasks swiftly might answer randomly or interpret questions in their own way.

To address this, future research should employ diverse approaches, such as face-to-face interviews, allowing respondents to provide detailed, accurate information and clarify any ambiguities. Face-to-face interactions can yield unexpected responses, enhancing the depth of understanding. Moreover, the scope of this study investigates a restricted set of variables concerning both the direct and indirect impacts on employees' intentions.

Another limitation involved the difficulty and time-consuming nature of finding suitable respondents during the online data collection process. Since the data is collected via an online Google Form. The absence of physical presence led to challenges in tracking genuine responses, particularly as respondents tend to overlook or disregard questionnaires on online platforms. Consequently, researchers had to distribute questionnaires individually or in small groups, a lengthy and time-intensive process, impacting overall data collection efficiency.

Hence, this study might not comprehensively capture cyber hygiene behaviour, intention, and attitude. Despite the convenience associated with online platforms, many individuals tend to disregard or decline online questionnaires. Consequently, researchers had to distribute questionnaires individually or in small groups, a process that proved time-consuming and reduced overall data collection efficiency.

Additionally, during data analysis, it was found that a professional license was necessary to use SmartPLS software for the analysis. The study was constrained by a 30-day free trial, limiting the analysis period.

These limitations highlight the need for careful consideration and diverse data collection methods in future research to enhance the depth, accuracy, and efficiency of research endeavors.

5.7.Future Research

This research opens avenues for future research, offering opportunities to enhance understanding of cybersecurity behaviour in SMEs and to design targeted interventions and policies for improved cyber hygiene practices and overall security. Several potential areas for future investigation are discussed below.

Future researchers can explore different industries such as nonprofit organizations, government agencies, and high-tech companies, broadening the scope beyond SMEs. Additionally, the study's focus on specific Malaysian geographic locations could be expanded to encompass diverse regions globally, allowing for a broader generalization of findings.

Future studies could adopt longitudinal approaches to monitor changes in cyber hygiene behaviours and attitudes within SMEs over time. Long-term studies offer insights into the sustainability of cyber hygiene practices and the effectiveness of interventions, enabling a deeper understanding of behavioural shifts.

Investigating the influence of cultural factors on cyber hygiene practices is crucial. Researchers in future can explore how cultural contexts shape attitudes

and behaviours, leading to tailored interventions that resonate with different cultural groups.

The influence of developing technologies such as Artificial Intelligence (AI), Internet of Things (IoT), and blockchain on cybersecurity behaviour has yet to be investigated. Future research could delve into how these technologies influence cyber hygiene practices, shedding light on innovative approaches to enhance security.

Future research endeavors ought to encompass a wider range of variables, encompassing environmental, technological, and social factors. This comprehensive approach will enable the exploration of how individuals are influenced by these factors and enhance our understanding of their effects and variations on employees' intentions. Understanding how individuals respond to specific events within these contexts can provide nuanced insights into attitude, intention, and behaviour changes.

Moreover, this study uses quantitative methods future researcher may utilize mixed research methods, which combine quantitative data with qualitative insights from interviews and related evidence, can offer a comprehensive view. Such an approach can paired with evidence from qualitative interviews, will provide insights for policymakers, ensuring a robust and proactive response to safeguard businesses, consumers, and society from the pervasive effects of cyberattacks.

Resources and time are significant aspects restricting the study so allocating substantial resources over extended periods for such studies ensures a robust analysis of present scenarios and future projections. Also make recommendations to address gaps in security that might influence broad

domains. Comparative studies with developed countries can provide valuable contrasts, highlighting differences in cybersecurity practices and identifying areas for improvement.

By exploring these research avenues, scholars can contribute significantly to the understanding of cybersecurity behaviour, leading to more effective interventions, policies, and protections for businesses, consumers, and society at large.

5.8.Summary

Chapter 5 offers a thorough conclusion of the study, presenting a summarizing overview of the research questions, objectives, and findings. Chapter proceeds to a detailed exploration of the significant findings, followed by a detailed analysis of the theoretical, practical, and policy implications arising from the study. Notably, the practical implications section of the chapter furnishes crucial insights for policymakers, practitioners, and the broader research community. The chapter also acknowledges the research limitations, underscoring the necessity for further study to expand upon these findings.

The chapter presents recommendations and suggests future research directions, providing valuable input for forthcoming studies in this domain.

REFERENCES

[1] M. Wallang, M. D. K. Shariffuddin, and M. Mokhtar, "CYBER SECURITY IN SMALL AND MEDIUM ENTERPRISES (SMEs)," *Journal of Governance and Development (JGD)*, vol. 18, no. 1, pp. 75–87, Dec. 2022, doi: 10.32890/jgd2022.18.1.5.

[2] MyCERT, "MyCERT. (n.d.). 'Home', MyCERT, available at: https://www.mycert.org.my/portal/index (accessed 1 May 2022). ," 2022.

[3] S. M. Yong, "4th Industry Revolution Digital Marketing Adoption Challenges in SMEs and its Effect on Customer Responsiveness," 2023.

[4] Z. Othman, B. Balakrishnan, M. F. A. Zaidi, and W. A. J. W. Yahaya, "Adoption Strategy for Electrical and Electronics (E&E) Small and Medium-Sized Enterprises (SMEs): Malaysia IR4.0 Perspective," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 28, no. 3, pp. 27–38, 2022, doi: 10.37934/araset.28.3.2738.

[5] S. Yussof[1], M. Naz'ri Mahrin[2], and A. S. Ariffin, "Operational Research Framework of Open Innovation Business Model Strategic Plan for Malaysian Small Medium Business Enterprise in Software Industry Article history," 2022.

[6] A. Fikry, M. I. Hamzah, Z. Hussein, and D. H. Saputra, "Cyber Hygiene Practices from The Lens of Professional Youth in Malaysia," *Environment-Behaviour Proceedings Journal*, vol. 8, no. 25, pp. 187–193, Jul. 2023, doi: 10.21834/e-bpj.v8i25.4827.

[7] N. Hawani Binti Mat Tuselim and S. Binti Ya, "An Exploratory Study and Impact of Digitalisation on Malaysian SMEs Article history," 2022.

[8] B. Nor Zuriati Amani Ab Rani, M. Khairi Ismail, V. Vija Kumaran, M. Zahid bin Muhamad, and N. Shuhada Ahmad Shaupi, "Analysing the Challenges in Adopting Digitalisation among Smes: A Case Study in Malaysia," *Social Science Journal*, vol. 12, pp. 1–11, 2022.

[9] R. Bin Satter and S. Sultana Snigdha, "Cybercrime of Present Era in Society of Asia," 2023, doi: 10.13140/RG.2.2.21869.56801/1.

[10] J. Chigada and R. Madzinga, "Cyberattacks and threats during COVID-19: A systematic literature review," *SA Journal of Information Management*, vol. 23, no. 1, Feb. 2021, doi: 10.4102/sajim.v23i1.1277.

[11] World Economic Forum, "https://www.weforum.org/agenda/2023/06/cyber-insurance-security-cybercrime/#:~:text=Losses%20from%20cybercrime%20are%20expected%20to%20surge%20in%20the%20next,to%20understand%20the%20insurance%20needs.," 2023.

[12] P. Kariuki, L. O. Ofusori, and P. R. Subramaniam, “Cybersecurity threats and vulnerabilities experienced by small-scale African migrant traders in Southern Africa,” *Security Journal*, Jun. 2023, doi: 10.1057/s41284-023-00378-1.

[13] M. Neri, F. Niccolini, and L. Martino, “Organizational cybersecurity readiness in the ICT sector: a quanti-qualitative assessment,” *Information & Computer Security*, Jul. 2023, doi: 10.1108/ICS-05-2023-0084.

[14] E. Kypriotelis, G. Kolias, and P. Pappa, “The Growth of Global Risks After the COVID-19 Pandemic,” *KnE Social Sciences*, Feb. 2023, doi: 10.18502/kss.v8i1.12633.

[15] A. Alahmari and B. Duncan, “Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence,” in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment, Cyber SA 2020*, Institute of Electrical and Electronics Engineers Inc., Jun. 2020. doi: 10.1109/CyberSA49311.2020.9139638.

[16] S. B. Mohd Yusof *et al.*, “The effectiveness of Women 4IR Cyber 3A #Aware, Avoid, Act Program in Malaysia,” in *2022 International Conference on Cyber Resilience (ICCR)*, IEEE, Oct. 2022, pp. 1–5. doi: 10.1109/ICCR56254.2022.9995864.

[17] A. Alexei and A. Alexei, “The problem of information systems security in SME,” in *Central and Eastern European eDem and eGov Days 2023*, New York, NY, USA: ACM, Sep. 2023, pp. 101–105. doi: 10.1145/3603304.3603346.

[18] A. H. Adleena Huzaizi, S. N. A. Ahmad Tajuddin, K. A. Bahari, K. A. Manan, and N. N. Abd Mubin, “Cyber-Security Culture towards Digital Marketing Communications among Small and Medium-Sized (SME) Entrepreneurs,” *Asian Culture and History*, vol. 13, no. 2, p. 20, Dec. 2021, doi: 10.5539/ach.v13n2p20.

[19] A. Tolah, S. M. Furnell, and M. Papadaki, “An Empirical Analysis of the Information Security Culture Key Factors Framework,” *Computer & Security*, pp. 1–35, 2021.

[20] A. Mahfuth, “Human Factor as Insider threat in Organizations,” *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 17, no. 12, pp. 42–47, 2019, [Online]. Available: https://sites.google.com/site/ijcsis/

[21] S. S. Alam, M. Y. Ali, and M. F. M. Jani, “An empirical study of factors affecting electronic commerce adoption among SMEs in Malaysia,” *Journal of Business Economics and Management*, vol. 12, no. 2, pp. 375–399, 2011, doi: 10.3846/16111699.2011.576749.

[22] A. E. Oke, J. Aliu, P. S. Jamir Singh, S. A. Onajite, M. Shaharudin Samsurijan, and R. Azura Ramli, “Appraisal of awareness and usage of digital technologies

for sustainable wellbeing among construction workers in a developing economy," *International Journal of Construction Management*, pp. 1–9, Mar. 2023, doi: 10.1080/15623599.2023.2179628.

[23] Q. A. Abdulaziz *et al.*, "Developing an IoT Framework for Industry 4.0 in Malaysian SMEs: An Analysis of Current Status, Practices, and Challenges," *Applied Sciences (Switzerland)*, vol. 13, no. 6, Mar. 2023, doi: 10.3390/app13063658.

[24] S. Hussein, A. Alghazo, N. Humaidi, and S. Noranee, "Assessing Information Security Competencies of Firm Leaders towards Improving Procedural Information Security Countermeasure: Awareness and Cybersecurity Protective Behavior," 2023.

[25] V. Venugopal Muthuswamy, "a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International (CC BY-NC-SA 4.0) License Cyber Security Challenges Faced by Employees in the Digital Workplace of Saudi Arabia's Digital Nature Organization," *International Journal of Cyber Criminology*, vol. 17, no. 1, pp. 1–14, 2023, doi: 10.5281/zenodo.4766603.

[26] Md. ZahidulIslam, K. A. Bin Mokhtar, N. H. B. M. B. Afandi, and R. Anzum, "Regulating Online Broadcast Media against Offensive Materials in Malaysia," *Indian J Sci Technol*, vol. 14, no. 15, pp. 1233–1238, Apr. 2021, doi: 10.17485/IJST/v14i15.595.

[27] C. Ugwu, M. Ezema, U. Ome, L. Ofusori, and E. Ukwandu, "A Study on the Impact of Gender, Employment Status and Academic Discipline on Cyber Hygiene: A Case Study of University of Nigeria, Nsukka," in *In Proceedings of the International Conference on Cybersecurity, Situational Awareness and Social Media: Cyber Science*, 2023, pp. 389–407.

[28] F. Alharbi *et al.*, "The impact of cybersecurity practices on cyberattack damage: The perspective of small enterprises in Saudi Arabia," *Sensors, MDPI*, vol. 21, no. 20, Oct. 2021, doi: 10.3390/s21206901.

[29] A. Chidukwani, S. Zander, and P. Koutsakis, "A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations," *IEEE Access*, vol. 10, pp. 85701–85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

[30] M. Heidt, J. P. Gerlach, and P. Buxmann, "Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments," *Information Systems Frontiers*, vol. 21, no. 6, pp. 1285–1305, Dec. 2019, doi: 10.1007/s10796-019-09959-1.

[31] T. Tam, A. Rao, and J. Hall, "The Invisible COVID-19 Small Business Risks," *Digital Government: Research and Practice*, vol. 2, no. 2, pp. 1–8, Apr. 2021, doi: 10.1145/3436807.

[32] W. Ali, S. Malebary, A. A. Ahmed Abdullah, T. A. Abdullah, and A. Ali Ahmed, “A Review of Cyber Security Challenges, Attacks and Solutions for Internet of Things Based Smart Home,” 2019. [Online]. Available: https://www.researchgate.net/publication/336717887

[33] H. Samudra Roosman, “Information Systems Security Countermeasures: An Assessment of Older Workers in Indonesian Small and Medium-Sized of Older Workers in Indonesian Small and Medium-Sized Businesses Businesses,” 2022. [Online]. Available: https://nsuworks.nova.edu/gscis_etd

[34] S. Teufel, B. Teufel, M. Aldabbas, and M. Nguyen, “ Cyber security canvas for SMEs.,” in *In Information and Cyber Security:19th International Conference, ISSA 2020, Pretoria, South Africa, August 25–26, 2020,* 2020, pp. 20–33.

[35] I. Fernandez De Arroyabe and J. C. Fernandez de Arroyabe, “The severity and effects of Cyber-breaches in SMEs: a machine learning approach,” *Enterp Inf Syst*, vol. 17, no. 3, 2023, doi: 10.1080/17517575.2021.1942997.

[36] B. Ullah, “Developing cyber security strategies for business organization to prevent data breaches,” *KASBIT BUSINESS JOURNAL*, vol. 15, no. 4, pp. 1–18, 2022, [Online]. Available: www.kbj.kasbit.edu.pk

[37] A. Sukumar, H. A. Mahdiraji, and V. Jafari-Sadeghi, “Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors,” *Risk Analysis*, 2023, doi: 10.1111/risa.14092.

[38] V. Arya, “Cybersecurity for Small and Medium-sized Enterprises (SMEs),” *Cyber Security Insights Magazine, Vol 05,* pp. 1–4, 2022.

[39] P. Jarupunphol, N. Chouhan, M. Lloyd, and D. V. Amirtharaj, “Exploration of the Impact Cyber security awareness on Small and Medium Enterprises [SMEs] in Wales Using Intelligent Software to Combat Cybercrime.”

[40] W. C. Barker, W. Fisher, K. Scarfone, and M. Souppaya, “Ransomware risk management :,” Feb. 2022. doi: 10.6028/NIST.IR.8374.

[41] A. Almansoori, M. Al-Emran, and K. Shaalan, “Exploring the Frontiers of Cybersecurity Behavior: A Systematic Review of Studies and Theories,” *Applied Sciences*, vol. 13, no. 9, p. 5700, May 2023, doi: 10.3390/app13095700.

[42] P. Kobis, “Information risk management in SME sector enterprises,” *INTERNATIONAL SCIENTIFIC JOURNAL “INDUSTRY 4.0”* , vol. V, no. 2, pp. 1–4, 2020.

[43] Z. Aivazpour and V. S. Rao, “A Replication Study of the Impact of Impulsivity on Risky Cybersecurity Behaviors,” *AIS Transactions on Replication Research*, vol. 8, pp. 1–18, 2022, doi: 10.17705/1atrr.00074.

[44] Z. Z. F. Mthiyane, H. M. van der Poll, and M. F. Tshehla, “A Framework for Risk Management in Small Medium Enterprises in Developing Countries,” *MDPI*, vol. 10, no. 9, pp. 1–18, Sep. 2022, doi: 10.3390/risks10090173.

[45] Q. Ali, “Impact of Moral Disengagement on Counterproductive Work Behaviours in IT Sector, Pakistan,” in *Proceedings of the 21st European Conference on Cyber Warfare and Security*, 2022, pp. 25–36.

[46] M. Alsharif, S. Mishra, and M. AlShehri, “Impact of Human Vulnerabilities on Cybersecurity,” *Computer Systems Science and Engineering*, vol. 40, no. 3, pp. 1153–1166, Sep. 2021, doi: 10.32604/CSSE.2022.019938.

[47] T. Ncubukezi, “Human Errors: A Cybersecurity Concern and the Weakest Link to Small Businesses,” in *Proceedings of the 17th International Conference on Information Warfare and Security*, 2022, p. 395.

[48] M. Mburu and S. Mckeever, “CYBER SECURITY IN SMALL AND MEDIUM ENTERPRISES Perceived Challenges of Implementing Machine Learning-Based Intrusion Detection Systems In Small and Medium Enterprises,” 2023.

[49] S. Purkait and M. Damle, “Cyber Security and Frameworks: A Study of Cyber Attacks and Methods of Prevention of Cyber Attacks,” in *2023 International Conference on Sustainable Computing and Data Communication Systems (ICSCDS)*, IEEE, Mar. 2023, pp. 1310–1315. doi: 10.1109/ICSCDS56580.2023.10104823.

[50] S. Alahmari, K. Renaud, and I. Omoronyia, “Moving beyond cyber security awareness and training to engendering security knowledge sharing,” *Information Systems and e-Business Management*, vol. 21, no. 1, pp. 123–158, Mar. 2023, doi: 10.1007/s10257-022-00575-2.

[51] A. Alexei and A. Alexei, “THE DIFFERENCE BETWEEN CYBER SECURITY VS INFORMATION SECURITY,” *Journal of Engineering Science*, vol. 29, no. 4, pp. 72–83, Jan. 2023, doi: 10.52326/jes.utm.2022.29(4).08.

[52] A. K. Al Aamer and A. Hamdan, “Cyber Security Awareness and SMEs’ Profitability and Continuity: Literature Review,” 2023, pp. 593–604. doi: 10.1007/978-981-99-6101-6_43.

[53] S. A. Pawar and H. Palivela, “Importance of Least Cybersecurity Controls for Small and Medium Enterprises (SMEs) for Better Global Digitalised Economy,” 2023, pp. 21–53. doi: 10.1108/S1569-37592023000110B002.

[54] T. Rajaretnam, “A REVIEW OF DATA GOVERNANCE REGULATION, PRACTICES AND CYBER SECURITY STRATEGIES FOR BUSINESSES: AN AUSTRALIAN PERSPECTIVE,” 2020. [Online]. Available: http://myjms.moe.gov.my/index.php/ijtmis

[55] B. Mat, S. D. M. Pero, K. T. Zengeni, and A. Fakhrorazi, “Towards an Understanding of Emerging Cybersecurity Challenges of a Small State: A Case Study of Malaysia.,” *Tamkang Journal of International Affairs*, vol. 25, no. 3, pp. 45–107, 2022.

[56] M. A. Salem and A. E. E. Sobaih, “A Quadruple ‘E’ Approach for Effective Cyber-Hygiene Behaviour and Attitude toward Online Learning among Higher-Education Students in Saudi Arabia amid COVID-19 Pandemic,” *Electronics (Basel)*, vol. 12, no. 10, p. 2268, May 2023, doi: 10.3390/electronics12102268.

[57] T. Tam, A. Rao, and J. Hall, “The Good, The Bad and The Missing: A Narrative Review of Cyber-security Implications for Australian Small Businesses,” *Computer & Security*, pp. 1–56, Sep. 2021, doi: 10.1016/j.cose.2021.102385.

[58] M. M. A. Mutalib, Z. Zainol, and M. H. M. Halip, “Mitigating Malware Threats at Small Medium Enterprise (SME) Organisation: A Review and Framework,” in *2021 6th IEEE International Conference on Recent Advances and Innovations in Engineering, ICRAIE 2021*, Institute of Electrical and Electronics Engineers Inc., Feb. 2022. doi: 10.1109/ICRAIE52900.2021.9703991.

[59] H. Hakimi *et al.*, “SOFTWARE SECURITY READINESS MODEL FOR REMOTE WORKING IN MALAYSIAN PUBLIC SECTORS: CONCEPTUAL FRAMEWORK,” *J Theor Appl Inf Technol*, vol. 101, no. 8, 2023, [Online]. Available: www.jatit.org

[60] M. Maskun, I. Irwansyah, A. Yunus, A. Safira, and S. N. Lubis, “Cyber-Attack: Its Definition, Regulation, and ASEAN Cooperation to Handle with it,” *Jambe Law Journal*, vol. 4, no. 2, pp. 131–150, Nov. 2021, doi: 10.22437/jlj.4.2.131-150.

[61] CHUBB, “Malaysia SME Cyber Preparedness Report 2019, Chubb. [online] Available at: https://www.chubb.com/myen/ articles/malaysia-sme-cyber-preparedness-report-2019.aspx ,” Feb. 2019.

[62] M. Bada and J. R. C. Nurse, “Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs),” *Information and Computer Security*, vol. 27, no. 3, pp. 393–410, Jul. 2019, doi: 10.1108/ICS-07-2018-0080.

[63] M. C. Holland and J. M. Burchell, “Low Resource Availability and the Small-to Medium-sized Retail Enterprise’s Ability to Implement an Information Security Strategy,” *Business Management Research & Applications: A Cross-Disciplinary Journal*, vol. 1, no. 2, 2022, [Online]. Available: https://orcid.org/0000-0003-4927-5489

[64] A. Chidukwani, S. Zander, and P. Koutsakis, “A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations,” *IEEE Access*, 2022, doi: 10.1109/ACCESS.2022.3197899.

[65] H. Pathirana, “Use of Security Culture to Contribute on Enterprise Information Security for the Small and Medium Scale Enterprises (SMEs),” in *13th International Research Conference General Sir John Kotelawala Defence University*, pp. 1–9.

[66] P. Veerasingam, S. Abd Razak, A. Faisal Amri Abidin, M. Afendee Mohamed, and S. Dhalila Mohd Satar, “INTRUSION DETECTION AND PREVENTION SYSTEM IN SME’S LOCAL NETWORK BY USING SURICATA,” *MALAYSIAN JOURNAL OF COMPUTING AND APPLIED MATHEMATICS*, vol. 6, no. 1, 2023, doi: 10.37231/myjcam.2023.6.1.88.

[67] S. A. W. Saeedi, S. Juwaidah, and W. K. S. Kelly, “Intention On Adoption Of Industry 4.0 Technology Among Small And Medium Enterprises Article in,” *International Journal of Scientific & Technology Research*, vol. 9, p. 2, 2021, [Online]. Available: www.ijstr.org

[68] D. Pérez-González, S. T. Preciado, and P. Solana-Gonzalez, “Organizational practices as antecedents of the information security management performance: An empirical investigation,” *Information Technology and People*, vol. 32, no. 5, pp. 1262–1275, Sep. 2019, doi: 10.1108/ITP-06-2018-0261.

[69] L. Hadlington, J. Binder, and N. Stanulewicz, “Exploring role of moral disengagement and counterproductive work behaviours in information security awareness.,” *Comput Human Behav*, vol. 114, Jan. 2021, doi: 10.1016/j.chb.2020.106557.

[70] S. Kalhoro, M. Rehman, V. Ponnusamy, and F. B. Shaikh, “Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review,” *IEEE Access*, vol. 9. Institute of Electrical and Electronics Engineers Inc., pp. 99339–99363, 2021. doi: 10.1109/ACCESS.2021.3097144.

[71] A. Tamjidyamcholo, M. S. Bin Baba, H. Tamjid, and R. Gholipour, “Information security - Professional perceptions of knowledge-sharing intention under self-efficacy, trust, reciprocity, and shared-language,” *Comput Educ*, vol. 68, pp. 223–232, 2013, doi: 10.1016/j.compedu.2013.05.010.

[72] F. Abu-Amara, R. Almansoori, S. Alharbi, M. Alharbi, and A. Alshehhi, “A novel SETA-based gamification framework to raise cybersecurity awareness,” *International Journal of Information Technology (Singapore)*, vol. 13, no. 6, pp. 2371–2380, Dec. 2021, doi: 10.1007/s41870-021-00760-5.

[73] I. Ajzen, “The theory of planned behavior,” *Organ Behav Hum Decis Process*, vol. 50, no. 2, pp. 179–211, Dec. 1991, doi: 10.1016/0749-5978(91)90020-T.

[74] T. E. Gasiba, U. Lechner, and M. Pinto-Albuquerque, “CyberSecurity Challenges for Software Developer Awareness Training in Industrial Environments,” Feb. 2021, [Online]. Available: http://arxiv.org/abs/2102.05345

[75] V. Balakrishnan, “Actions, emotional reactions and cyberbullying – From the lens of bullies, victims, bully-victims and bystanders among Malaysian young adults,” *Telematics and Informatics*, vol. 35, no. 5, pp. 1190–1200, 2018, doi: 10.1016/j.tele.2018.02.002.

[76] K.-K. Soong, E. M. Ahmed, and K. S. Tan, “Factors influencing Malaysian small and medium enterprises adoption of electronic government procurement,” *Journal of Public Procurement*, vol. 20, no. 1, pp. 38–61, Jan. 2020, doi: 10.1108/JOPP-09-2019-0066.

[77] MSME Statistics, “http://www.smecorp.gov.my/index.php/en/policies/2020-02-11-08-01-24/sme-statistics.”

[78] I. Ajzen and M. Fishbein, “8-918e.g., Calder & Ross,” Tittle & Hill, 1977.

[79] H. C. Pham, I. Ulhaq, M. N. Nguyen, and M. Nkhoma, “An Exploratory Study of the Effects of Knowledge Sharing Methods on Cyber Security Practice.”

[80] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, “Information security conscious care behaviour formation in organizations,” *Comput Secur*, vol. 53, pp. 65–78, Jun. 2015, doi: 10.1016/j.cose.2015.05.012.

[81] L. C. de Kok, D. Oosting, and M. Spruit, “The Influence of Knowledge and Attitude on Intention to Adopt Cybersecure Behaviour,” *Information & Security: An International Journal*, vol. 46, no. 3, pp. 251–266, 2020, doi: 10.11610/isij.4618.

[82] S. Kabanda, M. Tanner, and C. Kent, “Exploring SME cybersecurity practices in developing countries,” *Journal of Organizational Computing and Electronic Commerce*, vol. 28, no. 3, pp. 269–282, Jul. 2018, doi: 10.1080/10919392.2018.1484598.

[83] N. S. Safa and R. Von Solms, “An information security knowledge sharing model in organizations,” *Comput Human Behav*, vol. 57, pp. 442–451, Apr. 2016, doi: 10.1016/j.chb.2015.12.037.

[84] J. Shropshire, M. Warkentin, and S. Sharma, “Personality, attitudes, and intentions: Predicting initial adoption of information security behavior,” *Comput Secur*, vol. 49, pp. 177–191, Mar. 2015, doi: 10.1016/j.cose.2015.01.002.

[85] A. Kovacevic, N. Putnik, and O. Toskovic, “Factors Related to Cyber Security Behavior,” *IEEE Access*, vol. 8, pp. 125140–125148, 2020, doi: 10.1109/ACCESS.2020.3007867.

[86] R. S. Deora and D. M. Chudasama, “Brief Study of Cybercrime on an Internet Information Systems Audits for eCommerce View project Grocery Deals View project,” *Journal of Communication Engineering & Systems*, vol. 11, no. 1, pp. 1–7, 2021, doi: 10.37591/JoCES.

[87] A. R. Neigel, V. L. Claypoole, G. E. Waldfogle, S. Acharya, and G. M. Hancock, “Holistic cyber hygiene education: Accounting for the human factors,” *Comput Secur*, vol. 92, May 2020, doi: 10.1016/j.cose.2020.101731.

[88] G. Laws, M. Nowatkowski, J. Heslen, and S. Vericella, “Guidelines for Cyber Hygiene in Online Education,” 2018. [Online]. Available: http://cyber.army.mil/Events/CyCON-US/.

[89] A. Vishwanath *et al.*, “Cyber hygiene: The concept, its measure, and its initial tests,” *Decis Support Syst*, vol. 128, Jan. 2020, doi: 10.1016/j.dss.2019.113160.

[90] A. A. Cain, M. E. Edwards, and J. D. Still, “An exploratory study of cyber hygiene behaviors and knowledge,” *Journal of Information Security and Applications*, vol. 42, pp. 36–45, Oct. 2018, doi: 10.1016/j.jisa.2018.08.002.

[91] D. Singh, S. O. Anusandhan, S. Swagatika, and S. Kumar, “Cyber-hygiene: The key Concept for Cyber Security in Cyberspace Evaluation of Scheduling and Load Balancing Techniques In Mobile Grid Architecture View project SLA-aware task allocation with resource optimisation on cloud environment View project,” *TEST Engineering and management*, vol. 83, pp. 8145–8152, 2020, [Online]. Available: https://www.researchgate.net/publication/342069141

[92] A. M. Abukari and E. Kwedzo Bankas, “Some Cyber Security Hygienic Protocols For Teleworkers In Covid-19 Pandemic Period And Beyond,” *Int J Sci Eng Res*, vol. 11, no. 4, 2020, [Online]. Available: http://www.ijser.org

[93] M. Trevors and C. M. Wallen, “Cyber Hygiene: A Baseline Set of Practices,” 2017.

[94] M. A. Almomani *et al.*, “Using an Expert Panel to Validate the Malaysian SMEs-Software Process Improvement Model (MSME-SPI),” in *Software Engineering Perspectives in Intelligent Systems: Proceedings of 4th Computational Methods in Systems and Software 2020, Vol. 1 4* . , 2020, pp. 844–859. doi: 10.1007/978-3-030-63-6_72.

[95] J. Rajamäki *et al.*, “Improving the Cybersecurity Awareness of Finnish Podiatry SMEs,” *WSEAS TRANSACTIONS ON COMPUTERS*, vol. 22, pp. 198–205, Oct. 2023, doi: 10.37394/23205.2023.22.23.

[96] T. Oluwaseun Abrahams, S. Kuzankah Ewuga, S. Onimisi Dawodu, A. Oluwatoyin Adegbite, A. Olanipekun Hassan, and C. Author, “A REVIEW OF CYBERSECURITY STRATEGIES IN MODERN ORGANIZATIONS: EXAMINING THE EVOLUTION AND EFFECTIVENESS OF CYBERSECURITY MEASURES FOR DATA PROTECTION,” *Computer Science & IT Research Journal*, vol. 5, no. 1, pp. 1–25, 2024, doi: 10.51594/csitrj.v5i.699.

[97] R. Heartfield and G. Loukas, “Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework,” *Computer & Security*, pp. 101–127, 2018.

[98] N. Sohrabi Safa, R. Von Solms, and S. Furnell, “Information security policy compliance model in organizations,” *Comput Secur*, vol. 56, pp. 70–82, Feb. 2016, doi: 10.1016/j.cose.2015.10.006.

[99] K. Renaud and J. Ophoff, “A cyber situational awareness model to predict the implementation of cyber security controls and precautions by SMEs,” *Organizational Cybersecurity Journal: Practice, Process and People*, vol. 1, no. 1, pp. 24–46, Oct. 2021, doi: 10.1108/OCJ-03-2021-0004.

[100] T. Gundu, “Acknowledging and Reducing the Knowing and Doing Gap in Employee Cybersecurity Compliance,” in *14th International Conference on Cyber Warfare and Security (pp. 94-102).*, 2019, pp. 94–102. [Online]. Available: https://www.researchgate.net/publication/333044935

[101] A. Cartwright, E. Cartwright, and E. S. Edun, “Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies,” *Comput Secur*, vol. 131, p. 103288, Aug. 2023, doi: 10.1016/j.cose.2023.103288.

[102] S. Furnell, “Home working and cyber security-an outbreak of unpreparedness?,” 2020.

[103] E. Derouet, “Fighting phishing and securing data with email authentication,” *Computer Fraud and Security*, vol. 2016, no. 10, pp. 5–8, Oct. 2016, doi: 10.1016/S1361-3723(16)30079-3.

[104] H. L. Kim and J. Han, “Do employees in a ‘good’ company comply better with information security policy? A corporate social responsibility perspective,” *Information Technology and People*, vol. 32, no. 4, pp. 858–875, Sep. 2019, doi: 10.1108/ITP-09-2017-0298.

[105] W. He, Z. (Justin) Zhang, and W. Li, “Information technology solutions, challenges, and suggestions for tackling the COVID-19 pandemic,” *Int J Inf Manage*, vol. 57, Apr. 2021, doi: 10.1016/j.ijinfomgt.2020.102287.

[106] D. J. Borkovich and R. J. Skovira, “WORKING FROM HOME: CYBERSECURITY IN THE AGE OF COVID-19,” *Issues In Information Systems*, 2020, doi: 10.48009/4_iis_2020_234-246.

[107] M. Z. Hasan, M. Z. Hussain, I. Alam, N. Sarwar, A. M. Qureshi, and A. Irshad, “Impact of Cybercrime on Enterprises in Cloud Computing Environment: A Review,” in *2023 IEEE International Conference on Emerging Trends in Engineering, Sciences and Technology (ICES&T)*, IEEE, Jan. 2023, pp. 1–6. doi: 10.1109/ICEST56843.2023.10138873.

[108] M. Yıldırım and I. Mackie, “Encouraging users to improve password security and memorability,” *Int J Inf Secur*, vol. 18, no. 6, pp. 741–759, Dec. 2019, doi: 10.1007/s10207-019-00429-y.

[109] J. M. Biju, N. Gopal, and A. J. Prakash, “CYBER ATTACKS AND ITS DIFFERENT TYPES,” *International Research Journal of Engineering and Technology*, 2008, [Online]. Available: www.irjet.net

[110] N. F. M. Zaharon and M. Mohd Ali, “Phishing as Cyber Fraud: The Implications and Governance,” *HONG KONG JOURNAL OF SOCIAL SCIENCES*, vol. 57, pp. 120–133, 2021, [Online]. Available: www.malaysiaairlines.com,

[111] I. Ajzen, S. Lohmann, and D. Albarracin, “THE INFLUENCE OF ATTITUDES ON BEHAVIOR,” 2018. [Online]. Available: https://www.researchgate.net/publication/325114583

[112] Alireza Shojaifar, “Volitional Cybersecurity,” Utrecht University, 2023. doi: 10.33540/1953.

[113] J. Kaur and N. Mustafa, “Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME,” in *International Conference on Research and Innovation in Information Systems, ICRIIS*, 2013, pp. 286–290. doi: 10.1109/ICRIIS.2013.6716723.

[114] J. Abawajy, “User preference of cyber security awareness delivery methods,” *Behaviour and Information Technology*, vol. 33, no. 3, pp. 237–248, Mar. 2014, doi: 10.1080/0144929X.2012.708787.

[115] L. C. de Kok, D. Oosting, and M. Spruit, “The Influence of Knowledge and Attitude on Intention to Adopt Cybersecure Behaviour,” *Information & Security: An International Journal*, vol. 46, no. 3, pp. 251–266, 2020, doi: 10.11610/isij.4618.

[116] A. M. Ghouri, N. R. Khan, and O. B. Abdul Kareem, “Improving Employees Behavior through Extension in Theory of Planned Behavior: A Theoretical Perspective for SMEs,” *International Journal of Business and Management*, vol. 11, no. 11, p. 196, Oct. 2016, doi: 10.5539/ijbm.v11n11p196.

[117] D. J. Howard, “Development of the Cybersecurity Attitudes Scale and Modeling Cybersecurity Behavior and its Antecedents,” PhD Thesis, College of Arts and Sciences, University of South Florida, 2018. [Online]. Available: https://scholarcommons.usf.edu/etd

[118] N. Etezady, “A Common Description and Measures for Attitude in Information Security for Organizations,” *International Journal of Cyber Research and Education*, vol. 1, no. 2, pp. 1–11, Jul. 2019, doi: 10.4018/IJCRE.2019070101.

[119] D. P. Johnson, “ScholarWorks How Attitude Toward the Behavior, Subjective Norm, and Perceived Behavioral Control Affects Information Security Behavior Intention,” 2017. [Online]. Available: https://scholarworks.waldenu.edu/dissertations

[120] A. Farooq, J. Rumo, A. Ndiege, and J. Isoaho, “Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior; Factors Affecting Security Behavior of Kenyan Students: An Integration of Protection Motivation Theory and Theory of Planned Behavior,” 2019.

[121] C. Hiranrat, A. Harncharnchai, and C. Duangjan, “Theory of Planned Behavior and the Influence of Communication Self-Efficacy on Intention to Pursue a Software Development Career,” *Journal of Information Systems Education*, vol. 32, no. 1, pp. 40–52, 2021.

[122] C. Castanier, T. Deroche, and T. Woodman, “Theory of planned behaviour and road violations: The moderating influence of perceived behavioural control,” *Transp Res Part F Traffic Psychol Behav*, vol. 18, pp. 148–158, 2013, doi: 10.1016/j.trf.2012.12.014.

[123] C. Gerdenitsch, D. Wurhofer, and M. Tscheligi, “Working conditions and cybersecurity: Time pressure, autonomy and threat appraisal shaping employees’ security behavior,” *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, vol. 17, no. 4, Sep. 2023, doi: 10.5817/CP2023-4-7.

[124] M. Zwilling, G. Klien, D. Lesjak, Ł. Wiechetek, F. Cetin, and H. N. Basim, “Cyber Security Awareness, Knowledge and Behavior: A Comparative Study,” *Journal of Computer Information Systems*, vol. 62, no. 1, pp. 82–97, 2022, doi: 10.1080/08874417.2020.1712269.

[125] C. Conetta, “Individual Differences in Cyber Security,” *McNair Research Journal SJSU*, vol. 15, Jun. 2019, doi: 10.31979/mrj.2019.1504.

[126] M. Antunes, C. Silva, and F. Marques, “An Integrated Cybernetic Awareness Strategy to Assess Cybersecurity Attitudes and Behaviours in School Context,” *Applied Sciences*, vol. 11, no. 23, p. 11269, Nov. 2021, doi: 10.3390/app112311269.

[127] J.-W. Lian, “Understanding cloud-based BYOD information security protection behaviour in smart business: in perspective of perceived value,” *Enterp Inf Syst*, vol. 15, no. 9, pp. 1216–1237, Oct. 2021, doi: 10.1080/17517575.2020.1791966.

[128] J. S. Cheah, S. Mohd Isa, and S. Yang, “The Impact of Perceived Usefulness, Perceived Value, and Perceived Security on Mobile Payment App Loyalty through Satisfaction: User Interface as Moderator,”

[129] R. Apau and F. N. Koranteng, “Impact of cybercrime and trust on the use of e-commerce technologies: An application of the theory of planned behavior,” *International Journal of Cyber Criminology*, vol. 13, no. 2, pp. 228–254, Jul. 2019, doi: 10.5281/zenodo.3697886.

[130] L. Hadlington, J. Binder, and N. Stanulewicz, “Fear of Missing out Predicts Employee Information Security Awareness above Personality Traits, Age, and Gender,” *Cyberpsychol Behav Soc Netw*, vol. 23, no. 7, pp. 459–464, Jul. 2020, doi: 10.1089/cyber.2019.0703.

[131] P. Lopez-Aguilar and A. Solanas, “Human Susceptibility to Phishing Attacks Based on Personality Traits: The Role of Neuroticism,” in *2021 IEEE 45th Annual Computers, Software, and Applications Conference (COMPSAC)*, IEEE, Jul. 2021, pp. 1363–1368. doi: 10.1109/COMPSAC51774.2021.00192.

[132] E. D. Frauenstein and S. Flowerday, “Susceptibility to phishing on social network sites: A personality information processing model,” *Comput Secur*, vol. 94, p. 101862, Jul. 2020, doi: 10.1016/j.cose.2020.101862.

[133] L. de F. Carvalho, G. Pianowski, and A. P. Gonçalves, “Personality differences and COVID-19: are extroversion and conscientiousness personality traits associated with engagement with containment measures?,” *Trends Psychiatry Psychother*, vol. 42, no. 2, pp. 179–184, Jun. 2020, doi: 10.1590/2237-6089-2020-0029.

[134] J. Shropshire, M. Warkentin, and S. Sharma, “Personality, attitudes, and intentions: Predicting initial adoption of information security behavior,” *Comput Secur*, vol. 49, pp. 177–191, 2015, doi: 10.1016/j.cose.2015.01.002.

[135] Y. Hong and S. Furnell, “Organizational formalization and employee information security behavioral intentions based on an extended TPB model,” 2019.

[136] H. Al Jardali, F. Abdallah, and K. Barbar, “Measuring Intentions among Employees toward the Use of a Balanced Scorecard and Information System: A Conceptual Approach Using the Theory of Planned Behavior and the Technology Acceptance Model,” *Procedia Economics and Finance*, vol. 26, pp. 1146–1151, 2015, doi: 10.1016/s2212-5671(15)00944-2.

[137] J. Zhang, B. J. Reithel, and H. Li, “Impact of perceived technical protection on security behaviors,” *Information Management and Computer Security*, vol. 17, no. 4, pp. 330–340, Oct. 2009, doi: 10.1108/09685220910993980.

[138] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, “Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q),” *Comput Secur*, vol. 42, pp. 165–176, 2014, doi: 10.1016/j.cose.2013.12.003.

[139] T. Sommestad, H. Karlzén, and J. Hallberg, “The sufficiency of the theory of planned behavior for explaining information security policy compliance,” *Information and Computer Security*, vol. 23, no. 2, pp. 200–217, 2015, doi: 10.1108/ICS-04-2014-0025.

[140] Y. Hong and S. Furnell, “Organizational formalization and employee information security behavioral intentions based on an extended TPB model,” in *2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, IEEE, Jun. 2019, pp. 1–4. doi: 10.1109/CyberSecPODS.2019.8885405.

[141] N. S. Sulaiman, M. A. Fauzi, W. Wider, J. Rajadurai, S. Hussain, and S. A. Harun, “Cyber–Information Security Compliance and Violation Behaviour in Organisations: A Systematic Review,” *Soc Sci*, vol. 11, no. 9, p. 386, Aug. 2022, doi: 10.3390/socsci11090386.

[142] T. van Steen and J. R. A. Deeleman, “Successful Gamification of Cybersecurity Training,” *Cyberpsychol Behav Soc Netw*, vol. 24, no. 9, pp. 593–598, Sep. 2021, doi: 10.1089/cyber.2020.0526.

[143] K. H. Chan, L.-L. Chong, and T. H. Ng, “Integrating extended theory of planned behaviour and norm activation model to examine the effects of environmental practices among Malaysian companies,” *Journal of Entrepreneurship in Emerging Economies*, vol. 14, no. 5, pp. 851–873, Nov. 2022, doi: 10.1108/JEEE-08-2021-0317.

[144] S. GaikLan, S. R. M. Zainal, and A. Amran, “The theory of planned behaviour and transformational leadership: an examination of corporate philanthropy among SMEs in Malaysia,” *International Journal of Sustainable Strategic Management*, vol. 7, no. 1/2, p. 67, 2019, doi: 10.1504/IJSSM.2019.099034.

[145] I. Ajzen, “From intentions to actions: A theory of planned behavior. In Action control,” in *Springer, Berlin, Heidelberg.*, 1985, pp. 11–39.

[146] N. S. Safa and R. Von Solms, “An information security knowledge sharing model in organizations,” *Comput Human Behav*, vol. 57, pp. 442–451, Apr. 2016, doi: 10.1016/j.chb.2015.12.037.

[147] L. Hadlington, “Human factors in cybersecurity; examining the link between [3 _ T D $ D I F F] Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours,” *Heliyon*, vol. 3, p. 346, 2017, doi: 10.1016/j.heliyon.2017.

[148] M. , Fishbein and I. Ajzen, *Belief, Attitude, Intention, and Behavior: An Introduction to Theory and Research.* Addison-Wesley, 1975.

[149] L. Mura, T. Zsigmond, and R. Machová, “The effects of emotional intelligence and ethics of SME employees on knowledge sharing in Central-European countries,” *Oeconomia Copernicana*, vol. 12, no. 4, pp. 907–934, Dec. 2021, doi: 10.24136/oc.2021.030.

[150] Amitabh Anand and Audrey Dalmasso, “Supervisor Effects on Employee Knowledge Sharing Behaviour in SMEs,” *Journal of the Knowledge Economy (SpringerLink)*, pp. 1430–1453, 2020.

[151] M. Yasir, A. Majid, Z. Yousaf, A. A. Nassani, and M. Haffar, “An integrative framework of innovative work behavior for employees in SMEs linking knowledge sharing, functional flexibility and psychological empowerment,” *European Journal of Innovation Management*, vol. 26, no. 2, pp. 289–308, Mar. 2023, doi: 10.1108/EJIM-02-2021-0091.

[152] J. Ortiz, S.-H. Chang, W.-H. Chih, and C.-H. Wang, “The contradiction between self-protection and self-presentation on knowledge sharing behavior,” *Comput Human Behav*, vol. 76, pp. 406–416, Nov. 2017, doi: 10.1016/j.chb.2017.07.031.

[153] N. U. Zia, “Knowledge-oriented leadership, knowledge management behaviour and innovation performance in project-based SMEs. The moderating role of goal orientations,” *Journal of Knowledge Management*, vol. 24, no. 8, pp. 1819–1839, Jul. 2020, doi: 10.1108/JKM-02-2020-0127.

[154] D. Magni, R. Chierici, M. Fait, and K. Lefebvre, “A network model approach to enhance knowledge sharing for internationalization readiness of SMEs,” *International Marketing Review*, vol. 39, no. 3, pp. 626–652, Jun. 2022, doi: 10.1108/IMR-03-2021-0110.

[155] L.-W. Wong, V.-H. Lee, G. W.-H. Tan, K.-B. Ooi, and A. Sohal, “The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities,” *Int J Inf Manage*, vol. 66, p. 102520, Oct. 2022, doi: 10.1016/j.ijinfomgt.2022.102520.

[156] N. Virmani, S. Sharma, A. Kumar, and S. Luthra, “Adoption of industry 4.0 evidence in emerging economy: Behavioral reasoning theory perspective,” *Technol Forecast Soc Change*, vol. 188, p. 122317, Mar. 2023, doi: 10.1016/j.techfore.2023.122317.

[157] A. Onumo, I. Ullah-Awan, and A. Cullen, “Assessing the Moderating Effect of Security Technologies on Employees Compliance with Cybersecurity Control Procedures,” *ACM Trans Manag Inf Syst*, vol. 12, no. 2, pp. 1–29, Jun. 2021, doi: 10.1145/3424282.

[158] X. T. NGUYEN and Q. K. LUU, “Factors Affecting Adoption of Industry 4.0 by Small- and Medium-Sized Enterprises: A Case in Ho Chi Minh City, Vietnam,” *The Journal of Asian Finance, Economics and Business*, vol. 7, no. 6, pp. 255–264, Jun. 2020, doi: 10.13106/jafeb.2020.vol7.no6.255.

[159] M. Alanazi, M. Freeman, and H. Tootell, “Exploring the factors that influence the cybersecurity behaviors of young adults,” *Comput Human Behav*, vol. 136, p. 107376, Nov. 2022, doi: 10.1016/j.chb.2022.107376.

[160] H. G. Alotaibi and M. E. Aloud, “Investigating Behavior Intention Toward S-Commerce Adoption by Small Businesses in Saudi Arabia,” *International Journal of E-Business Research*, vol. 19, no. 1, pp. 1–27, Apr. 2023, doi: 10.4018/IJEBR.322094.

[161] N. P. Matlala, “Behavioural Insights Into Cybersecurity Practices Among Digital Banking Consumers in South Africa,” *Indonesian Journal of Business Analytics*, vol. 3, no. 4, pp. 1425–1442, Sep. 2023, doi: 10.55927/ijba.v3i4.5515.

[162] M. Tischer *et al.*, “Users Really Do Plug in USB Drives They Find,” in *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, Institute of Electrical and Electronics Engineers Inc., Aug. 2016, pp. 306–319. doi: 10.1109/SP.2016.26.

[163] L. Hadlington, M. Popovac, H. Janicke, I. Yevseyeva, and K. Jones, “Exploring the role of work identity and work locus of control in information security awareness,” *Comput Secur*, vol. 81, pp. 41–48, Mar. 2019, doi: 10.1016/j.cose.2018.10.006.

[164] L. Bekkers, S. van ’t Hoff-de Goede, E. Misana-ter Huurne, Y. van Houten, R. Spithoven, and E. R. Leukfeldt, “Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model,” *Comput Secur*, vol. 127, p. 103099, Apr. 2023, doi: 10.1016/j.cose.2023.103099.

[165] Olfa Ismail, “Designing Information Security Culture Artifacts to Improve Security Behavior: An Evaluation in SMEs,” in *International Conference on Design Science Research in Information Systems and Technology*, 2022, p. 1.

[166] Z. Awang, A. Rahlin, and A. Afthanorhan, “Conceptual framework for the best practices of behavior-based safety performance evaluation in small and

medium enterprises (SMEs)," *Journal of Applied Engineering Science*, vol. 17, no. 4, pp. 504–513, 2019, doi: 10.5937/jaes17-19962.

[167] L. Bekkers, S. van 't Hoff-de Goede, E. Misana-ter Huurne, Y. van Houten, R. Spithoven, and E. R. Leukfeldt, "Protecting your business against ransomware attacks? Explaining the motivations of entrepreneurs to take future protective measures against cybercrimes using an extended protection motivation theory model," *Comput Secur*, vol. 127, p. 103099, Apr. 2023, doi: 10.1016/j.cose.2023.103099.

[168] Z. Abet, M. Ashraff Mohd Anuar, M. Mursyid Arshad, and I. Arif Ismail, "Factors Affecting Turnover Intention of Nigerian Employees: The Moderation Effect of Organizational Commitment," 2023, doi: 10.20944/preprints202306.2229.v1.

[169] H. Prapavessis, A. Gaston, and S. DeJesus, "The Theory of Planned Behavior as a model for understanding sedentary behavior," *Psychol Sport Exerc*, vol. 19, pp. 23–32, Jul. 2015, doi: 10.1016/j.psychsport.2015.02.001.

[170] S. Abdul, W. Saeedi, J. Sharifuddin, K. Wong, and K. Seng, "Intention On Adoption Of Industry 4.0 Technology Among Small And Medium Enterprises," *INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH*, vol. 9, p. 2, 2020, [Online]. Available: www.ijstr.org

[171] Q. A. Aigbefo, Y. Blount, and M. Marrone, "The influence of hardiness and habit on security behaviour intention," *Behaviour & Information Technology*, vol. 41, no. 6, pp. 1151–1170, Apr. 2022, doi: 10.1080/0144929X.2020.1856928.

[172] S. Rakshit, N. Islam, S. Mondal, and T. Paul, "Mobile apps for SME business sustainability during COVID-19 and onwards," *J Bus Res*, vol. 135, pp. 28–39, Oct. 2021, doi: 10.1016/j.jbusres.2021.06.005.

[173] I. Arpaci and M. Baloɬlu, "The impact of cultural collectivism on knowledge sharing among information technology majoring undergraduates," *Comput Human Behav*, vol. 56, pp. 65–71, Mar. 2016, doi: 10.1016/j.chb.2015.11.031.

[174] H. Y. S. Tsai, M. Jiang, S. Alhabash, R. Larose, N. J. Rifon, and S. R. Cotten, "Understanding online safety behaviors: A protection motivation theory perspective," *Comput Secur*, vol. 59, pp. 138–150, Jun. 2016, doi: 10.1016/j.cose.2016.02.009.

[175] M. R. Adisty, J. M. Mundandar, and I. M. Sumertajaya, "Factors Influencing Informal Workers' Registration for Social Security: A Comparative Analysis Between Indonesia and Taiwan," *Jurnal Aplikasi Bisnis dan Manajemen*, May 2023, doi: 10.17358/jabm.9.2.523.

[176] T. Sommestad, H. Karlzén, P. Nilsson, and J. Hallberg, “An empirical test of the perceived relationship between risk and the constituents severity and probability,” *Information and Computer Security*, vol. 24, no. 2, pp. 194–204, 2016, doi: 10.1108/ICS-01-2016-0004.

[177] M. van Haastrecht, I. Sarhan, A. Shojaifar, L. Baumgartner, W. Mallouli, and M. Spruit, “A Threat-Based Cybersecurity Risk Assessment Approach Addressing SME Needs,” in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, New York, NY, USA: ACM, Aug. 2021, pp. 1–12. doi: 10.1145/3465481.3469199.

[178] A. Shojaifar and H. Järvinen, “Classifying SMEs for Approaching Cybersecurity Competence and Awareness,” in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, New York, NY, USA: ACM, Aug. 2021, pp. 1–7. doi: 10.1145/3465481.3469200.

[179] M. Wilson, S. McDonald, D. Button, and K. McGarry, “It Won’t Happen to Me: Surveying SME Attitudes to Cyber-security,” *Journal of Computer Information Systems*, vol. 63, no. 2, pp. 397–409, Mar. 2023, doi: 10.1080/08874417.2022.2067791.

[180] M. Siponen, M. Adam Mahmood, and S. Pahnila, “Employees’ adherence to information security policies: An exploratory field study,” *Information and Management*, vol. 51, no. 2, pp. 217–224, Mar. 2014, doi: 10.1016/j.im.2013.08.006.

[181] L.-W. Wong, V.-H. Lee, G. W.-H. Tan, K.-B. Ooi, and A. Sohal, “The role of cybersecurity and policy awareness in shifting employee compliance attitudes: Building supply chain capabilities,” *Int J Inf Manage*, vol. 66, p. 102520, Oct. 2022, doi: 10.1016/j.ijinfomgt.2022.102520.

[182] K. A. Saban, S. Rau, and C. A. Wood, ““SME executives’ perceptions and the information security preparedness model”,” *Information & Computer Security*, vol. 29, no. 2, pp. 263–282, Aug. 2021, doi: 10.1108/ICS-01-2020-0014.

[183] I.-H. Hwang and H.-Y. Lee, “The Employee’s Information Security Policy Compliance Intention : Theory of Planned Behavior, Goal Setting Theory, and Deterrence Theory Applied,” *Journal of Digital Convergence*, pp. 155–166, 2016.

[184] L. Alzahrani and K. P. Seth, “The Impact of Organizational Practices on the Information Security Management Performance,” *Information*, vol. 12, no. 10, p. 398, Sep. 2021, doi: 10.3390/info12100398.

[185] Y. E. Kim, Y. S. Kim, and H. Kim, “Effective Feature Selection Methods to Detect IoT DDoS Attack in 5G Core Network,” *Sensors*, vol. 22, no. 10, pp. 1–21, May 2022, doi: 10.3390/s22103819.

[186] P. Y. Cheng, J. Te Yang, C. S. Wan, and M. C. Chu, “Ethical contexts and employee job responses in the hotel industry: The roles of work values and perceived organizational support,” *Int J Hosp Manag*, vol. 34, no. 1, pp. 108–115, Sep. 2013, doi: 10.1016/j.ijhm.2013.03.007.

[187] J. W. Lian, “Understanding cloud-based BYOD information security protection behaviour in smart business: in perspective of perceived value,” *Enterp Inf Syst*, pp. 1–22, 2020, doi: 10.1080/17517575.2020.1791966.

[188] A.-I. Neicu, A.-C. Radu, G. Zaman, I. Stoica, and F. Răpan, “Cloud Computing Usage in SMEs. An Empirical Study Based on SMEs Employees Perceptions,” *Sustainability*, vol. 12, no. 12, p. 4960, Jun. 2020, doi: 10.3390/su12124960.

[189] S. S. Abed, “Social commerce adoption using TOE framework: An empirical investigation of Saudi Arabian SMEs,” *Int J Inf Manage*, vol. 53, p. 102118, Aug. 2020, doi: 10.1016/j.ijinfomgt.2020.102118.

[190] A. Lutfi, “Understanding the Intention to Adopt Cloud-based Accounting Information System in Jordanian SMEs,” *The International Journal of Digital Accounting Research*, pp. 47–70, Mar. 2022, doi: 10.4192/1577-8517-v22_2.

[191] A. Lutfi *et al.*, “Factors Influencing the Adoption of Big Data Analytics in the Digital Transformation Era: Case Study of Jordanian SMEs,” *Sustainability*, vol. 14, no. 3, p. 1802, Feb. 2022, doi: 10.3390/su14031802.

[192] M. Al-Okaily, A. F. Alkhwaldi, A. A. Abdulmuhsin, H. Alqudah, and A. Al-Okaily, “Cloud-based accounting information systems usage and its impact on Jordanian SMEs’ performance: the post-COVID-19 perspective,” *Journal of Financial Reporting and Accounting*, vol. 21, no. 1, pp. 126–155, Mar. 2023, doi: 10.1108/JFRA-12-2021-0476.

[193] A. A. Al-Tit, “E-COMMERCE DRIVERS AND BARRIERS AND THEIR IMPACT ON E-CUSTOMER LOYALTY IN SMALL AND MEDIUM-SIZED ENTERPRISES (SMES),” *Business: Theory and Practice*, vol. 21, no. 1, pp. 146–157, Mar. 2020, doi: 10.3846/btp.2020.11612.

[194] Y. H. Chen, T. P. Lin, and D. C. Yen, “How to facilitate inter-organizational knowledge sharing: The impact of trust,” *Information and Management*, vol. 51, no. 5, pp. 568–578, 2014, doi: 10.1016/j.im.2014.03.007.

[195] I. Akman and A. Mishra, “Gender, age and income differences in internet usage among employees in organizations,” *Comput Human Behav*, vol. 26, no. 3, pp. 482–490, May 2010, doi: 10.1016/j.chb.2009.12.007.

[196] J. Bryce and J. Fraser, “The role of disclosure of personal information in the evaluation of risk and trust in young peoples’ online interactions,” *Comput Human Behav*, vol. 30, pp. 299–306, 2014, doi: 10.1016/j.chb.2013.09.012.

[197] C. Donalds and K.-M. Osei-Bryson, “Cybersecurity compliance behavior: Exploring the influences of individual decision style and other antecedents,” *Int J Inf Manage*, vol. 51, p. 102056, Apr. 2020, doi: 10.1016/j.ijinfomgt.2019.102056.

[198] S. Anawar, D. L. Kunasegaran, M. Z. Mas’ud, and N. A. Zakaria, “ANALYSIS OF PHISHING SUSCEPTIBILITY IN A WORKPLACE: A BIG-FIVE PERSONALITY PERSPECTIVES,” 2019.

[199] S. Kalhoro, R. K. Ayyasamy, A. K. Jebna, A. Kalhoro, K. Krishnan, and S. Nodeson, “How Personality Traits Impacts on Cyber Security Behaviors of SMEs Employees,” in *2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT)*, IEEE, Nov. 2022, pp. 635–641. doi: 10.1109/3ICT56508.2022.9990621.

[200] Q. A. Aigbefo, Y. Blount, and M. Marrone, “The influence of hardiness and habit on security behaviour intention,” *Behaviour & Information Technology*, vol. 41, no. 6, pp. 1151–1170, Apr. 2022, doi: 10.1080/0144929X.2020.1856928.

[201] O. M. A. Ababneh, “Team engagement for boosting team innovative behaviour in small and medium enterprises: An integrating framework of attitudinal and trait-related determinants,” *The International Journal of Entrepreneurship and Innovation*, p. 146575032311568, Feb. 2023, doi: 10.1177/14657503231156876.

[202] E. Gimmon and L. Zysberg, “Personal characteristics of small business owners and their strategic change behavior during the COVID-19 pandemic,” *Management Research Review*, Jul. 2023, doi: 10.1108/MRR-10-2021-0721.

[203] S. Seshadri and G. M. Broekemier, “Small Business Executives’ Online Survey Response Intentions: The Effects of Incentives and Survey Length,” *Small Business Institute Journal*, vol. 18, no. 2, Jul. 2022, doi: 10.53703/001c.32575.

[204] M. Greaves, L. D. Zibarras, and C. Stride, “Using the theory of planned behavior to explore environmental behavioral intentions in the workplace,” *J Environ Psychol*, vol. 34, pp. 109–120, Jun. 2013, doi: 10.1016/j.jenvp.2013.02.003.

[205] G. Mahlangu, C. Chipfumbu Kangara, and F. Masunda, “Citizen-centric cybersecurity model for promoting good cybersecurity behaviour,” *Journal of Cyber Security Technology*, vol. 7, no. 3, pp. 154–180, Jul. 2023, doi: 10.1080/23742917.2023.2217535.

[206] J. W. Creswell, *Research design : qualitative, quantitative, and mixed methods approaches*. Sage, 2009.

[207] Frank. Crossan, “Research philosophy: Towards an understanding ,” vol. 11, no. 1, pp. 46–55, 2003.

[208] M. M. Al-Ababneh, “Linking Ontology, Epistemology and Research Methodology,” *Science & Philosophy*, vol. 8, no. 1, pp. 75–91, 2020, doi: 10.23756/sp.v8i1.500.

[209] K. Williamson and G. Johanson, “Research methods: Information, systems, and contexts,” in *Chandos Publishing.*, 2017, pp. 1–11.

[210] M. Saunders, P. Lewis, and A. Thornhill, “ Chapter 4: Understanding research philosophy and approaches to theory development,” 2012, p. 1.

[211] M. T. Holden and P. Lynch, “Choosing the Appropriate Methodology: Understanding Research Philosophy.”

[212] M. J. (2017). . Goertzen, “Introduction to quantitative research and data.,” 2017.

[213] A. D. Wahyudi and S. Kempa, “Mobile Banking Transactions for Small and Medium Enterprise (SME) RELEVANCE: Journal of Management and Business,” *RELEVANCE: Journal of Management and Business* ▪, vol. 6, no. 1.

[214] N. Hazirah, B. Hamdan, S. Binti, H. Kassim, and P. C. Lai, “THE COVID-19 PANDEMIC CRISIS ON MICRO-ENTREPRENEURS IN MALAYSIA: IMPACT AND MITIGATION APPROACHES.” [Online]. Available: www.gbse.com.my

[215] K. E. Howell, *An Introduction to the Philosophy of Methodology - Sage Publications Ltd.* 2012.

[216] Anne. Lazaraton, “‘Quantitative research methods.,’” in *Handbook of research in second language teaching and learning* , 2005, pp. 209–224.

[217] L. C. Beckett, E. Eriksson, Johansson, and C. Wikström, “Multivariate Data Analysis (MVDA). 2017.,” 2017.

[218] R. B. Kline, “Principles and Practice of Structural Equation Modeling, Fourth Edition - Rex B. Kline,” in *Google Books.*, 2011.

[219] M. , S. J. Harris, “‘Confirmatory modelling in organizational behaviour/human resource management,’ J. Manage.,” *human resource management,” J. Manage*, vol. 16, p. 2, 1990.

[220] J. F. Hair, J. J. Risher, M. Sarstedt, and C. M. Ringle, “When to use and how to report the results of PLS-SEM,” *European Business Review*, vol. 31, no. 1. Emerald Group Publishing Ltd., pp. 2–24, Jan. 14, 2019. doi: 10.1108/EBR-11-2018-0203.

[221] R. V. Krejcie and D. W. Morgan, “Determining Sample Size for Research Activities,” *Educ Psychol Meas*, vol. 30, no. 3, pp. 607–610, Sep. 1970, doi: 10.1177/001316447003000308.

[222] Amaratunga, Dilanthi;Baldry, David;Sarshar, Marjan;Newton, and Rita, “Quantitative and qualitative research in the built environment: Application of ‘mixed’ research a,” 2002.

[223] H. T. Schreuder, T. G. Gregoire, and J. P. Weyer, “FOR WHAT APPLICATIONS CAN PROBABILITY AND NON-PROBABILITY SAMPLING BE USED?,” 2001.

[224] V. Vehovar, V. Toepoel, and S. Steinmetz, “Non-probability sampling.” [Online]. Available: https://www.researchgate.net/publication/307546330

[225] I. Benbasat, D. K. Goldstein, and H. B. School, “The Case Research Strategy in Studies of Information Systems.”

[226] A. M. Kennedy, “Macro-Social Marketing Research: Philosophy, Methodology and Methods,” *Journal of Macromarketing*, vol. 37, no. 4, pp. 347–355, Dec. 2017, doi: 10.1177/0276146717735467.

[227] T. Prasad Bhatta, “Case Study Research, Philosophical Position and Theory Building: A Methodological Discussion.”

[228] G. Norman, “Likert scales, levels of measurement and the ‘laws’ of statistics,” *Advances in Health Sciences Education*, vol. 15, no. 5, pp. 625–632, Dec. 2010, doi: 10.1007/s10459-010-9222-y.

[229] S. Pabian and H. Vandebosch, “Using the theory of planned behaviour to understand cyberbullying: The importance of beliefs for developing interventions,” *European Journal of Developmental Psychology*, vol. 11, no. 4. Taylor & Francis, pp. 463–477, 2014. doi: 10.1080/17405629.2013.858626.

[230] P. Ifinedo, “Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition,” *Information and Management*, vol. 51, no. 1, pp. 69–79, 2014, doi: 10.1016/j.im.2013.10.001.

[231] K. H. Ehrhart, S. C. Roesch, M. G. Ehrhart, and B. Kilian, “ A test of the factor structure equivalence of the 50-item IPIP Five-factor model measure across gender and ethnic groups. ,” *J Pers Assess*, vol. 90, no. 5, pp. 507–516, 2008.

[232] L. R. Goldberg *et al.*, “The international personality item pool and the future of public-domain personality measures. ,” *J Res Pers*, vol. 40, no. 1, pp. 84–96, 2006.

[233] A. Bryman, “Social Research Methods,” vol. 3, no. 2, pp. 54–67, 2012.

[234] A. Petasis, “A Descriptive Analysis of the Development and the Americans with Disabilities Act.” [Online]. Available: https://www.researchgate.net/publication/356850053

[235] M. N. K. Saunders, P. LEWIS, and A. THORNHILL, *Research Methods for Business Students*, vol. 3, no. 4. 2019. doi: 10.1108/qmr.2000.3.4.215.2.

[236] U. Sekaran and R. Bougie, “Business Research Methods: A skill-building approach. ,” p. 1, 2011.

[237] U. Sekaran and R. Bougie, “ Research methods for business : a skill-building approach, Seventh. Wiley, 2016.,” *Wiley*, 2016.

[238] H. Taherdoost, “Validity and Reliability of the Research Instrument; How to Test the Validation of a Questionnaire/Survey in a Research,” *SSRN Electronic Journal*, 2016, doi: 10.2139/ssrn.3205040.

[239] A. M. Julian, C. Novitsky, K. Lee, and M. C. Ashton, “Convergent validity of three brief six-factor measures of personality,” *Pers Individ Dif*, vol. 188, p. 111436, Apr. 2022, doi: 10.1016/j.paid.2021.111436.

[240] A. M. Farrell and J. M. Rudd, “ Factor analysis and discriminant validity:a brief review of some practical issues,” 2009.

[241] M. R. Ab Hamid, W. Sami, and M. H. Mohmad Sidek, “Discriminant Validity Assessment: Use of Fornell & Larcker criterion versus HTMT Criterion,” in *Journal of Physics: Conference Series*, Institute of Physics Publishing, Sep. 2017. doi: 10.1088/1742-6596/890/1/012163.

[242] J. F. Hair, M. Sarstedt, L. Hopkins, and V. G. Kuppelwieser, “Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research,” *European Business Review*, vol. 26, no. 2. Emerald Group Publishing Ltd., pp. 106–121, 2014. doi: 10.1108/EBR-10-2013-0128.

[243] G. D. Hutcheson and N. Sofroniou, *The Multivariate Social Scientist : Introductory Statistics Using Generalized Linear Models* . London, 1999.

[244] M. R. Mullen, G. R. Milne, and P. M. Doney, “An International Marketing Application of Outlier Analysis for Structural Equations: A Methodological Note,” *Journal of International Marketing*, vol. 3, no. 1, pp. 45–62, Mar. 1995, doi: 10.1177/1069031X9500300104.

[245] C. M. Ringle, M. Sarstedt, R. Mitchell, and S. P. Gudergan, “Partial least squares structural equation modeling in HRM research,” *The International Journal of Human Resource Management*, vol. 31, no. 12, pp. 1617–1643, Jul. 2020, doi: 10.1080/09585192.2017.1416655.

[246] J. F. Hair, “A primer on partial least squares structural equations modeling (PLS-SEM),” *European Journal of Tourism research*, p. 307, 2014.

[247] J. Henseler, C. M. Ringle, and M. Sarstedt, “A new criterion for assessing discriminant validity in variance-based structural equation modeling,” *J Acad Mark Sci*, vol. 43, no. 1, pp. 115–135, Jan. 2015, doi: 10.1007/s11747-014-0403-8.

[248] R. Joshi and R. Yadav, “An Integrated SEM Neural Network Approach to Study Effectiveness of Brand Extension in Indian FMCG Industry,” *Business Perspectives and Research*, vol. 6, no. 2, pp. 113–128, Jul. 2018, doi: 10.1177/2278533718764502.

[249] A. D. Arndt, J. B. Ford, B. J. Babin, and V. Luong, “Collecting samples from online services: How to use screeners to improve data quality,” *International Journal of Research in Marketing*, vol. 39, no. 1, pp. 117–133, Mar. 2022, doi: 10.1016/j.ijresmar.2021.05.001.

[250] R. Palanisamy, A. A. Norman, and M. L. Mat Kiah, “BYOD Policy Compliance: Risks and Strategies in Organizations,” *Journal of Computer Information Systems*, vol. 62, no. 1. Taylor and Francis Ltd., pp. 61–72, 2022. doi: 10.1080/08874417.2019.1703225.

[251] C. Nitzl, “The use of partial least squares structural equation modelling (PLS-SEM) in management accounting research: Directions for future theory development,” *Journal of Accounting Literature*, vol. 37, pp. 19–35, Dec. 2016, doi: 10.1016/j.acclit.2016.09.003.

[252] A. M. Julian, C. Novitsky, K. Lee, and M. C. Ashton, “Convergent validity of three brief six-factor measures of personality,” *Pers Individ Dif*, vol. 188, p. 111436, Apr. 2022, doi: 10.1016/j.paid.2021.111436.

[253] C. FORNELL and D. F. LARCKER, “Evaluating Structural Equation Models with Unobservable Variables and Measurement Error,” 1981.

[254] M. Pett, N. Lackey, and J. Sullivan, *Making Sense of Factor Analysis*. 2455 Teller Road, Thousand Oaks California 91320 United States of America : SAGE Publications, Inc., 2003. doi: 10.4135/9781412984898.

[255] A. Y. J. Akossou and R. Palm, “Impact of Data Structure on the Estimators R-Square And Adjusted R-Square in Linear Regression,” 2013.

[256] J. F. Hair, G. T. M. Hult, C. M. Ringle, M. Sarstedt, N. P. Danks, and S. Ray, *Partial Least Squares Structural Equation Modeling (PLS-SEM) Using R*. Cham: Springer International Publishing, 2021. doi: 10.1007/978-3-030-80519-7.

[257] M. Kalhoro, H. N. A. Yong, and R. S. Charles, “Understanding the factors affecting pro-environment behavior for city rail transport usage: Territories’ empirical evidence—Malaysia,” *Sustainability (Switzerland)*, vol. 13, no. 22, Nov. 2021, doi: 10.3390/su132212483.

[258] L. Xiong, H. Wang, and C. Wang, “Predicting mobile government service continuance: A two-stage structural equation modeling-artificial neural network approach,” *Gov Inf Q*, vol. 39, no. 1, p. 101654, Jan. 2022, doi: 10.1016/j.giq.2021.101654.

[259] A. K. Singh and F. Liébana-Cabanillas, “An SEM-Neural Network Approach for Predicting Antecedents of Online Grocery Shopping Acceptance,” *Int J Hum Comput Interact*, pp. 1–23, Dec. 2022, doi: 10.1080/10447318.2022.2151223.

[260] S. Parhi, K. Joshi, T. Wuest, and M. Akarte, “Factors affecting Industry 4.0 adoption – A hybrid SEM-ANN approach,” *Comput Ind Eng*, vol. 168, p. 108062, Jun. 2022, doi: 10.1016/j.cie.2022.108062.

[261] S. K. Sharma and M. Sharma, “Examining the role of trust and quality dimensions in the actual usage of mobile banking services: An empirical investigation. ,” *Int J Inf Manage*, vol. 44, pp. 65–75, 2019.

[262] A. Mehedintu and G. Soava, “A Hybrid SEM-Neural Network Modeling of Quality of M-Commerce Services under the Impact of the COVID-19 Pandemic,” *Electronics (Basel)*, vol. 11, no. 16, p. 2499, Aug. 2022, doi: 10.3390/electronics11162499.

[263] L. Y. Leong, N. I. Jaafar, and S. Ainin, “Understanding Facebook commerce (f-commerce) actual purchase from an artificial neural network perspective.,” *Journal of Electronic Commerce Research*, vol. 19, no. 1, p. 1, 2018.

[264] Y. Karaca, M. Moonis, Y. D. Zhang, and C. Gezgez, “ Mobile cloud computing based stroke healthcare system. ,” *Int J Inf Manage*, vol. 45, pp. 250–261, 2019.

[265] S. K. Sharma, A. Gaur, V. Saddikuti, and A. Rastogi, “Structural equation model (SEM)-neural network (NN) model for predicting quality determinants of e-learning management systems,” *Behaviour & Information Technology*, vol. 36, no. 10, pp. 1053–1066, Oct. 2017, doi: 10.1080/0144929X.2017.1340973.

[266] M. Sharma, S. Joshi, S. Luthra, and A. Kumar, “Impact of Digital Assistant Attributes on Millennials’ Purchasing Intentions: A Multi-Group Analysis using PLS-SEM, Artificial Neural Network and fsQCA,” *Information Systems Frontiers*, Sep. 2022, doi: 10.1007/s10796-022-10339-5.

[267] Adi Widodo, Firdaus Putra, Multi Nadeak, Dewiana Novitasari, and Masduki Asbari, “Information Technology Adoption and Knowledge Sharing Intention: The Mediating Role of Leadership Style ,” *INTERNATIONAL JOURNALOF SOCIAL AND MANAGEMENT STUDIES (IJOSMAS)*, vol. 3, no. 1, pp. 258–268, 2022.

[268] A. Michna and R. Kmieciak, “Open-Mindedness Culture, Knowledge-Sharing, Financial Performance, and Industry 4.0 in SMEs,” *Sustainability*, vol. 12, no. 21, p. 9041, Oct. 2020, doi: 10.3390/su12219041.

[269] H. Mustika, A. Eliyana, T. S. Agustina, and A. Anwar, “Testing the Determining Factors of Knowledge Sharing Behavior,” *Sage Open*, vol. 12, no. 1, p. 215824402210780, Jan. 2022, doi: 10.1177/21582440221078012.

[270] S. Natu and M. Aparicio, “Analyzing knowledge sharing behaviors in virtual teams: Practical evidence from digitalized workplaces,” *Journal of Innovation & Knowledge*, vol. 7, no. 4, p. 100248, Oct. 2022, doi: 10.1016/j.jik.2022.100248.

[271] I. A. Marin, P. Burda, N. Zannone, and L. Allodi, “The Influence of Human Factors on the Intention to Report Phishing Emails,” in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, Apr. 2023, pp. 1–18. doi: 10.1145/3544548.3580985.

[272] R. Jiang and J. Zhang, “The impact of work pressure and work completion justification on intentional nonmalicious information security policy violation intention,” *Comput Secur*, vol. 130, p. 103253, Jul. 2023, doi: 10.1016/j.cose.2023.103253.

[273] S. AlGhamdi, K. T. Win, and E. Vlahu-Gjorgievska, “Employees’ intentions toward complying with information security controls in Saudi Arabia’s public organisations,” *Gov Inf Q*, vol. 39, no. 4, p. 101721, Oct. 2022, doi: 10.1016/j.giq.2022.101721.

[274] M. C. Almeida, A. C. Yoshikuni, R. Dwivedi, and C. L. C. Larieira, “Do Leadership Styles Influence Employee Information Systems Security Intention? A Study of the Banking Industry,” *Global Journal of Flexible Systems Management*, vol. 23, no. 4, pp. 535–550, Dec. 2022, doi: 10.1007/s40171-022-00320-1.

[275] X. Ma, “IS professionals’ information security behaviors in Chinese IT organizations for information security protection,” *Inf Process Manag*, vol. 59, no. 1, p. 102744, Jan. 2022, doi: 10.1016/j.ipm.2021.102744.

[276] J. Zhen, K. Dong, Z. Xie, and L. Chen, “Factors Influencing Employees’ Information Security Awareness in the Telework Environment,” *Electronics (Basel)*, vol. 11, no. 21, p. 3458, Oct. 2022, doi: 10.3390/electronics11213458.

[277] R. R. Brooks, K. J. Williams, and S. Y. Lee, “ Personal and Contextual Predictors of Information Security Policy Compliance: Evidence from a Low-Fidelity Simulation,” *Journal of Business and Psychology,* pp. 1–21, 2023.

[278] X. Zou, Q. Chen, Y. Zhang, and R. Evans, “Predicting COVID-19 vaccination intentions: the roles of threat appraisal, coping appraisal, subjective norms,

and negative affect," *BMC Public Health*, vol. 23, no. 1, p. 230, Feb. 2023, doi: 10.1186/s12889-023-15169-x.

[279] S. Sharifi, "A Novel Approach to the Behavioral Aspects of Cybersecurity," Jan. 2023.

[280] P. Przymuszała, J. Szmelter, Ł. Zielińska-Tomczak, M. Cerbin-Koczorowska, and R. Marciniak, "Future physicians' behavioral intentions towards collaborative practice-a qualitative study on polish final-year medical students guided by the theory of planned behavior.," *BMC Med Educ*, vol. 23, no. 1, pp. 1–14, 2023.

[281] E. Amankwa, G. Amissah, and R. Okoampa-Larbi, " Cashless economy–the nexus of COVID-19 and E-wallet usage intentions: a multi-group analysis between formal and informal sector workers in Ghana. ," *Journal of Science and Technology Policy Management.*, p. 1, 2023.

[282] A. Mady, S. Gupta, and M. Warkentin, "The effects of knowledge mechanisms on employees' information security threat construal," *Information Systems Journal*, vol. 33, no. 4, pp. 790–841, Jul. 2023, doi: 10.1111/isj.12424.

[283] N. F. Khan, N. Ikram, H. Murtaza, and M. Javed, "Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model," *Comput Secur*, vol. 125, p. 103049, Feb. 2023, doi: 10.1016/j.cose.2022.103049.

[284] C. A. Yue and J. Walden, "Guiding employees through the COVID-19 pandemic: An exploration of the impact of transparent communication and change appraisals," *Journal of Contingencies and Crisis Management*, vol. 31, no. 2, pp. 198–211, Jun. 2023, doi: 10.1111/1468-5973.12430.

[285] P. Ifinedo, N. Mengesha, and O. Longe, "Factors that Influence Workers' Participation in Unhygienic Cyber Practices: A Pilot Study from Nigeria," in *15th International Conference on Social Implications of Computers in Developing Countries (ICT4D)*, 2019. doi: 10.1007/978-3-030-19115-3_25ï.

[286] Ajufo, George, and Abubaker Qutieshat., "'An Examination of the Human Factors in Cybersecurity: Future Direction for Nigerian Banks.' ," *Indonesian Journal of Information Systems*, vol. 6, no. 1, pp. 1–16, 2023.

[287] Jesus M. Mosqueda, "Perceptions and Knowledge of Information Security Policy Compliance in Organizational Personnel ," Walden University, 2023.

[288] C. K. Riemenschneider, L. L. Burney, and S. Bina, "The influence of organizational values on employee attitude and information security behavior: the mediating role of psychological capital.," *Information & Computer Security*, vol. 31, no. 2, pp. 172–198, 2023.

[289] A. J. Sakaya, " Fear of COVID-19 and green bank service purchase intention: the mediating effect of customer empowerment and customers' perceived value of digital service transactions. ," *Arab Gulf Journal of Scientific Research.*, p. 1, 2023.

[290] S. Saeed, "Digital Workplaces and Information Security Behavior of Business Employees: An Empirical Study of Saudi Arabia," *Sustainability*, vol. 15, no. 7, p. 6019, Mar. 2023, doi: 10.3390/su15076019.

[291] M. N. Alraja, U. J. Butt, and M. Abbod, "Information security policies compliance in a global setting: An employee's perspective," *Comput Secur*, vol. 129, p. 103208, Jun. 2023, doi: 10.1016/j.cose.2023.103208.

[292] Fika Yusti Harahap, Amrin Fauzi, and Syafrizal Helmi Situmorang, "THE INFLUENCE OF DIGITAL CUSTOMER EXPERIENCE AND ENJOYMENT ON FLIP E-WALLET E-LOYALTY THROUGH E-TRUST IN MEDAN CITY MILLENIAL GENERATIONS," *International Journal of Economic, Business, Accounting, Agriculture Management and Sharia Administration (IJEBAS)*, vol. 3, no. 2, pp. 488–505, Apr. 2023, doi: 10.54443/ijebas.v3i2.785.

[293] I. A. Marin, P. Burda, N. Zannone, and L. Allodi, "The Influence of Human Factors on the Intention to Report Phishing Emails," in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, New York, NY, USA: ACM, Apr. 2023, pp. 1–18. doi: 10.1145/3544548.3580985.

[294] B. D. McLarty, V. Skorodziyevskiy, and J. Muldoon, "The Dark Triad's incremental influence on entrepreneurial intentions," *Journal of Small Business Management*, vol. 61, no. 4, pp. 2097–2125, Jul. 2023, doi: 10.1080/00472778.2021.1883042.

[295] R. A. Alsharida, B. A. S. Al-rimy, M. Al-Emran, and A. Zainal, "A systematic review of multi perspectives on human cybersecurity behavior," *Technol Soc*, vol. 73, p. 102258, May 2023, doi: 10.1016/j.techsoc.2023.102258.

[296] M. Alanazi, M. Freeman, and H. Tootell, "Exploring the factors that influence the cybersecurity behaviors of young adults," *Comput Human Behav*, vol. 136, p. 107376, Nov. 2022, doi: 10.1016/j.chb.2022.107376.

[297] L.-Y. Leong, T.-S. Hew, K.-B. Ooi, V.-H. Lee, and J.-J. Hew, "A hybrid SEM-neural network analysis of social media addiction," *Expert Syst Appl*, vol. 133, pp. 296–316, Nov. 2019, doi: 10.1016/j.eswa.2019.05.024.

[298] N. Rawindaran, A. Jayal, E. Prakash, and C. Hewage, "Perspective of small and medium enterprise (SME's) and their relationship with government in overcoming cybersecurity challenges and barriers in Wales," *International Journal of Information Management Data Insights*, vol. 3, no. 2, p. 100191, Nov. 2023, doi: 10.1016/j.jjimei.2023.100191.

[299] A. K. Al Aamer and A. Hamdan, “Cyber Security Awareness and SMEs’ Profitability and Continuity: Literature Review,” 2023, pp. 593–604. doi: 10.1007/978-981-99-6101-6_43.

[300] K. Kioskli, T. Fotis, S. Nifakos, and H. Mouratidis, “The Importance of Conceptualising the Human-Centric Approach in Maintaining and Promoting Cybersecurity-Hygiene in Healthcare 4.0,” *Applied Sciences*, vol. 13, no. 6, p. 3410, Mar. 2023, doi: 10.3390/app13063410.

APPENDIX A

Questionnaire of the study

Improving Cybersecurity Behaviour through Cyber Hygiene among Employees of Software Development SMEs

Introduction:

Dear participant, I am Shadab Kalhoro, a PhD student at Universiti Tunku Abdul Rehman in Kampar, Malaysia. I have attached a questionnaire for my study. I kindly ask you to dedicate 15-20 minutes of your time to complete this questionnaire. Your participation is greatly valued.

Purpose: The purpose of this questionnaire is to assess the cybersecurity practices of employees working in software development SMEs, focusing on cyber hygiene. The questionnaire comprises two sections. Part-I pertains to background information, while Part-II is about variable information of cyber hygiene behaviour; the variables are knowledge sharing, cyber hygiene attitude, cyber hygiene subjective norms, cyber hygiene perceived behavioural control, threat appraisal, cyber hygiene knowledge, cyber trust, personality traits and cyber hygiene intention.

Confidentiality: I truly value your time and effort in completing this survey. ALL ANSWERS ARE STRICTLY CONFIDENTIAL. No identity of any respondent will be disclosed. Moreover, identity of everyone will also remain confidential.

Yours sincerely,

Shadab Kalhoro
Student ID: 20ACD06698
Faculty of Information & Communication Technology
Universiti Tunku Abdul Rahman, Kampar Campus, Perak
E-mail: shadabkalhoro@1utar.my

INSTRUCTIONS

- Base your answers on your own feelings and experiences.
- Read directions carefully and mark only one answer for each question.
- Please write clearly making dark marks or just tick the suitable answer.
- Avoid stray marks and if you make corrections erase marks completely.

I provide my consent to take part in this survey.

YES [ ] (If so, please continue)

NO [ ] (If not, kindly return the questionnaire to the researcher)

PART-I

BACKGROUND INFORMATION

This section includes questions about your demographic details. Please indicate your answers by CHECKING THE BOX [√] that best corresponds to your situation.

1. **Gender**
   - □ Male
   - □ Female
2. **Age group**
   - □ 18-20 years
   - □ 21-30 years
   - □ 31-40 years
   - □ 41-50 years
   - □ 51 years old and above
3. **Ethnicity**
   - □ Malay
   - □ Chinese
   - □ Indian
   - □ Others (please specify) _____
4. **Education level**
   - □ Diploma/ Certification
   - □ Bachelor
   - □ Post-Graduate
   - □ Other (please specify)_____
5. **Occupation**
   - □ Software designer
   - □ Software programmer
   - □ Software requirement engineer
   - □ Software developer
   - □ Software tester
   - □ Software analyst
   - □ Software project manager
   - □ Other (please specify): _____
6. **Experience**
   - □ 1-5 years
   - □ 6-10 years

- 11-15 years
- 16-20 years
- More than 20 years

7. How frequently do you utilize third-party services (such as USB drives, smartphones, tablets, Dropbox, Google Docs) for storing or processing work-related documents?

- I actively use different third-party services for work purposes.
- I use third-party services from time to time for work purposes.
- I seldom use third party services for work purposes.
- I do not use any third-party services for work purposes.

8. How often do you bring your own device (BYOD) for storing or processing work related documents?

- I actively bring my own device for work purposes.
- I bring my own device from time to time for work purposes.
- I seldom bring my own device for work purpose.
- I do not bring my own device for work purposes.

Part II

Variables Information

Please rate statements mentioned below using following scale where 1 denotes that you strongly disagree and 5 shows that you strongly agree with the statements.

①	②	③	④	⑤
StronglyDisagree SD	**Disagree D**	**Neither Agree nor Disagree NA**	**Agree A**	**StronglyAgree SA**

Section-A

Cyber Hygiene behaviour

The degree to which an individual adopts various cybersecurity measures to mitigate the specific types of cyber threats they are susceptible to.

		SD	DA	NA	A	SA
1	I have installed anti-virus software, firewall, and anti-spyware on my computer.	①	②	③	④	⑤
2	I consistently update the anti-virus software I have installed.	①	②	③	④	⑤
3	I become suspicious if my computer slows down significantly.	①	②	③	④	⑤
4	I avoid downloading free anti-virus software from unknown sources.	①	②	③	④	⑤
5	I disable the anti-virus on my work computer to download information from websites.	①	②	③	④	⑤
6	I scan removable drives before using them on my personal computer.	①	②	③	④	⑤
7	I download data and materials from websites on my work computer without verifying their authenticity.	①	②	③	④	⑤
8	I bring my own USB to work to transfer data.	①	②	③	④	⑤
9	I create passwords that are not very complex, often using family names and birthdates.	①	②	③	④	⑤
10	I share passwords with friends and colleagues.	①	②	③	④	⑤
11	I use different passwords for various applications.	①	②	③	④	⑤
12	I include lowercase, uppercase, numbers, and special characters in my passwords.	①	②	③	④	⑤
13	I use passwords longer than 8 characters.	①	②	③	④	⑤
14	I rarely change my passwords.	①	②	③	④	⑤

15	I sometimes use the "Remember my password" option.	①	②	③	④	⑤
16	I occasionally write down passwords.	①	②	③	④	⑤
17	I do not use password hints to recover forgotten passwords.	①	②	③	④	⑤
18	I educate myself about phishing by reading materials on the topic.	①	②	③	④	⑤
19	I avoid providing confidential information in any type of email.	①	②	③	④	⑤
20	I do not open email attachments from strangers.	①	②	③	④	⑤
21	I avoid clicking hyperlinks in email messages.	①	②	③	④	⑤
22	I am cautious about email messages announcing contests/prizes.	①	②	③	④	⑤
23	I prefer typing URLs in a new browser rather than clicking hyperlinks.	①	②	③	④	⑤
24	I click on links contained in emails from trusted friends or colleagues.	①	②	③	④	⑤
25	I refrain from clicking links in unsolicited emails from unknown sources.	①	②	③	④	⑤
26	I do not establish trusted online relationships with strangers.	①	②	③	④	⑤
27	I ignore SMS messages announcing contests involving large sums of money.	①	②	③	④	⑤
28	I do not send personal information to strangers over the Internet.	①	②	③	④	⑤
29	I do not enter payment information on websites lacking clear security information.	①	②	③	④	⑤
30	I check URL spellings before any transactions.	①	②	③	④	⑤
31	I never accept any amount of money for services offered by online sites.	①	②	③	④	⑤
32	I am aware of and can identify the latest online scams.	①	②	③	④	⑤
33	I do not accept parcels and gifts from Internet friends.	①	②	③	④	⑤
Attitudes towards Cyber Hygiene						
		SD	**DA**	**NA**	**A**	**SA**
1	Adhering to organizational cyber hygiene policies is crucial.	①	②	③	④	⑤
2	Practicing cyber hygiene significantly reduces the risk of information security breaches.	①	②	③	④	⑤
3	Engaging in cyber hygiene is a prudent practice that minimizes the risk of information security incidents.	①	②	③	④	⑤

4	Demonstrating cyber hygiene behaviour is a valuable asset within the organization.	①	②	③	④	⑤
5	Implementing cyber hygiene serves as a beneficial behavioural tool to protect the organization's information assets.	①	②	③	④	⑤
Cyber Hygiene Knowledge						
		SD	**DA**	**NA**	**A**	**SA**
1	I am well-versed in the organization's cybersecurity policies and my duties to safeguard organizational resources.	①	②	③	④	⑤
2	I comprehend the necessity of creating and using robust passwords.	①	②	③	④	⑤
3	I am knowledgeable about defending against 'social engineering,' 'phishing,' and 'cybercrime.'	①	②	③	④	⑤
4	I exercise caution to avoid discussing sensitive information in public spaces.	①	②	③	④	⑤
5	While browsing or downloading from the Internet, I exclusively visit trustworthy and reputable websites.	①	②	③	④	⑤
6	When downloading software, I adhere to all license and copyright regulations.	①	②	③	④	⑤
7	I exercise prudence when opening email attachments and clicking on links.	①	②	③	④	⑤
Knowledge Sharing						
		SD	**DA**	**NA**	**A**	**SA**
1	Sharing knowledge within the organization holds significant value.	①	②	③	④	⑤
2	Sharing knowledge with colleagues within the organization is advantageous.	①	②	③	④	⑤
3	I regularly share my knowledge at work to mitigate security risks.	①	②	③	④	⑤
4	I believe knowledge sharing enhances my comprehension of the effectiveness of cybersecurity policies within my organization.	①	②	③	④	⑤
5	Sharing knowledge motivates me to adhere to cybersecurity policies and procedures.	①	②	③	④	⑤
Threat Appraisal						
		SD	**DA**	**NA**	**A**	**SA**
1	Safeguarding my organization’s information is crucial.	①	②	③	④	⑤
2	Security threats to my organization’s information pose significant risks.	①	②	③	④	⑤
3	I perceive cybersecurity attacks on my organization as detrimental.	①	②	③	④	⑤

4	At work, unauthorized access to my confidential information is a grave concern for me.	①	②	③	④	⑤
5	Data loss due to hacking deeply concerns me.	①	②	③	④	⑤
6	I recognize that my organization could be at risk of security breaches if I do not follow its cyber hygiene policy.	①	②	③	④	⑤
7	I could be susceptible to malicious attacks if I neglect my organization's cyber hygiene policy.	①	②	③	④	⑤
Cyber Hygiene Subjective Norms						
		SD	**DA**	**NA**	**A**	**SA**
1	My colleagues think that we should share our cyber hygiene knowledge.	①	②	③	④	⑤
2	The head of the department regards cyber hygiene as a cultural value.	①	②	③	④	⑤
3	Senior staff members in my company hold a positive perspective on cyber hygiene.	①	②	③	④	⑤
4	My office friends motivate me to share my cyber hygiene knowledge.	①	②	③	④	⑤
5	Both my family and friends encourage me to share knowledge about cyber hygiene.	①	②	③	④	⑤
Cyber Hygiene Perceived Behavioural Control						
		SD	**DA**	**NA**	**A**	**SA**
1	I possess sufficient knowledge about cyber hygiene to educate other staff members.	①	②	③	④	⑤
2	I am capable of sharing cyber hygiene knowledge to reduce the risk of cybersecurity breaches.	①	②	③	④	⑤
3	Cyber hygiene tasks are straightforward and enjoyable for me.	①	②	③	④	⑤
4	I have valuable resources to impart cyber hygiene knowledge to fellow employees.	①	②	③	④	⑤
5	I refrain from sharing my personal information on social platforms.	①	②	③	④	⑤
Cyber Trust						
		SD	**DA**	**NA**	**A**	**SA**
1	I trust in the reliability of my colleague's knowledge about cyber hygiene.	①	②	③	④	⑤
2	I have confidence in the effectiveness of my colleague's cyber hygiene knowledge.	①	②	③	④	⑤

3	I believe my colleague's understanding of cyber hygiene reduces the risk of cybersecurity breaches.	①	②	③	④	⑤
4	I find my colleague's cyber hygiene knowledge valuable.	①	②	③	④	⑤
5	I trust that my colleagues would not misuse the cyber hygiene knowledge we share.	①	②	③	④	⑤
Cyber Hygiene Intention						
		SD	**DA**	**NA**	**A**	**SA**
1	I am intend to share my knowledge of cyber hygiene to minimize risks.	①	②	③	④	⑤
2	I intend to share my cyber hygiene experiences with colleagues to enhance their awareness.	①	②	③	④	⑤
3	I will inform fellow staff about new methods and software that can mitigate cyber hygiene risks.	①	②	③	④	⑤
4	I will share reports on cyber hygiene incidents with others to mitigate risks.	①	②	③	④	⑤
5	I consistently review privacy settings to minimize cyber hygiene issues.	①	②	③	④	⑤
Perceived Cyber hygiene value						
		SD	**DA**	**NA**	**A**	**SA**
1	I am satisfied with the cybersecurity awareness campaign conducted in our organization.	①	②	③	④	⑤
2	Our organization has well-documented cybersecurity policies that are readily available if needed.	①	②	③	④	⑤
3	The perceived level of cybersecurity service matches the ideal standard.	①	②	③	④	⑤
4	I am pleased that cyber hygiene is a top priority for everyone in the organization.	①	②	③	④	⑤
5	The perceived performance in cyber hygiene exceeds expectations.	①	②	③	④	⑤
Personality traits						
		SD	**DA**	**NA**	**A**	**SA**
1	I feel comfortable around people.	①	②	③	④	⑤
2	I make friends easily.	①	②	③	④	⑤
3	I excel in handling social situations.	①	②	③	④	⑤
4	I am the center of attention at gatherings.	①	②	③	④	⑤
5	I know how to engage people.	①	②	③	④	⑤
6	I am not very talkative.	①	②	③	④	⑤
7	I prefer to stay in the background	①	②	③	④	⑤
8	I would describe my experiences as somewhat dull.	①	②	③	④	⑤

9	I don’t like drawing attention to myself.	①	②	③	④	⑤
10	I am reserved in my speech.	①	②	③	④	⑤
11	I speak positively about others.	①	②	③	④	⑤
12	I believe in the good intentions of others.	①	②	③	④	⑤
13	I hold others in high regard.	①	②	③	④	⑤
14	I accept people as they are.	①	②	③	④	⑤
15	I put others at ease.	①	②	③	④	⑤
16	I have a sharp tongue.	①	②	③	④	⑤
17	I cut others to pieces.	①	②	③	④	⑤
18	I suspect hidden motives in others.	①	②	③	④	⑤
19	I get back at others.	①	②	③	④	⑤
20	I insult people.	①	②	③	④	⑤
21	I am always prepared.	①	②	③	④	⑤
22	I pay attention to details.	①	②	③	④	⑤
23	I get chores done right away.	①	②	③	④	⑤
24	I carry out my plans.	①	②	③	④	⑤
25	I make plans and stick to them.	①	②	③	④	⑤
26	I waste my time.	①	②	③	④	⑤
27	I find it difficult to get down to work.	①	②	③	④	⑤
28	I do just enough work to get by.	①	②	③	④	⑤
29	I don’t see things through.	①	②	③	④	⑤
30	I avoid my responsibilities.	①	②	③	④	⑤
31	I frequently feel sad.	①	②	③	④	⑤
32	I have a negative view of myself.	①	②	③	④	⑤
33	I often feel low.	①	②	③	④	⑤
34	I experience mood swings.	①	②	③	④	⑤
35	I easily become anxious.	①	②	③	④	⑤
36	I rarely get annoyed.	①	②	③	④	⑤
37	I seldom feel down.	①	②	③	④	⑤
38	I am comfortable with who I am.	①	②	③	④	⑤
39	I am not easily bothered by things.	①	②	③	④	⑤
40	I am content with myself.	①	②	③	④	⑤
41	I value the importance of art.	①	②	③	④	⑤
42	I have a vivid imagination.	①	②	③	④	⑤
43	I tend to vote for liberal candidates.	①	②	③	④	⑤
44	I carry the conversation to a higher level.	①	②	③	④	⑤
45	I enjoy hearing new ideas.	①	②	③	④	⑤
46	I am not interested in abstract ideas.	①	②	③	④	⑤
47	I do not like art.	①	②	③	④	⑤
48	I avoid philosophical discussions.	①	②	③	④	⑤
49	I do not enjoy going to art museums.	①	②	③	④	⑤
50	I tend to vote for conservative candidates.	①	②	③	④	⑤

We sincerely appreciate your valuable time, your honest responses, and your insightful feedback.

Thanks for taking the time to fill out this survey!

APPENDIX B

LIST OF PUBLICATIONS

S. Kalhoro, M. Rehman, V. Ponnusamy, and F. B. Shaikh, “Extracting key factors of cyber hygiene behaviour among software engineers: A systematic literature review,” IEEE Access, vol. 9. Institute of Electrical and Electronics Engineers Inc., pp. 99339–99363, 2021. doi: 10.1109/ACCESS.2021.3097144.

S. Kalhoro, R. K. Ayyasamy, A. K. Jebna, A. Kalhoro, K. Krishnan, and S. Nodeson, “How Personality Traits Impacts on Cyber Security Behaviors of SMEs Employees,” in 2022 International Conference on Innovation and Intelligence for Informatics, Computing, and Technologies (3ICT), IEEE, Nov. 2022, pp. 635–641. doi: 10.1109/3ICT56508.2022.9990621.