Cyber Security Behavioural Intentions for Trade Secret Protection

by

Mazin M. Al Zaidi

A thesis submitted to the University of Warwick

in partial fulfilment of the requirements

for the degree of

Doctor of Philosophy

Cyber Security Centre, WMG
University of Warwick

September 2017

Contents

List of Figures

List of Tables

Acknowledgements

I would like to start by thanking Jay Bal for accepting me at the beginning as a PhD student and giving me the opportunity to pursue my PhD at the University of Warwick. I would also like to thank Tim Watson for all his support and encouragement during my PhD journey.

Finally, I would like to express my deepest gratitude to my mentor and supervisor Duncan Hine. Without his guidance, help, and full support, I would not have made it through my PhD degree.

This thesis is dedicated to

my wife Maram and my two boys Wabil and Hattan

Declaration

This thesis is submitted to the University of Warwick in support of my application for the degree of Doctor of Philosophy. I hereby declare that, except where acknowledged, the work in this thesis has been composed by myself, and has not been submitted elsewhere for the purpose of obtaining an academic degree.

Mazin M. Al Zaidi

Signature:

Abstract

Trade secrets have become an important aspect of competitive advantage for new and established businesses in the new digital economy. This is particularly true in corporate venturing, where most corporates rely on new entrepreneurial ventures with creative ideas to drive innovation and fuel growth. In this manner, these corporates run corporate venturing units such as corporate accelerators to support entrepreneurs creating new ventures. During the accelerated pace of venturing, trade secrets become the core intangible asset that requires protection for any new venture. Yet, people remain the weakest link in the cyber security chain and that requires more understanding to enhance cyber security protection.

A new approach was suggested in this study to explore the protection of trade secrets through the confidentiality of information, the ownership of intellectual property and the secrecy of commercial secrets. This study developed a conceptual model to explore cyber security behaviour for trade secret protection within corporate accelerators. Well-established theories were adopted to develop the research conceptual model for trade secret protection, integrating the protection motivation theory (PMT), social bond theory (SBT) and the concept of psychological ownership.

This study began with a comprehensive up-to-date systematic literature review in the field of cyber security behavioural intentions over the past decade. The top 10 journals in the field of cyber security behaviour were reviewed and 46 publications that used 35 behaviour theories were identified. A concept matrix based on a concept-centric approach was applied to present the behavioural theories used in the relevant literature. By analysing the relevant literature results, the key cyber security behaviour elements were identified and illustrated via a concept map and matrix. Based on the output of the literature review analysis, valuable findings and insights were presented.

This study investigates entrepreneurs' cyber security behavioural intentions to protect trade secrets in agile dynamic corporate environments. The research design adopted a hypothetico-deductive approach using a quantitative survey for empirical data collection. To evaluate the conceptual model, a partial least squares method of structural equation modelling (PLS-SEM) analysis was used. This involved validity and reliability assessments, in addition to hypotheses testing. The research results found statistically significant relationships for severity, vulnerability, response efficacy, response cost, involvement and personal norms in relation to cyber security behavioural intentions to protect trade secrets.

Chapter 1

Introduction

Due to the rapid technology change and disruption facing most corporates today in different industries, open innovation and corporate venturing are used as new approaches for corporate survival and growth. Large corporates have started to adopt new venturing models to innovate and build new ventures. In particular, corporate accelerators have become the new innovation machines for most corporates, and therefore, require more attention in regards to cyber security threats.

Trade secrets, also known as confidential business information, are today considered one of the most valuable and yet vulnerable assets of new ventures. Trade secrets are a type of intellectual property that businesses rely on to maintain competitive advantage. Moreover, trade secrets are becoming the most preferable IP mechanism for new ventures because of the complexity of other types of IP (e.g. patents) that take a long time to be granted. In addition, with advances in technology and growing competition in all industries, maintaining secrets has become a significant issue for entrepreneurs.

An example to illustrate how dangerous this can be is easily drawn from a recent news article that shows the death of a new start-up before it was even born. The news article talks about an entrepreneur that launched a crowd funding campaign on Kickstarter.com for an innovative smartphone case that unfolds into a selfie stick. However, one week after posting the product on the crowd funding website he found that his invention was available for sale online at Alibaba.com (Horwitz, 2016). This incident shows the importance of protecting trade secrets at the creation phase of a new venture.

For this reason, and because of the importance of behavioural aspects in cyber security and protecting confidential information, this research focuses on cyber security behaviour for trader secret protection. This research will investigate the impact of entrepreneurs' cyber security behavioural intentions for trade secrets protection. In addition, the research suggests a new approach to protect trade secrets using well established theories in the field of cyber security behaviour. The research will look into the impact of protection motivation, social bonding and psychological ownership on entrepreneurs to perform protective cyber security actions when faced with cyber threats. Therefore, the research aims to explore entrepreneurs' cyber security behavioural intentions in protecting trade secrets within the context of corporate venturing.

The chapter aims to describe the research problem, defines the research questions and then identifies the research value.

1.1. Research Problem: Innovation vs. Security

Cyber security breaches result in data loss or leakage, intellectual property theft, legal issues and reputational damage. In a recent information security breaches survey 2015 conducted by PwC (2015), such breaches have increased since last year to 90% in large companies, and 74% in small businesses.

One of the key security challenges facing corporate innovation is leakage of IP that results in damaging competitiveness and innovation, and leads to commercial losses

(Warren, 2015). According to a report by Akerman et al. from McAfee (2009), hackers have moved beyond traditional cyber theft of credit card details to intellectual property theft. In addition, Pooley (2015) argues that trade secrets are the most valuable assets of modern business. Hence, the economic value of trade secrets makes it a tempting target for those that are willing to steal them.

In a report issued by Detica (2011) in partnership with Office of Cyber Security and Information Assurance ate the Cabinet Office, stated that the cost of cybercrime to the UK comes from the significant theft of IP at an estimated cost of £9 billion (See Figure 1.1). In addition, a more recent report published by HM Government and Marsh (2015) notes as one of its key findings that IP theft has the highest severity of impact on UK businesses.

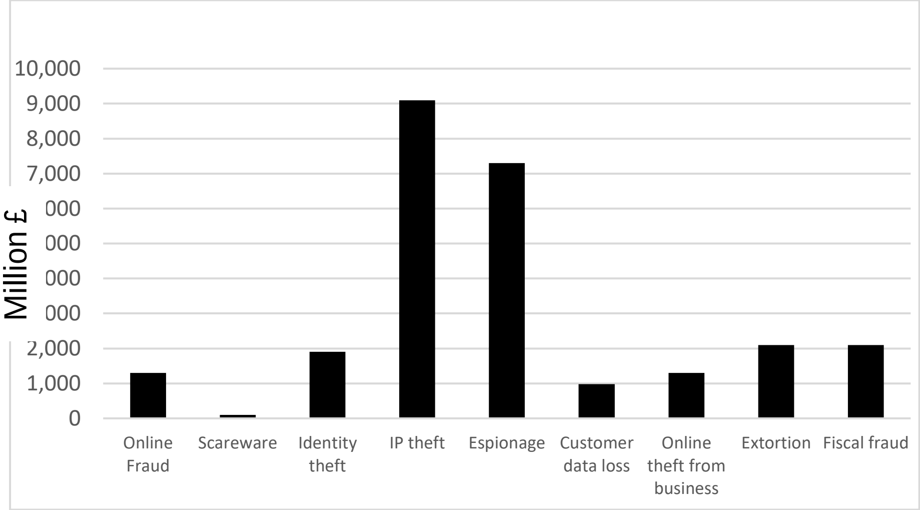


Figure 1.1: Cost of different types of cybercrime to the UK economy (based on Detica, 2011)

In a TV interview on CNN in 2015, Brian Burch VP, of Global Consumer and Small Business Segment Marketing at Symantec, stated that "Start-ups are incredibly vulnerable to cyber-attacks in their first 18 months. If a business thinks that it's too small to matter to cybercriminals, then it's fooling itself with a false sense of security" (CNN, 2013). The importance of protecting intangible assets for start-ups can be explained in one way by the attention that venture capitalists (VCs) give to start-ups' intellectual property assets during the evaluation of new start-ups for investments. (Block et al., 2014). Therefore, for entrepreneurs starting new ventures, protection of their sensitive business information is usually required to innovate and grow in the market. Hence, new start-ups depend heavily on the intangible assets that they won during the early stage of the venturing process.

According to Weiblen and Chesbrough (2015) when corporates usually engages with a start-up in a corporate venturing programme, managing intellectual property becomes a concern. Corporate venturing units usually use different approaches to manage intellectual property rights. For example, the AT&T Foundry which was established in the US in 2011, requires everybody involved in the unit to sign a non-disclosure agreement. However, other accelerators do not give any attention to intellectual property, and are unlikely even to sign a NDA, such as Y-Combinitor, Techstars and Microsoft Ventures. This shows that there is an issue in the legal protection of entrepreneurs' trade secrets in accelerators.

Along with the acceleration of new ventures in a dynamic agile environment comes risks. Among them are the risks of entrepreneurs' trade secrets getting stolen. According to the UTSA, for information to be considered as trade secrets, a reasonable effort must be made to maintain the confidentiality of information (Uniform Law Commission, 1985). When a large company needs to disclose trade secrets to others such as suppliers, consultants, manufactures, etc., it requires them to sign a NDA so that information confidentiality can be enforced. However, in the case of entrepreneurs engaging in a cooperate accelerator, companies refuse to sign an NDA to protect entrepreneurs IP for legal purposes to avoid getting into any law suits. This includes all people during the programme that will be engaging with entrepreneurs, such as mentors, experts, investors, etc. Moreover, the agile methodology in an accelerator does not make IP protection a priority or a concern at the start-up validation stage.

In addition, large corporates have been able to design and maintain cyber security mechanisms to protect their core businesses to their best of their ability. However, it is clearly noted that exploration environments such as new innovation business units require different management, operation and strategy approaches from traditional business methods. This includes all business functions; therefore, for cyber security measures in a dynamic agile environment, traditional security methods might not be suitable. For an example, an entrepreneur uses cloud storage such as Dropbox.com to store his electronic documents for easy access and sharing, where, most large businesses would not allow such an activity for cyber risk concerns. Although corporates cannot guide or manage entrepreneurs in terms of complying with corporate information security procedures they should still be obligated to offer entrepreneurs a secure environment that does not conflict with the way they operate.

Despite the large amounts of money invested in technology, security threats remain a significant concern. According to Mancuso et al. (2014) cyber security research has focused more on technology applications; however, recently, research on the human factor part of cyber security has been growing. In addition, recent cyber security issues that have been overlooked in academia and industry have been focusing on the technological issue of cyber threats. People remain the weakest link in the cyber security chain. Moreover, entrepreneurs and the impact that they make through their new creative ideas and innovative services /products, fall apart when someone else has stolen their secrets and is first in the market. The fast-growing discipline of cyber security has expanded to include different types of information assets, such as intellectual property.

Although entrepreneurs are within corporate accelerators for a specific period, corporates should have an obligation to protect entrepreneurs' trade secrets. This presents a security dilemma, whereby companies have no control over entrepreneurs' confidential business information. The reason for this is that when entrepreneurs interact with different people during the accelerator programme and share their ideas and plans, they have different attitudes towards cyber security and ownership of IP.

Moreover, entrepreneurs adopt new agile methods such as lean start-up methodology; therefore, their focus is on failing fast to learn and iterate quicker (Reis, 2011). This type of an approach that is based on experimentation requires entrepreneurs to focus on getting the product-market-fit through a minimal viable product (MVP). This prototyping of an MVP involves developing the product/service with the minimum features possible to test it in the market and validate its viability. This in return means that entrepreneurs might not consider any security countermeasures to protect their trade secrets.

There is a considerable volume of research that states that to protect trade secrets, individuals with access and knowledge of these secrets should not disclose them. However, previous research in security behaviour lacks an explanation of how entrepreneurs may protect trade secrets in a dynamic agile environment such as corporate accelerators. Most companies state that they would not ask for entrepreneurs' "secret sauce" when joining their accelerator programme, and at the same time, they expose them and their ideas to a variety of people during the accelerator programme. Moreover, most corporate accelerators do not sign an NDA, and at the same time, state that they respect confidentiality. In addition, corporates do not offer entrepreneurs security training or awareness programmes to help them protect their trade secrets which are their most valuable intangible asset. The research argues that this is a huge problem for the following reasons:

- Cyber-attacks, including IP theft and social engineering are becoming more sophisticated.

- Start-ups as large corporates are being targeted by cyber criminals.

- Emerging start-ups are growing fast and are disrupting multiple industries.

- Trade secrets are increasing in value, thus becoming a target for cyber criminals.

- Corporates have no control over entrepreneurs' trade secrets in corporate accelerators.

- Start-ups at the venturing stage are usually not able to afford a Chief Security Officer (CSO).

- Dynamic agile environments require different cyber security countermeasures.

- New start-up methodologies and approaches differ from traditional corporate R&D methods, therefore, incorporate different types of cyber risks.

- There are significant differences between entrepreneurs and employees' characteristics.

Bos et al. (2015) state that during the innovation process of development and commercialisation, trade secrets require protection to prevent the secrets from leaking. Additionally, Row (2016) argue that for large companies to have an effective security, they must integrate people within the security function. Hence, to support the protection of intangible assets within a corporate venturing process, there is an implicit need to explore cyber security behaviour. This is because to date, people remain the weakest link in the cyber security chain.

Therefore, the security paradox that is facing corporate venturing today is that the confidentiality of information remains an important aspect of protecting business information (i.e. trade secrets); however, open innovation requires exploration inside and outside the organisation for the pursuit of new opportunities. The issue of protecting trade secrets within corporate accelerators is not only a technology issue, nor a security management issue. It is rather more a people issue that is concerned with the threats facing entrepreneurs and the required security behaviours to protect trade secrets against cyber risks.

To illustrate the risks that involve cyber theft of trade secrets facing entrepreneurs, Figure 1.2 shows a cyber-risk assessment for trade secrets. The assessment assumes that people (i.e. entrepreneurs) are the main vulnerability and trade secrets are the target asset in this case. Therefore, the impact of an IP cyber theft incident could result in the risk of venture losing its competitive edge during the venturing process.

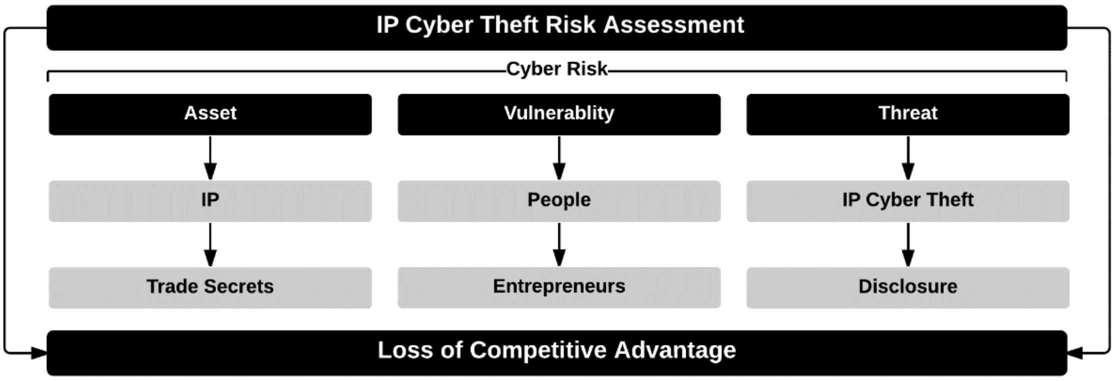


Figure 1.2: IP cyber-risk assessment

The reasoning behind this focus of research is that entrepreneurs should maintain the protection of their trade secrets by performing an effective cyber security behaviour for trade secret protection. However, due to the dynamic environment of a corporate accelerator and the nature of exploration within an accelerator, entrepreneurs may not have a positive cyber security-based behaviour towards protecting trade secrets. This requires an understanding of what drives entrepreneurs to perform protective cyber security actions to protect trade secrets. This research argues that there is great potential to enhance entrepreneurs' cyber security behaviour to protect trade secrets as one component of corporates security countermeasures to manage cyber security threats in an agile dynamic environment.

1.2. Research Proposal

This research proposes a novel approach to exploring the intangible nature of trade secret protection. This approached is built on the intangible fundamental principles underlying the bases of trade secrets. Trade secrets as illustrated in Figure 1.3 are based on three dimensions: information, intellectual property and secrets.

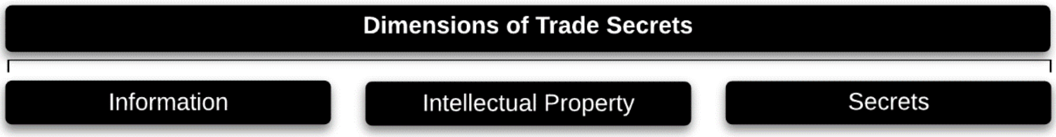


Figure 1.3: The dimensions of trade secrets

Generally, as an intangible item, information may be considered as secrets but might not necessarily be considered as an intellectual property. Similarly, intellectual property could be considered a type of information but might not necessarily be considered as secrets. The same is true for secrets, they could be considered as information but they might not necessarily be considered as intellectual property. On the contrary, trade secrets as intangible items, is defined as information, intellectual property and secrets at the same time. Therefore, this research aims to explore trade secret protection based on its three unique dimensions.

All three trade secret dimensions in a business context require some type of protection. However, since every dimension is viewed in different way their protection is required for three different protection purposes, for: confidentiality, ownership and secrecy. Therefore, this research assumes that the best way to protect trade secrets is by considering the different dimensions of trade secrets. This research aims to develop a conceptual model that explores the protection trade secrets by focusing on the protection of the three dimensions through three protection lenses. Thus, trade secret protection consists of confidentiality, ownership and secrecy.

Furthermore, the research proposes the integration of three theories, each focusing on one purpose of protection to provide a comprehensive approach for exploring the research problem. Therefore, as illustrated in Figure 1.4 the research explores trade secrets as information through the protective motivation theory; as an intellectual property through the theory of psychological ownership; and as secrets through the social bonding theory.

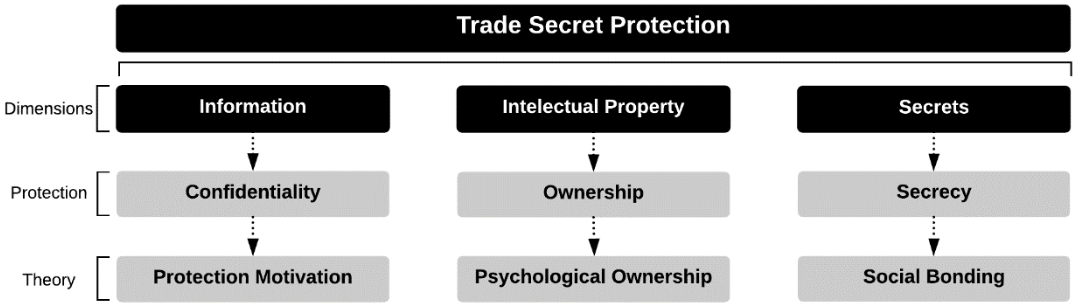


Figure 1.4: The viewed types of trade secrets

As illustrated in Figure 1.4 above, the research explores trade secrets using protective motivation theory based on the purpose of confidentiality, psychological ownership based on the purpose of ownership; and social bonding theory based on the purpose of secrecy.

Protection motivation is a well-defined theory that has been used in the field of information security. Moreover, the underlying theory of protection motivation is based on evaluating threats and the coping ability of taking actions to prevent an incident. Therefore, protection motivation will be used for confidentiality to protect trade secrets.

Additionally, ownership is a legal aspect of protecting intellectual property. However, trade secrets do not offer clear legal ownership of trade secrets, although trade secrets are considered proprietary information. Therefore, psychological ownership was used for ownership to protect trade secrets.

Generally, secrets are kept between two or more people. Therefore, for an individual to keep a secret within a group, having strong ties between the group members is necessary. Therefore, social bonding will be used for secrecy to protect trade secrets.

A new contribution is achieved in this research by seeking to understand what influences entrepreneurs' security behaviour or trade secret protection, so that corporations can design and implement effective cyber security countermeasures. There are a number of theories and models in the literature that have been used to understand employees' security behaviour in an organisational context. However, none has investigated the security behaviour of an outsider's 'entrepreneurs' within a corporate dynamic agile experimental environment that is based on open innovation.

This research explores the protection of trade secrets, focusing on the three dimensions of trade secrets and the three defined protection aspects. This involves investigating the impact of protection motivation on confidentiality protection, psychological ownership on ownership protection and social bonding on secrecy protection.

1.3. Research Questions and Objectives

Research Question: How can entrepreneurs' cyber security behavioural intentions impact trade secret protection within agile dynamic environments?

This research question is divided into three sub-research questions.

- RQ1: What are the significant protection motivation factors that influence entrepreneurs' cyber security behavioural intentions to protect trade secrets within a corporate venturing unit?

- RQ2: What impact does psychological ownership have on entrepreneurs' security behaviour to protect trade secrets within a corporate venturing unit?
- RQ3: What impact does the significant social bonding factors have on entrepreneurs' cyber security behaviour to protect trade secrets within a corporate venturing unit?

To answer these questions and address the research problem, the following objectives need to be achieved:

1. Conduct a systematic literature review in the field of cyber security behaviour theories.
2. Define the research constructs and develop the research conceptual model and hypotheses.
3. Design a research methodology to collect and analyse the empirical research data.
4. Develop the research data collection instrument and assess its validity and reliability.
5. Assess and prepare the collected quantitative data for multivariate analysis.
6. Analyse the research participants' demographics using descriptive statistics.
7. Examine the validity and reliability of the research's measurement model.
8. Examine the research's structural model capabilities and test hypotheses.
9. Define the research's final cyber security model for trade secret protection.
10. Report and discuss the research findings and draw conclusion and future research.

1.4. Design/Methodology

The research adopts a hypothetico-deductive approach that involves the design of a theory and developing determinates of assumptions. The deductive approach will be used to test the developed theory and confirm or reject the research hypotheses as illustrated in Figure 1.5.

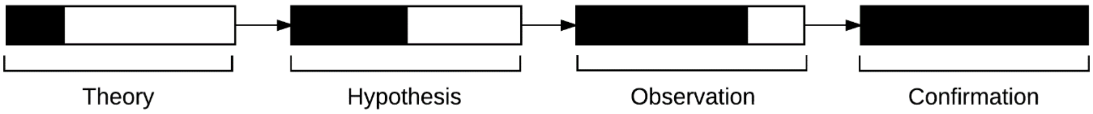


Figure 1.5: Deductive approach (adopted from Trochim (2001))

The research uses a quantitative research approach by developing a survey instrument. Therefore, an online questionnaire will be used for data collection purposes (See Appendix A). The questionnaire items are adapted from previous research in the field of cyber security behaviour. Therefore, this research instrument adopts measures from the previous literature, and modifies them to make them relevant to the research context and reflects the research needs. Participants will be asked to indicate the level of agreement or disagreement with the items in each construct of the conceptual model.

The collected data from the survey will be analysed using SPSS and SmartPLS. In addition, in order to achieve research objectives, the following data analysis methods will be used:

- Descriptive analysis of demographic variables.
- Cronbach Reliability Analysis (Reliability testing).
- Exploratory Factor Analysis (EFA) (Reliability and validity testing).
- Structural Equation Modelling (SEM) (Hypothesis testing).

1.5. Research Scope

This research addresses individuals' behaviour within a dynamic agile environment context (i.e. corporate venturing units). Although entrepreneurs within such a unit operate within a corporation function, they have their own characteristics that differ from corporate employees (Engle, Mah, & Sadri, 1997). Therefore, the research looks specifically to entrepreneurs' behaviour within a corporate accelerator.

From a business perspective, trade secrets are an important asset in maintaining a competitive advantage for new ventures. In addition, cyber security is not limited to technology only, and covers the wider area of security methods, information assets and people involvement. Therefore, the present research focuses on entrepreneurs' cyber security behaviour in regards to their most valuable and vulnerable intangible asset when joining a corporate accelerator, namely their business trade secrets (e.g. processes, algorithms, methods, etc.).

Given the research interest in exploring entrepreneurs' cyber security behavioural intentions in protecting trade secrets within corporate accelerators', entrepreneurs in corporate accelerators in London chosen as the research target population. This is due to the fact that the UK has the largest number of corporate accelerators in Europe, with the vast majority of them in London (Future Asia Ventures, 2016). Thus, the scope of this research has been explained to clarify the research focus and boundaries and help to set the research direction.

1.6. Research Value

This research adopts the view that if entrepreneurs' cyber security behaviour towards trade secrets can be enhanced, the theft and leakage of trade secrets can be lessened, and competitive advantage of start-ups during a corporate accelerator programme may be maintained. Therefore, the outcomes of this research will be of considerable value to different corporations, especially those interested in enhancing entrepreneurs' cyber security behaviours to protect trade secrets within corporate accelerator programmes.

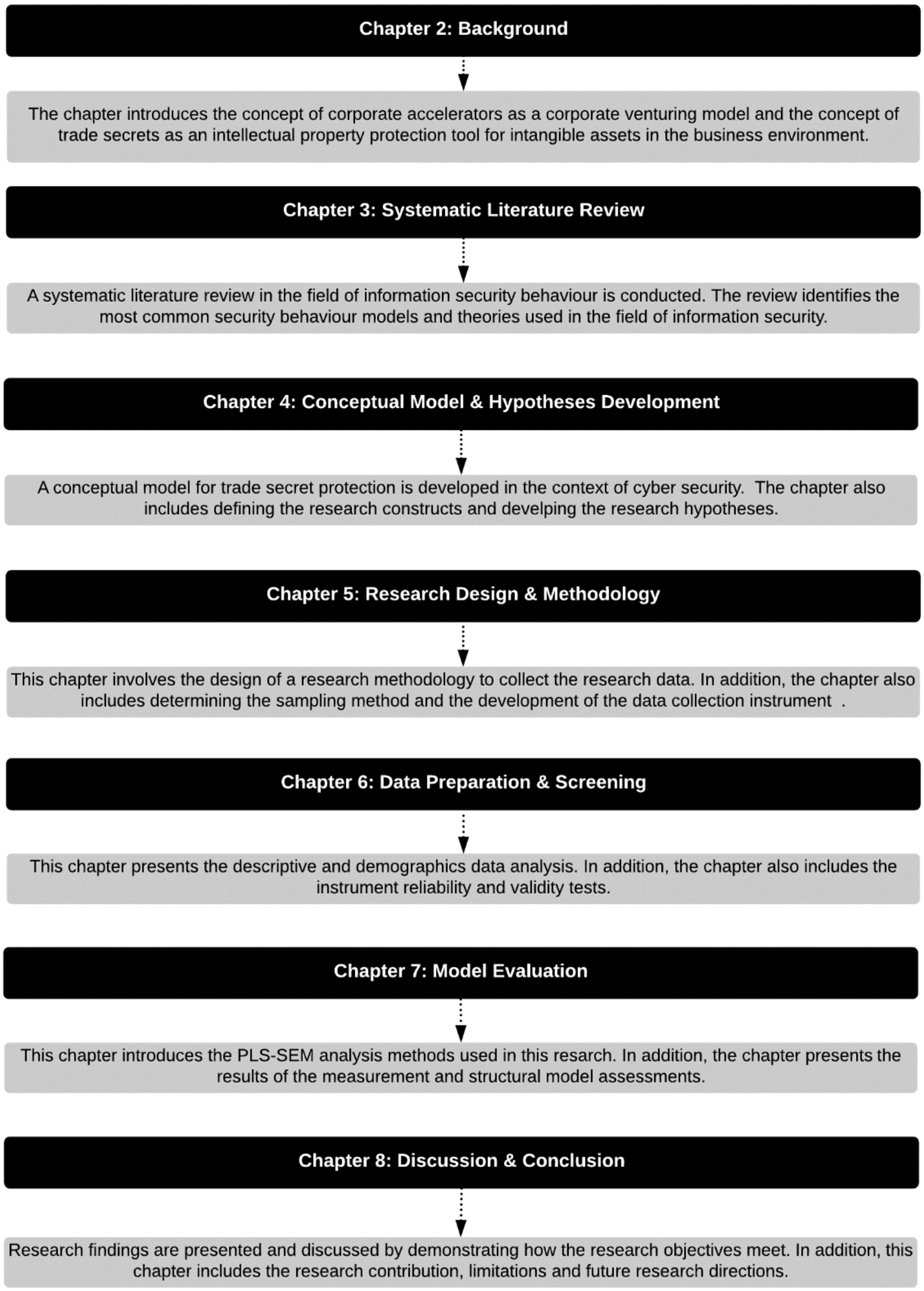
In particular, this research will be of value to:

- Large corporations, in designing countermeasures, procedures and initiatives to enhance the protection of trade secrets in corporate venturing units.
- Those in management positions within corporations such as corporate venturing managers and top management, to encourage entrepreneurs' cyber security behaviours, which can enhance the protection of new ventures competitive advantages.
- Government agencies that are concerned with the protection of Intellectual Property (IP) for new ventures by understanding the importance of cyber security behaviour and the factors that have an impact on protecting trade secrets in dynamic agile environments.
- Researchers that are interested in understanding the factors that influence cyber security behaviour in new ventures, to conduct further research in the field.

In addition, the research will contribute to current knowledge in the field of cyber security behavioural intentions. The significant research contribution will be presented in the final chapter after conducting the research analysis and evaluation.

1.7. Thesis Outline

The following outline illustrates the structure of the thesis and provides a summery for each chapter.



Chapter 2: Background

The chapter introduces the concept of corporate accelerators as a corporate venturing model and the concept of trade secrets as an intellectual property protection tool for intangible assets in the business environment.

Chapter 3: Systematic Literature Review

A systematic literature review in the field of information security behaviour is conducted. The review identifies the most common security behaviour models and theories used in the field of information security.

Chapter 4: Conceptual Model & Hypotheses Development

A conceptual model for trade secret protection is developed in the context of cyber security. The chapter also includes defining the research constructs and develping the research hypotheses.

Chapter 5: Research Design & Methodology

This chapter involves the design of a research methodology to collect the research data. In addition, the chapter also includes determining the sampling method and the development of the data collection instrument .

Chapter 6: Data Preparation & Screening

This chapter presents the descriptive and demographics data analysis. In addition, the chapter also includes the instrument reliability and validity tests.

Chapter 7: Model Evaluation

This chapter introduces the PLS-SEM analysis methods used in this resarch. In addition, the chapter presents the results of the measurement and structural model assessments.

Chapter 8: Discussion & Conclusion

Research findings are presented and discussed by demonstrating how the research objectives meet. In addition, this chapter includes the research contribution, limitations and future research directions.

Chapter 2

2. Background

2.1. Introduction

In today's globally competitive marketplace, innovation is essential to enable large companies to grow and survive. Corporates are focusing on sustainable innovation to improve current products and retain competitive edge. Meanwhile, significant changes in the start-up ecosystem in the last decade are allowing start-ups to compete with large corporates by bringing their ideas to the market in a faster, more agile way, and in a more affordable manner than was the case in the early 2000s. Furthermore, access to capital through angel investors and venture capitalists, in addition to the access to business incubators and accelerators, all serve to support the growth potential of start-ups. This has forced corporates to reconsider their strategies and practices by adopting new models of corporate venturing programmes (Battistini et al., 2013; Engel, 2011). Weiblen and Chesbrough (2015) argue that start-ups could be a vital source of innovation and growth for large companies.

Corporate Venturing (CV) has emerged as a driving force behind corporate disruptive innovation (Kuiper and Ommen, 2015). In addition, Intellectual Property (IP) has become a key protection method for companies' intellectual assets. Both corporate venturing and intellectual property are shaping corporates' new innovation strategies to transform the way corporates innovate and create a competitive advantage.

This chapter offers a background about cyber security, corporate venturing and intellectual property in relation to entrepreneurial activity and innovation within a company. The aim of this background is to introduce the concepts that are used as a foundation for this research.

2.2. Cyber Security Essentials

Information security refers to "*the preservation of confidentiality, integrity, and availability of information*" (ISO/IEC 27000, 2016, p.6). Information can come in different forms: a digital form (e.g. data files on a system), a physical form (e.g. on paper) and in the form of knowledge (e.g. know-how). According to Hult and Sivanesan (2013) cyber security involves the protection of IT systems and information security. In regard to cyber security, Refsdal et al. state that "*Cybersecurity goes beyond information security in that it is not limited to the protection of information assets and the preservation of confidentiality, integrity, and availability of information. Information security, on the other hand, goes beyond cybersecurity in that it is not limited only to threats that arise via a cyberspace.*" (p.30, 2015).

In this regard, the ISO/IEC 27001 (2013) defines the requirements for information security. These involve three key aspects of information security, often described as the CIA triad: confidentiality, integrity and availability. Confidentiality involves the 'property that information is not made available or disclosed to unauthorized individuals, entities, or processes' (ISO/IEC 27000, p.4, 2016). In other words, in order to protect the confidentiality of information they need to be kept secret. Pfleeger and Pfleeger (2006) state that confidentiality is also referred to secrecy.

According to Bos et al (2015), secrecy is a protection mechanism that offers a great protection for companies that depend on knowledge to perform innovation activities as a source of competitive advantage. Secrecy has been an important social aspect that was first studied by Simmel (1906) in the early twentieth century. Simmel (1906) described secrecy as an individual's ability to keep a secret. Posthumus & Solms (2004), stated that preserving the confidentiality of information in an organisation can be achieved through applying two approaches, either by restricting access to confidential information or encrypting confidential information.

However, information in general is exposed to three main elements: technology, people and processes (Posthumus & Solms, 2004). Information in an organisation is defined as intangible assets that require protection. In the information systems research field, the term information security has been used interchangeably with the term cyber security. In this research, the term cyber security will be used, given its broader application for security.

2.3. Corporate Venturing

2.3.1.Review of Corporate Venturing

The significance of corporate venturing is best expressed by its fostering of innovation and amazing economic growth. Corporate venturing is an important element of corporations' economic development (Antoncic and Hisrich, 2001). In this regard, corporates are adopting entrepreneurial activities to survive in this rapidly changing environment.

Corporate venturing is a term that describes entrepreneurial activities used to start a new venture within a large corporate organisation (Kuiper and Van Ommen 2015;

Gündoğdu, 2012; MacMillan et al., 1986). There have been other different terms used in the literature to describe these entrepreneurial activities within established companies, such as corporate entrepreneurship (Burgelman, 1983, 1985), intrapreneurship (Antoncic and Hisrich, 2001; Pinchot, 1985) and corporate venture capital (CVC) (Lerner, 2013). Scholars have also called this new business creation and corporate innovation (Garvin, 2004).

Morris et al. (2010) noted that the term corporate entrepreneurship and corporate venturing have often been used interchangeably in the literature to describe the new business creation phenomena. In addition, the concept of corporate venturing has suffered during the last four decades, in that there has not been an agreed definition for the concept. Where there have been different definitions and classifications of corporate venturing. Some scholars limit the definition of corporate venturing to activities of corporate venture funding (Lerner, 2013), while others (Wolcott and Lippitz, 2007) differentiate between corporate entrepreneurship and corporate venture capital. Other researchers have conceptualized corporate venturing as being part of a bigger umbrella of corporate entrepreneurship (Phan et al., 2009). Kuratko and Audretsch (2013) state that the concept has evolved during the last couple of decades, and at the same time, definitions have varied greatly.

Corporate Entrepreneurship (CE) is defined by Sharma and Chrisman as "*the process whereby an individual or a group of individuals, in association with an existing organization, create a new organization or instigate renewal or innovation within that organization.*" (1999, p.18). More recently Wolcott and Lippitz (2007) defined corporate entrepreneurship as "the process by *which teams within an established company* *conceive, foster, launch, and manage a new business that is distinct from the parent company but leverages the parent's assets, market position, capabilities or other resources*" (p. 75). A simple understanding of corporate entrepreneurship is used in this research, as described by Guth and Ginsberg (1990), namely that CE describes the creation process of new ventures from within an existing company.

Moreover, Kuiper and Van Ommen (2015) have discussed the issue of defining corporate venturing, and different views in regards to this. A different view looks at corporate venturing as an external fund activity limited to a corporate venture fund. On the other hand, there is a second view that looks at corporate venturing as constituting all entrepreneurial activates that aim to create a new venture in co-operation with a large corporation. Moreover, there is a large amount of literature that limits the concept of corporate venturing to corporate venturing capital. The reason for the later view is that the four previous waves were confined to one specific model, namely the corporate venture funding model. More recently, in the last couple of years, a new wave of corporate venturing models has emerged on the surface.

There have been five waves of corporate venturing development since the appearance of corporate venturing activities in the 1960s. In the first four waves, corporates focused on corporate venturing capital as the main activity to create new ventures. Moreover, in the 1980s and 1990s, the vast majority of new ventures were created by large corporations. This developed and changed dramatically since the financial crisis in 2008, which initiated the fifth wave of corporate venturing (Kuiper and Van Ommen, 2015). Corporates are thus no longer only offering capital in exchange for equity, but are becoming more collaborative by offering different corporate resources.

By reviewing the literature, it is also clear that there are different classifications and models of corporate venturing. Some authors have classified corporate venturing on the basis of financial equity into equity models and non-equity models (Weiblen and Chesbrough, 2015). Equity models (e.g. corporate venture capital) are the more mature and established ones that have been in existence for a number of years. In contrast, the non-equity models (e.g. corporate accelerators) are new models that aim to enable corporations to engage with a larger number of start-ups in a fast agile way. Others argue that corporate venturing is divided into two key activities: internal corporate venturing activities and external corporate venturing activities (Sharma and Chrisman, 2007).

Despite the different definitions and classifications of corporate venturing, they all aim to support the creation of new ventures by offering entrepreneurs different corporate resources (i.e. expertise, mentoring, financial capital, technology, intellectual property, work space, etc.). The importance of corporate venturing has arisen due to its remarkable growth across industry, and across academia as a field of research (Fayolle and Wright, 2014; Kuratko et al., 2015). For decades, corporations have been investing in R&D units to create new revenue streams. The flexibility of corporate venturing today helps companies implement change more quickly and cheaply in regards to technology and business models than traditional R&D (Lerner, 2013). Henry and Treanor (2013) describe R&D as a closed innovation model that has become unsustainable, and therefore, corporations have been moving to open innovation models for growth and sustainability. Open innovation is a term used by Chesbrough (2012) that involves businesses that preform collaboration with others to innovate and survive. As described by Pooley, open innovation is “the process of reaching outside the enterprise for tomorrow’s inventive ideas” (2015, p.9).

Companies’ survival and growth depend to a large extent on their ability to innovate (Dushnitsky, 2015). Thus, companies today not only depend on internal R&D, but are increasingly engaging with external partners via open innovation (Dushnitsky, 2015). According to Hayton (2005b) an organisation can accumulate intellectual property using two sources, through internal development (i.e. R&D) or through an external knowledge source (i.e. corporate venturing). Corporate venturing is a concept that has been pursued by many corporations around the globe and has certainly emerged as one of the corporate buzz words that goes beyond the traditional corporate R&D and business development. Companies are adopting entrepreneurial activities via corporate venturing to survive in this rapidly changing environment.

A significant change in the perception of the importance of corporate venturing for large corporations has taken place in the last five years. This change has made corporations redefine their practices in innovation and investment. According to Mawson (2011) the activities of corporate venturing have been growing since 2011 and are described as the golden age. Today, corporations are adopting newer corporate venture models that offer entrepreneurs working space, technology, intellectual property, business support and mentorship (Kuiper and Ommen, 2015; Weiblen & Chesbrough, 2015). These new models are adopting an open innovation approach that is based on collaboration with start-ups in order to exploit new opportunities. According to Kuiper and Van Ommen (2015) corporate venturing is expanding beyond its traditional models to include new models that are not only limited to corporate venturing capital. Corporates used to focus on investment in late stage start-ups; however, they have now started to focus on early stage start-ups. This new focus has made corporates adopt the accelerator model that provides start-ups with the resources required to accelerate the growth and success of their new business ideas.

When comparing new corporate venturing models to traditional 30 year CVC models, the new models are still less mature. This is because corporations have been focusing on equity models in the past 30 years, which offer start-up capital in exchange for equity.

2.3.2. Corporate Accelerators

Accelerators emerged in the mid-2000s as a new generation of incubators, due to the shortcoming of traditional incubators (Pauwels et al., 2016). Y-Combinator (YC) is the first accelerator to be established in 2005 in Cambridge, Massachusetts, to accelerate early stage start-ups. There have been a number of successful companies that graduated from YC, such as Reddit, DropBox, and Airbnb. Today, there are more than 235 accelerator programmes worldwide that have supported 5,693 ventures, with more than 12 billion dollars of funding (Christiansen, 2013). Thus, accelerators have played a critical role in the start-up ecosystem, and are worth billions of dollars. Table 2.1 shows the key differences between accelerators and incubators.

Table 2.1: Key difference between incubators and accelerators (Cohen and Hochberg, 2014)

	Incubators	Accelerators
Programme Duration	1 to 5 years	3 to 6 months
Cohorts	No	Yes
Business Model	Rest	Investment
Selection	Non-competitive	Competitive
Venture Stage	Early or late	Early

Mentorship	Minimal	Intense
Location	On site	On site

An accelerator is defined as "an organization which aims to accelerate new venture creation by providing education and mentoring to cohorts of ventures during a limited time" (Pauwels et al., 2016, p.2). Historically, corporate venturing depended on offering traditional financial capital funding to start-ups in exchange for equity. Corporates have recently adopted the accelerator model, where most of the corporate accelerators were established after 2010 (Kuiper and Van Ommen 2015). According to a recent report by Future Asia Ventures (2016), there are 131 corporate accelerators worldwide. Figure 2.1 illustrates the growth of accelerators at a rate of 73% in 2015.

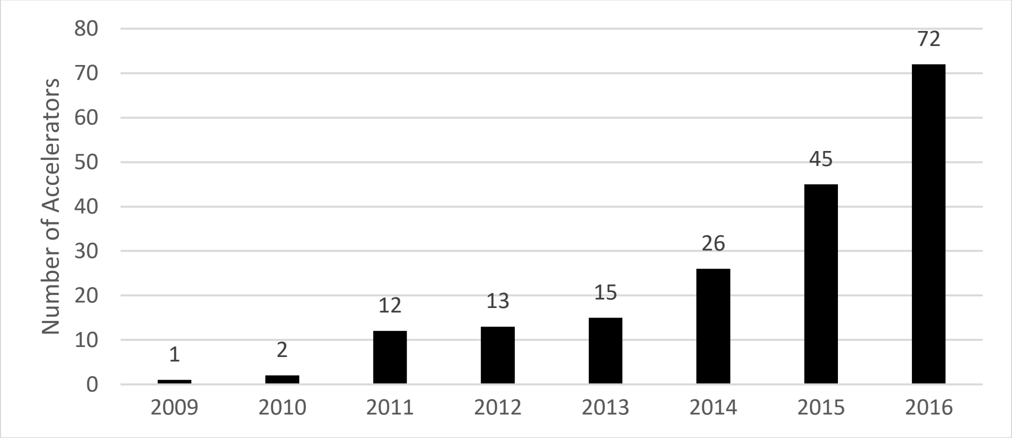


Figure 2.1: Corporate accelerators annual growth (FAV, 2016; The Corporate Accelerator DB, 2016)

The difference between a seed accelerator (i.e. YC) and a corporate accelerator is that the latter has more resources in terms of technology, intellectual property, expertise and funding. Therefore, these new corporate accelerator programmes have emerged to offer more valuable resources to start-ups.

Corporate accelerators are defined as a "company-supported programs of limited duration that support cohorts of start-ups during the new venture process via mentoring, education, and company-specific resources." (Kohler, 2016, p.2). Accelerators generally share the following features (Kohler, 2016):

- A competitive open application;
- A focus on teams not individuals;
- A limited time programme;
- A cohort-based programme.

For example, the Wayra accelerator was established by Telefónica Telecommunication Company in 2011. This accelerator is a 6-month programme that offers start-ups seed funding investment, acceleration services, mentors and access to Telefónica resources. Moreover, start-ups have received $24.2 million from the accelerator, and in addition, received more than $126 million from other investors. In addition, the corporate accelerator model has been adopted by different industry corporations, such as insurance (Allianz), automotive (BMW), entertainment (Disney), media (BBC), banks (Barclays) and other industries.

Boston Consultancy Group (BCG), in a recent report, analysed the development of accelerators and incubators in large companies in comparison with other venturing tools (i.e. CVC and innovation labs) between the years 2010 and 2015. The report states that the number of accelerators/incubators in the largest 30 companies across seven industries (i.e. media, telecommunications, technology, financial services, chemicals, automotive and consumer goods) increased from 2% in 2010 to 44% in 2015 exceeding the number of CVCs and innovation labs in these companies. This shows that accelerators are becoming the main innovation vehicle in large companies.

One of the main features of accelerators in general is to provide access to the start-up ecosystem network. This usually exposes entrepreneurs to mentors, investors, other entrepreneurs, corporate executives and venture capitalists (Hochberg, 2015).

2.4. Intellectual Property

Intellectual Property (IP) has played a major role in the innovation and competitiveness of large corporations. Intellectual property is defined as "legally protected rights concerning ownership of specific intellectual assets such as patents, copyrights, trademarks, and trade secrets" (Hayton, 2005a, p.141). Furthermore, Moberly (2014) identifies IP as one form of intangible asset in businesses. The key benefit of obtaining IP rights is that it grants a company the ability to exclude others from using their intellectual property. In addition, IP as a protection tool gives companies the right to take legal action against any competitors invading their intellectual property rights. The different types of IP (WIPO, 2004) are described as follows:

- Patents: are obtained by receiving a document issued by a government office that gives exclusive ownership of an invention to a company or individual for a period of time, usually 20 years.
- Copyright: is granted to protect the creativity work of an individual or a company, such as music, books, drawings and other original creations.
- Trademarks: are an exclusive right given to a company to use special identities for their services and products, which may be a combination of letters, words and numbers, or symbols.

- Trade Secrets: are any business information that is not disclosed to the public and gives a company a competitive advantage in the marketplace.

According to Alkaersig et al. (2015) different forms of intellectual property are used as multiple layers of protection to safeguard companies' intangible assets. For example, a company may patent part of an invention and keep another part as a trade secret, which makes it difficult for its competitors to work around the invention. This shows that companies need different types of IP tools to protect their intangible assets.

With regard to intellectual property tools, trade secrets provide the foundation for intellectual asset protection for most companies. During the early stage of creating a new venture, trade secrets are usually used as the main tool to protect the by-product of any new ventures. This emphasises the importance of trade secrets in the current competitive market. According to Pooley (2013), secrecy of information is an essential part of the innovation process. In the case of obtaining a patent, for example, secrecy of information regarding the invention must be retained until the filling day of the patent application.

Boldrin and Levine (2008) argue that Google, YouTube and Skype did not use patent protection to gain a competitive advantage in the market. While this may be true, other forms of intellectual property have been used for intellectual protection. For example, Google's search engine algorithm is considered to be a trade secret that has given Google a competitive edge in the digital era (Halt et al., 2014).

2.4.1. Trade Secrets as a Competitive Advantage

The importance of trade secrets has arisen due to the phenomenal growth of intangible assets market value and the sophisticated cyber theft of corporate intellectual property. A recent report by PwC estimates that the annual loss of trade secrets in the US economy is between 1% to 3% of the nation's GDP (Create.org and PwC, 2014). Trade secrets are becoming a key source of competitive advantage, and at the same time, the most vulnerable type of intellectual property (Robertson et al., 2015; Villasenor, 2015). The Uniform Trade Secrets Act (UTSA) defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique, or process, that: (i) derives independent economic value, actual or potential, from not being generally known, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and (ii) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy" (Uniform Law Commission, 1985, p.5). Moreover, Halt et al. define trade secrets as any "information that has economic value and is secret" (2014, p.25).

Trade secrets can be in different forms. The World Intellectual Property Organization (WIPO, 2004) identified the following as trade secrets:

- Production methods
- Chemical formulae
- Blueprints or prototypes
- Sales methods
- Distribution methods
- Contract forms
- Business schedules
- Details of price agreements
- Consumer profiles
- Advertising strategies
- Lists of suppliers or clients

However, WIPO have also stated that the information that is considered to be a trade secret varies from one case to another. For instance, in Japan and the US, a trade secret is referred to as any information on manufacture, business and technology that is not available to the public, and is considered to provide a competitive advantage in the marketplace.

In a report issued by the European Commission (COM (2013) 0402, final) entitled “Study on Trade Secrets and Confidential Business Information in the Internal Market”, it is stated that trade secrets have received little atention in the past years, compared to patents and copyright. Yet the report states that the value of trade secrets has been growing, and that economists are not focusing on trade secrets as enablers of innovation.

The economic impact of disclosing trade secrets can to some extent affect the success of some companies (Hemphill, 2004). For example, the disclosure of the Coca-Cola formula, which is one of the most famous trade secrets, could result in economic damage to the company (Bloom, 2006). Additionally, in recent research, by Crittenden et al. (2015) which investigates the strategic objectives of various company trades secrets, they noted that trade secrets range from food products (i.e. Krispy Kreme) to advanced technologies (i.e. Tesla Motors Inc.). Therefore, trade secrets have been used in different industries to protect different types of information. This illustrates the fact that companies are relying comprehensively on trade secrets to develop their competitive advantage.

There are a number of advantages of trade secrets as an intellectual property tool in contrast to patents. Trade secrets have no time limit, whereas patents are granted for about 20 years, and then become free for public use. In addition, trade secrets involve no registration process, whereas a patent application takes about 18 months before the patent is granted. Moreover, one of the main advantages of trade secrets is that no information disclosure is required, whereas obtaining a patent involves full disclosure of information and publishing to be available to the general public.

According to Almeling (2012), trade secrets are increasingly important in today's economy, for the following reasons:

1. New technologies make it easier to steal information;
2. The increasing number of employees changing workplace;
3. The increasing value of trade secrets as intangible assets;
4. Trade secrets law is growing and gaining more attention;
5. The scope of information regarded as trade secret is expanding;
6. The increase of international threat of cyber security IP theft;
7. The overlapping of trade secrets with patent protection.

Furthermore, in the early stages of starting new ventures, entrepreneurs usually take time to validate their business idea, going through a number of iterations until they find a viable business model. Therefore, filing a patent might not be the best decision before validating a business idea. Thus, trade secrets offer the first layer of protection for the intangible assets of new ventures.

In the last four decades, there has been an increasing value of companies' intangible assets. Although it is difficult to accurately value intangible assets, economists have been assessing the value of trade secrets as part of companies' intellectual property (Almeling, 2012). As illustrated in Figure 2.2, the intangible asset value of S&P 500 companies' total value has increased from 17% in 1975, to 87% in 2015 (Ocean Tomo, 2015). Also, research conducted by Forrester Research estimates that the value of trade secrets is two-thirds of the total intangible assets in most companies (Forrester

Research, 2010). This shows a significant change in companies' asset value, where tangible assets are dominated by intangible assets. Phillips (2015) stated that "Facebook is now worth more than Walmart", where Facebook's market value of $236 billion exceeded Walmart's $235 billion.

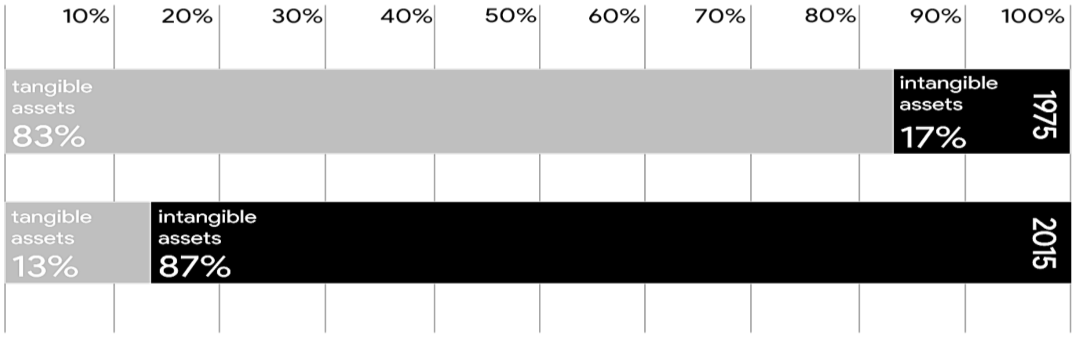


Figure 2.2: Intangible assets vs. tangible assets based on Ocean Tomo (2015, p.22)

The value of trade secrets is becoming an important aspect of companies' competitive advantage. This requires companies to adopt more security countermeasures to protect its value. Therefore, the protection of trade secrets is becoming a necessity for most new ventures in the knowledge-based economy.

2.4.2. How Are Trade Secrets Protected?

The basic concept of trade secrets is the requirement for confidentiality of information. The protection of trade secrets relies on efforts to keep the critical business information confidential and not to disclose it to public. Compliance in regards to secrecy of information is required by many legal laws in different countries to consider any information as trade secret.

According to Pooley (2013) the most frequent form of IP used by companies to protect their competitive advantage is secrecy. Yet, it is the most vulnerable IP tool (Robertson et al., 2015; Villasenor, 2015). In a report submitted by the European Commission to the

European Parliament (COM (2013) 0402, final), the report noted that trade secrets are one of the most common IP protection forms used by companies to protect their intangible assets. However, at the same time, trade secrets enjoy the least legal IP protection in regards to potential disclosure. This is because trade secret laws are the newest among the four types of intellectual property (Almeling, 2012), and in comparison with other IP laws (i.e. patent law) they have not yet been as fully developed. According to Gollin (2008) start-ups depend strongly on trade secrets as an intellectual property strategy to protect its intellectual assets. In addition, in an early stage venture, Non-Disclosure Agreements (NDAs) and employment agreements are considered to be IP protection strategies. NDAs refer to "a contract that protects confidential or trade secret information ("Confidential Information") from disclosure to third parties" (Halt et al., 2014, p.77).

Chapter 3

3. Literature Review

3.1. Introduction

In the previous chapter, the research problem was identified: that is, there is a need to protect trade secrets for new ventures within a corporate venturing unit in order to protect competitive advantage. In other words, it is important to understand the factors that influence entrepreneurs' cyber security behaviour to be able to design the appropriate security countermeasures for the protection of trade secrets in an agile dynamic environment. Therefore, the objective of this chapter is to provide a review of the existing academic literature in the field of cyber security behaviour. This objective is achieved by conducting a systematic literature review of cyber security behaviour in the information systems (IS) security literature.

The literature review in this research focuses on the information systems domain. This is because research in information security behaviour is more associated with research in the information systems domain. In addition, most information security behaviour research is published in information systems' journals and conferences. Therefore, the literature review in this research will focus on information security behaviour in the information systems domain. However, other information security literature that is relevant to the research topic in information security literature will not be neglected.

A quick review of the literature showed that there is a massive literature available in both journals and conferences. Therefore, this research focuses on top journals due to the large existing body of literature and the limitation of time. The focus on reviewing top journals in one research domain would have some limitations were there could be some relevant research in conference papers and in other research domains. However, by adopting a systematic literature approach that documents the whole process this would make the output of the reviewed literature sufficient for this research topic.

In IS security research, scholars have conducted literature reviews to provide a theoretical basis for further research (Lebek, 2014). For example, Mishra and Dhillon (2005) conducted a review of behaviour theories in IS security to introduce a new theory to the research field. Likewise, Aurigemma and Panko (2012) conducted a structured literature review for behavioural theories in IS security to develop a model for behavioural compliance with IS security policies.

This chapter aims to present a systematic review of the cyber security behaviour literature by identifying the latest publications and main theories in the cyber security behaviour domain. In addition, this chapter provides an understanding of the applied behaviour theories in the context of cyber security. Finally, analysing and synthesizing the identified relevant cyber security behaviour literature and presenting the key findings and insights.

3.2. Review Methodology

According to Baker (2000), conducting a literature review is the first step and foundation in research. In addition, Levy and Ellis (2006) define a literature review process as 'sequential steps to collect, know, comprehend, apply, analyse, synthesize, and evaluate quality literature in order to provide a firm foundation to a topic and research method' (p.182). Systematic reviews are defined as '... *literature reviews that adhere closely to a set of scientific methods that explicitly aim to limit systematic error (bias), mainly by attempting to identify, appraise and synthesize all relevant studies (of whatever design) in order to answer a particular question (or set of questions)*' (Petticrew and Roberts, 2008, p.9).

In this study, the systematic literature review consists of two phases. First, a structured search process is conducted as illustrated in Figure 3.1 to identify the relevant literature in the cyber security behaviour research field. Second, the identified cyber security behaviour literature is analysed for findings and insights.

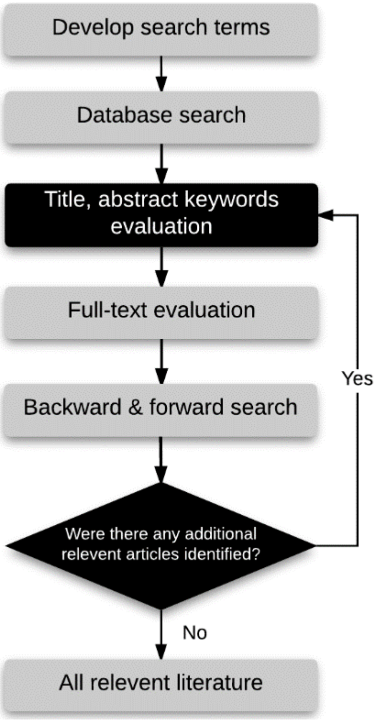

Develop search terms
Database search
Title, abstract keywords evaluation
Full-text evaluation
Backward & forward search
Were there any additional relevent articles identified?
Yes
No
All relevent literature

Figure 3.1: Literature search process

3.2.1. Literature Search Process

According to vom Brocke et al. (2009), the search process conducted determines the quality of a literature review. Moreover, the process of a literature search involves the identification of the relevant literature and then the evaluation of their applicability to the research topic (Levy and Ellis, 2006). This literature search is conducted systematically by adopting Webster and Watson’s (2002) structured approach for the identification process of relevant literature and also the guidelines of Vom Brocke et al. (2009) on rigorous literature.

Vom Brocket et al. (2009) states that a rigorous literature review search consists of two evaluation criteria: the validity and reliability of the search process. Validity refers to the ‘degree to which the literature search accurately uncovers the sources that the reviewer is attempting to collect’ (vom Brocket et al., 2009, p.3). According to Lebek et al. (2014), the validity of a literature search is achieved through the type of publication selected, covered period, the keywords used, and the process of forward and backward searching. Reliability, on the other hand, refers to ‘the replicability of the search process, hence, making it substantial for any review article to comprehensively document the literature search’ (vom Brocket et al., 2009, p.3). This requirement is achieved by documenting the literature search process comprehensively (vom Brocke et al., 2009; Lebek et al., 2014).

To achieve the validity requirement for a rigorous literature review, and to produce an efficient literature review, this study focuses only on leading journals and selected conference proceedings (i.e. peer reviewed) as recommended by Webster and Watson (2002) and vom Brocke et al. (2009). In addition, following the guidelines of vom Brocket et al. (2009), the study will review the top 10 ranked peer-reviewed journals based on the AIS MIS journal ranking list (AIS, 2016) and the top 10 ranked IS conferences (Levy and Ellis, 2006). This will help avoid the pitfall of garbage-in/garbage-out, which can produce an inefficient literature review.

This review did not include journals that are not peer reviewed (i.e. Harvard Business Review), are unrelated to the study subject (i.e. Artificial Intelligence and AI Magazine), and include publications of different quality and relevance (i.e. IEEE Transactions). Therefore, we have only taken into account the top 10 IS journals that contain relevant publications in the security behaviour domain as illustrated in Table 3.1.

According to Webster and Watson (2002), IS is an interdisciplinary field, therefore, researchers must consider journals from outside the IS literature. By searching the top 10 journals in security and privacy, based on the 'Microsoft Academic Search', we found that only two journals (i.e. 'Computers & Security' and 'Information Management & Computer Security') contained literature relevant to the research topic. This is because most of the top 10 security journals are specialised security journals in specific security fields (e.g. cryptology and forensics). Nevertheless, this supports Lebek et al.'s (2014) suggestion, where they found that two IS security journals included numerous publications in the field of security behaviour. Hence, these two IS security journals have been included in the literature search process.

The literature search has been conducted through eight databases: ACM Digital Library, IEEE Xplore Digital Library, Elsevier Science Direct, Springer LINK, Emerald, JSTOR, ProQuest (ABI/Inform) and EBSCOhost. The querying of databases used the following defined search terms: 'security behaviour'; 'behaviour security'; 'behavioural security'; 'security behavioural'; 'human behaviour information security'; 'user behaviour security; ‘security human behaviour’; ‘behavioural information security’ and ‘security behavioural theories’.

Table 3.1: The considered journals for the search process

	Journal	Database
IS Journals	MIS Quarterly	ProQuest (ABI/Inform)
	Information Systems Research	EBSCOhost
	Communications of the ACM	ACM Digital Library
	Management Science	JSTOR
	Journal of MIS	ProQuest (ABI/Inform)
	Decision Sciences	ProQuest (ABI/Inform)
	European Journal of IS	ProQuest (ABI/Inform)
	Decision Support Systems	Elsevier Science Direct
	IEEE Software	IEEE Xplore Digital Library
	Information & Management	Elsevier Science Direct
IS Security Journals	Computers & Security	Elsevier
	Information Management & Computer Security	Emerald

The search process started with a database search using search terms to identify the potential relevant publications. This initial search resulted in 175 potentially relevant publications. Afterwards, a forward and backward search was conducted to identify any additional relevant publications. The backward search was conducted manually by evaluating the publications’ titles. This involved reviewing the references of the identified publications resulting from the keyword search. The forward search was conducted using Web of Science (www.webofscience.com). Thus, the forward and backward search resulted in identifying 41 additional publications, making a total of 216 potential relevant publications.

The first evaluation of the potential publications was based on the evaluation of the publication’s title, abstract, and keywords. Following this, a second in-depth evaluation was conducted on the full-text of the publications to identify the relevant publications for the literature analysis. Although the focus of this review is on the organisational context, the review included other studies involved in different contexts to obtain more valuable insights on the topic. In addition, in order to select relevant and up-to-date literature, the literature search process only took into account publications since 2005. Figure 3.2 shows the steps for identifying the relevant publications through the literature search process.

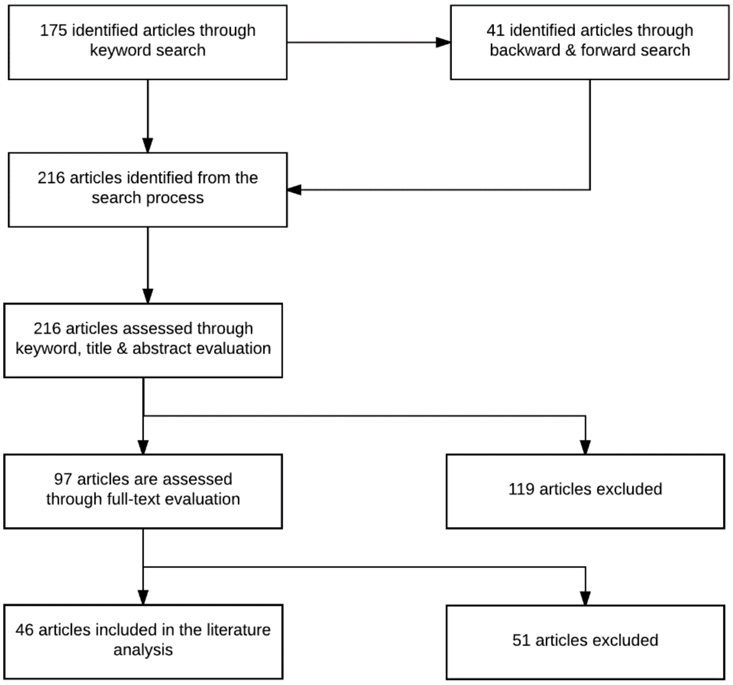

175 identified articles through keyword search
41 identified articles through backward & forward search
216 articles identified from the search process
216 articles assessed through keyword, title & abstract evaluation
97 articles are assessed through full-text evaluation
119 articles excluded
46 articles included in the literature analysis
51 articles excluded

Figure 3.2: The numbers of the identified and evaluated publications from the search process

3.2.2. Literature Analysis

In this section, we first present an overview of the relevant studies in the behavioural security domain, which have been identified in the literature review search process (see Table 2.2). According to Webster and Watson (2002), tables should be more than lists of articles that should add value.

Table 3.2: Overview of behavioural cyber security relevant literature

#	*Study*	*Context (user)*	*Theory applied*	*Methodology*	*Sample size (response rate)*	*Country*	*Related constructs*	*Behaviour Type*
1	Anderson & Agarwal (2010)	Home (ISP subscribers & undergraduate students)	PMT	Survey & Experiment	594	US	▪ Concern regarding security threats ▪ Security behaviour self-efficacy ▪ Perceived citizen efficacy ▪ Subjective norm ▪ Descriptive norm ▪ Psychological ownership for the Internet ▪ Psychological ownership for own computer ▪ Attitude toward performing security-related behaviour ▪ Intentions to perform security-related behaviour (Internet) ▪ Intentions to perform security-related behaviour (own computer)	Individuals' intentions to protect their own computers & the internet at home
2	Chen & Zahedi (2016)	1.UG and PG students & others 2.Socail networks	PMT & TTAT	Survey	1.480 2.333	1.US 2.China	▪ Perceived threat ▪ Perceived susceptibility ▪ Perceived severity ▪ Perceived security response efficacy ▪ Perceived security self-efficacy ▪ Protective actions ▪ Avoidance ▪ Seeking help	Individual security behaviours & their antecedents in a cross-national context.
3	Johnston & Warkentin (2010)	University (faculty, staff and students at a large university)	PMT	Experiment	311 (40%)	--	▪ Behavioural intent ▪ Social influence ▪ Response efficacy ▪ Self-efficacy ▪ Threat severity ▪ Threat susceptibility	Individuals' intentions to comply with recommendations to protect their informational assets
4	Siponen & Vance (2010)	Organisation (employees from multiple organisations)	NT & GDT	Survey (scenario-based)	395 (27%)	Finland	▪ Neutralization ▪ Defense of Necessity ▪ Appeal to Higher Loyalties ▪ Condemn the Condemners ▪ Metaphor of the Ledger ▪ Denial of Injury ▪ Denial of Responsibility ▪ Formal Sanctions	Intention to violate information systems security policy

							▪ Informal Sanctions ▪ Shame ▪ Intention to Violate IS Security Policy	
5	Johnston et al. (2015)	Organisation (employees from multiple organisations)	PMT	Survey	559 (22.6%)	Finland	▪ Threat severity ▪ Threat susceptibility ▪ Self-efficacy ▪ Response efficacy ▪ Formal sanction severity ▪ Informal sanction severity ▪ Formal sanction certainty ▪ Informal sanction certainty ▪ Sanction celerity ▪ Compliance intention	Employees’ intentions to information security policy compliance
6	Boss et al. (2015)	1.MBA students 2. Undergraduate students	PMT	Experiment	1.125 2.327	US	▪ Perceived severity ▪ Vulnerability ▪ Fear ▪ Response efficacy ▪ Self-efficacy ▪ Response cost ▪ Intentions	Make backup to protect computing resources 2.increase use participants’ use of anti-malware software
7	Bulgurcu et al. (2010)	Organisation (employees from multiple organisations)	TPB & RCT	Survey	464 (42%)	US	▪ General ISA (subconstruct), ▪ ISP Awareness (subconstruct) ▪ Perceived Benefit of Compliance ▪ Intrinsic Benefit ▪ Safety of Resources ▪ Rewards ▪ Perceived Cost of Compliance ▪ Work Impediment ▪ Perceived Cost of Noncompliance ▪ Intrinsic Cost ▪ Vulnerability of Resources ▪ Sanctions, Attitude ▪ Normative Beliefs ▪ Self-Efficacy to Comply ▪ Intention to Comply	Employees’ intentions to comply with information security policy
8	Steinbart et al. (2016)	Organisation (UG students at a large private university)	TTAT & CYT	Experiment	568	US	▪ Credential strength ▪ Login failures ▪ Mobile UI ▪ Mobile UI practice ▪ Coping behaviour	Employees’ intentions to configure their mobile devices to require authentication

9	D'Arcy et al. (2009)	Organisation (employees from multiple organisations)	GDT	Survey	269 (38%)	US	▪ Perceptions certainty ▪ Perceptions severity ▪ Moral commitment ▪ IS misuse intention	Employees' intentions to IS misuse
10	Herath & Rao (2009)	Organisation (employees)	DTPB, TPB, OC & GDT	Survey	312	US	▪ Punishment severity ▪ Security policy compliance intention ▪ Detection certainty ▪ Security policy attitude ▪ Perceived probability of security breach ▪ Self-efficacy ▪ Perceived severity of security breach ▪ Subjective norm ▪ Security breach concern level ▪ Descriptive norm ▪ Response efficacy ▪ Resource availability ▪ Response cost ▪ Organisational commitment	Employees' intentions to security policy
11	Warkentin et al. (2011)	Organisations (healthcare professionals)	SLT	Survey	202	US	▪ Self-efficacy ▪ Behavioural intent ▪ Situational support ▪ Vicarious experience ▪ Verbal persuasion	Intention to comply with information privacy policies
12	Myyry et al. (2009)	Organisation (employees & part-time master's students)	TCMD & TMTV	Survey	132	Finland	▪ Preconventional reasoning ▪ Conventional reasoning ▪ Postconventional reasoning ▪ Values	Employee adherence to information security policies
13	Foth (2016)	Organisation (employees)	TPB & GDT	Survey	557	Germany	▪ Detection Certainty ▪ Intention to comply with data protection ▪ Punishment Severity ▪ Attitude ▪ Subjective Norm ▪ Perceived Behavioural Control	Employees' intention to comply with data protection regulations in hospitals
14	Johnston et al. (2016)	Organisation (employees)	PMT & GDT	Survey	242	--	▪ Stability ▪ Sanction severity ▪ Sanction certainty ▪ Threat vulnerability ▪ Threat severity ▪ Self-efficacy ▪ Response efficacy	Employees' intention to violate organisational information security polices

							▪ Response costs	
15	Lee & Larsen (2009)	Organisation (executives from multiple organisations)	PMT	Survey	239	US	▪ Perceived severity ▪ Perceived vulnerability ▪ Response efficacy ▪ Self-efficacy ▪ Response cost ▪ Social influence ▪ Vendor support ▪ IT budget ▪ Firm size ▪ Adoption intention	SMB executives' anti-malware software adoption
16	Boss et al. (2009)	Organisation (employees)	CT	Survey	1698	US	▪ Specification ▪ Evaluation ▪ Reward ▪ Mandatoriness ▪ Precautions taken ▪ Computer Self Efficacy ▪ Apathy	Individuals' security precaution-taking behaviour
17	Guo et al. (2011)	Organisation (employees)	CBM & NMSV	Survey	306	--	▪ Perceived identity match ▪ Attitude toward security policy ▪ Perceived security risk of NMSV ▪ Relative advantage for job performance ▪ Perceived sanctions ▪ Workgroup norm ▪ Attitude toward NMSV ▪ NMSV intention	End user tendencies to voluntarily engage in actions that violate the organization's security policies
18	Posey et al. (2015)	Multiple organisations (employees-panellists)	PMT	Survey	380	US	▪ Intrinsic maladaptive rewards ▪ Extrinsic maladaptive rewards ▪ Threat vulnerability ▪ Threat severity ▪ Fear ▪ Response efficacy ▪ Self-efficacy ▪ Response costs ▪ Protection motivation ▪ Past protection-motivated behaviours ▪ Affective organizational commitment ▪ Job satisfaction ▪ Financial incentives ▪ Managerial support	Insiders protecting their organisation from security threats

19	D'Arcy et al. (2014)	Organisation (employees-panellists)	COT & MDT	Survey	539	--	▪ SRS overload ▪ SRS complexity ▪ SRS uncertainty ▪ Reconstrue conduct ▪ Obscure or distort ▪ Devalue the target ▪ Violation intention	Employees' intention to stressful information security requirements
20	Vance et al. (2013)	Organisation (IS students)	AT	Survey	96	--	▪ Identifiability ▪ Monitoring awareness ▪ Evaluation awareness ▪ Social presence awareness	Insiders' intention to commit access policy violation in information systems
21	Hu et al. (2012)	Organisation (Alumni of the MIS & MBA programs of a large public university)	TPB, CVF & ITAS	Survey	148 (17%)	US	▪ Behavioural intention ▪ Attitudes towards behaviour ▪ Subjective norm ▪ Perceived behavioural control ▪ Perceived goal orientation ▪ Perceived rule orientation ▪ Perceived top management participation	Top management influence on employees' intention to comply with information security polices
22	Ng et al. (2009)	Organisation (Part-time students & IT employees)	HBM	Survey	134 (31%)	US	▪ Behaviour ▪ Perceived susceptibility ▪ Perceived severity ▪ Perceived benefits ▪ Perceived barriers ▪ Cues to action ▪ General security orientation ▪ Self-efficacy ▪ Technical controls ▪ Security familiarity	User's computer security behaviour
23	Herath & Rao (2009)	Organisations (employees from multiple organisations)	GDT & AGT	Survey	312	US	▪ Perceived effectiveness ▪ Severity of penalty ▪ Certainty of detection ▪ Normative beliefs ▪ Peer behaviour ▪ Policy compliance intentions	Employees' compliance to information security policies'
24	Li et al. (2010)	Multiple organisations (employees)	RCT	Survey	246	--	▪ Detection probability ▪ Sanction severity ▪ Subjective norms ▪ Perceived security risk ▪ Perceived benefits of Internet abuses	Employees' intention to comply with Internet use police

							▪ Personal norms ▪ Organizational norms ▪ Organizational identification ▪ Intent	
25	Ifinedo (2014)	Multiple organisations (business managers and IS professionals)	TPB, SCT & SBT	Survey	124	Canada	▪ Attachment ▪ Commitment ▪ Involvement ▪ Personal norms ▪ Attitude toward compliance with ISSP ▪ Subjective norms ▪ Locus of control ▪ Self-efficacy ▪ ISSP compliance behavioural intentions	Employees' information systems security policy compliance
26	Siponen et al. (2014)	Multiple organisations (employees)	PMT, TRA & CET	Survey	669	Finland	▪ Actual compliance ▪ Intention to comply ▪ Attitude ▪ Severity ▪ Vulnerability ▪ Rewards ▪ Normative beliefs ▪ Response efficacy ▪ Self-efficacy	Employees' security policies compliance
27	Son (2011)	Multiple organisations (employees)	EMM & IMM	Survey	602 (30.1%)	US	▪ Compliance ▪ Perceived Deterrent certainty ▪ Perceived Deterrent severity ▪ Perceived Legitimacy ▪ Perceived Value congruence	Employees' motivation to comply with IS security policies
28	Vance et al. (2012)	Organisation (employees)	HT & PMT	Survey	210 (42%)	Finland	▪ Habit ▪ Intention to comply with ISP ▪ Perceived severity ▪ Perceived vulnerability ▪ Response efficacy ▪ Self-efficacy ▪ Perceived realism ▪ Response cost ▪ Rewards	Employees' intention to comply with information security policies

29	Hovav & D'Arcy (2012)	Organisation (MBA students & employees)	GDT	Survey	US: 366 Korea: 360	US & Korea	▪ Perceived certainty of sanctions ▪ Perceived severity of sanctions ▪ Moral belief ▪ IS misuse intention ▪ Procedural countermeasures ▪ Technical countermeasures	Employees' intention to intentional IS misuse
30	Cheng et al. (2013)	Organisations (employees)	GDT & SBT	Survey	185 (41%)	China	▪ Violation intention ▪ Perceived certainty ▪ Perceived severity ▪ Attachment ▪ Commitment ▪ Involvement ▪ Belief ▪ Subjective Norm ▪ Co-worker Behaviour	Employees' ISSP violation intentions
31	Dang-Pham & Pittayachawan (2015)	Students at Australian university	PMT	Survey	252	Australia	▪ Intention to perform malware avoidance behaviours ▪ Vulnerability ▪ Severity ▪ Rewards ▪ Response efficacy ▪ Self-efficacy ▪ Response cost	Intention avoid malware in BYOD context
32	Flores et al. (2014)	Multiple Organisations (information security executives)	Behavioural Information Security Governanc e Model	Survey	82 (15.2%)	US, Sweden, Finland & UK	▪ Coordinating information security processes ▪ Business-based information security management ▪ Organizational structure ▪ Formal organizational structure ▪ Coordinating organizational structure ▪ Security knowledge sharing ▪ Formal knowledge sharing arrangements ▪ Support for knowledge transfer	The influence of behavioural information security governance on security knowledge sharing in organisations
33	Flores & Ekstedt (2016)	Multiple organizations (IT users)	Social Engineering Resistance Model	Survey	1583 (37%)	Sweden	▪ Transformational leadership ▪ Information security culture ▪ Information security awareness ▪ Self-efficacy ▪ Attitude ▪ Normative beliefs	Employees' intention to resist social engineering
34	Ifinedo (2012)	Multiple organisations (non-IS managers & IS professionals)	TPB & PMT	Survey	124	--	▪ Perceived vulnerability ▪ Perceived severity ▪ Response efficacy ▪ Response cost	Information systems security policy (ISSP) compliance

							▪ Self-efficacy ▪ Attitude toward compliance with ISSP ▪ Subjective norms ▪ ISSP compliance behavioural intention	
35	Rhee et al. (2009)	Organisation (graduate students)	SCT	Survey	415	--	▪ Computer/Internet experience ▪ Security breach incidents ▪ General controllability ▪ Self-efficacy in information security ▪ Security practice-technology usage ▪ Security practice-security conscious care behaviour ▪ Intention to strengthen the efforts	Individuals' information security promoting behaviour
36	Safa et al. (2015)	Organisation (Information Security Experts & IT Professionals)	PMT & TPB	Survey	212	Malaysia	▪ Information security awareness ▪ Information security organizational policy ▪ Information security experience and involvement ▪ Attitude toward performing information security conscious care behaviour ▪ Subjective norms ▪ Perceived behavioural control ▪ Threat appraisal ▪ Information security self-efficacy ▪ Information security conscious care behaviour	Information security conscious care behaviour
37	Safa et al. (2016)	Organisation (employees from multiple companies)	SBT & IVT	Survey	302	Malaysia	▪ Information security knowledge sharing ▪ Information security collaboration ▪ Information security intervention ▪ Information security experience ▪ Attachment ▪ Commitment ▪ Personal norms ▪ Attitude towards compliance with ISOP ▪ ISOP compliance behavioural intentions	Employees' information security behaviour, in line with information security organizational policies and procedures (ISOP)
38	Shropshire et al. (2015)	Organisation (undergraduate students)	TAM & BFM	Experiment & Survey	170	US	▪ Perceived ease of use ▪ Perceived usefulness ▪ Perceived organizational support ▪ Adoption intention ▪ Conscientiousness ▪ Agreeableness	Employees' adoption intention and initial use of security software

39	Tsai et al. (2016)	online security for home computer users	PMT	Survey	988	--	▪ Threat severity ▪ Threat susceptibility ▪ Prior experience with safety hazards ▪ Coping self-efficacy ▪ Response efficacy ▪ Subjective norms ▪ Response costs ▪ Safety habit strength ▪ Personal responsibility ▪ Perceived security support	Online users' security protection behaviour
40	Al-Mukahal & Alshare (2015)	Organisation (employees from multiple companies)	GDT, NT & TPB	Survey	234	Qatar	▪ Awareness of information security policy ▪ Trust ▪ Impact of information security policy on work environment ▪ Scope of information security policy ▪ Uncertainty Avoidance ▪ Individualism/Collectivism	information security policy violations
41	D'Arcy & Greene (2014)	Organisation (industrial panel)	security Culture & Organizational Behaviour Model	Survey	127	US	▪ Top management commitment ▪ Security communication ▪ Computer monitoring ▪ Job satisfaction ▪ Perceived organizational support ▪ Security compliance intention	employees' security compliance
42	Zhang et al. (2009)	Organisation (online industrial panellists)	TPB & RICT	Survey	176	--	▪ Perceived security protection mechanism ▪ Subjective norms ▪ Perceived behavioural control ▪ Attitude ▪ Behavioural intention	end-users' intention to comply with security policies
43	Sommestad et al. (2015)	Organisation (employees in a research agency)	TPB & PMT	Survey	306	Sweden	▪ Current behaviour ▪ Intention ▪ Attitude ▪ Perceived norm ▪ Perceived behaviour control ▪ Anticipated regret ▪ Vulnerability ▪ Severity ▪ Response efficacy ▪ Response cost	Employees' information security policy compliance
44	Hu et al. (2011)	Organisation (employees from	GDT & RCT	Survey (scenario-based)	207	China	▪ Low self-control ▪ Moral beliefs ▪ Perceived certainty of sanctions	Employees' intention to violet information

		multiple organisations)					▪ Perceived severity of sanctions ▪ Perceived celerity of sanctions ▪ Perceived extrinsic benefits ▪ Perceived intrinsic benefits ▪ Perceived formal risk ▪ Perceived informal risk ▪ Perceived risk of shame ▪ Intention to commit violation	security police toward computer systems
45	Gurung et al. (2009)	Consumer (business undergraduate students)	PMT	Survey	232	US	▪ Perceived severity ▪ Perceived vulnerability ▪ Self-efficacy ▪ Response efficacy ▪ Response cost ▪ Use of anti-spyware	Consumers' intention to adopt and use antispyware tools
46	Lai et al (2012)	(business undergraduate students)	TTAT	Survey	117 (75.5%)	US	▪ Self-efficacy ▪ Perceived effectiveness ▪ Social influence ▪ Conventional coping ▪ Technological coping ▪ Identity theft	Individuals' intention to protect their identity from theft

- General Deterrence Theory (GDT)
- Protection Motivation Theory (PMT)
- Theory of Planned Behaviour (TPB)
- Decomposed Theory of Planned Behaviour (DTPB)
- Agency theory (AGT)
- Moral Disengagement Theory (MDT)
- Theory of Reasoned Action (TRA)
- Risk Compensation Theory (RCT)
- Social Learning Theory (SLT)
- Theory of Cognitive Moral Development (TCMD)
- Theory of Motivational Types of Values (TMTV)
- Control Theory (CT)
- Nonmalicious Security Violation Model (NMSV);
- Organisational Commitment (OC)
- Technology Acceptance Model (TAM);
- Health Belief Model (HBM)
- Accountability Theory (AT)
- Neutralization Theory (NT)
- Big Five Model (BFM)
- Rational Choice Theory (RCT)
- IT Assimilation Model (ITAS)
- Social Cognitive Theory (SCT)
- Involvement Theory (IVT)
- Coping Theory (COT)
- Social Bond Theory (SBT)
- Cognitive Evaluation Theory (CET)
- Extrinsic motivation model (EMM)
- Intrinsic Motivation Model (IMM)
- Habit Theory (HT)
- Technology Threat Avoidance Theory (TTAT)
- Competing Values Framework (CVF)
- Composite Behaviour Model (CBM)

In order to analyse the accumulated knowledge from a literature search, Webster and Watson (2002) discussed two structural approaches for literature analysis: an author-centric approach and a concept-centric approach. According to Bem (1995), the author-centric approach usually produces lists of citations and findings, which he describes as 'a phone book – impressive case, lots of numbers, but not much plot' (p.172). Additionally, the author-centric approach fails to provide a synthesised literature review analysis (Webster and Watson, 2002). In contrast, the concept-centric approach helps to analyse and synthesise the accumulated knowledge from the literature search by organising the review based on the concepts of the research topic instead of categorising it based on authors.

This research adopts the concept-centric approach by applying the 'Concept Matrix' method to systematically analyse the search results. Moreover, according to Webster and Watson (2002), the concepts are used as building blocks of the structured framework of a review. Hence, by analysing the relevant literature, the determined applied theories are used as concepts in this analysis and synthesis.

The relevant studies identified in Table 2.2 include different types of theories used to investigate IS behaviours across various technologies in both work and non-work contexts. According to Kerlinger and Lee (2000), theory is defined as 'a set of interrelated constructs (concepts), definitions, and propositions that present a systematic view of phenomena by specifying relationships among variables, with the purpose of explaining and predicting the phenomena' (p.11). Following Kerlinger and Lee's (2000) definition of 'theory', 35 theories have been used separately and combined in 46 studies to explain IS behaviour. Additionally, the relevant studies identified have adopted theories from criminology, psychology and sociology to predict individuals' information security-related behaviours. These theories were used to investigate factors that have an impact on the behavioural aspects of individuals' cyber security behaviour.

Most of the theories identified were used in one or two studies. Nonetheless, only eight theories were used frequently more than once in the relevant identified studies identified. The primary theories used are listed in Figure 3.3, along with the frequency of use.

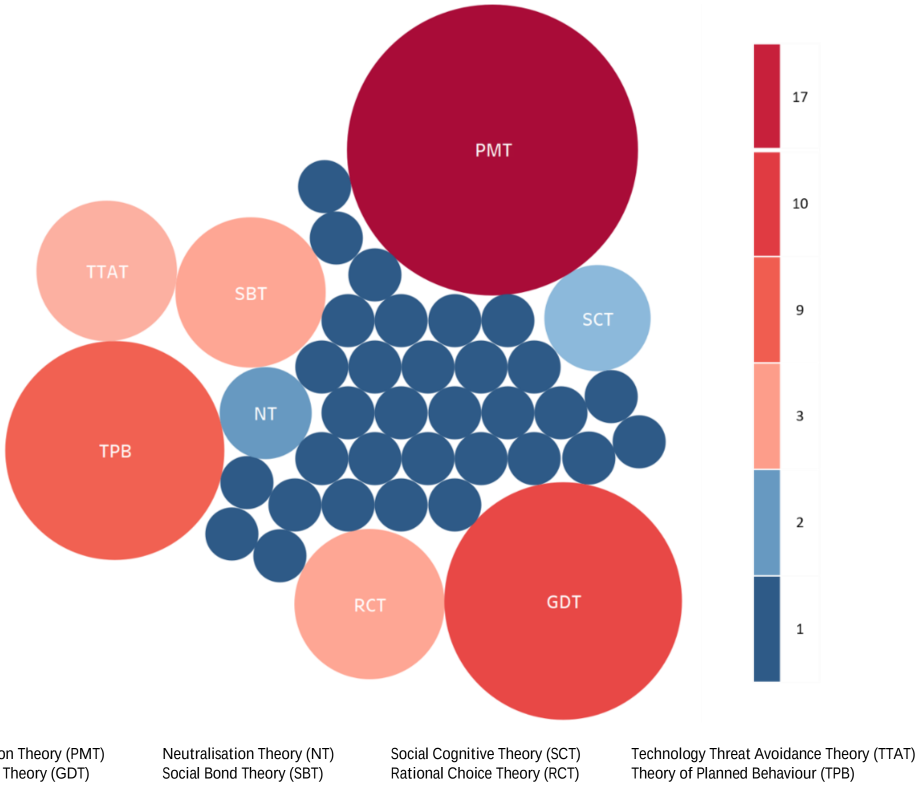


Figure 3.3: The frequency of each theory in the cyber security behaviour systematic review

As stated previously, the systematic review will adopt a concept-centric approach. This is achieved through the identified theories as concepts that will be used as the building blocks of the structured base for this review. Table 2.3 of the concept matrix lists the studies in the left column of the matrix, while the other columns represent the concepts (i.e. theories) that were identified from the reviewed literature on cyber security behaviour. The structure of the literature review is based on the identified theories used in the cyber security behavioural domain. Therefore, in the remaining part of the chapter, an in-depth analysis of the eight identified applied behavioural theories will be conducted to provide valuable insight in the research field of cyber security behaviour.

Table 3.3: A concept matrix illustrating the theories in the cyber security behaviour

Study		GDT	PMT	TPB	RCT	SCT	SBT	NT	TTAT
1	Anderson & Agarwal (2010)		X						
2	Chen & Zahedi (2016)		X						X
3	Johnston & Warkentin (2010)		X						
4	Siponen & Vance (2010)	X						X	
5	Johnston et al. (2015)		X						
6	Boss et al. (2015)		X						
7	Bulgurcu et al. (2010)			X	X				
8	Steinbart et al. (2016)								X
9	D'Arcy et al. (2009)	X							
10	Herath & Rao (2009)	X	X						
11	Foth (2016)	X		X					
12	Johnston et al. (2016)	X	X						
13	Lee & Larsen (2009)		X						
14	Posey et al. (2015)		X						
15	Hu et al. (2012)			X					
16	Herath & Rao (2009)	X							
17	Li et al. (2010)				X				
18	Ifinedo (2014)			X		X	X		
19	Siponen et al. (2014)		X						
20	Vance et al. (2012)		X						
21	Hovav & D'Arcy (2012)	X							
22	Cheng et al. (2013)	X					X		
23	Dang-Pham & Pittayachawan (2015)		X						
24	Ifinedo (2012)		X	X					
25	Rhee et al. (2009)					X			
26	Safa et al. (2015)		X	X					
27	Safa et al. (2016)						X		
28	Tsai et al. (2016)		X						
29	Al-Mukahal & Alshare (2015)	X		X				X	
30	Zhang et al. (2009)			X					
31	Sommestad et al. (2015)		X	X					
32	Hu et al. (2011)	X			X				
33	Gurung et al. (2009)		X						
34	Lai et al. (2012)								X
Frequency		10	17	9	3	2	3	2	3

3.3. Behavioural Theories in Cyber Security Behaviour

In the cyber security literature, the science of behavioural security has frequently used multidisciplinary theories (e.g. criminology and psychology). This section aims to analyse and synthesise the most frequently used theories in the field of security behaviour from the systematic literature review.

3.3.1. Theory of Planned Behaviour

Theory of planned behaviour (TPB) is one of the most widely used behavioural theories that explains an individual's intention to perform a specific behaviour. Ajzen extended TPB from the theory of reasoned action (TRA) (Ajzen and Fishbein, 1980; Fishbein and Ajzen, 1975) to include perceived behavioural control overcoming the lack of social factors (1991). Thus, TPB states that an individual's intentions to behave in a certain manner can be influenced by the following determinants:

- Attitude towards behaviour refers to an individual's degree of favourability toward performing a specific behaviour.
- Subjective norm refers to an individual's perception of social influence on performing a specific behaviour.
- Perceived behavioural control refers to an individual's ability to perform a specific behaviour.

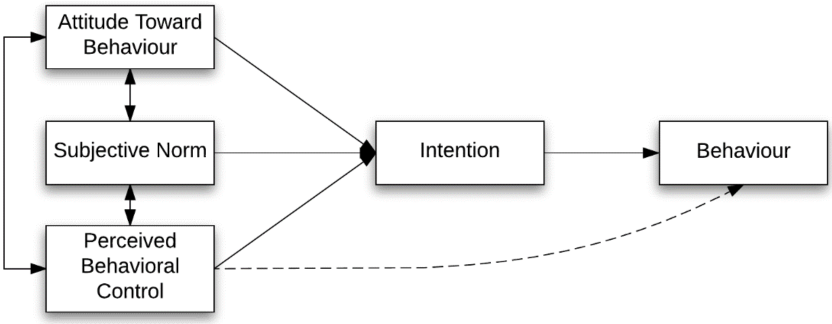


Figure 3.4: Theory of planned behaviour (TPB)

According to Ajzen and Fishbein (2005), the science of attitude has been the base of social psychology studies since the early days (Thomas and Znaniecki, 1918; Watson, 1925) because attitude was the basis for understanding human behaviour. In addition, Ajzen (2012) states that people producing a certain behaviour is usually based on a number of behavioural beliefs that they hold, which will produce a particular outcome. Beliefs are based on a wide range of people's background factors (Ajzen and Fishbein, 2005). Thus, behavioural, normative, and control beliefs provide the accessibility to attitudes, subjective norms, and perceived behavioural control, respectively. Furthermore, Ajzen (2012) argues that beliefs guide individuals' attitudes, subjective norms, and perceptions of control, and, therefore, influence their intentions to produce a course of behavioural action.

3.3.2. General Deterrence Theory

Originally a criminology theory, general deterrence theory (GDT) has been applied to different research fields. Deterrence theory can be traced back to the sixteenth century as Thomas Hobbes (1588–1678), Cesare Beccaria (1738–1794), and Jeremy Bentham (1748–1832) shaped the foundation of deterrence and punishment theory in criminology (Onwudiwe et al., 2005).

GDT is based on two constructs (D'Arcy et al., 2009):

- Severity (PS) of sanctions refers to the degree of punishment associated with an individual committing a specific action.
- Certainty (PC) of sanctions refers to the probability of an individual facing punishment for committing a specific action.

Furthermore, this theory states that if punishment is severe and certain, an individual will balance the benefits and costs before committing any action that may result in punishment (Lebek et al., 2014; Onwudiwe et al., 2005). However, few studies have shown that deterrence has an effect on security behaviour. Herath and Rao (2009b) found that severity of punishment in organisations had no significant impact on security behaviour intentions to comply with information security policies. In addition, Foth (2016) noted that deterrence had no significant impact on intention to comply with security regulations within an organisation.

3.3.3.Protection Motivation Theory

Rogers developed protection motivation theory (PMT) in 1975 as an extension of the expectancy-value theory to provide a more understandable explanation of the effect of fear appeals on human attitudes and behaviours (Rogers, 1975). Moreover, PMT has been used for disease prevention and health promotion for several decades (Floyd et al., 2000).

Fear appeals are defined as ‘persuasive messages designed to scare people by describing the terrible things that will happen to them if they do not do what the message recommends’ (Witte, 1992, p.329). The earliest attempt to explain the effects of fear appeals in motivating individuals towards a desired behaviour was by Hovland et al. (1953) using the ‘fear-as-acquired-drive model’. This model suggests that fear drives individuals to adopt a specific behaviour to reduce or mitigate the fear. Nonetheless, according to Tunner et al. (1991), the intention of using fear appeals is not merely to make people frighten, but to motivate them to preform protective behaviours.

In addition, there has been a large amount of research in various areas using PMT in understanding people's behaviour actions when facing threats. This research involving protective behaviours has crossed different areas of research, such as prevention of heart disease (Plotnikoff and Higginbotham, 1998), food safety (Schafer et al., 1993), environmental hazards (Vaughn, 1993), and prevention of nuclear war (Axelrod and Newton, 1991). Floyd et al. (2000) state that PMT is one of the most powerful theories in predicting people's intentions to take proactive actions.

Based on the review of the PMT literature, Rogers (1975) identified two cognitive processes: threat appraisal and coping appraisal. Threat appraisal involves an individual's assessment of threats impact, the probability of threats occurring (likelihood), and the benefits of not taking a protective action. On the other hand, coping appraisal involves an individual's evaluation of his or her ability to respond to threats and the resources available for coping, as well as the cost of not taking a protective action. The threat appraisal involves two constructs:

- Vulnerability refers to the probability of a threat occurring if not taking a protective action.
- Severity refers to the potential impact and consequences of a threat occurring.

The coping appraisal involves two constructs:

- Response efficacy refers to an individual's belief that taking a protective action will mitigate a threat.
- Response cost refers to the costs (e.g. financial, personal) associated with the protective action.

PMT has been enhanced and extended over the years in a number of publications. In the most recent version of PMT, Maddux and Rogers (1983) extended the theory by adding self-efficacy and reward to the original theory, as a coping and threat appraisal respectively. According to Bandura (1992), self-efficacy is considered as an important influencing component in motivational and cognitive processes in behaviour theory.

- Self-efficacy refers to an individual's perceived ability to carry out a protective action.
- Reward refers to the physical or psychological pleasure of starting or continuing taking unsecure behaviour

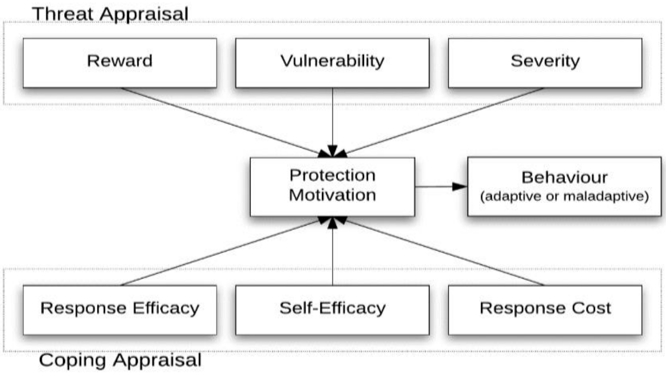


Figure 3.5: The protection motivation theory (PMT)

Rewards, in other words, may be understood when an individual faces a threat and the rewards (e.g. benefits of ignoring security procedures) of continuing or starting an unhealthy behaviour outweighs the risks associated to the threat, then the individual will not take a protective action.

3.3.4. Rational Choice Theory

Becker developed rational choice theory (RCT) in 1968 to examine an individual's criminal decision-making when faced with choices. The main purpose of the theory is to determine an individual’s action by the evaluating the costs and benefits of a specific action.

3.3.5.Social Cognitive Theory

Social cognitive theory (SCT) is a learning theory that is an extension of social learning theory (SLT). SCT is concerned with how the perception of individuals’ capabilities can affect their motivation and action and cause behavioural change (Bandura, 1977). SCT encompasses two key elements: locus of control (Rotter, 1966) and self-efficacy (Bandura, 1977). Locus of control refers to a generalised expectancy that predicts individuals’ behaviour across situations, depending on whether they view an outcome as controllable (internal) or controlled (external) in the first place (Rotter, 1966 cited in Workman et al., 2008). Self-efficacy refers to an individual’s belief to be able to perform a specific action.

3.3.6. Social Bond Theory

Hirschi proposed social bond theory (SBT), also called social control theory, in 1969. This theory describes the bounding ties that an individual has with his or her group. In addition, it has been used in many criminal behaviour studies (Cheng et al., 2013). The theory states that when individuals build bonds, their desire to yield to antisocial behaviours is reduced. Moreover, Hirschi identifies four key elements of social bond: attachment, commitment, involvement, and belief.

3.3.7. Neutralisation Theory

Sykes and Matza introduced neutralisation theory (NT) in 1957. NT states that people are aware of their moral obligations to abide the law and also aware of their moral obligations to avoid any criminal acts. In addition, the theory contains five main elements: denial of responsibility, denial of injury, denial of the victim, condemnation of the condemners, and appeal to higher loyalties. Nevertheless, other additional elements were added during the years (i.e. the metaphor of the ledger by Klockars (1974) and the defence of necessity by Minor (1981)).

3.3.8. Technology Threat Avoidance Theory

Liang and Xue (2009) argue that individuals' adoption and avoidance behaviours are qualitatively different; therefore, they have developed technology threat avoidance theory (TTAT) in order to understand and explain individuals' behaviour to avoid the threat of malicious IT. TTAT is a constant dynamic and positive feedback loop that aims to explain an individual's avoidance behaviour. This theory is based on PMT, and also draws on cybernetic and coping theory.

3.4. Cyber Security Behaviour Elements

According to Fishbein and Ajzen (2011) human behaviour is composed of four elements: an *action* to be performed; a *target* to be performed toward; a *context* to be performed within; and a specific *time* to be performed at. Based on the analysis of the systematic literature review, a concept map of was developed to visualise the elements of cyber security behaviour. The analysis of cyber security behaviours is built upon the basis of three human behavior elements: *action*, *target* and *context*. The fourth element of behaviour '*time*' was neglected for being irrelevant to the context of cyber security behaviour. Figure 3.6 visualises the cyber security behvaiour elements using concept mapping.

This visualisation provides a holistic overview of cyber security behvaiour elements, with an understanding of the cyber security actions performed, the assets targeted and the context that the behaviour is performed within. Additionally, Table 3.4 shows a concept matrix illustrating the cyber security behavior elements for the identified relevant literature of this study's systematic literature review.

The output of the literature analysis shows that eight theories identify cyber security behavioural intentions in regards to different security actions, assets and context as illustrated in Figure 3.6. Therefore, these theories are grouped together because they can identify cyber security behavioural intentions to take action on an asset within a specific context.

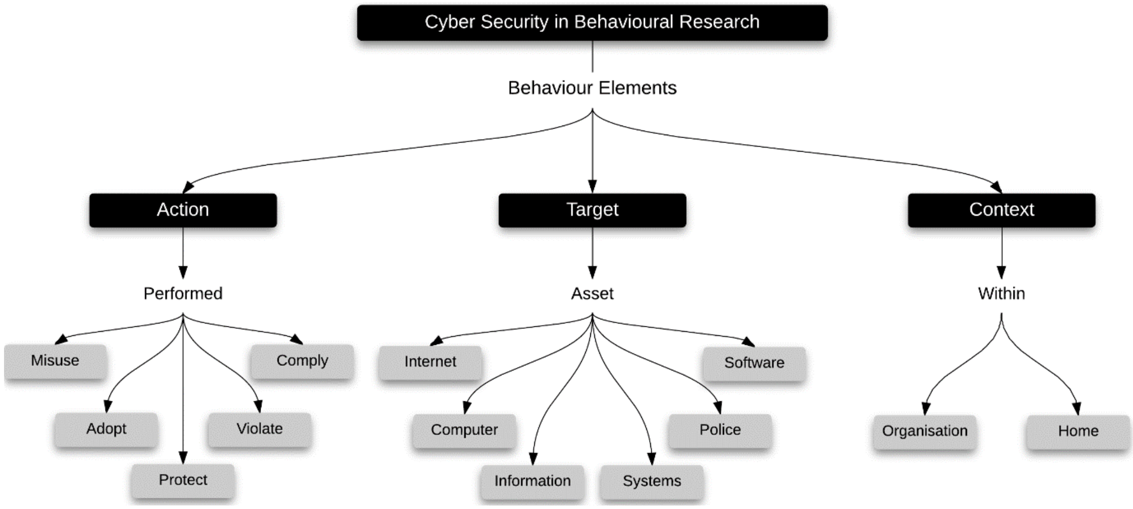


Figure 3.6: A concept map visualisation of cyber security behaviour elements

Table 3.4: A concept matrix illustrating the cyber security behaviour elements

		Behaviour Elements												
		Action					Target						Context	
Concept Study		Protect	Comply	Violate	Misuse	Adopt	Computer	Internet	Policy	Information	Systems	Software	Organisation	Home
1	Anderson & Agarwal (2010)	X					X	X						X
2	Chen & Zahedi (2016)	X					X						X	
3	Johnston & Warkentin (2010)					X						X	X	
4	Siponen & Vance (2010)			X					X				X	
5	Johnston et al. (2015)		X						X				X	
6	Boss et al. (2015)	X								X			X	
7	Bulgurcu et al. (2010)		X						X				X	
8	D'Arcy et al. (2009)				X						X		X	
9	Herath & Rao (2009)		X						X				X	
10	Foth (2016)		X						X				X	
11	Johnston et al. (2016)			X					X				X	
12	Lee & Larsen (2009)					X						X	X	
13	Posey et al. (2015)	X								X			X	
14	Hu et al. (2012)		X						X				X	
15	Herath & Rao (2009)		X						X				X	
16	Ifinedo (2014)		X						X				X	
17	Siponen et al. (2014)		X						X				X	
18	Vance et al. (2012)		X						X				X	
19	Hovav & D'Arcy (2012)				X					X		X	X	
20	Cheng et al. (2013)			X					X				X	
21	Dang-Pham & Pittayachawan (2015)	X								X				X
22	Ifinedo (2012)		X						X				X	
23	Safa et al. (2015)		X						X				X	
24	Tsai et al. (2016)	X					X							X
25	Al-Mukahal & Alshare (2015)			X					X				X	
26	Zhang et al. (2009)		X						X				X	
27	Sommestad et al. (2015)		X						X				X	
28	Hu et al. (2011)			X					X				X	
29	Gurung et al. (2009)					X						X	X	
Total		6	13	5	2	3	3	1	18	4	1	4	26	3

The term 'security behaviour' has been used very broadly in the literature. This analysis shows that there are a set of cyber security actions that are considered essential for security behaviours. These actions are illustrated in Figure 3.6 as misuse, violate, protect, comply and adopt actions.

However, only two studies involve information as a target for protection in an oragnisational context (Boss et al., 2015; Posey et al., 2015). Moreover, the study by Boss et al. (2015) was more a theoretical research focused on theory confirmation, rather than focusing on the security behavioural elements. This leaves us with only one study by Posey et al. (2015) that focuses on protection as a behavioural action to protect information in an organisation. This shows that there is a need for more research focusing on protecting information in general within organisations and more specifically protecting confidential information.

Table 3.4 shows that the research context included both work and home context. The studies that were in a home context were included in the literature review since they were identified during the literature review process.

3.5. Discussion

The systematic review highlights the most common behavioural theories used in the field of cyber security behaviour over the last decade. In addition, the review showed that there is a lack in research on cyber security behaviour focusing on the factors that affect individuals' behaviours and attempts to perform protective actions.

All of the theories reviewed in the literature have been integrated with one another to form a model for exploring the impact of cyber security behaviour. The vast majority of studies have used surveys as a data collection method of 89%, while only 11% of studies used field experiments.

The majority of studies focus on the security behaviour compliance of information security policies (ISP). On the other hand, only a few studies investigated security behaviour in regards to taking protective action by using or adopting security tools or methods. In addition, the human element in these studies depends on complying with the organisations' information security rules and policies.

However, in this section only the top three theories used will be discussed (i.e. PMT, TPB and GDT) as illustrated in Figure 3.7. These three theories were used in the majority (more than 85%) of the relevant studies obtained from the systematic literature review.

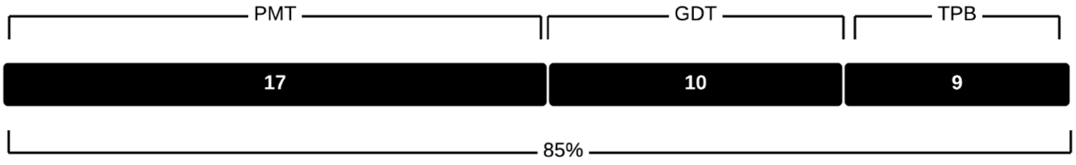


Figure 3.7: An illustration of the top three used theories in ISS behaviour

The systematic review showed that the most used theory in the field of security behaviour is that of protection motivation theory. This is because PMT is a motivational theory that explains the variables that underline decisions to carry out a protective behaviour against a specific threat. In addition, PMT differs from other theories due to the element of fear appeals that shows a significant effect on human behaviour and has been used in other disciplines especially in the field of health and criminology. Furthermore, PMT focuses on the factors that cause the motivation to protect a specific asset.

It has been noted that research results can be impacted by different targeted study subjects. For example, Larsen and Lee (2009) found in their study using PMT to understand the adoption of anti-malware software in SMEs, that IT experts are affected more by threat appraisal while non IT experts where affected by coping appraisal. This shows that people with different background and experience could have different intentions and behaviour in looking at security threats.

The theory of planned behaviour, on the other hand, focuses on explaining the relationship between attitude, intention and behaviour. Moreover, TPB indicates the individuals' behaviours are predicted the bases of attitudes, subjective norms and behavioural control. In addition, TPB has been widely used in the context of information security police compliance.

Additionally, subjective norms showed a high significance in most studies through social pressure on individuals' behaviours. This shows that social influence is an important aspect of motivating individuals and behaviour to perform protective security actions.

Deterrence theory has also been used widely in IS security studies, especially in the field of IS misuse and police violation research. This may be because the theory is rooted in criminology, and based on humans' view rational choice. In addition, GDT is built on the concept of deterrence and parchment to minimize IS misuse, abuse and security police violations. Therefore, this theory has been applied to the field of IS security using deterrent mechanisms to increase the perceived threat of punishment.

In summary, the three above discussed theories (i.e. PMT, TPB and GDT) are the most used theories in the cyber security behaviour domain for predicting human behaviour. Yet these theories differ in their core function where each theory has a specific focus.

- The protection motivation theory gives more understandable explanation of the effect of threat and copying appraisal on human intentions and how people balance cost and benefit in response of a threat and perform protective actions.
- The deterrence theory, on the other hand, is based on the concept of punishment and the assumption that employees are mandatorily expected to comply with organisational rules, policies and regulations.
- The theory of planned behaviour is a general theory that provides a general understanding of an individual's attitude to carry out a specific action in relation to the individual's intention to perform a specific behaviour.

3.6. Summary

The aim of this chapter has been to review the theories used in the field of cyber security behaviour, and identify the key applied theories in the context of cyber security. This was achieved by presenting a systematic literature review of the existing literature in cyber security behaviour. The systematic review identified 35 different theories that have been applied to 46 relevant studies in the field of cyber security behaviour. Nonetheless, only eight theories have been used more than twice in the relevant literature, and therefore have been included in the in the systematic analysis. Thus, the literature analysis produced a comprehensive overview of behavioural cyber security relevant literature (see Table 3.2). Additionally, a concept matrix approach was used to illustrate the theories based on a concept-centric approach (see Table 3.3).

Furthermore, 35 studies based on the main key theories (i.e. PMT, TPB and GDT) in the cyber security behaviour literature were systematically analysed to produce a concept map and matrix for cyber security behaviour elements (see Figure 3.6 and Table 3.4). A summary of findings from the systematic review analysis are as follows:

- The need for security behaviour has been recognised by the cyber security community as an important aspect of security; however previous work has focused on two main research streams: computer abuse/misuse and employees' information security policy compliance.
- The reviewed literature shows an increase in focus on protection motivation theory rather than GDT and TPB. This could be because deterrence is based on control and TPB is based on general behaviour whereas PMT is more based on evaluating the threat and the coping ability for performing a protective behaviour.
- The majority of studies in the domain of cyber security behaviour research focus on employees as target subjects.
- Most of the studies assume a stable organisational context, where there are policies and regulations that require employees to comply with as a mandatory work activity.
- Only a few studies took into consideration the effect of individuals' personality characteristics on security intentions and behaviour.
- Some studies have focused on specific security countermeasures or controls such as anti-malware software, e-mail authentication and data backup of critical data.

In conclusion, there has generally been a lack of theorising in cyber security behaviour in the context of trade secret protection. In addition, no single study discussed cyber security behaviour for trade secret protection. In addition, entrepreneurs are considered the fuel of the economy; however, there has been no attention given to entrepreneurs as study subjects and the factors that might have an impact on their cyber security behaviour. Therefore, there is a clear need for research to consider agile dynamic environments, where cyber security cannot be achieved through forcing compliance, and which require new ways of enhancing trade secrets protection during the venturing process.

Therefore, the findings of the systematic literature review in this chapter confirm that further research is required in new areas that consist of new behavioural elements in the field of cyber security behaviour. Moreover, by visualising the data analysis of the systematic literature review using concept mapping and a concept matrix approach, it is clear that this research aims to fill in a research gap and add valuable knowledge to the research field of cyber security behaviour.

Chapter 4

4. Conceptual Model and Hypotheses Development

4.1. Introduction

In the previous chapter, a systematic literature review was conducted using a structural approach for identifying and reviewing relevant literature in the field of cyber security behaviour. The aim of reviewing the latest cyber security behaviour literature is to identify the main behavioural theories applied in the cyber security behaviour domain, and to understand their applications in cyber security behaviour.

The review identified 46 relevant studies that used 35 theories from different research fields (e.g. criminology, sociology and psychology). Furthermore, the output of the literature review analysis identified eight behavioural theories that are recognised as the most dominant theories applied in the cyber security behaviour research domain. According to Saunders et al. (2009), understanding theories from other disciplines helps in the development of research conceptual models.

The objective of this chapter is to develop the research conceptual model and hypotheses. This starts by determining the research cyber security behavioural elements for trade secret protection. In addition, in this chapter the theoretical foundation of the conceptual model is introduced. This is achieved by defining the model constructs and the hypothetical relationships of the conceptualised research model. In the following chapters, the conceptual model is analysed to explore entrepreneurs' cyber security behaviours for trade secret protection.

4.2. The Research Behavioural Elements

The systematic literature review in Chapter 2 confirms that further research is required in new areas that consist of new behavioural elements in the field of cyber security behaviour. Therefore, based on the key research gaps of trade secret protection in the cyber security literature and the lack of cyber security behavioural elements for trade secret protection, this research explores new elements of behaviour for trade secret protection as illustrated in Figure 4.1.

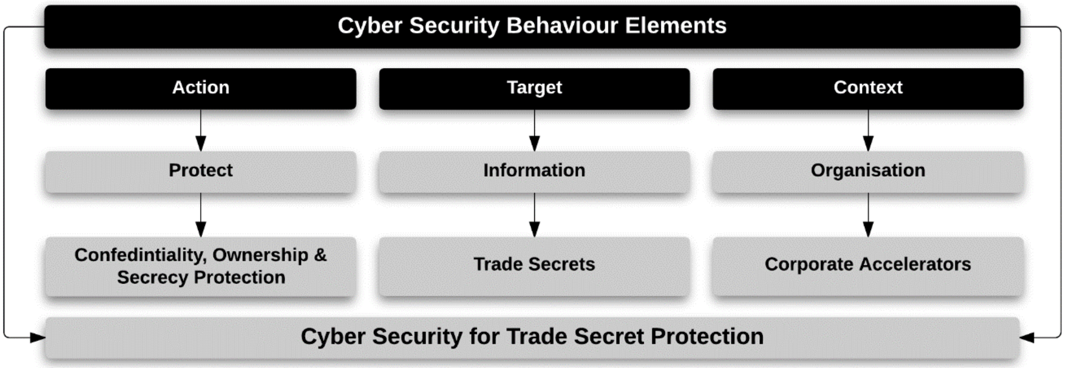

Cyber Security Behaviour Elements
Action
Target
Context
Protect
Information
Organisation
Confedintiality, Ownership & Secrecy Protection
Trade Secrets
Corporate Accelerators
Cyber Security for Trade Secret Protection

Figure 4.1: Cyber security behaviour elements for trade secret protection

Therefore, this research focuses on trade secret protection through the following cyber security behaviour elements:

- Action – The action is based on confidentiality, ownership and secrecy protection.
- Target – The target assets by the action behaviour are entrepreneurs' trade secrets.
- Context – The context of behaviour action is within agile dynamic environments.

This shows that the emphasis in this research is on new cyber security behavioural elements that aim to explore entrepreneurs' cyber security behaviour to perform protective actions toward trade secrets based on confidentiality protection of information; ownership protection of intellectual property and secrecy protection of commercial secrets. This action is within an agile dynamic environment (i.e. a corporate venturing unit) that is considered a new organisational context in cyber security behaviour research.

4.3. Conceptual Framework and Hypotheses Development

Figure 4.2 illustrates how the structured conceptualisation of the trade secret dimensions and protection aspects are mapped to the behavioural theories that are used as theoretical basis for the development of the research conceptual model. Additionally, this shows a theoretical explanation to support the logical existence of the cause and effect relationships developed in the research conceptual model below.

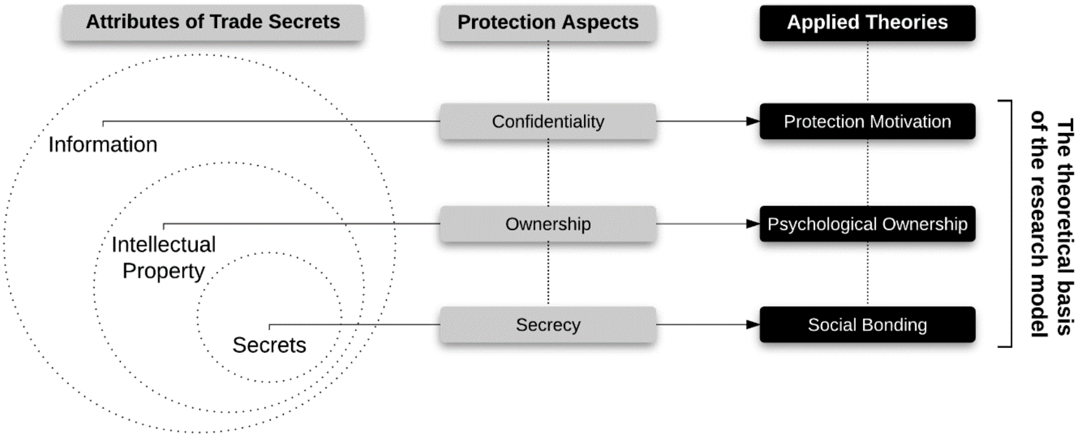


Figure 4.2: The conceptualisation of the theoretical basis of the research conceptual model

The mapping in Figure 4.2 shows how this research defines the theoretical formation of the research conceptual model for trade secret protection. Protection motivation is used as the core theoretical foundation for the development of this research's conceptual model. This involves the threat and coping appraisal to address confidentiality protection of trade secrets. Confidential information is defined by as "*information that is not publicly available and that confers a competitive advantage to the organizations that possess it*" (Burshtein, 2000, cited in Hannah and Robertson, 2015, p.382). Therefore, from a theoretical prospective of information, confidentiality is seen as an important aspect of protection. According to Floyd et al (2000), protection motivation is a powerful theory for predicting individuals' intentions to perform protective actions. In addition, it was clear from the systematic literature review in Chapter 3 that protection motivation is the most used theory in cyber security behaviour. Thus, protection motivation was used to develop the conceptual research model, so as to investigate entrepreneurs' cyber security behaviours towards confidentiality protection of trade secrets.

The second theory used in forming the research conceptual model, that of psychological ownership, aims to address ownership protection of trade secret. Pooley describes the ownership of intellectual information as the ability to protect information by preventing others from obtaining it while keeping it as a secret (2015, p.40). Moreover, from the theoretical prospective of intellectual property, ownership is also believed to be an important aspect of protection. Thus, psychological ownership was used in the development of the research conceptual model for investigating entrepreneurs' cyber security behaviour towards ownership protection of trade secrets.

Finally, social bonding theory was used to form the last part the conceptual model to address secrecy protection of trade secrets. A secret is defined as "*a piece of information that is intentionally withheld by one or more social actor(s) from one or more social actor(s)*" (Scheppele 1988, P.12). According to Vela-McConnell (2017) to maintain secrecy between a group of individuals within an organisation, strong social bonds are required. Therefore, from the theoretical perspective of prospective of secrets, secrecy is seen as an important aspect of protection. Thus, social bonding was used in the development of the research conceptual model for investigating entrepreneurs' cyber security behaviour towards secrecy protection of trade secrets.

The development of the conceptual model illustrated in Figure 4.3 was based on the foundation of the protective motivation theory, the social bond theory and the concept of psychological ownership. According to Hair et al. (2016a) research questions lead to the development of research hypotheses. Based on the research questions introduced in Chapter 1, the research hypotheses for this research were developed. Thus, the formulated conceptual model aims to answer the research questions by evaluating entrepreneurs' cyber security behavioural intentions to engage in protective cyber security actions, and hence protect trade secrets.

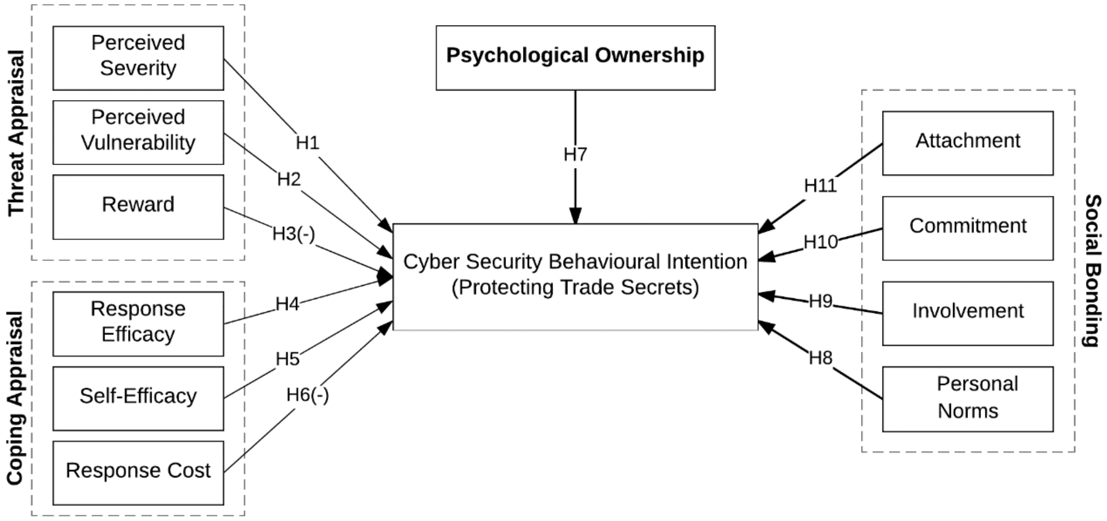


Figure 4.3: The developed research conceptual model

The research conceptual model incorporates 12 constructs that will be tested through 11 developed research hypotheses. Moreover, the model constructs and their relationships will be investigated through empirical data collection and multivariate analysis.

The aim of this model is to understand the drivers of entrepreneurs' intentions to perform cyber security behaviour. Although this research focuses on intentions rather than behaviour, this is because of the difficulties to assess actual behaviour in the security context (Anderson and Agarwal, 2010; Vroom and von Solms 2004). Moreover, previous research has shown that actual behaviour is determined by an individual's intention to perform that specific behaviour. (Ajzen and Fishbein, 2005).

According to Fishbein and Ajzen (2011), behavioural intentions are the most important direct determinant of behaviour. Behavioural intentions are defined as an individual's readiness to perform a specific behaviour (Fishbein and Ajzen, 2005). In the context of this research, cyber security behavioural intentions refer to the indications of an entrepreneur's readiness to perform a cyber security behaviour. Therefore, cyber security behavioural intention is incorporated in the research model to predict entrepreneurs' cyber security behaviours to perform protective security actions. The following sections of this chapter discuss the hypothesised relationships between the 11 model constructs (i.e. independent variables) and cyber security behavioural intention (i.e. dependent variable).

4.4. Hypothesis Development

4.4.1. Protection Motivation

According to Boss et al. (2015) threat and coping appraisal are the two key components of protection motivation that represent the foundation that forms protection intentions. In this research, the threat appraisal and coping appraisal are used in the formulated research conceptual model. Thus, in this section, the constructs of threat and coping appraisal are discussed, and the associate hypotheses are developed.

4.4.1.1. Threat Appraisal Constructs

Threat appraisal consists of three constructs: perceived severity, perceived vulnerability and reward. Perceived severity is defined as the potential impact and consequences of a threat occurrence. The severity of threat measures the perceived degree that an individual holds toward the significance of a security threat (Johnston & Warkentin, 2010). According to Workman et al. (2008) individuals will adjust their behaviour if they perceive high risk of threat. On the other hand, the opposite is true as well, namely that when individuals perceive lower risk of threat, they tend to behave in a less cautious manner.

Perceived severity is considered as one of the effective predictors of behavioural intention to perform security behaviours (Lee and Larsen, 2009; Dang-Pham and

Pittayachawan, 2015). In a security policy compliance context, Herath and Rao (2009a), found that perceived severity has a significant effect on employees' behavioural intentions to comply with information security policy. Thus, individuals' perceived severity tends to be associated with their behavioural intentions to perform security actions (Pechmann et al., 2003).

In the context of this research, an assumption is made that the entrepreneurs' perception of perceived severity of a threat will have a positive influence on their behavioural intention to protect trade secrets. Therefore, perceived severity is included in the research conceptual model as a direct determinant of cyber security behavioural intentions, and helps to predict intentions to take protective actions to protect trade secrets. Thus, the following hypothesis is formulated:

H1: Perceived severity will have a positive influence on entrepreneurs' cyber security behavioural intentions to protect trade secrets.

Vulnerability is defined as the probability of a threat occurring provided no protective security action is performed. The perception of vulnerability is associated with the likelihood of a threat occurring for not performing security actions. Thus, the likelihood of taking protective actions increases when an individual perceives high vulnerability of a threat incident (Lee and Larsen, 2009).

Lee and Larsen (2009) found that vulnerability has a significant influence on individuals' intentions to adopt security software. According to Siponen et al. (2014), the increase of perceived vulnerability has a significant impact on an individual's intention to behave in a cautious manner in regards to the compliance of information security policies.

In the context of this research, an assumption is formulated that the entrepreneurs' perception of the perceived vulnerability of a threat occurring will have a positive influence on their behavioural intention to protect trade secrets. Therefore, perceived vulnerability is included in the research conceptual model as a direct determinant of cyber security behavioural intentions and helps to predicting intentions to take protective actions to protect trade secrets. Thus, the following hypothesis is formulated:

H2: Perceived vulnerability will have a positive influence on entrepreneurs' cyber security behavioural intentions to protect trade secrets.

Reward is defined as the physical or psychological pleasure of starting or continuing to engage in secure behaviour. These benefits (i.e. rewards) can be perceived in different forms, as financial value, time saved or physical pleasure (Chou and Chou, 2016).

According to Boss et al (2016) an individual might decide to accept a threat and not perform any protective action if the rewards outweigh the threats. Moreover, high perceived rewards associated with threat appraisal might decrease the likelihood of performing protective actions (Lee and Larsen, 2009).

In the context of this research, rewards represent the realised benefits by entrepreneurs of not protecting trade secrets to gain more time or save efforts. Moreover, an assumption is formulated that entrepreneurs' positive perception of rewards increases the possibility of a threat occurrence.

Therefore, rewards are included in the research conceptual model as a direct determinant of cyber security behavioural intentions and help predict intentions to take protective actions to protect trade secrets. Thus, the following hypothesis is formulated:

H3: Rewards will have a negative influence on entrepreneurs' cyber security behavioural intentions to protect trade secrets.

4.4.1.2. Coping Appraisal Constructs

Coping appraisal consists of three constructs: response efficacy, self-efficacy and response costs. In the coping assessment, response efficacy is the belief that performing a protective cyber security action will be effective.

According to Johnston and Warkentin (2010), individuals' response efficacy plays a major role in behavioral intention. In addition, Gurung et al's (2009) research involving consumers' usage of security tools supported the positive impact of response efficacy on security behavioural intentions. This indicates that an individual with high response efficacy will perform a protective security behavioural intention.

In the context of this research, an assumption is made that entrepreneurs that have high confidence in the effectiveness of cyber security response, are more likely to perform a protective action. Moreover, an assumption is formulated that entrepreneurs' positive perception of response efficacy increases the possibility of a coping response.

Response efficacy is included in the research conceptual model as a positive direct determinant of cyber security behavioural intentions and helps to predict intentions to take protective actions to protect trade secrets. Thus, the following hypothesis is formulated:

H4 Response efficacy will have a positive influence on entrepreneurs' security behavioural intentions to protect trade secrets.

Self-efficacy was added to the original theory of protective motivation (Rogers, 1983; Maddux and Rogers, 1983) by adopting Bandura's (1977) social cognitive theory. Moreover, in a study related to security policy compliance, Herath and Rao (2009a) found that self-efficacy positively influenced behavioural intentions. Furthermore, self-efficacy has shown a significant impact on employees' intention to comply with information security policies (Siponen et al., 2014).

The influence of self-efficacy on security behaviour has been established empirically (Herath and Rao 2009; LaRose et al. 2008; Workman et al. 2008). Lee and Larson (2009) found that self-efficacy can influence an individual's security behaviour. Moreover, self-efficacy has shown to be a strong influence on behavioural intentions to perform protective security actions (Milne et al, 2000; Lee and Larson, 2009). Echoing the prior literature, this research also anticipates that self-efficacy will positively influence entrepreneurs' protection of trade secrets.

In the context of this research, an assumption is formulated that entrepreneurs with high confidence that they have the ability to conduct a cyber security action, are more likely to perform a protective action. Therefore, self-efficacy is included in the research conceptual model as a direct determinant of cyber security behavioural intentions, and aids in predicting intentions to take protective actions to protect trade secrets. Thus, the following hypothesis is formulated:

H5: Self-**efficacy will have a positive influence on entrepreneurs' security** behavioural intentions to protect trade secrets.

According to Floyd et al. (2000) individuals perceive response costs as any personal costs (e.g. money, effort or time) that are associated with performing protective actions. These costs involve the costs of using cyber security protections (Tsai et al., 2016). Posey et al. (2015) state that costs reduce the likelihood of an individual performing a response action.

Workman et al. (2008) argue that individuals could adjust their coping behaviour based on the costs of damage that results from a threat. Moreover, Herath and Rao (2009) found that response cost has a negative influence on security behaviour to comply with security policies. Therefore, based on previous literature, this research anticipates that response cost will negatively influence entrepreneurs' protection of trade secrets.

In the context of this research, an assumption is formulated that entrepreneurs that perceive high cost to conduct a cyber security action are more likely to have negative behavioural intentions towards the protection of trade secrets. Therefore, response cost is included in the research conceptual model as a direct determinant of cyber security behavioural intentions and helps to predict intentions to take protective actions to protect trade secrets. Thus, the following hypothesis is formulated:

H6: Response cost will have a negative influence on entrepreneurs' security behavioural intentions to protect trade secrets.

Six hypotheses have been formulated, based on threat appraisal and coping appraisal. An entrepreneur goes through the threat appraisal by assessing the severity, vulnerability and benefits of performing protective cyber security actions to protect trade secrets. This is followed by the entrepreneur's personal assessment of his/her ability to cope with a potential threat and perform protective cyber security actions to protect trade secrets. In essence, the core premise of the threat and coping appraisals is to investigate the significance of their constructs in impacting entrepreneurs' cyber security behavioural intentions to protect the confidentiality of trade secrets in corporate venturing environment.

4.4.2. Psychological Ownership Construct

According to Pierce et al. (2003) psychological ownership is the state when an individual feels that he/she owns an object and that it belongs to him or her. Moreover, the core of psychological ownership is based on possession (Van Dyne and Pierce, 2004). Furthermore, the sense of ownership can also be associated with nonphysical targets such as creative ideas (Isaacs, 1933, cited in Anderson and Agarwal, 2010, p.621). Additionally, Dawkins et al. (2017) state that targets of ownership could be tangible or intangible.

Moreover, Anderson and Agarwal (2010) argue that an individual seeks to protect an object that he/she owns and values. This clearly indicates that the psychological ownership of trade secrets that are owned and valued by an entrepreneur could be a target for protection.

Anderson and Agarwal (2010) investigate the impact of psychological ownership on computers and the Internet for home users in the context of security. The study showed that psychological ownership has a significant impact on home users' security behavioural intentions.

In the context of this research, it is anticipated that entrepreneurs who feel a strong sense of psychological ownership toward trade secrets will have a stronger behavioural intention to perform appropriate protective cyber security actions to protect these trade secrets. Moreover, an assumption is formulated that entrepreneurs' positive psychological ownership increases the possibility of a taking protective cyber security action.

Therefore, psychological ownership is included in the research conceptual model as a positive direct determinant of cyber security behavioural intentions, and helps to predict intentions to take protective actions to protect trade secrets. Thus, the following hypothesis is formulated:

H7: Psychological ownership of trade secrets will have a positive influence on **entrepreneurs' cyber security behavioural inten**tions to protect trade secrets.

4.4.3. Social Bonding Constructs

The theory of social bonding, also referred to as social control, was introduced by Hirschi (1969). Social bonding is a sociological concept that is considered as a type of social informal control that has been widely used in the field of criminology, but has been rarely used in the field of cyber security (Cheng et al., 2013).

Hirschi (1969) identified four bonding components that represent an individual's bond to a social action within a group: attachment, commitment, involvement and personal norms. The theory states that people with stronger social ties are less likely to engage in deviant behaviour. This can include any unaccepted behaviour that violates social or cultural norms.

The systematic literature review in Chapter 2 showed that social bonding has been used in cyber security behaviour studies regarding employees' police violation. For example, Ifinedo (2014) examined the impact of social bonding on information security compliance and found that the four components of bonding have influence employees' motivation to comply with information security policies. Moreover, Hirschi (1969) argues that an individual with a strong bond with a social group will more likely not violate the group rules. Therefore, since entrepreneurs within a team form a social group, social bonding is used as an informal social control to protect secrecy of commercial secrets within a venturing team.

Thus, in this research, the social bond theory is used in the formulated research conceptual model. In addition, in this section, constructs of the social bonding are discussed and the associate hypotheses are developed.

According to Cheng et al. (2013) people with strong attachment are less likely engage in unacceptable behaviour such as violation of security policies and perform a compliance action. Attachment in this research refers to the social attachment between an entrepreneur and his/her team members. Therefore, an entrepreneur with a strong attachment with his/her team will be more likely to perform a protective cyber security action to protect trade secrets. In contrast, an entrepreneur with weak attachments is assumed to be less protective to trade secrets and unconcerned with performing cyber security behaviour.

In the context of this research, it is anticipated that the stronger the attachment between an entrepreneur and his/her team members, the stronger the cyber security behavioural intention to perform appropriate protective cyber security actions to protect trade secrets.

H8: Attachment will have a positive effect on entrepreneurs' cyber security behavioural intentions to protect trade secrets.

According to Safa et al (2016), commitment in security involves the commitment to safeguard information assets in an organisation. Commitment in this research refers to an entrepreneur's responsibility and commitment to protect trade secrets. Therefore, an entrepreneur with a strong commitment will be more likely to perform a protective cyber security action to protect trade secrets. In contrast, an entrepreneur with weak commitment is assumed to be less protective to trade secrets and unconcerned with performing cyber security behaviour.

In the context of this research, it is anticipated that the stronger the commitment of an entrepreneur, the stronger the cyber security behavioural intention to perform appropriate protective cyber security actions to protect trade secrets.

H9: Commitment will have a positive effect on entrepreneurs' security behavioural intentions to protect trade secrets.

According to Ifinedo et al (2014), involvement is simply an individual's engagement and participation in an activity. Involvement in this research refers to an entrepreneur's engagement efforts with team members to protect trade secrets. Therefore, an entrepreneur with strong involvement with his/her team members will be more likely to perform a protective cyber security action to protect trade secrets. In contrast, an entrepreneur with weak involvement is assumed to be less protective to trade secrets, and unconcerned with performing cyber security behaviour.

In the context of this research, it is anticipated that the stronger the involvement of an entrepreneur, the stronger the cyber security behavioural intention to perform appropriate protective cyber security actions to protect trade secrets.

H10: Involvement will have a positive effect on entrepreneurs' security behavioural intentions to protect trade secrets.

According to Lee et al (2004) personal norms represent the moral element of behaviour that form an individual's beliefs. Personal norms in this research refer to an entrepreneur's values and views on trade secret protection. Therefore, an entrepreneur with high personal norms will be more likely to perform a protective cyber security action to protect trade secrets. In contrast, an entrepreneur with low personal norms is assumed to be less protective to trade secrets and unconcerned with performing cyber security behaviour.

In the context of this research, it is anticipated that the higher the personal norms of an entrepreneur, the stronger the cyber security behavioural intention to perform appropriate protective cyber security actions to protect trade secrets.

H11: Personal norms will have a positive effect on entrepreneurs' **security** behavioural intentions to protect trade secrets.

4.5. Summary

In this chapter, the research conceptual model was developed to explore entrepreneurs' cyber security behaviours for trade secret protection. The model builds upon previous behavioural theories from the literature. The structured model consists of 12 constructs from three theories: protective motivation, psychological ownership and social bonding. Based on the theses theories, the model constructs were defined and 11 research hypotheses were developed. Table 4.1 presents the model constructs and the research hypotheses. In the following chapters, multivariate analysis is used to assess the reliability and validity of the research conceptual model.

Table 4.1: The research hypotheses

Constructs	Hypotheses	Theory	Source
Perceived Severity	H1: Perceived severity will have a positive influence on entrepreneurs' security behavioural intentions to protect trade secrets.	Protection Motivation	Workman et al. (2008); Posey et al. (2015); Witte et al. (1996)
Perceived Vulnerability	H2: Perceived vulnerability will have a positive influence on entrepreneurs' security behavioural intentions to protect trade secrets.	Protection Motivation	Posey et al. (2015); Workman et al. (2008); Witte et al. (1996)
Reward	H3: Rewards will have a negative influence on entrepreneurs' security behavioural intentions to protect trade secrets.	Protection Motivation	Boss et al., 2015; Myyry et al., 2009; Dang-Pham & Pittayachawan (2015)
Response Efficacy	H4 Response efficacy will have a positive influence on entrepreneurs' security behavioural intentions to protect trade secrets.	Protection Motivation	Posey et al. (2015); Workman et al. (2008); Rippetoe and Rogers (1987); Milne et al.'s (2000)
Self-Efficacy	H5: Self-efficacy will have a positive influence on entrepreneurs' security behavioural intentions to protect trade secrets.	Protection Motivation	Posey et al. (2015); Workman et al. (2008)
Response Cost	H6: Response cost will have a negative influence on entrepreneurs' security behavioural intentions to protect trade secrets.	Protection Motivation	Boss et al., 2015; Woon et al., 2005
Psychological Ownership	H7: Psychological ownership of trade secrets will have a positive influence on entrepreneurs' security behavioural intentions to protect trade secrets.	Psychological Ownership	Dyne & Pierce, 2004; Anderson & Agarwal, 2010
Attachment	H8: Attachment will have a positive effect on entrepreneurs' security behavioural intentions to protect trade secrets.	Social Bonding	Ifinedo (2014); Lee et al. (2004)
Commitment	H9: Commitment will have a positive effect on entrepreneurs' security	Social Bonding	Ifinedo (2014); Herath & Rao (2009), Lee et al., (2004)

	behavioural intentions to protect trade secrets.		
Involvement	H10: Involvement will have a positive effect on entrepreneurs' security behavioural intentions to protect trade secrets.	Social Bonding	Ifinedo (2014); Lee et al. (2004)
Personal norms	H11: Personal norms will have a positive effect on entrepreneurs' security behavioural intentions to protect trade secrets.	Social Bonding	Ifinedo (2014); Li et al. (2010)

Chapter 5

5. Research Methodology

5.1. Introduction

In the previous chapter, the research conceptual model was developed based on established behavioural theories. Moreover, the formation reasoning of the conceptual model was explained and the model constructs were defined. In addition, a set of hypotheses were developed to describe and examine the cause-and-effect of relationships between the model constructs.

This chapter aims to introduce the research methodology used to conduct this research. Research methodology is defined as "*the systematic process of solving a research problem*" (Sahu, 2013, p.3). Therefore, this chapter introduces the research design including the process that results into answering the research questions. The research design encompasses the various steps followed in this research for data collection and analysis. The chapter starts with the research design justifying the chosen research philosophy and approach. In addition, the chapter discusses the sampling process and the development of the measurement instrument (i.e. questionnaire).

5.2. Research Design

According to Hair et al. (2016a) there are three types of research design: exploratory, descriptive or casual. An exploratory research design is usually used in studies that involve unclear research questions and lack available theories to support hypotheses development. A descriptive research design, on the other hand, describes the characteristics of a specific research topic. In contrast, the explanatory research design, also called causal research, tests the hypothesised cause-and-effect relationship between constructs (Zikmund, 2003).

This research adopted an exploratory and causal research design approach that aims to explore the research problem. This is based on the needs of the research to meet the research objectives and answer the research questions. The following sections describe the type of research philosophy and research method approach employed in this research design.

5.3. Research Paradigm

In the field of IS research different research methods and paradigms are used. Positivism is one of the most widely used research paradigms in IS research (Niehaves and Stahl. 2006). According to Gill and Johnson (2010) one of the main characteristics of positivist epistemology is that it tests theories that are hypothetic-deductive based.

It has been noticed that this type of approach has been used in the relevant literature reviewed in Chapter 2 (e.g. Anderson and Agarwal, (2010); Herath and Rao, (2009); Posey et al., (2015); Ifinedo, (2014); Safa et al., 2015). In addition, since this research aims to test a conceptual model based on hypothesized relationships, the research adopts a positivism approach.

5.4. Research Approach

There are two analytical reasoning approaches: inductive and deductive (Hair et al., 2016). The inductive reasoning involves a discovery approach that aims to develop a theory or conceptual framework from the collected data. Conversely, the deductive reasoning approach aims to develop a theory or conceptual framework and hypotheses before data collection and analysis. Moreover, Wilson (2014) states that a deductive approach is concerned with hypotheses development based on existing theories and testing these hypotheses. Figure 5.1 illustrates the inductive and deductive approach.

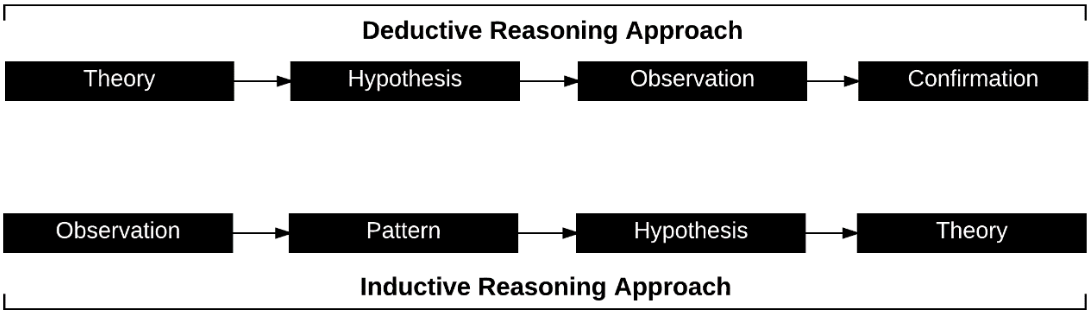


Figure 5.1: Deductive vs. inductive reasoning approach (Adopted from Trochim (2001))

Exploratory research design can adopt quantitative or qualitative methods (Hair et al., 2016a). However, in this research, the exploratory research design adopts a quantitative research method based on a deductive reasoning approach.Moreover, the exploratory research approach is also supported by findings of the systematic literature review analyse (Chapter 2) that showed that the majority of relevant studies (89%) used quantitative approach based on a survey instrument to support the research hypotheses testing. This shows that in the field of information security behaviour science, quantitative research is generally the main research approach. Therefore, the quantitative research approach for data collection adopted in this research is consistent with other research designs from similar studies in the literature of information security behaviour.

5.5. Sample

One of the main steps of a quantitative research approach is the sampling procedure. For the data to be collected and hypothesised relationships tested, a subset (i.e. sample) of a representative population is required. This sample is determined through a probability procedure that is usually used in quantitative research. According to Hair et al. (2016) the probability procedure consists of a sample selection of a representative sample from a specific population in a random procedure that guarantees the objectivity of the sampling data. On the other hand, nonprobability sampling is sampling procedure is based on the researcher's judgment to select an appropriate sample size. Thus, this type of sampling procedure lacks accuracy in regards to the generalisation of the research findings. Therefore, in this research, and based on the research needs, a nonprobability sample design is used to determine the sample size.

Hair et al. (2016a) defined a sampling process for obtaining representative samples. Figure 5.2 illustrates the sampling process used in this research.

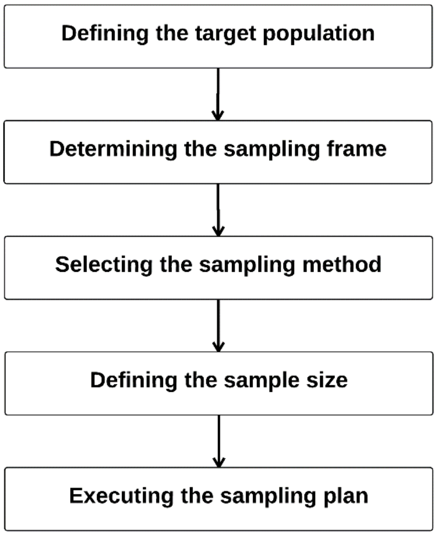

Defining the target population
Determining the sampling frame
Selecting the sampling method
Defining the sample size
Executing the sampling plan

Figure 5.2: The research sampling process

The research population is the first element in the sampling process that needs to be determined. In this research, the population consists of entrepreneurs starting their new ventures within a corporate accelerator in London. However, since there is no formal data available that shows the number of entrepreneurs in corporate venturing units (i.e. accelerators) in London, the population is determined based on a bigger population that consists of all entrepreneurs that are starting their new venture in London. The selection of this population ensures that the research sample size is accurate, and minimises the possibility of errors in the sampling process. Moreover, the choice of all entrepreneurs that started new ventures in London guarantees that the sample represents the population it is drawn from. According to a recent report by the Office for National Statistics (2016) the number of business births in London in 2015 totalled 101,000. The sample size (n=384) was determined using Krejcie and Morgan's (1970) table of sample sizes, specifying a five percent margin of error.

Since this is the only known number of entrepreneurs in London the research target sample was taken based on this, to determine the sample size. Figure 5.3 illustrates how the target population are entrepreneurs in corporate accelerators in London.

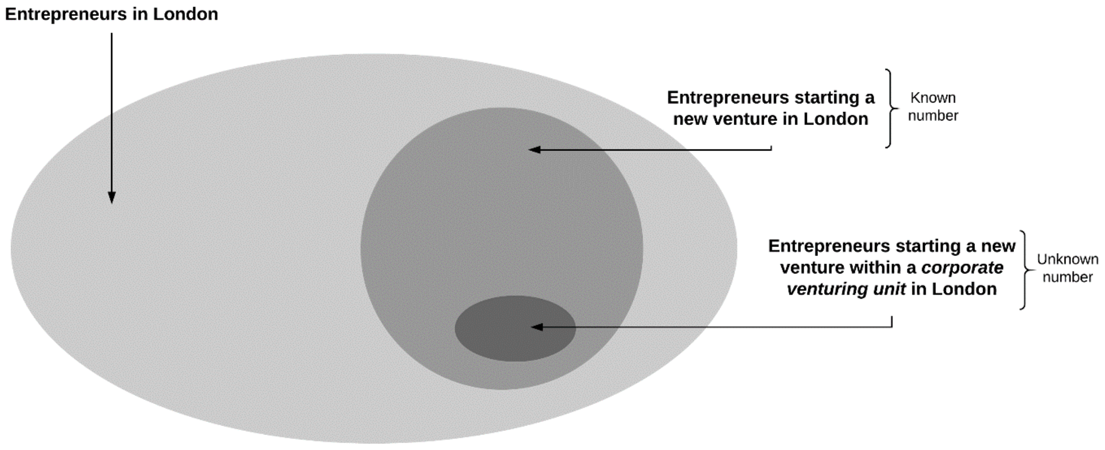

Entrepreneurs in London
Entrepreneurs starting a new venture in London
Known number
Entrepreneurs starting a new venture within a *corporate venturing unit* in London
Unknown number

Figure 5.3: The research population and target sample

Hair et al. defined the sampling frame as “a comprehensive list of the elements from which the sample is drawn.” (p.174, 2016a). The research determined sampling frame is based on a dataset of 24 accelerators in London. This data list of the corporate accelerators in London has been identified by the researcher based on different resources. These include journal articles, online databases and corporate reports.

The sampling method was based on a judgment design, with 24 corporate accelerators as the primary sampling unit targeting entrepreneurs within these accelerators. Non-probability sampling across accelerators was employed because the total population is distributed over several accelerators. This method was found to be the most appropriate because of difficulty to gain access a large number of corporates and because of the nature of the sensitivity of research topic to some corporates that involves cyber security and intellectual property.

According to a recent report by the Office for National Statistics (2016) the number of business births in London in 2015 totalled 101,000. The sample size (n=384) was determined using Krejcie and Morgan’s (1970) table of sample sizes, specifying a five percent margin of error. Moreover, Sommestad et al. (2015) state that a response rate of 30% is considered acceptable. The overall response rate in this research was 36% which is considered adequate.

In addition, in this research, the required sample size for the multivariate analysis technique has been met. This is based on Hair et al (2016b) recommendation that a sample size should exceed 100, and an ideal case would have 10 times the maximum number arrowheads pointing at a latent variable. The appropriate sample size for a multivariate analysis is calculated as follows:

10 * 11 (latent variable) = 110 (ideal sample size for a multivariate analysis)

The sampling plan to distribute the questionnaire started with an invitation email that was sent to the identified corporate accelerators, asking them to participate in the study by distributing the invitation email to entrepreneurs in their accelerator program. The email described the research aim and objectives and included the ethical approval.

In addition, definitions were included at the start of the questionnaire to clarify the meaning of important terms such as Trade Secrets, Cyber Security Threats and Protective Cyber Security Actions. Moreover, examples of some trade secrets and security threats were listed to minimize any ambiguity of these terms within the questionnaire.

According to Mesly (2015) to obtain a reprehensive sample, there are three criteria that need to be met. The sample should be random, representative and meet the minimum number for the analysis method. The sample for this research is random, because emails were sent to all accelerators; the sample is representative, because only specific subjects (i.e. entrepreneurs in corporate accelerators) were targeted. Finally, the number of participants is above the minimum number required by the analysis method used in this research (i.e. PLS-SEM).

5.6. Instrument Development

Selecting the appropriate research design depends on the research questions. In this research, the questions address cause-and-effect relationships; therefore, a research instrument is developed on this basis to collect the research data.

All the construct measures were adopted from previous research in the field of cyber security behaviour (Table 5.1). In addition, appropriate modification has been made to ensure that the items are relevant to the research context. Moreover, the designed survey instrument used a seven-point Likert scale, ranging from 1 (strongly disagree) to 7 (strongly agree), to indicate the level of agreement for each single statement. Figure 5.4 illustrates the research measurement that is based on a matric scale to capture participants' opinions and the level of agreement and disagreement. Moreover, the use of a minimum scale of a seven-point Likert scale is recommended by Hair et al (2016a) when adopting an established measurement scale.

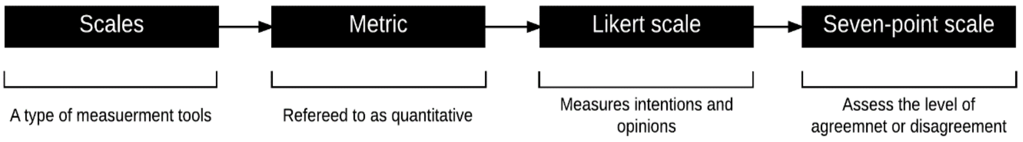

Scales
Metric
Likert scale
Seven-point scale
A type of measuerment tools
Refereed to as quantitative
Measures intentions and opinions
Assess the level of agreemnet or disagreement

Figure 5.4: The research measurement scale

Table 5.1: The research instruments

	Constructs	Code	Items	Source
1	Psychological Ownership	POC1.	This is my venture and my trade secrets.	Dyne & Pierce, 2004; Anderson & Agarwal, 2010
		POC2.	I feel a high degree of personal ownership for my venture's trade secrets.	
		POC3.	I sense that these are my trade secrets.	

2	**Reward**	REW1	Not performing protective cyber security actions toward trade secrets saves me time.	Boss et al., 2015; Myyry et al., 2009
		REW2	Not performing protective cyber security actions toward trade secrets saves me money.	
		REW3	Not performing protective cyber security actions toward trade secrets keeps me from being confused.	
		REW4	Not performing protective cyber security actions toward trade secrets requires less effort of me.	Dang-Pham & Pittayachawan (2015)
		REW5	Not performing protective cyber security actions toward trade secrets makes me feel less stressful.	
3	**Vulnerability**	VUL1.	My venture's trade secrets are vulnerable to cyber security threats.	Posey et al. (2015); Workman et al. (2008)
		VUL2.	It is likely that a cyber security attacks will occur against my venture's trade secrets.	
		VUL3.	My venture's trade secrets are at risk to cyber security threats.	Posey et al. (2015); Witte et al. (1996)
		VUL4.	My venture's trade secrets are defenceless against cyber security threats.	

4	**Severity**	SEV1.	Cyber threats to the security of my venture's trade secrets are severe.	Workman et al. (2008); Posey et al. (2015)
		SEV2.	In terms of cyber threats, attacks on my venture's trade secrets are severe.	
		SEV3.	I believe that cyber threats to the security of my venture's trade secrets are serious.	Witte et al. (1996); Posey et al. (2015)
		SEV4.	I believe that cyber threats to the security of my venture's trade secrets are significant.	
5	**Response Efficacy**	REF1.	Efforts to keep my venture's trade secrets safe from cyber threats are effective.	Posey et al. (2015); Workman et al. (2008); Rippetoe and Rogers (1987); Milne et al.'s (2000)
		REF2.	The available measures that can be taken to protect my venture's trade secrets from security threats are effective.	
		REF3.	The preventive measures available to me to stop people from getting my venture's trade secrets are adequate.	
		REF4.	If I perform the preventive cyber security measures available to me, my venture's trade secrets are less likely to be exposed to a cyber threat.	

6	Self-Efficacy	SEF1.	For me, taking cyber security precautions to protect my venture's trade secrets is easy.	Posey et al. (2015); Workman et al. (2008)
		SEF2.	I have the necessary skills to protect my venture's trade secrets from cyber threats.	
		SEF3.	My skills in stopping cyber threats against my venture's trade secrets are adequate.	
7	Response Cost	COS1.	The benefits of performing protective cyber security actions toward my venture's trade secrets outweigh the costs (R).	Boss et al., 2015; Woon et al., 2005
		COS2.	I would be discouraged from performing protective cyber security actions toward my venture's trade secrets in the future because it would take too much time.	
		COS3.	The time taken to perform protective cyber security actions toward my venture's trade secrets in the future would cause me too many problems.	
		COS4.	Taking protective cyber security actions would require considerable investment of effort as well as time.	

8	Behavioural Intentions	INT1.	I am likely to take protective cyber security action to protect my venture’s trade secrets.	Anderson & Agarwal, 2010; Taylor & Todd 1995
		INT2.	It is possible that I will take protective cyber security action to protect my venture’s trade secrets.	
		INT3.	I am certain that I will take protective cyber security action to protect my venture’s trade secrets.	
9	Attachment	ATC1.	I usually have conversations about the protection of my venture’s trade secrets with team members.	Ifinedo (2014); Lee et al. (2004)
		ATC2.	I respect my team members’ views and opinions about the protection of our venture’s trade secrets.	
		ATC3.	I communicate the importance of protecting the venture’s trade secrets to team members.	
10	Commitment	CMT1	I strongly believe that the protection of my venture’s trade secrets can help the venture to succeed.	Ifinedo (2014); Herath & Rao (2009), Lee et al., (2004)
		CMT2	I am committed to protecting my venture 's trade secrets.	

		CMT3	I am willing to invest energy and effort in making the protection of my venture's trade secrets a success.	
		CMT4	I am willing to put in a great deal of effort to help my venture succeed.	
11	Involvement	IVT1.	I value the opportunity to participate in informal meetings related to my venture's information security.	Ifinedo (2014); Lee et al. (2004)
		IVT2.	I work on building personal relationships with team members in my venture in relation to trade secret concerns.	
		IVT3.	I actively involve myself in activities related to my venture's growth.	
12	Personal norms	PEO1.	It is a serious matter if I don't perform the protective cyber security actions to protect my venture's trade secrets.	Ifinedo (2014); Li et al. (2010)
		PEO2.	It is unacceptable not to perform ALL the protective cyber security actions to protect my venture's trade secrets.	
		PEO3.	To me, performing the protective cyber security actions to protect my	

			venture's trade secrets is NOT a trivial offence.	
		PEO4.	To me, it is unacceptable to ignore the protection of my venture's trade secrets.	

When developing a measurement scale, it is important to reduce the measurement error of the research instrument. According to Hair et al. (2014), validity and reliability are the two main aspects of a measurement scale that need to be addressed. Therefore, reliability and validity will be evaluated in the later part of this research.

5.7. Pre-Test

The questionnaire was pre-tested by five researchers from different fields that have previous experience in conducting quantitative based research. The aim of the pre-test is to assess the clarity and wording of the survey instrument. The feedback received has been used to improve the survey instrument design.

5.8. Pilot Study

A pilot study aims to investigate internal consistency of the constructs' measures (i.e. reliability). Reliability refers to the ability to generate the same output of results as other researchers when using the same analysis (Saunders et al., 2012). Cronbach's alpha (α) coefficient (Cronbach, 1951) is a well-known reliability analysis for determining the consistency of measures. In addition, the values of Cronbach's alpha ranges from 0 to 1.0, where above the cut-off point of 0.7 is considered acceptable (Kline, 1999; Field, 2009).

The pilot study was conducted to evaluate the reliability of the measurement scale for the developed research model. In the pilot study, 30 postgraduate students studying MSc in Innovation and Entrepreneurship at the University of Warwick participated in the study. The reliability of the questionnaire instrument was analysed using SPSS software.

The pilot data set screening showed missing data and clear patterned responses for unengaged respondents. Therefore, these inefficient responses were excluded and only twenty completed responses were used in the pilot study. The students sample was considered suitable for this research because the students represented an appropriate group of entrepreneurs who had previous experience of establishing their own business.

Concepts (i.e. constructs) in this research are measured through multi-item scales that consist of multiple items. The internal consistency reliability of the constructs were assessed using Cronbach's alpha, also known as coefficient alpha. Moreover, the range of the alpha coefficient ranges from zero to one. It is generally suggested that an alpha higher than 0.7 represents a good alpha value (Nunnally, 1978).

Table 5.2: Cronbach's alpha reliability analysis results

Construct	Cronbach's Alpha
Psychological Ownership	0.903
Reward	0.899

Vulnerability	0.816
Severity	0.933
Response Efficacy	0.756
Self-Efficacy	0.762
Response Cost	0.645
Behavioural Intentions	0.949
Attachment	0.867
Commitment	0.932
Involvement	0.866
Personal norms	0.925

All the constructs showed an acceptable level of internal consistency through reliability measures exceeding the 0.7 threshold, except for that of response cost. Cronbach's alpha value for response cost is 0.645 which is above the point of 0.6. Although some researchers may consider 0.6 a low alpha, it is still acceptable for construct with small number of items (e.g. three and four items) (Hair et al., 2016a; Hair et al., 2014). However, the item-to-total correlation for COS1 is 0.173, below the 0.3 cut-off recommended by Field (2009).

The COS1 low reliability could be because of the item's negative wordings. According to Hair et al (2016a), when "negative wordings" items fail to capture a consistent response, then they should be removed from the scale. Therefore, a decision was made to remove COS1, and this resulted in increasing the response cost value to 0.737.

Finally, based on the reliability analysis of Cronbach's alpha, and after deleting the response cost item (i.e. COS1) all the constructs exceeded the 0.7 threshold, which shows an acceptable level of internal consistency. Therefore, this ensures that the measurement scale for the developed conceptual model presents reliable measurements for this researcher.

5.9. Summary

The goal of this chapter was to report on the design of the research methodology, which sought to achieve the research objectives and answer the research questions. The chapter started by determining the research approach and methods. Research approaches were then discussed, and an exploratory and causal research design approach was adopted based on a hypothetic-deductive logic.

This approach is consistent with previous research in the cyber security behaviour field. This involved a questionnaire based data collection method. In addition, a sampling process was used to determine the research target sample. In addition, the research instrument was developed based on previous established measurement scales, and reliability was also tested to ensure internal consistency.

The following chapters will focus on the analysis part of this research. The analysis includes descriptive and multivariate analysis of the collected empirical data.

Chapter 6

6. Data Preparation

6.1. Introduction

Based on the research methodology in Chapter 4, an online questionnaire was distributed to participants in 24 corporate accelerators in London. The target sample was 384, and 140 responses were obtained for a response rate of 36%.

In this chapter, the captured demographic characteristic from the collected data is presented. In addition, descriptive analysis is used to understand the data through frequency distribution examination. These are illustrated using graphics and charts to describe more easily the descriptive statistics and demographic information.

In addition, this chapter aims to examine the collected data as an essential step for any multivariate analysis (Hair et al., 2014). This aims to prepare the data for analysis by identifying any issues related to the collected empirical data, such as missing data, outliers and data distribution. Furthermore, the chapter includes a validity analysis through an Exploratory Factor Analysis (EFA) using SPSS. Finally, a final step for data examination is testing the assumptions of multivariate analysis and assessing the threat of common method bias.

6.2. Demographic Characteristics

The target sample of this research is entrepreneurs establishing their new ventures within corporate accelerators. Only entrepreneurs within corporate accelerators in

London participated in this research. However, since non-probability sampling method was used, the results cannot be considered representative of the total population. Nevertheless, the participants' demographic information was captured such as gender, age, education level and experience. In this section, the demographic characteristics of respondents' is illustrated in the following figures.

6.2.1. Gender

In terms of gender as a demographic characteristic in this research, the highest number of respondents were male entrepreneurs, at 67%, compared to female entrepreneurs at 33% (see Figure 6.1). This shows that about two-third of the respondents were male entrepreneurs.

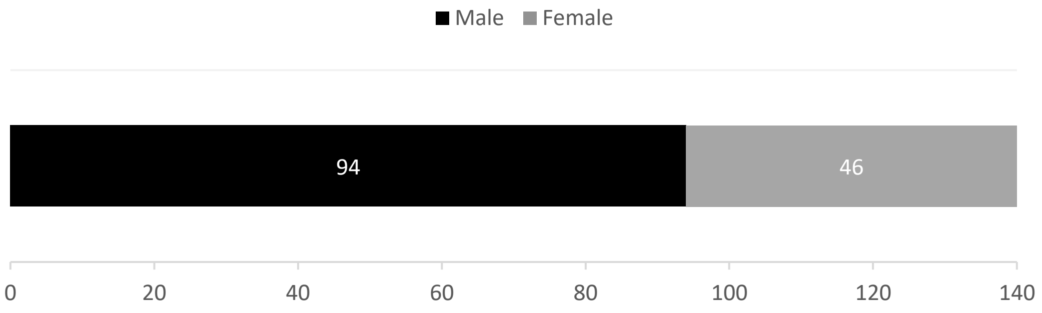


Figure 6.1: Demographic characteristic - Gender

6.2.2. Age

In terms of age, respondents' ages ranged from 18 to 49 years old, 76% of whom were aged between 18 to 29. Moreover, 23% are considered middle age ranging from 30 to 39 years old. Figure 6.2 illustrates respondents' different age groups.

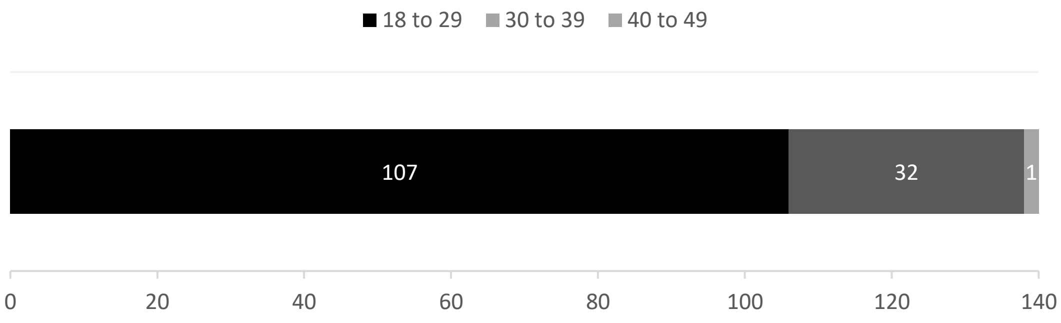


Figure 6.2: Demographic characteristic – Age

6.2.3. Education

The majority of respondents, about 93%, had obtained only a bachelor degree. Moreover, only 6% hold a master degree and only one respondent with a doctorate degree. Figure 6.3 illustrates the number of respondent in different education levels.

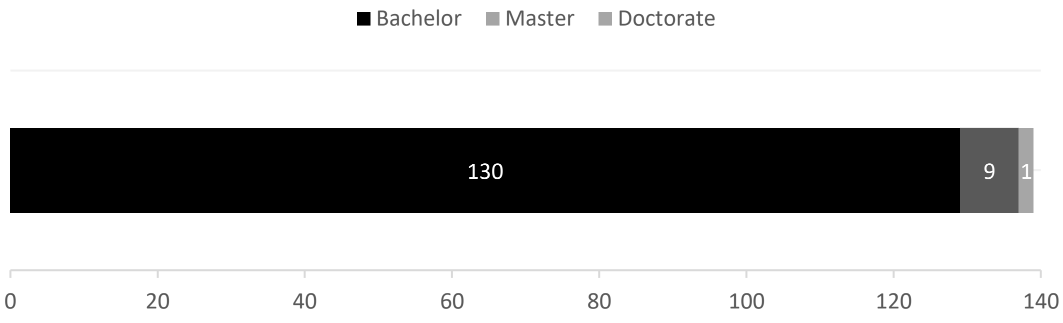


Figure 6.3: Demographic characteristic – Education

6.2.4. Venturing Experience

In terms of experience in establishing new ventures, most of the respondents had less than six months of experience. The results also show that 74% respondents have less than one year of experience is starting a new venture. Figure 6.4 illustrates the different years of experience in venturing for respondents in this research.

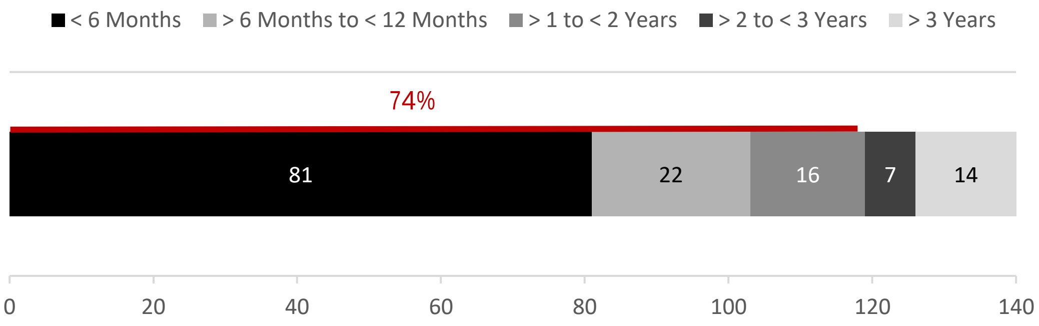


Figure 6.4: Demographic characteristic – Venturing experience

6.2.5. Number of Established Ventures

The number of ventures established by respondents was also captured via the questionnaire. The results show that more than 80% of respondents are establishing their first venture within a corporate accelerator. Figure 6.5 illustrates the number of established ventures by respondents in this research.

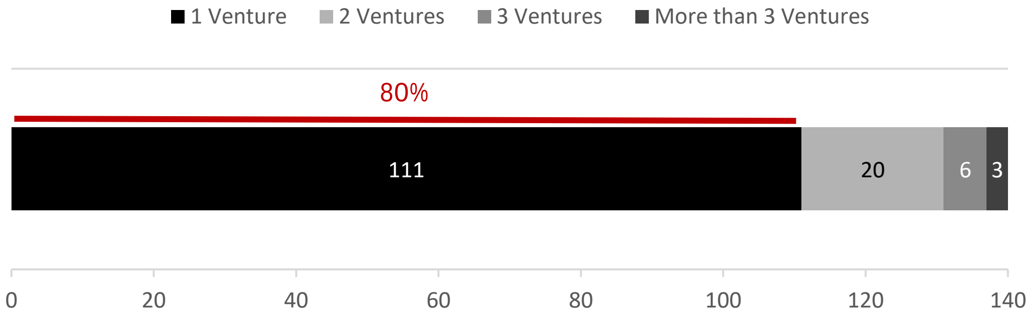


Figure 6.5: Demographic characteristic – Number of established ventures

6.3. Descriptive Statistics

Descriptive statistics are a quantitative analysis approach that helps to understand the collected data. The descriptive statistics for the constructs of this research consist of mean (i.e. arithmetic average) and standard deviation. Table 6.1 shows the descriptive statistics of this research.

Table 6.1: Descriptive statistics

	Constructs	Code	Items	Mean	S.D.
1	Psychological Ownership	POC1.	This is my venture and my trade secrets.	5.85	1.18
		POC2.	I feel a high degree of personal ownership for my venture's trade secrets.	5.99	1.02
		POC3.	I sense that these are my trade secrets.	5.82	1.04
2	Reward	REW1.	Not performing protective cyber security actions toward trade secrets saves me time.	3.30	1.69
		REW2.	Not performing protective cyber security actions toward trade secrets saves me money.	3.36	1.79
		REW3.	Not performing protective cyber security actions toward trade secrets keeps me from being confused.	3.20	1.54
		REW4.	Not performing protective cyber security actions toward trade secrets requires less effort of me.	3.83	1.80
		REW5.	Not performing protective cyber security actions toward trade secrets makes me feel less stressful.	3.07	1.61
3	Vulnerability	VUL1.	My venture's trade secrets are vulnerable to cyber security threats.	4.99	1.41
		VUL2.	It is likely that a cyber security attacks will occur against my venture's trade secrets.	4.99	1.32
		VUL3.	My venture's trade secrets are at risk to cyber security threats.	4.73	1.44
		VUL4.	My venture's trade secrets are defenceless against cyber security threats.	3.86	1.47
4	Severity	SEV1.	Cyber threats to the security of my venture's trade secrets are severe.	4.49	1.61
		SEV2.	In terms of cyber threats, attacks on my venture's trade secrets are severe.	4.68	1.52
		SEV3.	I believe that cyber threats to the security of my venture's trade secrets are serious.	4.92	1.59
		SEV4.	I believe that cyber threats to the security of my venture's trade secrets are significant.	4.95	1.50
5	Response Efficacy	REF1.	Efforts to keep my venture's trade secrets safe from cyber threats are effective.	5.14	1.10

		REF2.	The available measures that can be taken to protect my venture's trade secrets from security threats are effective.	5.05	1.09
		REF3.	The preventive measures available to me to stop people from getting my venture's trade secrets are adequate.	4.72	1.22
		REF4.	If I perform the preventive cyber security measures available to me, my venture's trade secrets are less likely to be exposed to a cyber threat.	5.17	1.31
6	Self-Efficacy	SEF1.	For me, taking cyber security precautions to protect my venture's trade secrets is easy.	3.74	1.45
		SEF2.	I have the necessary skills to protect my venture's trade secrets from cyber threats.	3.69	1.63
		SEF3.	My skills in stopping cyber threats against my venture's trade secrets are adequate.	3.67	1.51
7	Response Cost	COS2.	I would be discouraged from performing protective cyber security actions toward my venture's trade secrets in the future because it would take too much time.	3.33	1.58
		COS3.	The time taken to perform protective cyber security actions toward my venture's trade secrets in the future would cause me too many problems.	3.22	1.40
		COS4.	Taking protective cyber security actions would require considerable investment of effort as well as time.	5.15	1.30
8	Behavioural Intentions	INT1.	I am likely to take protective cyber security action to protect my venture's trade secrets.	5.76	0.97
		INT2.	It is possible that I will take protective cyber security action to protect my venture's trade secrets.	5.94	0.91
		INT3.	I am certain that I will take protective cyber security action to protect my venture's trade secrets.	5.63	1.22
9	Attachment	ATC1.	I usually have conversations about the protection of my venture's trade secrets with team members.	4.67	1.50
		ATC2.	I respect my team members' views and opinions about the protection of our venture's trade secrets.	5.59	1.05
		ATC3.	I communicate the importance of protecting the venture's trade secrets to team members.	5.49	1.38

10	Commitment	CMT1.	I strongly believe that the protection of my venture’s trade secrets can help the venture to succeed.	5.63	1.19
		CMT2.	I am committed to protecting my venture 's trade secrets.	5.81	0.98
		CMT3.	I am willing to invest energy and effort in making the protection of my venture’s trade secrets a success.	5.75	0.98
		CMT4.	I am willing to put in a great deal of effort to help my venture succeed.	6.20	0.92
11	Involvement	IVT1.	I value the opportunity to participate in informal meetings related to my venture’s information security.	5.33	1.14
		IVT2.	I work on building personal relationships with team members in my venture in relation to trade secret concerns.	5.55	1.07
		IVT3.	I actively involve myself in activities related to my venture’s growth.	6.15	0.845
12	Personal Norms	PEO1.	It is a serious matter if I don’t perform the protective cyber security actions to protect my venture’s trade secrets.	5.38	1.26
		PEO2.	It is unacceptable not to perform ALL the protective cyber security actions to protect my venture’s trade secrets.	4.80	1.47
		PEO3.	To me, performing the protective cyber security actions to protect my venture’s trade secrets is NOT a trivial offence.	4.83	1.22
		PEO4.	To me, it is unacceptable to ignore the protection of my venture’s trade secrets.	5.52	1.21

6.4. Data Preparation

Data examination is an initial step before any data analysis to ensure that the results obtained from the multivariate analysis are valid and reliable (Hair et al., 2014). This involves the evaluation of the collected set of data before conducting the main data analysis. The data preparation aims to clean the dataset to be suitable for the multivariate analysis. This data preparation testing involves missing data identification, suspicious response patterns and outlier detection (see Figure 6.6).

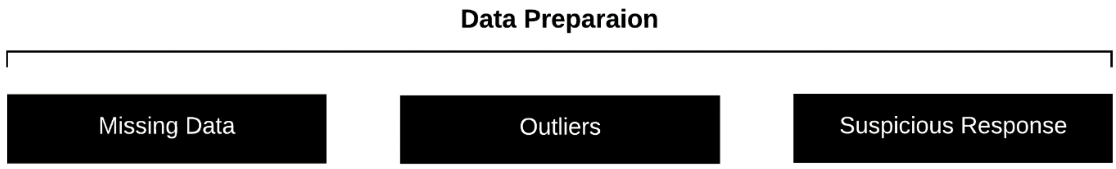


Figure 6.6: Data Preparation

6.4.1. Missing data

In this study, the distributed questionnaire required respondents to answer all questions to ensure no missing data issues. However, the data set was screened for missing data and no missing data were identified. Thus, no issues of missing data were reported.

6.4.2. Suspicious Responses

The data set was also examined for any suspicious responses that show unengaged respondents during the activity of answering the questionnaire. The examination identified two cases that showed clear unengaged response. The first case showed a patterned response and the second case had a zero-standard deviation. Therefore, these two cases were removed from the data set.

6.4.3. Detecting Outliers

An outlier is "a respondent (observation) that has one or more values that are distinctly different from the values of other respondents" (Hair et al., 2016a). The detection and evaluation of outliers in multivariate analysis is vital to be able to take a retention or deletion decision (Hire et al., 2014).

In this research, an investigation was conducted to identify outliers in the dataset. Moreover, the Median Absolute Deviation (MAD) as a univariate detection method was used to identify outliers. According to Hire et al (2014), univariate detection "examine all metric variables to identify unique or extreme observations" (Hire et al., 2014, p.65). Moreover, since the research sample size is considered small, MAD was used for its robustness and immunity to sample size (Leys et al., 2013). Three threshold values (2, 2.5 or 3) are usually used for detecting outlying values in univariate statistics. Based on Leys et al (2013) recommendation, this research will use a ± 2.5 as a moderately conservative value.

The univariate detection resulted in identifying 18 cases as potential outliers that exceed the threshold of ±2.5 on more than one item. According to Hair et al (2014) after the outliers have been identified in the dataset a decision to retain or delete them. This is achieved by examining the difference between an item's mean value and the 5% trimmed mean value to identify whether the outliers could affect the remaining part of the analysis. According to Pallant (2010), if the mean value of a variable and the 5% trimmed mean value involved a huge difference, this shows an associated influence of the outlier. Therefore, a comparison between the items' means and trimmed means has been made, and they did not show any huge differences (See Appendix B). This shows that the detected outliers have no significant influence on the dataset and therefore a decision was made to retain them. Finally, this concludes the data examination and preparation part.

6.5. Testing the Assumptions of Multivariate Analysis

Before multivariate data can be used for analysis, several assumptions underlying multivariate analysis should be examined. In this section, statistical assumptions recommended by Hair et al. (2014) were examined. However, a multicollinearity test was not appropriate in this multivariate analysis, since all items are reflective items (i.e. interchangeable items) and collinearity (i.e. high correlation between multiple items) is related to formative items (Hair et al., 2016b).

6.6. Normality

Normality refers to “the shape of the data distribution for an individual metric variable and its correspondence to the normal distribution“ (Hair et al., 2014, p.69). Although PLS-SEM does not require the data to be normally distributed, it should not be extremely nonnormal (Hire et al., 2016b). The data distribution has been examined using two measures: Skewness and Kurtosis. Moreover, the data have been examined in this study using the SPSS software.

Skewness measures the balance of the distributed data; if the distribution of data is stretched toward the right or left tail. Kurtosis, on the other hand, measures the peakedness of the distributed data; if the distribution of data is narrow in the center or flat. Table 6.2 illustrates the normality analysis of the skewness and kurtosis measures for the constructs items’.

Table 6.2: Skewness and Kurtosis Tests

Items	Skewness	Kurtosis
POC1	-1.312	1.966
POC2	-1.332	3.192
POC3	-0.903	0.495
REW1	0.319	-1.053
REW2	0.308	-1.098
REW3	0.345	-0.797
REW4	0.034	-1.195
REW5	0.472	-0.828
VUL1	-0.919	0.411
VUL2	-0.970	0.826

VUL3	-0.721	-0.108
VUL4	0.116	-0.601
SEV1	-0.520	-0.597
SEV2	-0.765	-0.288
SEV3	-0.932	0.072
SEV4	-0.727	-0.187
REF1	-0.570	0.596
REF2	-0.608	0.124
REF3	-0.407	-0.628
REF4	-1.025	1.031
SEF1	0.393	-0.921
SEF2	0.311	-1.001
SEF3	0.249	-0.911
COS2	0.505	-0.749
COS3	0.314	-0.607
COS4	-1.338	1.766
INT1	-1.021	1.281
INT2	-1.433	5.114
INT3	-1.089	1.177
INN1	-0.583	-0.107
INN2	-0.523	-0.360
INN3	-0.543	-0.295
INN4	-0.201	-0.861
RTK1	-0.312	-0.483
RTK2	-0.921	0.589
RTK3	-0.464	-0.446
PRO1	-1.111	2.268
PRO2	-0.441	0.084
PRO3	-1.302	2.447
ATC1	-0.622	-0.288
ATC2	-1.093	1.853
ATC3	-1.320	1.459
CMT1	-1.066	1.461
CMT2	-1.004	1.875

CMT3	-1.168	2.246
CMT4	-1.071	0.588
IVT1	-0.745	0.739
IVT2	-0.707	0.528
IVT3	-0.812	0.099
PEO1	-1.127	1.321
PEO2	-0.357	-0.572
PEO3	-0.434	0.101
PEO4	-1.387	2.973

According to the guideline of Hair et al. (2016b), kurtosis and skewness values outside the range of ±1 indicate a non-normal data distribution. On the other hand, other researchers (Gravetter and Wallnau, 2014; Trochim and Donnelly, 2006; Field, 2009) argue that skewness and kurtosis values in the range between -2 and +2 are acceptable.

Based on the kurtosis analysis, six items (POC2, INT2, PRO1, PRO3, CMT3 and PEO4) exceed the +2 threshold and indicate a positive skew that reflects a data shift to the left. Moreover, the skewness analysis showed that no values exceed the threshold ±2. Although the values of the data distribution analysis shown in Table 5.2 state that the data was not normally distributed, the values of the skewness and kurtosis values remain within an acceptable range. West et al. (1995) suggest that a skewness value > ±2 and a kurtosis value > ±7 show symptoms of sever non-normality.

According to Hair et al (2014) the size of a simple size has an impact on the normal distribution of the data. Additionally, a small sample size less than 200 could have effects of nonnormality on the data distribution. However, data distribution analysis showed no problematic issues of extreme non-normal distribution. Thus, a decision was made to retain all construct items because they were no extreme effects of non-normality on the distributed data.

6.7. Common Method Bias

According to Malhotra et al (2006), self-reported surveys are considered the most common data collection tool in information systems, psychology and organisational studies. However, data collection using a self-reported approach could be subject to common method bias (Podsakoff et al. 2003; Anderson and Agarwal, 2010). Thus, it was essential in this research to test the existence of common method bias.

Common method bias is defined as "variance that is attributable to the measurement method rather than to the constructs the measures represent" (Podsakoff et al., 2003, p.879). To test the possibility of common method bias in this study, two common method variance techniques were applied.

The first technique, as suggested by Podsakoff et al. (2003) was to use Harman's single-factor test to evaluate the common method variance. This was conducted through an exploratory factor analysis for 11 factors. The result output showed that the first factor explains only 20.4% of the variance, which is below the threshold of 50%, suggesting there is no threat of significant bias.

The second technique, as suggested by Lindell and Whitney (2001), was to use the marker variable technique. This was conducted using a marker variable that is not theoretically unrelated to the constructs of the model. The evaluation showed that the calculated variance accounted for only 4.84% that is below the threshold of 50%. These results indicate that there is no threat or concern regarding common method bias on collected data in this research.

6.8. Exploratory Factor Analysis (EFA)

The previous sections of this chapter examined the data preparation to ensure that the collected data is suitable for multivariate analysis. This section, involves the exploratory factor analysis (EFA) as multivariate statistical technique for validity. According to Hair et al. (2014) new research scales and even established scales adopted from previous research should be evaluated for validity. Factor analysis involves the correlation of a set of items to define highly intercorrelated items into a group (i.e. factor).

EFA aims to analyse the underlying patterns of items and identify constructs consistent of variable groupings (Hair et al., 2016a). However, it is necessary to have an appropriate sample in factor analysis to obtain effective results. According to Hair et al (2014) a sample size of 100 is an acceptable basis for conducting a factor analysis. Moreover, this research meets the minimum sample size requirement, with a study sample exceeding 100 observations (i.e. n=138).

Before starting the factor analysis, the extraction and rotation methods should be decided upon. There are different rotations methods that simplify the illustration of the data structure. According to Hair et al (2014), there are no clear rules to choose a rotation method. Nevertheless, Varimax as an orthogonal rotation method is the most common rotation method used in factor analysis (Costello and Osborne, 2005). Moreover, there are several methods of factor extraction. Principle Component Analysis (PCA) is a frequently used method for factor extraction (Schmitt, 2011), but more importantly also, it is consistent with partial least squares (PLS) (Ifinedo, 2014). In addition, PCA is recommended in cases were data is not normally distributed

(Costello and Osborne, 2005). Therefore, PCA as a factor extraction method was found to be more appropriate for this research because of data distribution and its association with later analysis carried out using PLS-SEM.

However, despite the above, Hair et al. (2014) note that if the research sittings involve more than 30 items and communalities above 0.60 for most items, than principle component analysis and other factor extraction methods yield similar results. In this research, the number of items is larger than 30, and communalities for all items exceed 0.6; therefore, factor extraction methods will give similar results. In this study, there are more than 30 items with communality values above 0.6 exceeding the 0.5 cut-off (Hair et al, 2014).

The factor analysis in this research was conducted using SPSS 24. The analysis was run using PCA as an extraction method and Varimax as a rotation method. In addition, the number of factors that were defined are 12 factors since they were already known in this research through the number of constructs of the developed conceptual model. After assessing 43 items, only 33 items were included and after a couple of iterations, the final EFA loadings are shown in Table 6.3, which explains approximately 73.9% of the total variance. The significant loading threshold was based on Hair et al's (2014) guidelines for a factor loading of 0.50 or greater. In addition, only loadings above the cut-off value of 0.50 were shown in Table 6.3.

The analysis showed five items with low loadings of below 0.5 (IVT3, REF4, CMT4, VUL4 and COS4) and one item with a cross loading exceeding 2.0 (PEO1). These items were drooped from further analysis. After the exclusion of these items, some CMT items showed cross-loading with INT. According to Hair et al (2014), when facing problematic items, a deletion decision could be considered based on the overall contribution of the item and its communality value. In addition, Hair et al (2014) note that interpreting factors involves subjective and objective judgment by the researcher. Therefore, a decision of deleting the CMT items was taken because INT had a higher contribution to this research.

According to Hair et al (2014), cross-loading occurs when items are significantly loading on more than one factor and therefore assessed for possible deletion. However, the loading items of VUL and SEV are not considered as cross-loading, since items of both constructs loaded on the same factor. Therefore, VUL and SEV items are associated with only one factor and a decision to retain the whole factor was taken.

In addition, at the end of the factor analysis two constructs (i.e. IVT and COS) had only two item-factors. Although Hair et al (2014) recommended three items for a factor, still two item-factors are acceptable. Also, the main benefit of summated scales is in overcoming measurement errors by not relying on a single item to measure a concept. Therefore, based on the above discussion, a decision was made to retain the two factors with two items.

Table 6.3: Exploratory Factor Analysis

Constructs	Item	1	2	3	4	5	6	7	8	9	10
Psychological Ownership	POC1.				.839						
	POC2.				.814						
	POC3.				.819						
Reward	REW1.		.781								
	REW2.		.766								
	REW3.		.754								
	REW4.		.720								
	REW5.		.747								

Vulnerability	VUL1.	.661									
	VUL2.	.776									
	VUL3.	.823									
Severity	SEV1.	.795									
	SEV2.	.775									
	SEV3.	.741									
	SEV4.	.699									
Response Efficacy	REF1.						.631				
	REF2.						.883				
	REF3.						.815				
Self-Efficacy	SEF1.					.749					
	SEF2.					.870					
	SEF3.					.888					
Response Cost	COS2.										.794
	COS3.										.820
Security Behavioural Intentions	INT1.			.698							
	INT2.			.829							
	INT3.			.780							
Attachment	ATC1.							.804			
	ATC2.							.652			
	ATC3.							.734			
Involvement	IVT1.									.774	
	IVT2.									.808	
Personal norms	PEO2.								.689		
	PEO3.								.830		
	PEO4.								.646		

Finally, assumptions in factor analysis were assessed to ensure they met the statistical requirements for an appropriate factor analysis. These were carried out by testing Kaiser-Mayer-Olkin (KMO) and Bartlett’s Test of Sphericity. According to Hair et al (2014) a KMO value between 0.7 and 0.8 is considered a meritorious value. In addition, a significant Bartlett’s test value less than 0.05 shows that adequate correlation exists between items.

The results of the EFA showed a KMO value of 0.731 and a Bartlett's test value of 0.000. Thus, the results suggest that the items meet the statistical requirements for sufficient intercorrelation for an appropriate factor analysis.

6.9. Summary

This chapter examined the collected data as an essential step for multivariate analysis. This involved data screening for missing data, outliers and data distribution. In addition, assessment of statistical assumptions of multivariate techniques was conducted. Furthermore, validity analysis was conducted through an Exploratory Factor Analysis (EFA) using SPSS.

Applying PCA with Varimax rotation for the exploratory factor analysis resulted in 10 clear set of factor loadings. In addition, KMO and Bartlett's test were conducted and suggested that the data is appropriate for factor analysis.

Common method bias was assessed in this research using two techniques: Harman's single-factor and common marker technique. Two tests assessing common method bias indicated no threat of significant bias in the research data.

However, it is necessary to highlight some important aspects that resulted from factor loading. First, two constructs (i.e. VUL and SEV) loaded on one factor. This was not considered as a cross-loading, since the items of both constructs loaded significantly on only one factor. This could be because individuals perceive vulnerability and severity as one concept. However, the SEVandVUL factor loading showed that the combined two constructs are valid in terms of convergence and discrimination validity. Therefore, VUL and SEV are loading on one factor, and it was decided to retain the factor and see in a later analysis if anything changes or if the items logically represent the construct.

The second important aspect to highlight is that two constructs (i.e. INT and CMT) showed cross-loading of more than one item. Looking at both constructs and evaluating their communality in addition to their importance and contribution within this research, a deletion decision of the CMT construct was made.

One possible explanation for this cross-loading could be that individuals perceive commitment and intention as a similar concept. Cohen and Levesque (1987) state that "the concept of intention as composed of two more basic concepts, choice (or goal) and commitment" (p.410, 1987). Therefore, looking at commitment as part of the intention could be the reason that individuals might feel they are similar concepts.

In the following chapter, PLS analysis is used to assess the measurement model and the structural model, and, thus test the research hypotheses.

Chapter 7

7. Model Evaluation

7.1. Introduction

Having examined the collected data and conducted the exploratory factor analysis that yielded in a 10-factor model in Chapter 5, this chapter presents further advanced multivariate analysis using structural equation modeling (SEM). The analysis involved using partial least squares (PLS) method of structural equation modeling, employing a principle component-based approach.

The core of this chapter begins with the assessment of the measurement model (also called outer model) followed up with the assessment of the structural model (also called inner model). The measurement model includes the constructs reliability and validity assessment. Additionally, the structural model includes the hypotheses testing.

To achieve the aim of this chapter, fist the PLS-SEM analysis method used is justified. A detailed discussion of why the PLS-SEM method was considered for this research is presented below. Afterwards, the initial assessment begins with the measurement model assessment than with the structural model assessment.

7.2. Structural Equation Modelling (SEM)

Linear regression is a first generation technique that has been applied by many researchers in different disciplines but suffers some limitations (Haenlein and Kaplan, 2004). SEM as a second-generation technique has been used to overcome first generation limitations. Structural equation modelling is a multivariate analysis technique that explains the relationship between multiple variables (Hair et al., 2016b; 2014). In addition, SEM allows researchers to test theories and concepts (Hair et al., 2012). Therefore, in this research SEM is used to test the research hypotheses for the developed conceptual model.

SEM may be conducted using one of two methods: Covariance-Based SEM (CB-SEM) and Partial Least Squares SEM (PLS-SEM). According to Hair t al., (2016b) CB-SEM is usually used when the purpose of the analysis is to confirm theories. In contrast, PLS-SEM is used in exploratory research when the purpose is to develop a theory. Moreover, PLS-SEM has recently been widely used in the field of information system research (Hair et al., 2017).

PLS-SEM is a second-generation causal modelling statistical technique has been gaining increased popularity in recent years. According to Hair et al. (2016b) PLS-SEM is considered an efficient approach for small sample sizes and complex developed models (i.e. many constructs). Moreover, PLS-SEM is a well-suited approach for the type of research that involves exploratory models and theory development (Bulgurcu et al., 2010).

The two SEM methods (i.e. CB-SEM and PLS-SEM) are based on different algorithms. The CB-SEM method is based only on common variance that requires model fit (i.e. goodness-of-fit). Therefore, it is only suitable for confirmatory research that is built on well-developed theories. In contrast, the PLS-SEM method is based on total variance and it is suitable for both confirmatory and exploratory research (Hair et al., 2017).

One of the main reasons for applying PLS-SEM is obtaining a mall sample size that can be regarded as the minimum sample size. Moreover, using minimum sample sizes in PLS-SEM safeguards the analysis results and ensures robustness. This is because PLS-SEM can achieve higher levels of statistical power with small sample sizes in comparison to CB-SEM (Hair et al., 2016b). On the other hand, a study by Boomsma and Hooglands (2001) states that CB-SEM requires large sample sizes to be able to achieve a robust parameter estimate. However, PLS-SEM is becoming a very commonly applied analysis method in the field of information systems (IS) (Hair et al., 2017).

Hair et al (2017) state the rules of thumb for choosing a SEM method. The main listed rules of applying PLS-SEM are: a complex research model (more than six constructs); a small sample size (n<200); and a non-normally distributed data.

The discussion above states that PLS-SEM is a suitable method for this research. Therefore, PLS-SEM has been chosen as a multivariate analysis method for this research. The reasoning behind choosing PLS-SEM analysis method is its capability to accommodate the complexity of the conceptual model, which is composed of 10 constructs, and because of its capability to function with small sample sizes less than 200.

The 10 times rule (Hair et al., 2016b) was adopted in this research to determine the minimum sample size required to conduct the PLS-SEM analysis. The maximum number of arrows that are pointing to a latent construct are 12. Therefore, the 10 times rule, 12 * 10 = 120 and the research observations collected (n=138) exceeded the minimum sample size to be suitable.

Moreover, guidelines by Hair et al (2017) for best practices in reporting PLS-SEM results in IS research is adopted in this research. In addition, (Ringle et al., 2015) was used in this research based on Hair et al (2017) recommendation that SmartPLS is a user-friendly software that is widely used for PLS-SEM analysis.

7.3. The path model

The PLS path model visualizes the research constructs, relationships and hypotheses. The elements of the PLS path modeling consist of two main elements: the measurement model and the structural model. The initial PLS path model created and estimated is displayed in Figure 7.1.

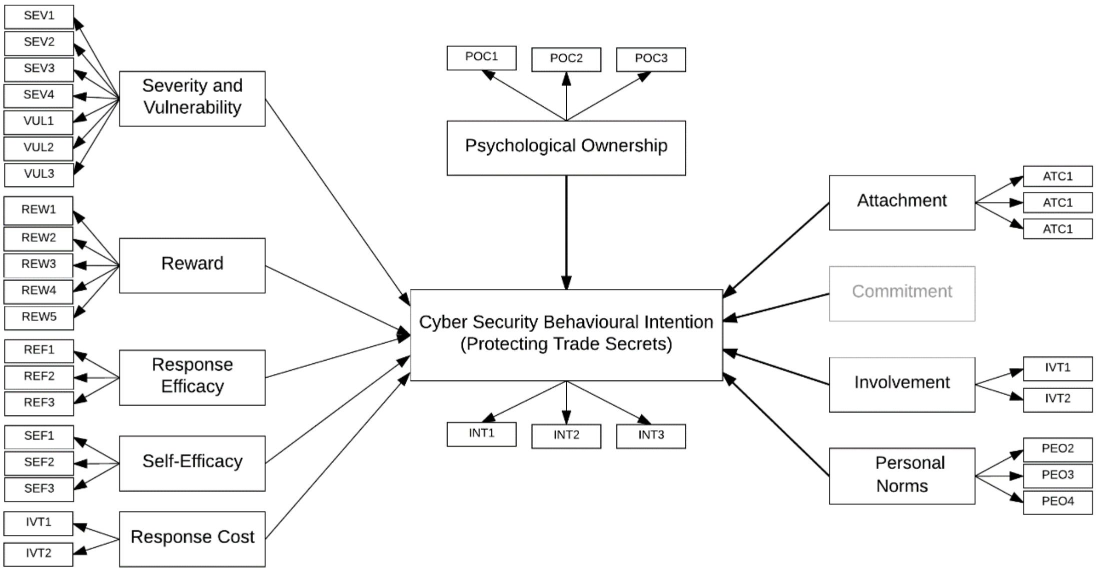


Figure 7.1: The initial PLS path model

To guide this evaluation and add structure to its analytical procedures, the guidelines for best PLS-SEM practice in information systems research by Hair et al. (2017) were employed. This process provided a systematic evaluation guideline for measurement models. Formally, the evaluation consists of the reflective measurement model and structural models. Therefore, through the following sections of this chapter, a detailed evaluation is carried out to assess the research PLS-SEM results.

7.4. Assessment of the Measurement Model

To evaluate the two elements of the PLS path model (i.e. the outer and inner models), the assessment begins with the constructs' reliability and validity assessment. The aim of the measurement model evaluation is to validate the conceptual model's constructs by assessing convergent validity and discriminate validity, in addition to the evaluation of internal consistency reliability for the measurement scales. Thus, the following sub-sections illustrate the assessment of the measurement model in detail.

7.4.1. Internal consistency

Reliability is determined through the assessment of the internal consistency reliability of the constructs. To evaluate the constructs' reliability two types of internal consistency reliability are used to determine the level of reliability for the measurement model: Cronbach's alpha and composite reliability.

Cronbach's alpha is considered to be one of the most common measures to assess internal consistency reliability. However, Hair et al (2016b) argue that Cronbach's alpha has some limitations due to its sensitivity regarding the number of items. Therefore, it was more appropriate to apply an additional reliability measure method as recommended by Hair et al (2016b). Thus, composite reliability was used as a different reliability measure method to evaluate the constructs' reliability. Reliability was assessed using composite reliability, and the constructs reliability assessment showed an acceptable level exceeding the threshold of 0.70 (Fornell and Larcker 1981) for all constructs, with the majority above 0.8. Also, the evaluation of Cronbach's alpha showed that all constructs' values are above 0.6, which is an acceptable but with a majority above 0.70. Table 7.1 illustrates the evaluation values of Cronbach's alpha and composite reliability.

Table 7.1: Internal consistency reliability

Constructs	Cronbach's Alpha	Composite Reliability
ATC	0.741	0.848
COS	0.717	0.862
INT	0.821	0.893
IVT	0.638	0.845
PEO	0.745	0.854
POC	0.832	0.899
REF	0.730	0.781
REW	0.828	0.859
SEF	0.678	0.861
SEVandVUL	0.894	0.915

Moreover, the evaluation of Cronbach's alpha showed that all constructs' values are above 0.70, except IVT and SEF that showed values above 0.60. Nevertheless, it is important to note that IVT and SEF each consist of only two items and according to Gliem and Gliem (2003) the increase of the alpha value is associated with the number of items. In addition, it is also important to note that composite reliability usually has a higher value than Cronbach's alpha because of the weighting process (Hair et al, 2015).

According to Hair et al (2016b) for exploratory research, such as this research, the values of the internal consistency reliability should be higher than 0.70. However, values between 0.60 and 0.70 are still considered acceptable for internal consistency reliability using Cronbach's alpha and composite reliability. As a conclusion, the reliability tests for all the model constructs yielded acceptable results that meet the essential criteria for a reliable measurement scale. Therefore, the next step is to assess the validity of the PLS path model by examining the convergent and discriminate validity.

7.4.2. Convergent Validity

Convergent validity refers to “the extent to which a measure correlates positively with alternative measures of the same constructs” (Hair et al, 2016b, p.112). To evaluate the measurement model in terms of convergent validity, constructs’ outer loadings are tested in addition to examining their average variance extracted (AVE) values.

According to a rule of thumb for assessing outer loadings (Hair et al, 2017; Hire et al, 2016b), the loading value should be above 0.70; however, values between 0.40 and 0.70 can be considered acceptable if deleting the item does not increase composite reliability and AVE above the threshold values. In addition, AVE values should be all above the threshold of 0.50 (Hire et al, 2017; Fornell and Larcker 1981).

One of the issues that occurred during the convergent evaluation was a low AVE (0.139) for SEF. In addition, SEF1 had a negative loading value of -0.444 in the outer loading test. If this negative value appeared during the EFA evaluation it would have been assumed that the item was reverse-scored, however this was not the case. According to Hair et al (2017) a low value below 0.40 should be deleted from the construct. Therefore, after deleting SEF1 the construct’s AVE value showed an increase to 0.756, which is above the threshold.

The convergent evaluation should have a low AVE value below the threshold for SEF (0.139). In addition, the evaluation should a negative value for the outer loading test for the SEF1 item (-0.444). If this negative value appeared during the EFA evaluation it could have been a sign that the item was reverse-scored, however this was not the case here. According to Hair et al. (2017) a low loading value below 0.40 should be deleted from the construct. Therefore, after deleting SEF1 the construct's AVE value showed an increase to 0.756 that is above the threshold. In addition, all items of the construct items showed a loading value above 0.70 except REF3, REW1, REW5, VUL1 and VUL4 that had a loading value between 0.40 and 0.70 with the majority above 0.60. These loading values were considered acceptable, since deleting them had no significant impact on the reliability of the constructs and AVE values. Table 7.2 illustrates the outer loadings for the model constructs.

Table 7.2: The PLS path model outer loadings

	ATC	COS	INT	IVT	PEO	POC	REF	REW	SEF	SEVandVUL
ATC1	0.761									
ATC2	0.742									
ATC3	0.909									
COS2		0.957								
COS3		0.776								
INT1			0.837							
INT2			0.843							
INT3			0.893							
IVT1				0.887						
IVT2				0.823						
PEO2					0.831					
PEO3					0.769					
PEO4					0.838					
POC1						0.917				
POC2						0.840				
POC3						0.834				
REF1							0.962			
REF2							0.725			

REF3							0.479			
REW1								0.615		
REW2								0.723		
REW3								0.847		
REW4								0.659		
REW5								0.843		
SEF1									0.874	
SEF3									0.865	
SEV1										0.760
SEV2										0.837
SEV3										0.857
SEV4										0.839
VUL1										0.687
VUL2										0.659
VUL3										0.795

In addition, the convergent validity assessed using AVE showed that all values of all the constructs are above the cut-off of 0.50. This means that the constructs explain more than 50% of the variance of its items. Table 7.3 illustrates the AVEs of the constructs. Overall, the convergent assessment results illustrate a strong convergent validity.

Table 7.3: The PLS path model constructs' AVEs

Constructs	Average Variance Extracted (AVE)
ATC	0.652
COS	0.759
INT	0.736
IVT	0.732
PEO	0.661
POC	0.747

REF	0.560
REW	0.553
SEF	0.756
SEVandVUL	0.608

7.4.3. Discriminate Validity

Discriminate validity refers to "the extent to which a construct is truly distinct from other constructs by empirical standards." (Hair et al., 2016b, p.115). To evaluate the measurement model in terms of discriminate validity, three criteria are applied: the Fornell-Larcker criterion, cross-loading and the Heterotrait-Monotrait ratio of correlations (HTMT).

The first test examines the cross-loadings of the measurement items. In this test, discriminant validity is achieved when an item's outer loading associated with a specific construct is greater than any of its cross-loadings on other constructs. The cross-loading results (see Appendix C) show that the outer loadings for all items exceed their cross-lodgings. These results demonstrate high discriminant validity for the tested model.

The second test to evaluate discriminate validity is the Fornell-Larcker criterion. The rule of thumb for assessing this requires the square root of every construct's AVE value being greater than the constructs value of variance associated between the construct and other constructs in the model. Table 7.4 illustrates that all the square roots of every construct's AVE value is greater than the correlation.

Table 7.4: Fornell-Larcker criterion analysis

	ATC	COS	INT	IVT	PEO	POC	REF	REW	SEF	SEVan dVUL
ATC	0.807									
COS	-0.129	0.871								
INT	0.333	-0.284	0.858							
IVT	0.378	-0.147	0.314	0.856						
PEO	0.368	-0.190	0.440	0.309	0.813					
POC	0.169	-0.140	0.355	0.179	0.295	0.864				
REF	0.159	-0.043	0.279	-0.010	0.087	0.127	0.749			
REW	-0.226	0.373	-0.174	-0.071	-0.243	-0.119	-0.172	0.743		
SEF	-0.145	0.083	0.030	0.033	0.034	0.000	0.019	0.041	0.870	
SEVan dVUL	0.379	-0.054	0.429	0.157	0.325	0.347	0.218	-0.015	-0.117	0.780

The third test for discriminant validity involves the examination of HTMT ratio correlations. According to Hair et al. (2017) HTMT values should be less than the cut-off of 0.85. Table 7.5 shows that all HTMT values are below 0.85. Furthermore, running a bootstrap confidence interval assessment showed that both confidence intervals (i.e. 90% and 10%) for each construct does not include the value 1 (see Appendix D). Based on the above assessment, the constructs' discriminant validity has been established for this model. Hence, the above analysis ensure that the discriminate validity of the constructs has been established for this model.

Table 7.5: HTMT criterion analysis

	ATC	COS	INT	IVT	PEO	POC	REF	REW	SEF	SEVan dVUL
ATC										
COS	0.173									
INT	0.395	0.335								
IVT	0.563	0.211	0.431							
PEO	0.498	0.236	0.554	0.444						
POC	0.196	0.150	0.415	0.250	0.364					
REF	0.168	0.121	0.235	0.161	0.111	0.139				
REW	0.288	0.496	0.173	0.135	0.316	0.155	0.198			
SEF	0.198	0.108	0.099	0.133	0.134	0.097	0.106	0.100		
SEVan dVUL	0.447	0.118	0.454	0.194	0.382	0.393	0.225	0.100	0.174	

The measurement model evaluation showed that the measures represent the conceptual model constructs, and therefore ensure adequacy. Furthermore, following the PLS-SEM assessment, the second step of the assessment process is followed up with the structural model assessment.

7.5. Assessment of the Structural Model

After ensuring the adequacy of the measurement model, the structural model is evaluated as the second part of PLS analysis. The aim of the structural model evaluation is to examine the model's capabilities to estimate the significance of the relationships between the model constructs (Hair et al, 2016b). The criteria used to assess the structural model are: the coefficient of determination (R^2), predictive relevance (Q^2) effect size and f^2 effect size.

One of the main differences between CB-SEM and PLS-SEM, is that the later does not need to be confirmed with goodness-of-fit (GoF) metrics, it is only confirmed with reliability and validity metrics (Hire et al., 2017). This is based PLS-SEM is based on conversances and therefore does not require a model fit measure. However, Hair et al (2016b) note that current researchers are developing model fit measures in PLS-SEM, but they are still in a very early stage of development. Hence, a decision was made not to assess the PLS path model using a GoF metric.

7.5.1. Path coefficients

The examination of the path coefficient (β) starts by running the SmartPLS 3.0 to obtain the estimates of the structural model relationships. The significance of the coefficient is measured through computing the t-values and the p values for the models' path coefficients. The t-values should be above a defined critical value to estimate the significance of the coefficients.

For interpreting the significance of the path coefficients, the critical value may be determined based on using a one-tailed or two-tailed tests. Ultimately, the difference between the two types of tests (i.e. one or two tails) is based on the hypotheses ability to predict the direction of the relationship (i.e. positive or negative). A one-tailed test is used when the hypothesised directional relationship is determined, and is either positive of negative. In contrast, a two-tailed test is used when the direction of the relationship is not determined (Hair et al., 2016a; Hair et al., 2016b). Table 7.6 illustrates the critical values for one and two tailed tests (Hair et al., 2016a, p.395).

Table 7.6: One-tailed and two tailed tests adopted from (Hair et al., 2016a; Hair et al., 2016b)

Level of confidence $(1 - \alpha)$	Significance Level (α)	Two-tailed critical value	One-tailed critical value
90%	10%	1.645	1.28
95%	5%	1.96	1.645
99%	1%	2.575	2.33

According to Hair et al. (2016b), researchers mostly choose a significance level of 5%, while a 1% significance level is still considered by conservative researchers in some fields of research. Additionally, in studies that have an exploratory nature, 10% significance level is acceptable.

In this research, all the hypotheses have directional relationships, and are defined as positive. Moreover, this research is considered an exploratory, given the research objectives and research context. Hence, a one-tailed test is used to evaluate the significance level of the research hypotheses.

Bootstrapping in PLS-SEM is used to assess the significance level of the path coefficients. The bootstrapping metrics for SmartPLS 3.0 settings were based on the best practices recommended by Hair et al. (2017). These included setting the number of bootstrap samples to 5,000 and setting the size of the bootstrap samples to the number of observations in the research. Table 7.7 illustrates the path coefficients obtained from the analysis.

Table 7.7: The path coefficient results

Path	Path Coefficient (β)
ATC → INT	0.052
COS → INT	-0.189
IVT → INT	0.142
PEO → INT	0.214
POC → INT	0.130
REF → INT	0.181
REW → INT	0.018
SEF → INT	0.064
SEVandVUL → INT	0.230

7.5.2. Coefficient of determination (R^2)

The square of the correlation coefficient results in the coefficient of determination (R^2) that is commonly used to in evaluating the structural model (Hair et al., 2016b). Falk and Miller (1992) recommended that the value of R^2 should not be less than 0.10 as a minimum accepted value. Moreover, Chin (1998) suggests that R^2 value of 0.67, 0.33 and 0.19 in PLS-SEM for a dependent variable can be respectively substantial, moderate and week. In addition, R^2 ranges from 0.00 to 1.00. and explains the level of variation of one construct by the other. In this research, the R2 value for the behavioural intention construct is 0.40, describing a moderate effect.

7.5.3. f^2 effect size

The third metric for assessing the structural model is the f^2 effect size. According to Sullivan and Fein (2012), although the p value can indicate the existence of an effect, this does not indicate the size of the effect. Therefore, the f^2 effect size metric is essential for an adequate analysis.

Hair et (2017) recommended Chin (1998) guidelines that state that the f^2 value for 0.02, 0.15 and 0.35 respectively indicate a small, medium and large effect size. Moreover, less than the value of 0.02 for f2 shows no effect size. Table 7.8 shows the f^2 effect size with three with no effect (ATC, REW and SEF) while the other represent a small effect.

Table 7.8: f^2 effect size

Construct	INT	Effect size
ATC	0.003	No effect size
COS	0.050	Small effect size
IVT	0.027	Small effect size
PEO	0.056	Small effect size
POC	0.023	Small effect size
REF	0.050	Small effect size
REW	0.000	No effect size
SEF	0.007	No effect size
SEVandVUL	0.063	Small effect size

7.5.4. Predictive relevance (Q^2)

Predictive relevance Q^2 is used to assess the predictive capability of a structural model in PLS through the blindfolding procedure (Hair et al., 201b). Table 7.9 shows that the Q^2 value for the model's dependent construct (i.e. INT) was above the value zero. (Hair et al, 2016b). This indicates that the structural model has predictive relevance for INT as a dependent construct.

Table 7.9: Q^2 effect size

Construct	SSO	SSE	Q² (=1-SSE/SSO)
ATC	414.000	414.000	
COS	276.000	276.000	
INT	414.000	313.875	0.242
IVT	276.000	276.000	
PEO	414.000	414.000	
POC	414.000	414.000	
REF	414.000	414.000	
REW	690.000	690.000	
SEF	276.000	276.000	
SEVandVUL	966.000	966.000	

7.6. Hypothesis Testing

The results of the multivariate data analysis show that the final path model consists of 10 reflectively measured constructs: Behavioral Intentions (INT); Perceived Severity and Perceived Vulnerability (SEVandVUL); Reward (REW); Response Efficacy (REF); Self-Efficacy Response(SEF) Cost (COS) Psychological Ownership (POC) Attachment (ATC) Involvement (IVT) and Personal Norms (POE). Table 7.10 presents the results of the hypotheses testing that includes the path coefficient (β), t values and p values. All research hypotheses were found to be positively significant $p < 0.05$ ($t= 1.645$) except H3, H5, H7 and H8. Moreover, all insignificant hypotheses have a low path coefficient (<100). The evaluation of the research hypotheses will be discussed in Chapter 8.

Table 7.10: Results of the hypotheses testing

Hypothesis	Hypothesised Path	Path Coefficient (β)	T Values	P Values	Significance
H1 H2	SEVandVUL → INT	0.230	2.656	0.004	Supported
H3	REW → INT	0.018	0.166	0.434	Not Supported
H4	REF → INT	0.181	2.299	0.011	Supported
H5	SEF → INT	0.064	0.802	0.211	Not Supported
H6	COS → INT	-0.189	2.405	0.008	Supported
H7	POC → INT	0.130	1.480	0.070	Not Supported
H8	ATC → INT	0.052	0.542	0.294	Not Supported
H9	CMT→ INT	Dropped from the study			
H10	IVT → INT	0.142	1.765	0.039	Supported
H11	PEO → INT	0.214	2.541	0.006	Supported

7.7. Summary

The research conceptual model has been analysed using partial least squares (PLS) by applying SmartPLS 3.0 (Ringle et al, 2005). The research used the PLS-SEM method rather than the CB-SEM method, because of its ability to analysis complex models and small sample sizes (Hair et al, 2016b). Furthermore, the PLS-SEM method is more suitable for exploratory research (Hair et al, 2017).

The evaluation of the PLS path model was based on recommendations by Hair et al (2017) for applying PLS-SEM in the field of IS research. The results of the PLS path model analysis demonstrate that the research conceptual model meets the rigorous criteria expected for IS research (Hair et al, 2017). The empirical results of the measurement and structural model analysis are summarised in Table 7.11 and are illustrated in the final research model in Figure 7.2. In the next chapter, the evaluation of the results is presented and finally, the research conclusions are drawn.

Table 7.11: Summary for the measurement and structural models

Construct	Items	Internal Consistency Reliability		Convergent Validity		Discriminant Validity		
		Cronbach’s Alpha	Composite Reliability	Outer Loadings	AVE	cross-loading	Fornell-Larcker criterion	HTMT
		>0.60	>0.70	>0.70	>0.50	Low cross-loadings	<0.85	CI ≠1
POC	POC1	0.832	0.899	0.917	0.747	Yes	0.864	Yes
	POC2			0.840				
	POC3			0.834				
ATC	ATC1	0.741	0.848	0.761	0.652	Yes	0.807	Yes
	ATC2			0.742				
	ATC3			0.909				
COS	COS2	0.717	0.862	0.957	0.759	Yes	0.871	Yes
	COS3			0.776				
INT	INT1	0.821	0.893	0.837	0.736	Yes	0.858	Yes
	INT2			0.843				
	INT3			0.893				
IVT	IVT1	0.638	0.845	0.887	0.732	Yes	0.856	Yes
	IVT2			0.823				
PEO	PEO2	0.745	0.854	0.831	0.661	Yes	0.813	Yes
	PEO3			0.769				
	PEO4			0.838				
REF	REF1	0.730	0.781	0.962	0.560	Yes	0.749	Yes
	REF2			0.725				
	REF3			0.479				
REW	REW1	0.828	0.859	0.615	0.553	Yes	0.743	Yes
	REW2			0.723				
	REW3			0.847				
	REW4			0.659				
	REW5			0.843				
SEF	SEF1	0.678	0.861	0.874	0.756	Yes	0.870	Yes
	SEF3			0.865				
SEV&SEV	SEV1	0.894	0.915	0.760	0.608	Yes	0.780	Yes
	SEV2			0.837				
	SEV3			0.857				
	SEV4			0.839				
	VUL1			0.687				
	VUL2			0.659				
	VUL3			0.795				

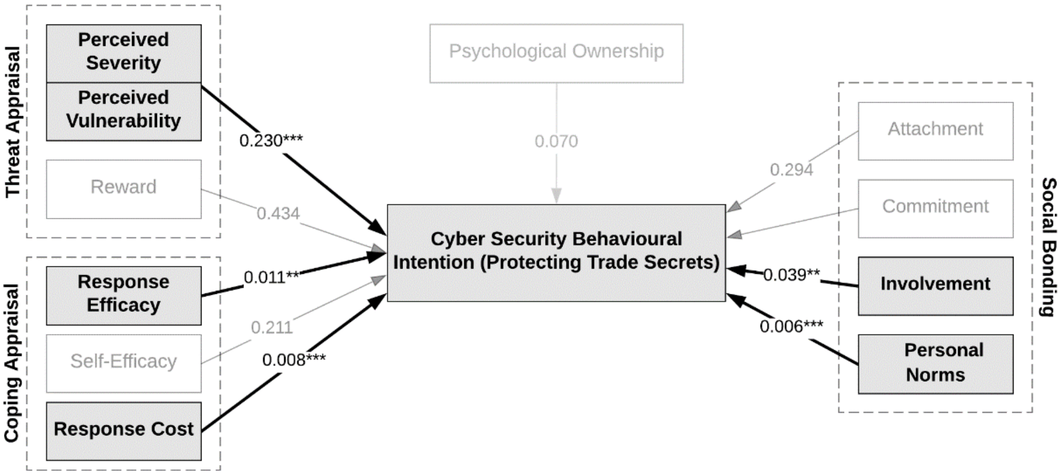


Figure 7.2: The final research model

Note: * significant at P<0.10 level; ** significant at P<0.05 level; *** significant at P<0.01 level

Chapter 8

8. Discussion & Conclusion

8.1. Introduction

Today, cyber security is becoming one of the biggest concerns to survival in the digital economy. This is true in well secured business units within a corporate and also in new business units. Moreover, open innovation has made it more difficult for corporates to secure their cyber boundaries. It was already difficult for corporates to protect and secure their information assets when they had closed doors, with open innovation opening the doors for external ideas making cyber security a bigger challenge. Hence, this leads to an extended surface of cyber threats that could impact companies' competitiveness.

Furthermore, Rowe (2016) states that trade secrets in the digital economy are becoming crucial to companies' survival and growth like never before in history. This makes trade secrets a potentially valuable intangible asset, and creates a need for more effective technology mechanisms to perform better protection for trade secrets.

However, cyber security is not only a technology aspect, nor a management aspect, but a human issue. This requires addressing human behaviours in corporate venturing beyond just the engagement of people with technology and police compliance to improve the protective cyber security actions performed by entrepreneurs.

Cyber security exists in large corporates and in many cases, incorporating the state of the art in cyber security technologies. However, the issue is that the cyber security aspects for such different type of users such as entrepreneurs in a new dynamic environment, such as a corporate accelerator within a corporation, is considered as a new challenge that entitles a different set of cyber risks.

But the question is how can entrepreneurs creating a new venture within a corporate venturing unit be influenced to perform positive cyber security protective actions? This requires an understanding of the cognitive, social and psychological aspects that could influence entrepreneurs in performing protective cyber security behaviours.

To support the protection of trade secrets within corporate accelerators, there is a need to understand the factors that drive entrepreneurs to protect trade secrets. In addition, it is essential to be able to design the appropriate security countermeasures to enhance the protection and mitigate the risks.

This research was conducted in the cyber security behaviour domain, and more specifically on the human factor aspect of cyber security for trade secret protection. The aim of this research was to explore the impact of protecting trade secrets as a competitive advantage for new ventures within a corporate venturing context. Furthermore, this research targeted entrepreneurs as the main subject of study, who are establishing new ventures within corporate accelerators.

The systematic literature review in Chapter 3 showed that there is a lack of research in the cyber security behaviour domain in respect of intellectual property protection, and more specifically, trade secret protection. In addition, the reviewed literature showed no studies targeting entrepreneurs as the main subject of research. Furthermore, most of the literature focused on traditional organizational environments, with only a few studies focusing on non-work environments such as homes.

As illustrated in Figure 8.1, the focus of this research was based on the protection of the core dimensions of trade secrets: information, intellectual property and secrets. Building on this focus, a conceptual model was developed in Chapter 4 to investigate the trade secret protection in respect of confidentiality, ownership and secrecy. The theoretical foundation of the conceptual model was built using the theories of protection motivation, psychological ownership and social bonding.

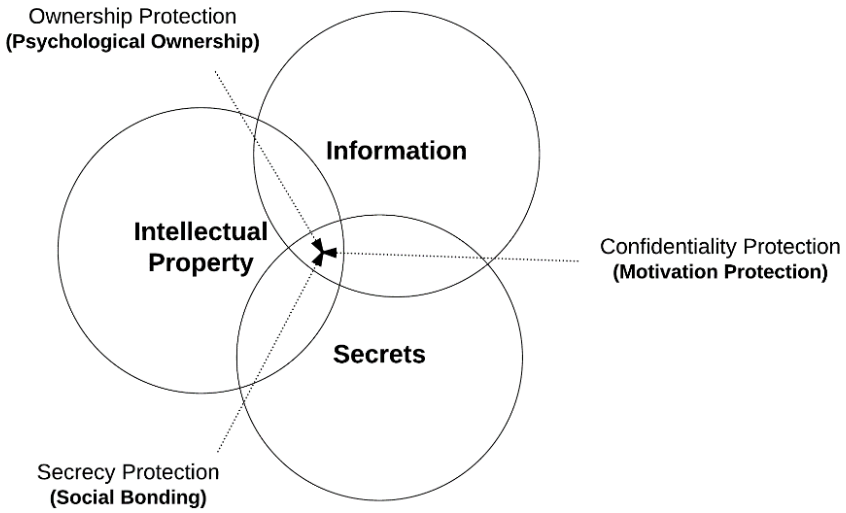


Figure 8.1: Trade secrets' core dimensions, protection aspects and applied model theories

Having completed the evaluation of the conceptual model in Chapter 7, this chapter takes a further step by illustrating and discussing the key research findings. This includes evaluating the conceptual model in addition to the hypothesis testing results.

More specifically, this chapter aims to discuss the key research findings based on the analysis of the measurement and structural model. The discussion is organised around the protection aspects of trade secrets that structured the development of the conceptual model. Additionally, this includes discussing the hypothesis testing and the significant factors that influence entrepreneurs' behavioral intentions to protect trade secrets.

Finally, this chapter ends the thesis by presenting the research conclusions. This includes describing how the research objectives have been meet in this research. Also, the chapter reports the contributions made to the research discipline and the practical limitations of the research.

8.2. Key Findings

The key findings of this research are discussed on the bases of the trade secret protection aspects of confidentiality, ownership and secrecy. Moreover, these three protection aspects have driven the development of the conceptual model by integrating protection motivation, psychological ownership and social bonding, as discussed in Chapter 4.

The key findings discussion is based on the hypothesis testing of the final research model, illustrated in Figure 7.2. This starts by discussing the key findings associated with the results of exploring the confidentiality protection of trade secrets. Next, the discussion moves to discussing the findings obtained from exploring the ownership protection of trade secrets as. Finally, the discussion ends by discussing the findings from exploring the secrecy protection of trade secrets.

8.2.1. Discussion of Results Related to Confidentiality Protection

8.2.1.1. Protection Motivation

The conceptual model integrated two appraisals of the protection motivation theory: threat appraisal and coping appraisal. The threat and coping appraisals aim to explore the factors that drive entrepreneurs to perform protective security actions to protect the confidentiality of trade secrets.

The threat evaluation part consists of three constructs that form the threat appraisal: severity, vulnerability and rewards. On the other hand, the coping appraisal consists of three constructs: response efficacy, self-efficacy and costs.

It is important to note that the analysis of validity in the exploratory factor analysis resulted in both the severity and vulnerability items in the threat appraisal to load on the same factor. According to Witte (1992) threat is perceived as two components: severity and vulnerability. In addition, a meta-analysis by Witte and Allen (2000) showed that some studies using PMT have demonstrated trough factor analysis, whereby severity and vulnerability are combined into a single factor called threat. Nevertheless, the combined SEVandVUL items loading showed that the combined two threat constructs are valid in terms of convergence and discrimination validity. It could thus be interpreted that entrepreneurs perceived severity and vulnerability as one concept.

The research results show that threat has a significant positive relationship with entrepreneurs' behavioural intentions to protect trade secrets (β =o.230 P<0.004), which supports H1 and H2. This shows that entrepreneurs that perceive that they are vulnerable to cyber threats, are more likely to perform protective security actions in response to cyber threats.

The research results show that response efficacy to have a significant positive relationship with entrepreneurs' behavioural intentions to protect trade secrets (β =0.181 P<0.011), which supports H4. This shows that entrepreneurs with positive perception of response efficacy are more likely to have a coping response in the protection of trade secrets.

The research results show that response costs to have a significant positive relationship with entrepreneurs' behavioural intentions to protect trade secrets (β =0.189 P<0.008), which supports H6. This shows that entrepreneurs that perceive costs associated with a security responses as insignificant are more likely to engage in the protection of trade secrets.

The threat construct (i.e. SEVandVUL) showed a stronger association to the security behavioural intentions than did the coping factors (i.e. response efficacy and costs). On the other hand, self-efficacy and rewards did not show any significant value, and therefore are not supported.

The findings showed that entrepreneurs faced with a cyber threat first assess the threat, then assess the effectiveness of performing a protective security response and the associated costs to performing that protective security action. The findings also suggests that entrepreneurs perceive cyber threat as one concept of threat. This means that entrepreneurs do not differentiate between the magnitude of a threat and the probability of its occurrence when faced with a cyber threat. This shows that entrepreneurs evaluate threat differently from how employees evaluate threat, based on more than on element of threat.

On the other hand, the findings suggest that positive coping response depend on entrepreneurs believes that taking protective security actions will be effective. In addition, coping also depends on the costs of taking these protective actions that they do not overweigh the benefits of performing a protective coping behaviour. Thus, response cost suggests that entrepreneurs will not take protective security actions required to protect trade secrets if it is associated with high cost (e.g. time, money, complexity, inconvenience and effort).

One explanation could be that entrepreneurs creating a new venture focus on building their business value propositions which requires a lot of resources (e.g. time, effort and money). Therefore, they might result in less attention given to performing protective security actions to protect trade secrets.

Moreover, a possible reasoning is that response cost is perceived as an overhead in terms of time consumption. Generally, entrepreneurs would have about three months to work on building and validating their product/service in a corporate accelerator. Therefore, if entrepreneurs perceive the cost to be high, this might decrease the likelihood of them performing security protective actions to protect their trade secrets.

The findings confirm the significant relationship between threat (i.e. severity and vulnerability) and cyber security behavioural intention. They also confirm the significant relationship between response efficacy and response costs with cyber security behavioural intention. Thus, the findings suggest that when entrepreneurs perceive that they are vulnerable to cyber threats, are more likely to perform protective security actions in response to cyber threats, as long as the entrepreneurs perceive the response effective and the costs associated with the security responses are insignificant.

8.2.2. Discussion of Results Related to Ownership Protection

8.2.2.1. Psychological Ownership

Based on the concept of psychological ownership, the research conceptual model was developed with the idea that entrepreneurs who are creating new ventures and hold strong feelings of psychological ownership about trade secrets are likely to perform protective security actions to protect these trade secrets. The aim of using psychological ownership is to investigate its impact on influencing entrepreneurs that own trade secrets to perform protective cyber security actions to protect the ownership of trade secrets during the establishment of a new venture.

This research differs from previous research of psychological ownership because of its emphasis on possession of trade secrets as a unique driver of performing protective security actions. In addition, this research looks at the possession of intangible objects (i.e. trade secrets) that are based on the absence of legal ownership.

The research results show that psychological ownership has no significant positive relationship with entrepreneurs' behavioural intentions to protect trade secrets (β =0.130 $P<0.070$), which does not support H7. According to Nuttin (1987), individuals with a sense of ownership toward an object are more likely to perform a positive attitude towards that object. Thus, the significant result of psychological ownership does not show that entrepreneurs are wailing to protect the ownership of trade secrets when they have a possession felling that they own these trade secrets. Therefore, psychological ownership is not viewed as a protection construct that provides an understanding of ownership protection and cyber security behaviour.

The research did not confirm the value of psychological ownership for protecting the ownership of trade secrets by entrepreneurs with feelings of possession towards trade secrets in a dynamic environment. Generally, the research findings are important, because they show that psychological ownership for trade secrets has no positive impact on entrepreneurs' security behaviours to perform cyber security actions.

8.2.3. Discussion of Results Related to Secrecy Protection

8.2.3.1. Social Bonding

The conceptual model included the integration of social bond elements: involvement, attachment, commitment and personal norms. The social bonding elements aim to explore the factors that have a positive effect on entrepreneurs to perform protective security actions to protect the secrecy of trade secrets.

It is important to note that the validity analysis in the exploratory factor analysis resulted in the commitment to construct cross-loading with behavioural intentions. Therefore, a decision was made to drop the commitment construct from further model analysis. The reason for the cross loading of commitment and intentions could be that entrepreneurs perceive commitment and intentions as one concept. This is because commitment is described as an essential part of intentions (Cohen and Levesque, 1987).

Usually in previous cyber security behaviour research, social bonding was used to describe how individuals with strong social ties would not attempt to an action that would cause a security risk by complying with cyber security policies. However, in this study, social bonding was used to explore social ties in influencing entrepreneurs to perform actions to protect the secrecy of trade secrets form a security risk. Therefore, the use of social bonding is to influence cyber security actions to increase the secrecy protection of trade secrets.

The research results show that involvement has a significant positive relationship with entrepreneurs' behavioural intentions to protect trade secrets (β =o.142 P<0.039), which supports H10. This shows that entrepreneurs tend to be more bonded with team members', when they are more socially involved and thus more likely to protect trade secrets.

The research results show that personal norms have a significant positive relationship with entrepreneurs' behavioural intentions to protect trade secrets (β =o.214 P<0.006), which supports H11. This shows that entrepreneurs with appropriate personal values are more likely to engage in the protection of trade secrets. In addition, personal beliefs towards protection of trade secrets have a larger effect than involvement.

Therefore, the research findings confirm that entrepreneurs who possess strong bonds with team members will more likely perform protective security actions to protect the secrecy of trade secrets. Additionally, the research findings also confirm that entrepreneurs who have strong personal beliefs towards protecting trade secrets are more likely perform protective security actions to protect the secrecy of trade secrets. Thus, the research findings revealed that social bonding in terms of involvement and personal norms has a significant effect on entrepreneurs to protect the secrecy of trade secrets.

8.3. Meeting Research Objectives

In accomplishing any research, one of the most important aspects is meeting the research objectives. The research objectives for this thesis were defined in Chapter 1.

This section below describes how the research objectives were achieved to answer the research questions.

- Research Objective No. 1

To extend the existing body of knowledge, a systematic literature review was conducted in the field of cyber security behaviour to obtain insights and build an understanding of behavioural concepts and theories. This review adopted a rigorous structured approach to conducting the literature search process and analysis. This review included relevant publications in top academic journals in the field of cyber security behaviour. The output of the literature review resulted in valuable findings and insights. This included a comprehensive overview of the cyber security behaviour literature for the last decade. In addition, the chapter produced a concept matrix for the key cyber security theories in the literature. Furthermore, a concept matrix was produced to illustrate the analysis of the cyber security behaviour elements. Also, a concept map was developed to visualise these cyber security behaviour elements.

- Research Objective No. 2

This objective is to develop the research conceptual model for investigating the protection of trade secrets in a cyber security context. The concept that structured the conceptualisation of the research model was based on taking advantage of trade secret's dimensions to define their protection aspects. This involved developing a conceptual model that focused on confidentiality, ownership and secrecy protection. The conceptual model was theoretically constructed based on three theories: protection motivation, psychological ownership and social bonding. In addition, the underlying constructs of the conceptual model were identified and discussed. Also, the hypotheses representing the relationships between the model constructs were developed.

- Research Objective No. 3

To be able to achieve the remaining research objectives, a research design was developed for collecting the empirical research data. The research adopted a quantitative research method based on a deductive reasoning approach. The data collection method was based on an online questionnaire. In addition, a sampling process was conducted to obtain a reprehensive sample. A nonprobability sampling was chosen as a sampling procedure that is based on the researcher's judgment to select an appropriate sample size.

- Research Objective No. 4

The research instrument was developed to support the research hypotheses testing. The instruments were adopted and developed based on previously valeted scales in the field of cyber security behaviour. This was followed up with a pre-test involving a group of researchers to make sure that the wording of the survey instrument was clear. In addition, a reliability analysis was conducted to investigate internal consistency of the constructs' measures and an Exploratory Factor Analysis (EFA) was conducted using SPSS for validation.

- Research Objective No. 5

To perform a multivariate analysis, an assessment was conducted to prepare the quantitative data for analysis. This involved the identification of any issues related to the collected empirical data, such as missing data, outliers and data distribution. In addition, the assumptions of multivariate analysis were evaluated and common method bias was tested.

- Research Objective No. 6

The captured demographic information from the collected data were analysed. Descriptive statistics were used to understand the descriptive nature of the collected data through a frequency distribution examination. This included and illustration of graphics and charts to easily describe the descriptive statistics and demographic characteristic.

- Research Objective No. 7

The validity and reliability analysis of the measurement model was conducted. This included the assessment of the measurement model in terms of convergent validity and discriminate validity, in addition to the evaluation of internal consistency reliability for the measurement scales. The SmartPLS application was used for the PLS-SEM analysis.

- Research Objective No. 8

The evaluation of the structural model was conducted through PLS-SEM analysis. The analysis involved the examination of the model's capabilities to estimate the significance of the hypothesized relationships between the model constructs. A number of criteria were used to assess the structural model: the coefficient of determination (R^2), predictive relevance (Q^2) effect size, f^2 effect size and q^2effect size.

- Research Objective No. 9

The final research model for cyber security protection of trade secrets was defined. The factors that showed significant impact on the cyber security behaviour were identified. This was shown at the end of chapter 7 (see Figure 7.2.)

- Research Objective No. 10

Based on achieving the previous nine objectives, this objective was also achieved within this chapter. This involved presenting the key research findings and draw the research conclusions and present future research.

8.4.Research Contributions

This research makes several important contributions to the cyber security behaviour research domain by exploring new cyber security behaviour elements. In addition, this research has taken a first step toward a greater understanding of an essential cyber security aspect of entrepreneurs' behaviour to protect trade secrets. The research contributions are described below:

1- Conducted an up to date systematic literature review in cyber security behaviour:

This research conducted an up to date systematic literature review in cyber security behaviour. The review adopted a structured approach to identify the relevant literature and also the guidelines on rigorous literature. The analysis of this review presented new findings and insights that resulted in the development of a concept matrix illustrating the major cyber security behavior theories. In addition, based on the review output, a concept map and matrix were developed that illustrated the cyber security behavior elements.

2- Targeted entrepreneurs as new subjects of study in the cyber security behavioural domain:

This research is the first to study cyber security behaviour for entrepreneurs based on the identified related studies from the systematic literature review. Although a considerable growing body of research has been made in the cyber security behaviour domain, none has investigated entrepreneurs' cyber security behaviour. Thus, this research fills part of the knowledge gap in understanding the behaviour of entrepreneurs in the context of cyber security.

3- Investigated a dynamic environment as a new context in the cyber security behavioural domain:

From a context perspective, previous studies have limited their focus to cyber security in traditional work environments that have well defined and mature information security countermeasures. Therefore, they do not explore other new work environments that are more dynamic and do not have well defined and established cyber security countermeasures. This research explores a new context that is considered as an agile dynamic environment for innovation and creating new ventures.

4- Investigated trade secrets as a new intangible target in the cyber security behavioural domain:

From a target perspective, previous studies focused on tangible and intangible items as main targets of cyber security behaviour. However, in regards to studies focusing on intangibility as a behaviour target, most of these studies address security compliance behaviours of polices. In contrast, fewer studies gave attention to intangible assets such as information. This research focuses on trade secrets as a behavioural target for cyber security behaviour.

5- Developed a new comprehensive approach to explore cyber security protection of trade secrets:

This research developed a novel approach of exploring the intangible nature of trade secret protection in the context of cyber security. The foundation of this approach is based on the three dimensions of trade secrets: information, intellectual property and secrets. The protection of these dimensions was through three protection lenses: confidentiality of information, ownership of intellectual property and the secrecy of commercial secrets. Thus, this research takes a new approach to exploring the cyber security behaviour protection of trade secrets.

6- Developed a new conceptual model for trade secret protection in the cyber security behavioural domain:

This research developed a conceptual model that extends the existing academic literature in the field of cyber security behaviour research. Although several behavioural theories and models have been applied in previous studies to the cyber security context (Johnston et al., 2015; Anderson & Agarwal, 2010; Boss et al., 2015; Ifinedo, 2012; Herath & Rao, 2009; Posey et al., 2015; Safa et al., 2015), this research extends the extent work in three new important behaviour elements, as illustrated in Figure 8.3.

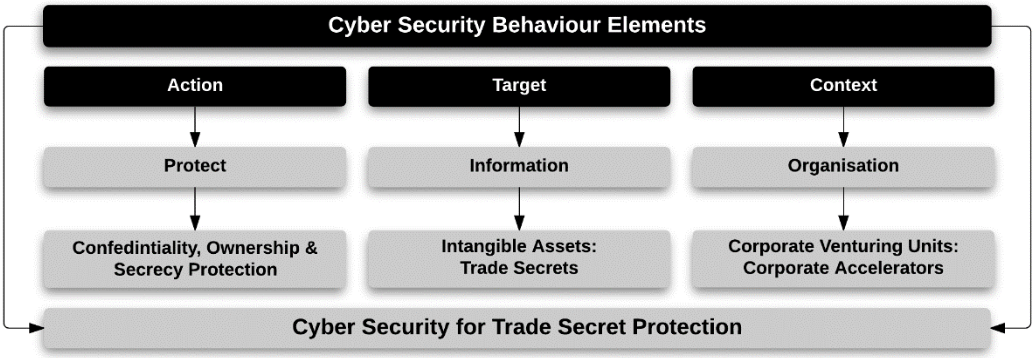

Cyber Security Behaviour Elements
Action
Target
Context
Protect
Information
Organisation
Confedintiality, Ownership & Secrecy Protection
Intangible Assets: Trade Secrets
Corporate Venturing Units: Corporate Accelerators
Cyber Security for Trade Secret Protection

Figure 8.2: Illustration of new cyber security behaviour elements

8.5. Research Limitations

Like any research, this research has a number of limitations and issues that are acknowledge in this section. The limitations of this research are as follows:

- Time limitation was the main issue in this research, where following procedures, gaining access to participants for data collection required a huge amount of time.
- Only top journals in cyber security behaviour were used in the systematic literature review, which might have not covered some relevant literature from other journals or conferences.
- Only key terms of information were used, so some relevant publications in the research field could be missing from the identified publications.
- Because of the complexity and diversity of the theories identified in the literature review, only a few were discussed. The research has a very small size of participants (138). This small sample size resulted in not being able to generalize the results.

- The data research was collected only from corporate accelerators in London, which also limited the number of participants.
- Direct access to entrepreneurs was not provided by corporate accelerators, which also limited the number of participants.
- The main collected data of this research is gathered by a self-reporting instrument, which might not capture participants' actual feelings or beliefs.

8.6. Future Research

Future research could consider exploring other concepts that are theoretically relevant to the protection of trade secrets. Similarly, although we examined protection motivation through threat and coping appraisal, future research should investigate other elements of protection motivation such as fear-appeal. In addition, investigating different moderation effects (e.g. age, education and work experience) on trade secret protection to understand its impact on entrepreneurs' cyber security behaviours. Additionally, other agile dynamic environment could be considered in future research such as innovation labs.

In regards to research design, this research used a single data collection method to gather and evaluate data, which is based on a quantitative approach. Future research, could consider using other data collection approaches. Moreover, using mixed methods by adding a qualitative data collection method could give a wider understanding for more in-depth research for similar context.

Another issue of interest for future research concerns the coping element of costs by investigating and identifying the types of costs that could impact the coping part of performing protective cyber security actions to protect trade secrets. A further issue concerns the ways that entrepreneurs weigh the costs in comparison to the ways they weigh benefits.

In regards to response rate and sample size, future research could try new ways to improve response rate and obtain a larger sample for generalisation. One possible approach is to target one company that has a number of accelerators in different geographical locations and try to obtain permission to have access communication with participants. Another approach would be through government agencies that support these types of accelerators to obtain official approval to support the research.

In regards to the literature review, further research interest could be in a broader systematic literature review to develop a more in-depth and detailed concept map of cyber security behaviour elements. This research was limited to a specific scope of research; therefore, other literature reviews could be built upon the results in this research, to develop a more comprehensive literature review that would include not only top journals in the research field but also top conference papers as well. In addition, a recommended future literature review could present a more in-depth analysis of the different theories related to cyber security behaviour.

8.7. Summary

Described as "the weakest link in the security chain" (Schneier, 2000. P.255), people are an essential core part of cyber security. While most research focuses on the technology and management aspects of cyber security, people are considered to be the most important aspect of them all. According to a statement by Emma W, the Leading People Centred Security at NCSC, "The way to make security that works is to make security that works for people. Because security that doesn't work for people, doesn't work." (2017). Therefore, focusing on the human factor in cyber security is based on the belief that people are the strongest link in the security chain.

The research results found statistically significant relationships for threat and coping appraisals and social bonding in relation to cyber security behavioural intentions to protect trade secrets. The findings provide insights for corporates managing corporate venturing units and attempt to develop and implement cyber security mechanisms to protect trade secrets among entrepreneurs whom may be faced with cyber threats during the venturing process. The empirical findings suggest that SEVandVUL, REF, COS, IVT and POE have an influence on entrepreneurs' cyber security behavioural intentions to perform protective security actions to protect trade secrets in a corporate accelerator. The research provides a new perspective in understanding cyber security behaviour to protect trade secrets. In addition, it provides a theoretical support and contribution to applying new protection avenue in the domain of cyber security behaviour.

The findings obtained in this research can guide corporates and entrepreneurs whose objectives are to protect trade secrets in corporate accelerators. First, the research findings confirm that trade secret protection can be viewed through three protection aspects and that it is important to encourage a positive behavioural intention toward performing protective cyber security actions. In this regard, perceiving trade secret protection as an effective activity can be achieved through confidentiality, ownership and secrecy protection.

To conclude, this research provides empirical evidence that the cyber security behaviour can influence the protection of trade secrets through three protection aspects to provide a more comprehensive protection of trade secrets. The contribution of this research is summarised in Figure 8.4, which presents an overview of the significant factors influencing the cyber security protection of trade secrets in agile dynamic environments.

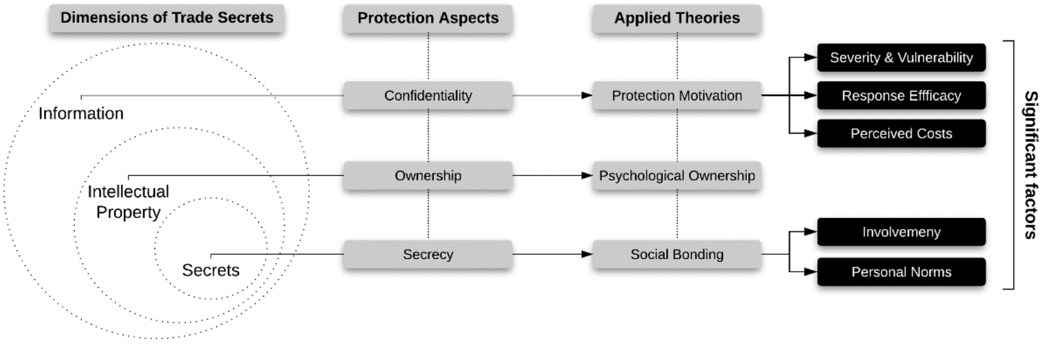


Figure 8.3: Overview the significant factors of the cyber security for trade secret protection

References

AIS (2010). MIS Journal Rankings [Online]. Available: https://aisnet.org/?JournalRankings. . Accessed June 27th, 2016

Ajzen, I. (1991). The theory of planned behaviour. *Organizational behavior and human decision processes*, **50**(2), pp.179-211.

Ajzen, I. (2012). Attitudes and persuasion, *The Oxford handbook of personality and social psychology*, pp.367-393.

Ajzen, I. and Fishbein, M. (1980). *Understanding attitudes and predicting social behaviour*. Prentice-Hall, 1980.

Ajzen, I. and Fishbein, M. (2005). *The influence of attitudes on behavior*, D. Albarracín, B. T. Johnson, & M. P. Zanna (eds.), The handbook of attitudes, Mahwah, NJ: Erlbaum,pp. 173-221.

Akerman et al.(2009). Unsecured economies report: protecting vital information. McAfee, Inc.: Santa Clara, CA.

Alkaersig, L. and Beukel, K. and Reichstein, T (2015). *Intellectual property rights management: rookies, dealers and strategists*. Palgrave Macmillan.

Almeling, D. (2012). Seven reasons why trade secrets are increasingly important. *Berkeley Technology Law Journal*, **27**(2), pp.1091-1117.

Al-Mukahal,H. and Alshare, K. (2015). An examination of factors that influence the number of information security policy violations in Qatari organizations, *Information & Computer Security*, **23**(1), pp.102-118.

Anderson, C. and Agarwal, R. (2010). Practicing safe computing: a multimethod empirical examination of home computer user security behavioral intentions, *MIS Quarterly*, **34**(3), pp. 613.

Antoncic, B. and Hisrich, R.D. (2001). Intrapreneurship: construct refinement and cross-cultural validation. *Journal of business venturing*, **16** (5), pp.495-527.

Aurigemma, S. and Panko, R. (2012). A composite framework for behavioral compliance with information security policies, proceeding of *45th Hawaii International Conference,* pp. 3248-3257.

Axelrod, L. and Newton, J. (1991). Preventing nuclear war: beliefs and attitudes as predictors of disarmist and deterrentist behaviour. *Journal of Applied Social Psychology*, **21**(1), pp.29-40.

Baker, M. (2000). Writing a literature review. *The Marketing Review*, **1**(2), pp.219-247.

Bandura, A. (1977). Self-efficacy: toward a unifying theory of behavioral change. *Psychological review*, **84**(2), p.191.

Battistini, B., Hacklin, F. and Baschera, P. (2013). The state of corporate venturing: Insights from a Global Study. *Research-Technology Management*, **56**(1), pp.31-39.

Becker, G. (1968). Crime and punishment: An economic approach, in *the Economic Dimensions of Crime.* Palgrave Macmillan UK, pp. 13-63.

Bem, D. (1995). Writing a review article for psychological bulletin. *Psychological Bulletin*, **118**(2), pp. 172-177.
Block, J., et al. (2014). Trademarks and venture capital valuation. *Journal of business venturing*, **29** (4), pp.525-542.

Bloom, M. (2006). Subpoenaed sources and the Internet: a test for when bloggers should reveal who misappropriated a trade secret. *Yale Law & Policy Review*, **24**(2), pp.471-483.

Boldrin, M and Levine, D. (2008). Against intellectual monopoly. Cambridge University Press.

Boss, S., et al. (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, **18**(2), pp.151-164.

Boss, S., et al. (2015). What do users have to fear? using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly,* **39**(4), pp.837-864.

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness*. MIS Quarterly*, **34**(3), pp.523-548.

Burgelman, R. A.(1983). Corporate entrepreneurship and strategic management: Insights from a process study. *Management science*, **29**(12), pp.1349-1364.

Chen, Y. and Zahedi, F.M. (2016). Individuals' Internet Security Perceptions and Behaviors: Polycontextual Contrasts Between the United States and China. *MIS Quarterly*, **40**(1), pp. 205.

Cheng, L., et al. (2013). Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory. *Computers & Security*, **39**, pp.447-459.

Chesbrough, H., (2012). Open innovation: Where we've been and where we're going. *Research-Technology Management*, **55**(4), pp.20-27.

Chin, W.W.(1998). The partial least squares approach to structural equation modeling. *Modern methods for business research*, ***295***(2), pp.295-336.

Chou, H.L. and Chou, C., 2016. An analysis of multiple factors relating to teachers' problematic information security behavior. *Computers in Human Behavior*, **65**, pp.334-345.

Christiansen, J. A (2013). Database of seed accelerators and their companies. Available at: www.seed-db.com. Accessed 13 April 2016.

CNN. (2013). New startups prime targets for cyberattacks. Available at: http://money.cnn.com/2013/05/23/technology/startup-cyberattack/. Accessed 20 April 2016.

Cohen, P.R. and Levesque, H.J. (1987). Intention = choice + commitment. In *Proceedings of the sixth National conference on Artificial intelligence - **2*** (AAAI'87), Vol. 2. AAAI Press 410-415.

Cohen, S. and Hochberg, Y.V. (2014). Accelerating startups: the seed accelerator phenomenon. Available at: https://ssrn.com/abstract=2418000

Costello, A.B. and Osborne, J.W. (2005). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Practical assessment, research & evaluation*, ***10***(7), pp.1-9.

Create.org and PwC, (2014). Economic Impact of Trade Secret Theft: A framework for companies to safeguard trade secrets and mitigate potential threats. Available at: https://create.org/resource/economic-impact-of-trade-secret-theft/. Accessed 04 April 2016.

Crittenden, W.F., Crittenden, V.L. and Pierpont, A. (2015). Trade secrets: Managerial guidance for competitive advantage. *Business Horizons*, **58**(6), pp.607-613.

Cronbach, L.J.(1951). Coefficient alpha and the internal structure of tests. Psychometrika, **16**(3), pp. 297-334.

Dang-Pham, D. and Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A Protection Motivation Theory approach. *Computers & Security*, **48**, pp.281-297.

D'Arcy, J. and Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, **22**(5)**,** pp.474-489.

D'Arcy, J., Herath, T. and Shoss, M.K. (2014). Understanding employee responses to stressful information security requirements: a coping perspective. *Journal of Management Information Systems*, **31**(2), pp.285-318.

D'Arcy, J., Hovav, A. and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, **20**(1), pp.79-98.

D'Arcy, J., Hovav, A. and Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, **20**(1), pp.79-98.

Detica. (2011). The Cost of the Cyber Crime. Guildford. Accessed 23 March 2016. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf.

Dushnitsky, G. (2015). Corporate Adventure in Venture. Venture Findings, 2, pp.104-110.

Engel, J. S. (2011). Accelerating corporate innovation: Lessons from the venture capital model. *Research-Technology Management*, **54**(3), pp. 36-43.

Engle, D.E., Mah, J.J. and Sadri, G. (1997). An empirical comparison of entrepreneurs and employees: Implications for innovation. *Creativity Research Journal,* **10**(1), pp.45-49.

Falk, R.F. and Miller, N.B. (1992). *A primer for soft modeling*. University of Akron Press.

Fayolle, A. and Wright, M. (2014). How to get published in the best entrepreneurship journals: a guide to steer your academic career. Edward Elgar Publishing.

Field, A. (2009). Discovering statistics using SPSS. London: SAGE.

Field, A. (2009). Discovering statistics using SPSS. Sage publications.

Fishbein, M. and Ajzan, I. (1975). *Belief, attitude, intention and behavior: An introduction to theory and research*. Addison-Wesley, 1975.

Fishbein, M. and Ajzen, I. (2011). Predicting and changing behavior: the reasoned action approach. Taylor & Francis.

Flores, W.R. and Ekstedt, M. (2016). Shaping intention to resist social engineering through transformational leadership, information security culture and awareness. *Computers & Security*, **59**, pp.26-44.

Flores, W.R., Antonsen, E. and Ekstedt, M. (2014). Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture. *Computers & Security*,**43**, pp.90-110.

Floyd, D.L., Prentice-Dunn, S. and Rogers, R.W. (2000). A meta-analysis of research on protection motivation theory. *Journal of applied social psychology*, ***30***(2), pp.407-429.

Fornell, C. and Larcker, D.F. (1981). Structural equation models with unobservable variables and measurement error: Algebra and statistics. *Journal of marketing research*, pp.382-388.

Fornell, C., and Larcker, D. F. (1981). Evaluating structural equations with unobservable variables and measurement error. *Journal of Marketing Research,* **18**(1), pp. 39-50.

Forrester Research, Inc. (2010). The Value of Corporate Secrets: How Compliance and Collaboration Affect Enterprise Perceptions of Risk. Available at: www.nsi.org/pdf/reports/The%20Value%20of%20Corporate%20 Secrets.pdf. Accessed 29 March 2016.

Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behaviour and deterrence. *European Journal of Information Systems*, **25**(2), pp. 91-109.

Future Asia Ventures. (2016). Corporate accelerators & booming startup sectors. [Online]. Available at: http://www.futureasiaventures.com/reports.html. Accessed 13 April 2016.

Garvin, D. A. (2004). What every CEO should know about creating new businesses. *Harvard Business Review,* **82**(7/8), pp.18-21.

Gill, J. and Johnson, P. (2010). *Research methods for managers*. Sage.

Gliem, J.A. and Gliem, R.R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. Midwest Research-to-Practice Conference in Adult, Continuing, and Community Education.

Gollin, M. A. (2008). Driving innovation: intellectual property strategies for a dynamic world. Cambridge University Press.

Gravetter, F. and Wallnau, L. (2014) *Essentials of statistics for the behavioral sciences* , 8th Edition edn., Belmont, CA: Wadsworth.

Gummesson, E. (2000). Qualitative methods in management research. Sage Publications.

Gündoğdu, M.Ç. (2012). Re-thinking entrepreneurship, intrapreneurship, and innovation: a multi-concept perspective. *Procedia-Social and Behavioral Sciences*, **41**, pp.296-303.

Guo, K.H., Yuan, Y., Archer, N.P. and Connelly, C.E. (2011). Understanding nonmalicious security violations in the workplace: a composite behavior model. *Journal of Management Information Systems*, **28**(2), pp.203-236.

Gurung, A., Luo, X. and Liao, Q. (2009). Consumer motivations in taking action against spyware: an empirical investigation. *Information Management & Computer Security*, **17**(3), pp.276-289.

Guth, W.D. and Ginsberg, A. (1990). Guest editors' introduction: Corporate entrepreneurship. *Strategic management journal*, pp.5-15.

Hair et al (2014) state that principle component and common factor analysis are two principals of exploratory factor analysis.

Hair Jr, J.F., Hult, G.T.M., Ringle, C. and Sarstedt, M. (2016b). *A primer on partial least squares structural equation modeling (PLS-SEM)*. Sage Publications.

Hair Jr, J.F., Wolfinbarger, M., Money, A.H., Samouel, P. and Page, M.J. (2016a). *Essentials of Business Research Methods*. Routledge.

Hair, J., Hollingsworth, C.L., Randolph, A.B., and Chong, A.Y.L., 2017. An updated and expanded assessment of PLS-SEM in information systems research. *Industrial Management & Data Systems*, *117*(3), pp.442-458.

Hair, J.F., Black, W.C., Babin, B.J. and Anderson, R.E., 2014. Multivariate data analysis (Pearson new internat. ed). *Harlow: Pearson*.

Hair, J.F., Ringle, C.M. and Sarstedt, M., 2011. PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice*, *19*(2), pp.139-152.

Hair, J.F., Sarstedt, M., Ringle, C.M. and Mena, J.A., 2012. An assessment of the use of partial least squares structural equation modeling in marketing research. *Journal of the academy of marketing science*, **40**(3), pp.414-433.

Halt Jr, G.B., Fesnak, R., Donch, J.C. and Stiles, A.R. (2014). Trade Secret Protection. In Intellectual Property in Consumer Electronics, Software and Technology Startups, pp. 25-32. Springer: New York.

Hayton, J.C. (2005a). Competing in the new economy: the effect of intellectual capital on corporate entrepreneurship in high-technology new ventures. *R&D Management*, **35**(2), pp.137-155.

Hayton, J.C. (2005b). Promoting corporate entrepreneurship through human resource management practices: A review of empirical research. *Human Resource Management Review*, **15**(1), pp.21-41.

Hemphill, T. A. (2004). The strategic management of trade secrets in technology-based firms. *Technology Analysis and Strategic Management*, **16**(4), 479- 494.

Henry, C., & Treanor, L. (2013). Where to now? New directions in supporting new venture creation. *Journal of Small Business and Enterprise Development,* **20**(2), 249-257.

Herath, T. and Rao, H. R. (2009a). Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems*, **18**, pp. 106-125.

Herath, T. and Rao, H.R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, **47**(2), pp.154-165.

Hirschi, T. and Stark, R. (1969). Hellfire and delinquency. *Social Problems*, **17**(2), pp.202-213.

Hochberg, Y.V. (2015). Accelerating entrepreneurs and ecosystems: the seed accelerator model. *In Innovation Policy and the Economy*, **16**. University of Chicago Press.

Hovav, A. and D’Arcy, J. (2012). Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management*, **49**(2), pp.99-110.

Hovland, C.I., Janis, I.L. and Kelley, H.H. (1953). Communication and persuasion; psychological studies of opinion change.

Hu, Q., Dinev, T., Hart, P. and Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, **43**(4), pp.615-660.

Hu, Q., Xu, Z., Dinev, T. and Ling, H. (2011). Does deterrence work in reducing information security policy abuse by employees?. *Communications of the ACM*, **54**(6), pp.54-60.

Hulme, E.W. (1896). The History of the Patent System under the Prerogative and at Common Law'. LQR, 12, p.141.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, **31**(1), pp.83-95.

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, **51**(1), pp.69-79.

International Standards Office, 2013. ISO/IEC 27001:2013: Information Security Management Systems - Requirements.

International Standards Office, 2016. ISO/IEC 27000:2016: Information technology - Security techniques – Information security management systems - Overview and vocabulary.

Johnston, A. C., and Warkentin, M. (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. *MIS Quarterly,* **34**(3), pp. 548-566.

Johnston, A.C., Warkentin, M. and Siponen, M.T.(2015). An Enhanced Fear Appeal Rhetorical Framework: Leveraging Threats to the Human Asset Through Sanctioning Rhetoric. *MIS Quarterly*, **39**(1), pp.113-134.

Johnston, A.C., Warkentin, M., Mcbride, M. and Carter, L. (2016). Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems*, **25**(3), pp. 231-251.

Kerlinger, F.N. and Lee, H.B. (2000). Survey research. *Foundations of behavioral research*, pp.599-619.

Kline, P. (1999). A Handbook of Psychological Testing, 2nd edn. London: Routledge.

Kline, R. B. (2012). Assumptions of structural equation modeling. In R. Hoyle (Ed.), Handbook of structural equation modeling (pp. 111-125). New York: Guilford Press.

Kline, R. B. (2013). Exploratory and confirmatory factor analysis. In Y. Petscher & C. Schatsschneider (Eds.), Applied quantitative analysis in the social sciences (pp. 171-207). New York: Routledge.

Kohler, T. (2016). Corporate accelerators: Building bridges between corporations and startups. *Business Horizons*, **59**(3), pp.347-357.

Krejcie, R.V. and Morgan, D.W. (1970). Determining Sample Size for Research Activities. Educational and Psychological Measurement, **30** (3), pp. 607-610.

Kuiper, C. and Van Ommen, F (2015). Corporate venturing: managing the innovation family in a dynamic world. 1st ed. Nijmegen: VOC Uitgevers.

Kuratko, D. F. and Audretsch, D. B. (2013). Clarifying the domains of corporate entrepreneurship. *International Entrepreneurship and Management Journal*, **9**(3), pp. 323-335.

Kuratko, D. F., Hornsby, J. S. and Hayton, J. (2015). Corporate entrepreneurship: the innovative challenge for a new global economic reality. *Small Business Economics*, **45**(2), pp.1-9.

Lai, F., Li, D. and Hsieh, C.T. (2012). Fighting identity theft: The coping perspective. *Decision Support Systems*, ***52***(2), pp.353-363.

LaRose, R., Rifon, N. J., and Enbody, R. (2008). Promoting personal responsibility for internet safety. *Communications of the ACM,* **51**(3), pp. 71-76.

Lebek, B., Uffen, J., Neumann, M., Hohler, B. and H. Breitner, M. (2014). Information security awareness and behavior: a theory-based literature review. *Management Research Review*, ***37***(12), pp.1049-1092.

Lee, S.M., Lee, S.G. and Yoo, S. (2004). An integrative model of computer abuse based on social control and general deterrence theories. *Information & Management*, **41**(6), pp.707-718.

Lee, Y. and Larsen, K.R. (2009). Threat or coping appraisal: determinants of SMB executives' decision to adopt anti-malware software. *European Journal of Information Systems*, **18**(2), pp. 177-187.

Lerner, J. (2013). Corporate venturing. *Harvard Business Review*, **91**(10), pp. 86-94.

Levy, Y. and Ellis, T.J. (2006). A systems approach to conduct an effective literature review in support of information systems research. *Informing Science: International Journal of an Emerging Transdiscipline*, ***9***(1), pp.181-212.

Li, H., Zhang, J. and Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, **48**(4), pp.635-645.

Li, H., Zhang, J. and Sarathy, R. (2010). Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems*, **48**(4), pp.635-645.

Lindell, M.K. and Whitney, D.J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of applied psychology*, **86**(1), p.114.

Lowry, P.B. and Gaskin, J., 2014. Partial least squares (PLS) structural equation modeling (SEM) for building and testing behavioral causal theory: When to choose it and how to use it. *IEEE Transactions on Professional Communication*, *57*(2), pp.123-146.

Lynn, R. (1991). The secret of the miracle economy: Different national attitudes to competitiveness and money. Social Affairs Unit.

MacMillan, I. C., Block, Z., and Narasimha, P. S. (1986). Corporate venturing: alternatives, obstacles encountered, and experience effects. *Journal of Business Venturing*, **1**(2), 177-191.

Maddux, J.E. and Rogers, R.W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of experimental social psychology*, ***19***(5), pp.469-479.

Malhotra, N.K., Kim, S.S. and Patil, A. (2006). Common method variance in IS research: a comparison of alternative approaches and a reanalysis of past research. *Management science*, **52**(12), pp.1865-1883.

Mancuso, V.F., Strang, A.J., Funke, G.J. and Finomore, V.S. (2014). Human factors of cyberattacks a framework for human-centered research. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting (Vol. 58, No. 1, pp. 437-441). SAGE Publications.

Mawson, J. (2011). Corporate venturing enters its golden age. Private equity news. [Online] Available at: www.penews.com/today/index/content/4068295507 . Accessed 23 March 2016.

Mesly, O. (2015. *Creating Models in Psychological Research*. Springer.

Mishra, S. and Dhillon, G. (2006). Information systems security governance research: a behavioral perspective. In *1st Annual Symposium on Information Assurance, Academic Track of 9th Annual NYS Cyber Security Conference*, pp. 27-35.

Moberly, M.D.(2014). Safeguarding Intangible Assets. Butterworth-Heinemann.

Morris, M.H., Kuratko, D.F. and Covin, J.G. (2010). Corporate entrepreneurship & innovation. Cengage Learning.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. and Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. *European Journal of Information Systems*, **18**(2), pp. 126-139.

Ng, B.Y., Kankanhalli, A. and Xu, Y.C. (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, **46**(4), pp.815-825.

Niehaves, B. and Stahl, B.C.(2006). Criticality, epistemology and behaviour vs. Design-information systems research across different sets of paradigms. In *ECIS* (pp. 50-61).

Ocean Tomo (2015). Annual Study of Intangible Asset Market Value from Ocean Tomo, LLC. [Online]. Available at: http://www.oceantomo.com/2015/03/04/2015-intangible-asset-market-value-study/. Accessed 29 March 2016.

Office for National Statistics. (2016). Business demography, UK: 2015 (p. 6). London: Office for National Statistics.

Ozaralli, N. and Rivenburgh, N.K. (2016). Entrepreneurial intention: antecedents to entrepreneurial behavior in the USA and Turkey. *Journal of Global Entrepreneurship Research*, **6**(1), pp.1-32.

Pajunen, K. (2008). Institutions and inflows of foreign direct investment: a fuzzy-set analysis. *Journal of International Business Studies.* **39**(4), pp.652-669.

Pallant, J. (2010). SPSS survival manual: A step by step guide to data analysis using SPSS (4th ed). New York: Open University Press.

Pauwels, C., Clarysse, B., Wright, M. and Van Hove, J. (2016). Understanding a new generation incubation model: The accelerator. *Technovation*, **50**, pp.13-24.

Pechmann, C., Zhao, G., Goldberg, M.E. and Reibling, E.T. (2003). What to convey in antismoking advertisements for adolescents: The use of protection motivation theory to identify effective message themes. *Journal of Marketing*, **67**(2), pp.1-18.

Petticrew, M. and Roberts, H. (2008). *Systematic reviews in the social sciences: A practical guide*. John Wiley & Sons.

Pfleeger, C.P. and Pfleeger, S.L. (2002). *Security in computing*. Prentice Hall Professional Technical Reference.

Phan, P. H., Wright, M., Ucbasaran, D. and Tan, W. L. (2009). Corporate entrepreneurship: Current research and future directions. *Journal of Business Venturing*, **24**(3), pp.197-205.

Phillips, M. (2015). Facebook is now worth more than Walmart. Quartz [Online]. Available at: http://qz.com/428524/facebook-is-now-worth-more-than-walmart/ . Accessed 20 April 2016]

Pinchot III, G. (1985). Intrapreneuring: Why you don't have to leave the corporation to become an entrepreneur. University of Illinois at Urbana-Champaign's Academy for Entrepreneurial Leadership Historical Research Reference in Entrepreneurship.

Plotnikoff, R.C. and Higginbotham, N. (1998). Protection motivation theory and the prediction of exercise and low-fat diet behaviours among Australian cardiac patients. *Psychology and Health*, ***13***(3), pp.411-429.

Podsakoff, P.M., MacKenzie, S.B., Lee, J.Y. and Podsakoff, N.P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology*, **88**(5), p.879.

Pooley, J. (2013). Trade Secrets: the other IP right. WIPO Magazine. (3), pp.2-4.

Pooley, J. (2015). SECRETS: Managing Information Assets in the Age of Cyberespionage. Menlo Park: Verus Press.

Posey, C., Roberts, T.L. and Lowry, P.B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, **32**(4), pp.179-214.

Posey, C., Roberts, T.L. and Lowry, P.B. (2015). The Impact of Organizational Commitment on Insiders' Motivation to Protect Organizational Information Assets. *Journal of Management Information Systems*, **32**(4), pp.179-214.

Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure, COM (2013) 0402, final.

PwC. (2015). Information security breaches survey. Available at: http://www.pwc.co.uk/assets/pdf/2015-isbs-executive-summary-02.pdf. Accessed 23 March 2016.

Refsdal, A., Solhaug, B. and Stølen, K. (2015). Cyber-risk management. In *Cyber-Risk Management,* pp. 33-47. Springer International Publishing.

Reis, E. (2011). *The lean startup*. New York: Crown Business.

Rhee, H.S., Kim, C. and Ryu, Y.U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers & Security*, **28**(8), pp.816-826.

Ringal, M., Taylor, A. and Zablit, H. (2017). The Most Innovative Companies 2016: Getting Past "Not Invented Here,". [online] Boston: Boston Consulting Group. Available at: https://media-publications.bcg.com/MIC/BCG-The-Most-Innovative-Companies-2016-Jan-2017.pdf. Accessed 18 February.

Ringle, C. M., Wende, S., and Will, A. (2005). Smart PLS 2.0, University of Hamburg, Hamburg, Germany (http://www.smartpls.de).

Ringle, Christian M., Wende, Sven, & Becker, Jan-Michael. (2015). SmartPLS 3. Bönningstedt: SmartPLS. Retrieved from http://www.smartpls.com

Robertson, K.M., Hannah, D.R. and Lautsch, B.A. (2015). The secret to protecting trade secrets: How to create positive secrecy climates in organizations. *Business Horizons*, **58**(6), pp.669-677.

Rogers, R.W. (1975). A protection motivation theory of fear appeals and attitude change1. *The journal of psychology*, ***91***(1), pp.93-114.

Rohrmann, B. (1997). Risk orientation questionnaire: attitudes towards risk decisions (pre-test version). Melbourne: Non-published manuscript, University of Melbourne.

Rotter, J.B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological monographs: General and applied*, ***80***(1), p.1.

Rowe, E.A. (2016). RATs, TRAPs, and Trade Secrets. *BCL Rev.*, ***57***, p.381.

Safa, N.S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N.A. and Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, **53**, pp.65-78.

Safa, N.S., Von Solms, R. and Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, **56**, pp.70-82.

Saunders, M., Lewis, P. and Thornhill, A. (2009). Research methods for business students.

Schafer, R.M. (1993). *The soundscape: Our sonic environment and the tuning of the world*. Inner Traditions/Bear & Co.

Schmitt, T.A. (2011). Current methodological considerations in exploratory and confirmatory factor analysis. *Journal of Psychoeducational Assessment*, ***29***(4), pp.304-321.

Schneier, B., 2000. Secrets & Lies: Digital Security in a Networked World, John Wiley & Sons. *Inc. New York, NY, USA*.

Sharma, P. and Chrisman, J.J. (1999). Toward a reconciliation of the definitional issues in the field of corporate entrepreneurship. *Entrepreneurship Theory and Practice*, **23**(3), pp.11–27.

Shropshire, J., Warkentin, M. and Sharma, S. (2015). Personality, attitudes, and intentions: predicting initial adoption of information security behaviour. Computers & Security, **49**, pp.177-191.

Simmel, G. (1906). The sociology of secrecy and of secret societies. *American journal of sociology*, **11**(4), pp.441-498.

Siponen, M., and Vance, A. (2010). Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations. *MIS Quarterly*, **34**(3), pp. 487-502.

Siponen, M., Mahmood, M.A. and Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & management, **51**(2), pp.217-224.

Sommestad, T., Karlzén, H. and Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, **23**(2), pp.200-217.

Sommestad, T., Karlzén, H. and Hallberg, J. (2015). The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security*, ***23***(2), pp.200-217.

Son, J.Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management*, **48**(7), pp.296-302.

Steinbart, P.J., Keith, M.J. and Babb, J. (2016). Examining the continuance of secure behavior: a longitudinal field study of mobile device authentication. *Information Systems Research*, **27**(2), pp.219-239.

Sullivan, G.M. and Feinn, R.(2012). Using effect size—or why the P value is not enough. *Journal of graduate medical education*, ***4***(3), pp.279-282.

Sykes, G.M. and Matza, D. (1957). Techniques of neutralization: A theory of delinquency. *American sociological review*, ***22***(6), pp.664-670.

Tanner Jr, J.F., Hunt, J.B. and Eppright, D.R.(1991). The protection motivation model: A normative model of fear appeals. *The Journal of Marketing*, **55**(3), pp.36-45.

The Corporate Accelerator Database. (2016). Database of corporate accelerators [Online]. Retrieved January 30, 2017, from: https://corporate-accelerators.net/database/index.html

Thomas, W.I. and Znaniecki, F. (1918). *The Polish peasant in Europe and America: Monograph of an immigrant group,* **2**, University of Chicago Press.

Trochim, W. and Donnelly, J., 2006. The research knowledge methods base. *Cincinnati, OH: Atomic Dog Publishing*.

Trochim, W.M. and Donnelly, J.P. (2001). Research methods knowledge base.

Tsai, H.Y.S., Jiang, M., Alhabash, S., LaRose, R., Rifon, N.J. and Cotten, S.R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security*, **59,** pp.138-150.

UK cyber security: the role of insurance in managing and mitigating the risk. (2015). [Online]. London. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/415354/UK_Cyber_Security_Report_Final.pdf. Accessed 23 March 2016.

Uniform Law Commission (1985). National Conference of Commissioners on Uniform State Laws: Uniform trade secrets act. [Online]. Available at: http://www.uniformlaws.org/shared/docs/trade%20secrets/utsa_final_85.pdf . Accessed 29 March 2016.

Vance, A., Lowry, P.B. and Eggett, D. (2013). Using accountability to reduce access policy violations in information systems. *Journal of Management Information Systems*, **29**(4), pp.263-290.

Vance, A., Siponen, M. and Pahnila, S. (2012). Motivating IS security compliance: insights from habit and protection motivation theory. *Information & Management*, **49**(3), pp.190-198.

Vaughan, E. (1993). Chronic exposure to an environmental hazard: risk perceptions and self-protective behavior. *Health Psychology*, ***12***(1), p.74.

Vela-McConnell, J.A. (2017). Behind closed doors: organizational secrecy, stigma, and sex abuse within the catholic church. In *Oppression and Resistance: Structure, Agency, Transformation* (pp. 19-49). Emerald Publishing Limited.

Villasenor, J. (2015). Corporate Cybersecurity Realism: Managing Trade Secrets in a World Where Breaches Occur. *American Intellectual Property Law Association Quarterly Journal,* **43**(2/3).

Vom Brocke, J., Simons, A., Niehaves, B., Riemer, K., Plattfaut, R. and Cleven, A. (2009). Reconstructing the giant: On the importance of rigour in documenting the literature search process. In *ECIS,* **9**, pp. 2206-2217.

W, E. 2017. People: The Strongest Link. [Online]. 15 March, CYBERUK 2017, Liverpool. [Accessed 19 July 2017]. Available from: https://www.youtube.com/watch?v=u6x9C7t_41s

Wales, W.J. (2016). Entrepreneurial orientation: A review and synthesis of promising research directions. *International Small Business Journal*, ***34***(1), pp.3-15.

Warkentin, M., Johnston, A.C. and Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, **20**(3), pp. 267-284.

Warren, M. (2015). Modern IP theft and the insider threat. *Computer Fraud & Security*, **2015**(6), pp.5-10.

Watson, J.B.(1925). What the nursery has to say about instincts. *The Pedagogical Seminary and Journal of Genetic Psychology*, **32**(2), pp.293-326.

Webster, J. and Watson, R.T. (2002). Analyzing the past to prepare for the future: Writing a literature review. *MIS Quarterly*, ***26***(2), p.R13.

Weiblen, T. and Chesbrough, H.W. (2015). Engaging with startups to enhance corporate innovation. *California Management Review*, **57**(2), pp.66-90.

Wilson, J. (2014). *Essentials of business research: A guide to doing your research project*. Sage.

WIPO. (2004). WIPO Intellectual Property Handbook: Policy, Law and Use. Geneva: WIPO publication, (489).

Witte, K. (1992). Putting the fear back into fear appeals: The extended parallel process model. *Communications Monographs*, ***59***(4), pp.329-349.

Witte, K. (1996). Predicting risk behaviors: development and validation of a diagnostic scale. *Journal of health communication*, **1**(4), pp.317-342.

Witte, K. and Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health education & behavior*, **27**(5), pp.591-615.

Wolcott, R. C. and Lippitz, M. J. (2007). The four models of corporate entrepreneurship. *MIT Sloan Management Review*, **49**(1), pp.75.

Workman, M., Bommer, W., and Straub, D. (2008). Security Lapses and the Omission of Information Security Measures: An Empirical Test of the Threat Control Model. *Journal of Computers in Human Behavior*, **24**(6), pp. 2799-2816.

Workman, M., Bommer, W.H. and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, ***24***(6), pp.2799-2816.

Workman, M., Bommer, W.H. and Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior*, **24**(6), pp.2799-2816.

Zhang, J., Reithel, B.J. and Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management & Computer Security*, **17**(4), pp.330-340.

Zikmund, W.G. (2003). Business research methods. Thomson South-Western publications.

Zimmerman, B.J., Bandura, A. and Martinez-Pons, M. (1992). Self-motivation for academic attainment: The role of self-efficacy beliefs and personal goal setting. *American educational research journal*, **29**(3), pp.663-676.

Appendix A: Questionnaire

You are being invited to participate in a research study. The purpose of this research study is to investigate the impact of cyber security behaviour on protecting trade secrets in new ventures within a corporate accelerator, and will take you approximately 10 to 15 minutes to complete. Your participation in this study is entirely voluntary, and you can withdraw at any time.

Demographic Information

The demographic information in this section will only be used in aggregate form, and will not be used to identify individual respondents. Please select only one item in each category.

Gender

○ Male
○ Female
○ Other.. _______________
○ Prefer not to say

Age

○ 18 to 29
○ 30 to 39
○ 40 to 49
○ 50 to 59
○ 60 and over

Education

❍ High school
❍ Diploma
❍ Bachelor
❍ Master
❍ Doctorate
❍ Other.. _______________

Experience (in starting and managing a new venture)

❍ < 6 months
❍ > 6 to < 12 months
❍ > 1 to < 2 years
❍ > 2 to < 3 years
❍ More than 3 years
❍ No previous experience

Established Ventures (the number of new ventures that you have started)

❍ None
❍ One
❍ Two
❍ Three
❍ More than three

Important Definitions

Trade secrets: refers to your start-up's confidential information (secret sauce) including any type of information that is not disclosed to the public and gives your start-up a competitive advantage in the marketplace.

Examples of trade secrets:

- Industrial design (e.g. iPhone 8)
- Software algorithm (e.g. pricing algorithms)
- Chemical formula (e.g. Coca-Cola)
- Blueprints or prototypes
- Customer lists

Cyber security threats: include any type of attacks (e.g. theft, hack, leakage, disclosure, etc.) that could put your venture's trade secrets at risk.

Performing protective cyber security actions: means taking one or more cyber security countermeasures to reduce the risk of cyber security attacks on your venture's trade secrets.

Examples of cyber security protective actions:

- Keeping information "secret" or "confidential".
- Signing confidentiality (nondisclosure) agreements.
- Installing antivirus software and firewalls.
- Encrypting electronic documents or information.

Thinking of your future actions, indicate the degree to which you agree or disagree with the following statements regarding your likelihood of taking protective cyber security actions to protect YOUR VENTURE'S TRADE SECRETS from an attack.

1-Psychological Ownership							
	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
This is my venture and my trade secrets.	○	○	○	○	○	○	○
I feel a high degree of personal ownership for my venture's trade secrets.	○	○	○	○	○	○	○
I sense that these are my trade secrets.	○	○	○	○	○	○	○

2- Reward							
	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
Not performing protective cyber security actions toward trade secrets saves me time.	○	○	○	○	○	○	○
Not performing protective cyber security actions toward trade secrets saves me money.	○	○	○	○	○	○	○
Not performing protective cyber	○	○	○	○	○	○	○

security actions toward trade secrets keeps me from being confused.							
Not performing protective cyber security actions toward trade secrets requires less effort of me.	○	○	○	○	○	○	○
Not performing protective cyber security actions toward trade secrets makes me feel less stressful.	○	○	○	○	○	○	○

3- Vulnerability

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
My venture’s trade secrets are vulnerable to cyber security threats.	○	○	○	○	○	○	○
It is likely that a cyber security attacks will occur against my venture’s trade secrets.	○	○	○	○	○	○	○
My venture’s trade secrets are at risk to cyber security threats.	○	○	○	○	○	○	○
My venture’s trade secrets are vulnerable to cyber security threats.	○	○	○	○	○	○	○

4- Severity

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
Cyber threats to the security of my venture’s trade secrets are severe.	○	○	○	○	○	○	○
In terms of cyber threats, attacks on my venture’s trade secrets are severe.	○	○	○	○	○	○	○
I believe that cyber threats to the security of my venture’s trade secrets are serious.	○	○	○	○	○	○	○
I believe that cyber threats to the security of my venture’s trade secrets are significant.	○	○	○	○	○	○	○

5- Response Efficacy

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
Efforts to keep my venture’s trade secrets safe from cyber threats are effective.	○	○	○	○	○	○	○

The available measures that can be taken to protect my venture’s trade secrets from security threats are effective.	❍	❍	❍	❍	❍	❍	❍
The preventive measures available to me to stop people from getting my venture’s trade secrets are adequate.	❍	❍	❍	❍	❍	❍	❍
If I perform the preventive cyber security measures available to me, my venture’s trade secrets are less likely to be exposed to a cyber threat.	❍	❍	❍	❍	❍	❍	❍

6- Self-Efficacy							
	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
For me, taking cyber security precautions to protect my venture's trade secrets is easy.	○	○	○	○	○	○	○
I have the necessary skills to protect my venture's trade secrets from cyber threats.	○	○	○	○	○	○	○
My skills in stopping cyber threats against my venture's trade secrets are adequate.	○	○	○	○	○	○	○
For me, taking cyber security precautions to protect my venture's trade secrets is easy.	○	○	○	○	○	○	○
I have the necessary skills to protect my venture's trade secrets from cyber threats.	○	○	○	○	○	○	○

7- Response Cost

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
The benefits of performing protective cyber security actions toward my venture’s trade secrets outweigh the costs (R).	❍	❍	❍	❍	❍	❍	❍
I would be discouraged from performing protective cyber security actions toward my venture’s trade secrets in the future because it would take too much time.	❍	❍	❍	❍	❍	❍	❍
The time taken to perform protective cyber security actions toward my venture’s trade secrets in the future would cause me too many problems.	❍	❍	❍	❍	❍	❍	❍
Taking protective cyber security actions would require considerable investment of effort as well as time.	❍	❍	❍	❍	❍	❍	❍

8- Behavioural Intentions

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
I am likely to take protective cyber security action to protect my venture’s trade secrets.	❍	❍	❍	❍	❍	❍	❍
It is possible that I will take protective cyber security action to protect my venture’s trade secrets.	❍	❍	❍	❍	❍	❍	❍
I am certain that I will take protective cyber security action to protect my venture’s trade secrets.	❍	❍	❍	❍	❍	❍	❍

9- Attachment

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
I usually have conversations about the protection of my venture’s trade secrets with team members.	❍	❍	❍	❍	❍	❍	❍
I respect my team members’ views and opinions about the protection of our venture’s trade secrets.	❍	❍	❍	❍	❍	❍	❍
I communicate the importance of protecting the venture’s trade secrets to team members.	❍	❍	❍	❍	❍	❍	❍

10- Commitment

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
I strongly believe that the protection of my venture’s trade secrets can help the venture to succeed.	❍	❍	❍	❍	❍	❍	❍
I am committed to protecting my venture 's trade secrets.	❍	❍	❍	❍	❍	❍	❍
I am willing to invest energy and effort in making the protection of my venture’s trade secrets a success.	❍	❍	❍	❍	❍	❍	❍
I am willing to put in a great deal of effort to help my venture succeed.	❍	❍	❍	❍	❍	❍	❍

11- Involvement

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
I value the opportunity to participate in informal meetings related to my venture's information security.	❍	❍	❍	❍	❍	❍	❍
I work on building personal relationships with team members in my venture in relation to trade secret concerns.	❍	❍	❍	❍	❍	❍	❍
I actively involve myself in activities related to my venture's growth.	❍	❍	❍	❍	❍	❍	❍

12- Personal norms

	Strongly disagree	Disagree	Somewhat disagree	Neutral	Somewhat agree	Agree	Strongly agree
It is a serious matter if I don't perform the protective cyber security actions to protect my venture's trade secrets.	❍	❍	❍	❍	❍	❍	❍
It is unacceptable not to perform ALL the protective cyber security actions to protect my venture's trade secrets.	❍	❍	❍	❍	❍	❍	❍
To me, performing the protective cyber security actions to protect my venture's trade secrets is NOT a trivial offence.	❍	❍	❍	❍	❍	❍	❍
To me, it is unacceptable to ignore the protection of my venture's trade secrets.	❍	❍	❍	❍	❍	❍	❍

Appendix B: Mean and Trimmed Mean

	Constructs	Code	Items	Mean	5% Trimmed Mean
1	Psychological Ownership	POC1.	This is my start-up and my trade secrets.	5.85	5.97
		POC2.	I feel a high degree of personal ownership for my start-up's trade secrets.	5.99	6.08
		POC3.	I sense that these are my trade secrets.	5.82	5.82
2	Reward	REW1.	Not performing protective security actions toward trade secrets saves me time.	3.30	3.26
		REW2.	Not performing protective security actions toward trade secrets saves me money.	3.36	3.29
		REW3.	Not performing protective security actions toward trade secrets keeps me from being confused.	3.20	3.15
		REW4.	Not performing protective security actions toward trade secrets requires less effort of me.	3.83	3.81
		REW5.	Not performing protective security actions toward trade secrets makes me feel less stressful.	3.07	3.02
3	Vulnerability	VUL1.	My start-up's trade secrets are vulnerable to information security threats.	4.99	5.07
		VUL2.	It is likely that an information security attack will occur against my start-up's trade secrets.	4.99	5.06
		VUL3.	My start-up's trade secrets are at risk to information security threats.	4.73	4.79
		VUL4.	My start-up's trade secrets are defenceless against information security threats.	3.86	3.85
4	Severity	SEV1.	Threats to the security of my start-up's trade secrets are severe.	4.49	4.54
		SEV2.	In terms of information security threats, attacks on my start-up's trade secrets are severe.	4.68	4.75
		SEV3.	I believe that threats to the security of my start-up's trade secrets are serious.	4.92	5.02
		SEV4.	I believe that threats to the security of my start-up's trade secrets are significant.	4.95	5.02
5	Response Efficacy	REF1.	Efforts to keep my start-up's trade secrets safe from information security threats are effective.	5.14	5.18

		REF2.	The available measures that can be taken to protect my start-up's trade secrets from security threats are effective.	5.05	5.08
		REF3.	The preventive measures available to me to stop people from getting my start-up's trade secrets are adequate.	4.72	4.76
		REF4.	If I perform the preventive measures available to me, my start-up's trade secrets are less likely to be exposed to a security threat.	5.17	5.26
6	Self-Efficacy	SEF1.	For me, taking information security precautions to protect my start-up's trade secrets is easy.	3.74	3.68
		SEF2.	I have the necessary skills to protect my start-up's trade secrets from information security threats.	3.69	3.65
		SEF3.	My skills in stopping information security threats against my start-up's trade secrets are adequate.	3.67	3.65
7	Response Cost	COS2.	I would be discouraged from performing protective security actions toward my start-up's trade secrets in the future because it would take too much time.	3.33	3.27
		COS3.	The time taken to perform protective security actions toward my start-up's trade secrets in the future would cause me too many problems.	3.22	3.19
		COS4.	Taking protective security actions would require considerable investment of effort as well as time.	5.15	5.17
8	Security Behavioural Intentions	INT1.	I am likely to take protective security action to protect my start-up's trade secrets.	5.76	5.82
		INT2.	It is possible that I will take protective security action to protect my start-up's trade secrets.	5.94	6.02
		INT3.	I am certain that I will take protective security action to protect my start-up's trade secrets.	5.63	5.73
9	Attachment	ATC1.	I usually have conversations about the protection of my start-up's trade secrets with team members.	4.67	4.72
		ATC2.	I respect my team members' views and opinions about the protection of our start-up's trade secrets.	5.59	5.67
		ATC3.	I communicate the importance of protecting the start-up's trade secrets to team members.	5.49	5.61
10	Commitment	CMT1.	I strongly believe that the protection of my start-up's trade secrets can help the start-up to succeed.	5.63	5.73
		CMT2.	I am committed to protecting my start-up's trade secrets.	5.81	5.88
		CMT3.	I am willing to invest energy and effort in making the protection of my start-up's trade secrets a success.	5.75	5.82
		CMT4.	I am willing to put in a great deal of effort to help my start-up succeed.	6.20	6.28
11	Involvement	IVT1.	I value the opportunity to participate in informal meetings related to my start-up's information security.	5.33	5.40

		IVT2.	I work on building personal relationships with team members in my start-up in relation to trade secret concerns.	5.55	5.60
		IVT3.	I actively involve myself in activities related to my start-up's growth.	6.15	6.22
12	Personal Norms	PEO1.	It is a serious matter if I don't perform the protective security actions to protect my start-up's trade secrets.	5.38	5.48
		PEO2.	It is unacceptable not to perform ALL the protective security actions to protect my start-up's trade secrets.	4.80	4.85
		PEO3.	To me, performing the protective security actions to protect my start-up's trade secrets is NOT a trivial offence.	4.83	4.87
		PEO4.	To me, it is unacceptable to ignore the protection of my start-up's trade secrets.	5.52	5.64

Appendix C: Cross-loadings

	ATC	COS	INT	IVT	PEO	POC	REF	REW	SEF	SEVandVUL
ATC1	0.761	-0.023	0.210	0.155	0.350	0.045	0.138	-0.177	-0.151	0.312
ATC2	0.742	-0.153	0.189	0.425	0.290	0.132	0.058	-0.197	-0.054	0.214
ATC3	0.909	-0.130	0.360	0.344	0.286	0.199	0.165	-0.187	-0.136	0.366
COS2	-0.161	0.957	-0.308	-0.146	-0.228	-0.172	-0.074	0.367	0.088	-0.100
COS3	-0.018	0.776	-0.142	-0.100	-0.047	-0.027	0.037	0.266	0.046	0.063
INT1	0.296	-0.353	0.837	0.315	0.359	0.306	0.137	-0.156	-0.041	0.312
INT2	0.208	-0.192	0.843	0.233	0.328	0.247	0.288	-0.097	0.139	0.347
INT3	0.344	-0.192	0.893	0.262	0.437	0.354	0.290	-0.188	-0.010	0.436
IVT1	0.269	-0.109	0.294	0.887	0.240	0.164	0.059	-0.039	0.079	0.138
IVT2	0.392	-0.146	0.240	0.823	0.297	0.141	-0.090	-0.088	-0.034	0.130
PEO2	0.242	-0.171	0.366	0.276	0.831	0.284	0.037	-0.205	0.144	0.308
PEO3	0.195	-0.143	0.304	0.151	0.769	0.190	0.081	-0.136	-0.064	0.136
PEO4	0.437	-0.149	0.394	0.309	0.838	0.239	0.094	-0.241	-0.011	0.326
POC1	0.163	-0.155	0.367	0.164	0.320	0.917	0.122	-0.123	-0.072	0.336
POC2	0.144	-0.016	0.295	0.111	0.188	0.840	0.111	-0.081	0.042	0.265
POC3	0.126	-0.205	0.236	0.200	0.243	0.834	0.094	-0.100	0.059	0.297
REF1	0.171	-0.008	0.311	-0.005	0.118	0.155	0.962	-0.160	0.014	0.239
REF2	0.052	-0.112	0.104	-0.014	-0.016	0.020	0.725	-0.138	0.017	0.098
REF3	0.103	-0.087	0.028	-0.026	-0.050	-0.033	0.479	-0.104	0.053	0.002
REW1	-0.090	0.316	0.012	-0.018	-0.134	0.132	-0.102	0.615	0.078	0.085

REW2	-0.150	0.286	-0.127	-0.115	-0.167	0.000	-0.086	0.723	-0.022	0.019
REW3	-0.229	0.318	-0.144	-0.046	-0.230	-0.164	-0.211	0.847	-0.008	0.001
REW4	-0.249	0.321	-0.034	-0.124	-0.279	-0.001	-0.083	0.659	0.025	0.025
REW5	-0.142	0.289	-0.157	-0.003	-0.163	-0.113	-0.123	0.843	0.120	-0.049
SEF1	-0.106	0.080	0.027	0.073	0.042	0.035	-0.044	0.001	0.874	-0.150
SEF3	-0.147	0.064	0.026	-0.018	0.016	-0.037	0.079	0.071	0.865	-0.052
SEV1	0.326	-0.004	0.177	0.146	0.128	0.286	0.138	0.061	-0.110	0.760
SEV2	0.359	-0.010	0.361	0.205	0.247	0.337	0.205	0.030	-0.080	0.837
SEV3	0.344	0.008	0.401	0.149	0.299	0.285	0.201	0.038	-0.057	0.857
SEV4	0.305	-0.052	0.451	0.138	0.248	0.260	0.331	-0.036	-0.128	0.839
VUL1	0.170	-0.070	0.314	0.051	0.262	0.319	0.019	-0.021	-0.123	0.687
VUL2	0.217	-0.120	0.160	0.005	0.236	0.140	0.079	-0.024	-0.024	0.659
VUL3	0.337	-0.091	0.285	0.100	0.320	0.233	0.087	-0.125	-0.100	0.795

Appendix D: Confidence Intervals Bias Corrected

	Original Sample (O)	Sample Mean (M)	Bias	10.0%	90.0%
COS -> ATC	c	0.216	0.043	0.079	0.234
INT -> ATC	0.395	0.403	0.008	0.251	0.528
INT -> COS	0.335	0.356	0.020	0.195	0.478
IVT -> ATC	0.563	0.571	0.008	0.405	0.714
IVT -> COS	0.211	0.236	0.025	0.088	0.364
IVT -> INT	0.431	0.433	0.001	0.273	0.584
PEO -> ATC	0.498	0.501	0.003	0.355	0.619
PEO -> COS	0.236	0.272	0.036	0.126	0.343
PEO -> INT	0.554	0.557	0.003	0.403	0.683
PEO -> IVT	0.444	0.456	0.012	0.286	0.609
POC -> ATC	0.196	0.230	0.034	0.096	0.292
POC -> COS	0.150	0.222	0.072	0.060	0.167
POC -> INT	0.415	0.409	-0.006	0.259	0.571
POC -> IVT	0.250	0.261	0.011	0.119	0.399
POC -> PEO	0.364	0.367	0.003	0.214	0.514
REF -> ATC	0.168	0.228	0.060	0.075	0.203
REF -> COS	0.121	0.190	0.070	0.034	0.132
REF -> INT	0.235	0.274	0.039	0.118	0.318
REF -> IVT	0.161	0.204	0.044	0.069	0.213

REF -> PEO	0.111	0.191	0.080	0.049	0.108
REF -> POC	0.139	0.177	0.038	0.066	0.201
REW -> ATC	0.288	0.307	0.018	0.182	0.380
REW -> COS	0.496	0.498	0.002	0.371	0.610
REW -> INT	0.173	0.214	0.041	0.096	0.224
REW -> IVT	0.135	0.207	0.071	0.062	0.145
REW -> PEO	0.316	0.331	0.015	0.195	0.432
REW -> POC	0.155	0.196	0.040	0.082	0.180
REW -> REF	0.198	0.242	0.044	0.107	0.274
SEF -> ATC	0.198	0.235	0.037	0.087	0.305
SEF -> COS	0.108	0.165	0.057	0.034	0.153
SEF -> INT	0.099	0.169	0.069	0.027	0.099
SEF -> IVT	0.133	0.191	0.057	0.041	0.179
SEF -> PEO	0.134	0.197	0.063	0.038	0.145
SEF -> POC	0.097	0.158	0.061	0.024	0.098
SEF -> REF	0.106	0.182	0.076	0.032	0.111
SEF -> REW	0.100	0.179	0.079	0.039	0.089
SEVandVUL -> ATC	0.447	0.453	0.006	0.320	0.563
SEVandVUL -> COS	0.118	0.175	0.057	0.056	0.124
SEVandVUL -> INT	0.454	0.459	0.005	0.311	0.573
SEVandVUL -> IVT	0.194	0.250	0.057	0.101	0.280
SEVandVUL -> PEO	0.382	0.395	0.013	0.253	0.503
SEVandVUL -> POC	0.393	0.395	0.002	0.268	0.508

SEVandVUL -> REF	0.225	0.258	0.033	0.136	0.280
SEVandVUL -> REW	0.100	0.171	0.071	0.074	0.074
SEVandVUL -> SEF	0.174	0.213	0.040	0.096	0.231