INFORMATION SECURITY GOVERNANCE: DIFFERENCES IN PERCEPTIONS OF POLICYMAKERS AND EMPLOYEES

AMIT ANNASAHEB NAIK

PhD

2019

INFORMATION SECURITY GOVERNANCE: DIFFERENCES IN PERCEPTIONS OF POLICYMAKERS AND EMPLOYEES

AMIT ANNASAHEB NAIK

A thesis submitted in partial fulfilment of the requirement of the University of Northumbria at Newcastle for the degree of Doctor of Philosophy

Research undertaken in the Faculty of Health and Life Sciences

December 2019

Abstract

There is a magnitude of technical controls which do more than half the job of securing the organisation. The rest falls on the employees. Employees are considered the weakest link in the security chain of the organisation this is primarily because they are the easiest to compromise. This could be due to external motivators, such as become a victim of social engineering or personal emotional motivators, such a disgruntled employee. It is most often the case that an employee gets blamed for a security breach. Security researchers fight from both employees and managements side and blame each other for being the problem. It is necessary to address this gap between policymakers and employees. And this study attempts to do that.

Two studies were conducted. The 1st study was a qualitative semi structured interview. From which I created a conceptual model. This model was used in preparing the 2nd study, which was a quantitative survey. The data from the survey was then used to create Structural equation model using SPSS and AMOS.

Differences in their perceptions of policymakers and employees and postulated relationship of these differences (constructs) with constructs of Protection Motivation Theory. Which we then confirmed using Structural equation model.

Key finding was usability of a tailored policy was used as a moderator to see its effect on all the relationship constructs. Use of a tailored policy dampened the relationships Perception of information security (POIS) and Threat appraisal (TA), between POIS and Coping appraisal (CA), between POIS and Behavioural intent (BI), and POIS and Actual behaviour (AB). It also dampened the relationship between perception of organisational interventions (POOI) and BI. It strengthened the relationship between, POOI and TA, POOI and CA, POOI and AB. Use of a tailored policy dampened the relationship between, TA and BI, but strengthened between CA and BI, CA and AB and TA and AB.

This research addresses these differences between policymakers and employees, across different organisations with varying organisational security levels, viz. low, medium and high security organisations and posits that through a tailored security policy security compliance behaviour can be improved.

Table of Contents

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVATIONS

AB	Actual Behavior
AMOS	Analysis of Moment Structures (IBM SPSS Amos - Software)
AUP	Acceptable Use policy
BI	Behavioral Intent
BOUT	Belief Outcomes
BS	British Standard
BYOD	Bring Your Own Device
CA	Coping Appraisal
CASS	Consequence Assessment
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CFA	Confirmatory Factor Analysis
CIA	Confidentiality, Integrity, Availability
COBIT	Control Objectives for Information Technologies
CONT	Perceived Controllability
CSO	Chief Security Officer
CTO	Chief Technical Officer
CVV	Card Verification Value
DPA	Data Protection Act
DTI	Department of Trade and Industry
EFA	Exploratory Factor Analysis
ENISA	European Union Agency for Cyber security
EPOS	Employee perception of Security
EU	European Union
GDPR	General Data Protection Regulation
GLS	Generalized Least Square
ICT	Information and Communication Technology
IEC	International Electrotechnical Commission
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Organization for Standardization
ISP	Information Security Policy
IT	Information Technology
JTC	Joint Technical Committee
KMO	Kaiser-Mayer-Olkin
KPI	Key Performance Indicators
LV	Latent Variable
ML	Maximum Likelihood
PBC	Perceived Behavioral Control

PBEN	Perceived Benefit
PCA	Principal Component Analysis
PCOMP	Perceived cost of Compliance
PDCA	Plan-Do-Check-Act
PECR	Privacy and Electronic Communications Regulation
PMT	Protection Motivation Theory
PNCOMP	Perceived cost of Non-Compliance
POC	Perception of Organisational Citizenship
POIS	Perception of Information Security
POOI	Perceptions of Organisational Interventions
PVUL	Perceived Vulnerability
PWC	PricewaterhouseCoopers
QOP	Quality of Policy Document
SCT	Social Cognitive Theory
SD	Standard Deviation
SDT	Self Determination Theory
SEFF	Self-Efficacy
SEM	Structural Equation Model
SPROB	Probability of Sanction
SPSS	Statistical Package for the Social Sciences (Software)
SSEV	Sanction Severity
TA	Threat Appraisal
TPB	Theory of Planned Behavior
UK	United Kingdom
WLS	Weighted Least Squares

Acknowledgements

This journey has been extremely delightful yet unbearably painful, quite literally. The delight was from the entire process of this research, from finding a research gap, the learning process, meeting people through to completing this thesis. The pain was from my double prolapsed disks. As such this research could not have been possible without several people. Though I would like to express the extent of my heartfelt gratitude these words would not suffice to express how truly grateful I am for your help and support.

I would first like to thank my supervisor Prof. Pamela Briggs for being my beacon of light and hope. I have learnt so much from you. I know I have not been the best of your students but thank you very much for being patient throughout my PhD journey. I found research to be very interesting and I have strayed many a times from the true path. It was your guidance that brought me back every time and has taught me the real meaning of how to conduct research while remaining focussed. I would also like to thank my second supervisor, Prof. Lynne Coventry, whose expertise and invaluable advice provided great insights during my research.

I would like to acknowledge and thank my colleagues from PaCT lab for welcoming me among them and showing me the ropes of doing initial research. I cannot single any of you out so in no particular order, Dr Lisa Thomas, Dr Andrew McNeill, Dr James Nicholson, Kerry McKellar and Dr John Blythe, I thank you all for being excellent colleagues and friends.

No matter how much I say, it will not be enough to how much my family has helped me throughout this journey. I would not be here without them. My mother, brother, and partner Jean. You all mean everything to me. Thank you for being my three pillars.

Lastly I would like to thank my examiners Dr Simone Strumpf and Dr Elizabeth Sillence for your patience and guidance.

Declaration

I declare that the work contained in this thesis has not been submitted for any other award and that it is all my own work. I also confirm that this work fully acknowledges opinions, ideas and contributions from the work of others.

Any ethical clearance for the research presented in this thesis has been approved. Approval has been sought and granted by the University Ethics Committee.

I declare that the Word Count of this Thesis is 73248 words

Name: AMIT ANNASAHEB NAIK

Signature:

Date:

1 CHAPTER 1 INTRODUCTION

1.1 Introduction

It is believed that poor and unacceptable user security behaviour leads to non-compliance of Information Security policies (ISP's) and the most common causes are user security error, carelessness, negligence, and attacks (Leach, 2003) Inversely it is also believed that good user security behaviour leads to better compliance of ISP's (Saint-Germain, 2005). It would be unfair to put the blame of non-compliance entirely on employees (Adams & Sasse, 1999) and employers are to be held equally responsible for implementing effective security policies (Merete Hagen, Albrechtsen, & Hovden, 2008) that are difficult to comprehend and follow (Leach, 2003)(Kirlappos, Parkin, & Sasse, 2014). Policy makers perceive they must consider a multitude of factors when designing security policies. They must adhere to industry standards and guidelines (Saint-Germain, 2005)(Mataracioglu & Ozkan, 2011)(Humphreys, 2008), legal regulations (Gerber & von Solms, 2008) and of course they must do this while keeping the organisations aims and objectives in mind. While employees perceive they must perform their daily tasks for which they have been hired to do and to be able to do these tasks effectively and efficiently to meet their agreed key performance indicators (KPI's). To facilitate better compliance to ISP's it is therefore necessary to bridge this gap between the perceptions of policymakers and employees, to find common grounds to create harmony which in turn will facilitate to achieve organisational aims and objectives while improving user security behaviour.

1.2 Motivation for this research

Professional Motivation

I have worked in the Information Technology (IT) industry for over 9 years. I went through various organisations to progress up from the position of technical support to Information security manager. After reaching this position I did what every other security manager does. I followed industry standards and guidelines to develop and implement Standard Information Security policies. I noticed employees were not following what I thought to be basic security practices, e.g. logging off your computer when you are not at the desk or memorising your password and not writing it down on a sticky paper. Being new to the position I wanted to improve our organisational

security policy compliance was when I started doing my own research to finding ways about to improve compliance. It was after reading a journal article I found that this was considered as a behaviour, which first got me interested in the human aspect of organisational security behaviour. I was later introduced to the concepts of awareness and training programs but soon realised there were inherent costs associated with them. I felt the most cost-effective way to improve organisational security behaviour was to improve the organisational security policy.

Motivation from Literature

Information security practitioners are still facing the issue of information security compliance within their organisations. While many researchers are addressing these issues and though the progress is incremental it is not complete. We still do not have a comprehensive plan for mitigating or reducing these issues. Originally, I had decided to start small, with first improving our Bring Your Own Device policy (BYOD). With further research I found multitude of research areas focussing on different aspects of technical and nontechnical measures such as organisational security behaviours have been studied however the area of improving a security policy itself was severely lacking. A properly implemented information security governance framework should facilitate proper implementations of organisational directives, however Information security policies are not normally disseminated at an organisational level (Von Solms, Thomson, & Maninjwa, 2011) thereby resulting in improper control of security behaviour within the organisation, making compliance measurement problematic. We have research focussing on smaller aspects of information security governance such as which awareness programs work (Y. Chen, Ramamurthy, & Wen, 2015) and which do not work, research on information security framework for a particular industry (Vithanwattana, Mapp, & George, 2017) and research focussing on a different individual aspects of employee behaviour (Valentine, 2006). The need for a comprehensive information security framework has been identified (Von Solms et al., 2011) while it is also true that 'one size fits all' approach doesn't work (Valentine, 2006), we still need a concept that fits all. It is important to focus on improving other security interventions such as awareness and training programs, it is equally important to improve the ways of developing security policies as they are also a form of intervention. The key advantage of improving a security policy is that users can always access security related information and refer to these policies more regularly than any other form of intervention. Thereby organisations can avoid recurring costs associated with other forms of interventions. This motivated me to do my own PhD research

focussing on the human aspect of information security governance, particularly focussing on the information security policy itself.

As described below in the following sections the field of Information security is quite vast and it took me a master's degree and various security certifications to even begin to understand its depth and importance and also that it is unfair to expect that level of understanding from all employees. For this PhD research the focus of this research had to be narrowed down. This thesis is a subset of Information security governance, with its primary focus on identifying the differences in perceptions of policymakers and employees with respect to the conduct of employees and their compliance behaviour with their organisational information security policies (ISP's). The general aim of this research is to identify if both policy makers and employees can work together to contribute towards designing effective security policies. Primary supporting idea behind this approach is that the policymakers know the standards and guidelines for designing an ISP, while the employees are the first line who face issues with complying those policies. Using this combined knowledge and experience of compliance / non-compliance issues, an attempt is made to add to the research gap of developing effective information security policies and see if a stronger usable policy that works for both policymakers (thereby satisfying the requirements of the standards and guidelines) and the employees (e.g., convenience, easy to follow, etc.) can be achieved. The main purpose of this research is to gain an insight into the perceptions of policymakers and employees and see if there are any differences in their perceptions about the ISP's. The aim is to identify if there are any key factors / determinants originating from these differences and if these factors / determinants lead to non-compliance.

1.3 Understanding Information security

In today's day and age, the knowledge to handle information is considered power. Information can be any information relevant to an individual or an organisation. This could be personal information, financial information, or an organisations confidential data. Personal information such as your name, address, date of birth, social security number, etc. are used to identify who you are. As such this information is widely used banks and various service providing organisations to verify and authenticate you, to establish you are who you say you are. Examples of financial information at an individual level include, you bank account number, sort code, the CVV number at the back of your card, or all the information on your payment card, debit or credit cards. At an organisational level, along with the bank details, this could include, payroll information, suppliers

account details, information about assets, equities, investments. Some individual or organisations use this knowledge to misuse information. These people are called hackers, who have a malicious intent to misuse information for personal benefit or gain. As such all information that can be used in a malicious way to cause harm to any individual or an organisation needs to be protected. Information security or Infosec for short, is a practice which deals with protecting all types information, be it a digital (on a computer) or physical format (on paper).

1.3.1 Cyber Security

Most people who do not have an IT background are easily confused with information security and Cyber security. The distinction is further complicated by their interchangeable use within research and media. But there is a clear distinction. Cyber security only deals with information that is of digital format. Its subdomains are broadly classed as Internet security, Network security, computer security, mobile security, Cyber warfare etc. All these sub domains overlap each other in concept as all these a connected to each other in some way. Computers connected to each other to form a wired or wireless network, networks connected to each to form the internet, mobiles connected to each other through a form of wireless network. And finally, cyberwarfare, the ongoing battle between security officers and hackers, to protect the digital network. Where users fall in this wide network are the first line to input or access information through a computer. Hence the computer is also termed as the endpoint, and its security as End point security.

1.3.2 Data Protection

Likewise, the concept of data protection widely deals with personal information only. This information can be in digital form e.g. stored on a computer or on a similar device, and in physical form, stored as a document or on a paper. In summary it deals with a specific type of information stored in any format. Most recently UK parliament, due to Brexit, announced a new Data protection ACT 2018 (DPA 2018). Before Brexit, UK government followed EU's Data protection standards, General Data Protection Regulation or GDPR. As such the previous Data protection Act 1998 has now been repealed. The Data Protection Act 2018 has the following 8 parts.

Table 1 Data Protection Act 2018

1	This Act makes provision about the processing of personal data.

2	Most processing of personal data is subject to the GDPR.
3	Part 2 supplements the GDPR (see Chapter 2) and applies a broadly equivalent regime to certain types of processing to which the GDPR does not apply
4	Part 3 makes provision about the processing of personal data by competent authorities for law enforcement purposes and implements the Law Enforcement Directive.
5	Part 4 makes provision about the processing of personal data by the intelligence services.
6	Part 5 makes provision about the Information Commissioner.
7	Part 6 makes provision about the enforcement of the data protection legislation.
8	Part 7 makes supplementary provision, including provision about the application of this Act to the Crown and to Parliament

Source 1 legislation.gov.uk

1.3.3 Information security

Confidentiality, Integrity, and Availability are the three pillars which form the core of Information security. In the information security domain these are most commonly known as the *CIA triad* (Wilson, de Zafra, Pitcher, Tressler, & Ippolito, 2009).

Confidentiality: This is to ensure data or information, in both digital and in paper format, are kept confidential. And data can be accessed only by authorised individuals or groups of individuals.

Integrity: This is to ensure data or information, in both digital and in paper format, is authentic and unaltered. And this data can only be modified by authorised individuals or groups of individuals.

Availability: This is to ensure all data or information, in both digital and paper format, is always available for use when it is needed. And is available only to those authorised to use the information.

Information security deals with security of all types of information, stored in all formats, digital and paper. And as such its protection includes natural disasters, technical malfunction, and physical theft, to name a few. Infosec deals with securing all information, cyber security deals with securing digital information, data protection deals with securing personal information. This similarity creates an overlapping appearance between them three.

In summary, Cyber security and data protection are a subsets or sub-categories of Information security. Cyber security and Data Protection form only a small part of the entire Information security practice. Information security further comprises of its governance, through Management standards, policies, procedures, guidelines, laws and regulations and finally becoming a part of the organisations security culture and behaviour.

1.4 Information Security Governance

Organizational Information security is primarily achieved through its governance, whose key general areas are, to govern the operations of the organizations and protect its assets, protect the organizations market share and stock price, govern the conduct of its employees, protect the reputation of the organization and ensure compliance requirements are met. We know information security's primary focus is to maintain confidentiality, integrity, and availability of data while maintaining effective policy implementation and overall organisational productivity. This is primarily achieved through a process of establishing an Information Security Management System or ISMS for short.

1.4.1 Information security management system (ISMS)

An information security management system is a term for a combination of various interrelated security elements of an organisation which forms as a centrally managed framework. This framework is defined by the ISO/IEC 27000 series particularly ISO/IEC 27001:2013 which

specifies the requirements for having an Information security management system. ISO is an independent, non-governmental international organisation, who has a membership of about 164 national standard bodies. ISO/IEC JTC 1 is the one such body which focusses on developing frameworks for Information technology.

1.4.1.1 Risk management

Information security begins with a thorough risk management process which primarily includes risk assessment, threat assessment and vulnerability assessment. There are a multitude of tools and methods available for risk assessment (ENISA, 2006). Good practise for risk assessments advices to carry out risk assessment while ensuring appropriate and adequate considerations of human factors (Gadd et al., 2003). Research conducted within the cross disciplinary research field of social sciences and information security primarily focusses on mitigating the risk of human factors viz human behaviour (Sohrabi Safa, Von Solms, & Furnell, 2016). Some consider employee behaviour as risk (Da Veiga & Eloff, 2010) while some say users are not the enemy (Adams & Sasse, 1999).

1.4.1.2 Vulnerability assessment

A vulnerability of an asset of an organisation is defined as an asset which can be compromised or harmed, e.g. loss of information or financial loss. Researchers suggest employees to be considered as assets as well (Von Solms & Van Niekerk, 2013). Employees should be considered as assets and protected because research indicates, users being vulnerable to various attacks (Hoofnagle, 2007) (Chou, Ledesma, Teraguchi, & Mitchell, 2004) (K. B. Anderson, Durbin, & Salinger, 2008). As such identification of an asset and understanding its vulnerability is one of the main requirements of effective ISMS (Broderick, 2006).

1.4.1.3 Threat assessment

A threat is defined as an entity that can exploit a vulnerability in order to cause harm to as asset. Many consider employees as threats (Colwill, 2009), others suggest users should not be considered a threat as they do not understand security events and as such management should be responsible (Adams & Sasse, 1999). While some speak on managements behalf, suggesting the managers lack trust towards employees which leads to creation of technical security measures (Reinfelder, Landwirth, & Benenson, 2019).

1.4.2 Policies, procedures and controls

For governance, organizations develop and implement policies. One of the key characteristics of implementing effective information security governance is that the staff are made aware of the security policies and trained in the appropriate use of IT systems and acceptable behaviours / conduct within the organizations. Many organizations do implement such organization wide security policies and invest heavily in securing the workplace with technology. Despite this a recent survey conducted by PWC-US (2015) showed significant rise in security incidents by 48%. In the summary of the result it was found that the top two most likely causes of those incidents were due to the actions of current employees (34.55%) and former employees (30.42%) with actual attacks from hackers coming in third at 14%.

1.5 Policy making guidelines

An information security policy is considered as a repeatable organisational process. It undergoes various stages, development, approval, implementation, audits, assessments to retirement and redevelopment (Knapp, Franklin Morris, Marshall, & Byrd, 2009). Various standards are used across the world for the creation of security policies. To name a few of the renowned industry standards, BS7799 (UK), ISO 27000 series, COBIT (industry standard). Another standard which is used in conjunction with these standards is the General Data protection Regulation (GDPR).

1.5.1 BS7799 (UK)

The British standard for BS7799 was introduced by the British standards institute as an information security management system in the 1990s (Broderick, 2006). This was later revised and accepted world-wide as ISO/IEC 17799 in 2000 (M Siponen & Willison, 2009). This standard has now been withdrawn and currently being used revised and used as ISO/IEC 27002:2013 (ISO/IEC, 2013). According to ISO these standards have a life cycle of 5 years before they are revised again. This also suggest every organisational security policy should be revised at least every 5 years.

1.5.2 ISO 27000 Series (Standard)

Later International Organisation for standardisation (ISO) which is an internal body for setting standards introduced their own standard ISO 27000 series for the regulation and management of IT systems. This series is a revised version of the original ISO/IEC 1799 standard which was

released in 2005 (Karabacak & Sogukpinar, 2006). Today these standards are being used in 100s of organisations worldwide (Humphreys, 2008). These standards however are under constant scrutiny of researchers who try to find a gap (Karabacak & Sogukpinar, 2006) or effective ways of using it along with other information security standards such COBIT (Mataracioglu & Ozkan, 2011).

1.5.3 COBIT (Framework)

Control Objectives for Information and Related technologies (COBIT) is an IT management framework developed by Information Systems Audit and Control Association (ISACA), which is an independent non-profit association and engages in development of information security body of knowledge and industry standard practices (ISACA, 2018). ISACA is also a certification body which certifies all security professionals and policymakers (Ifinedo, 2014).

These standards are just a few of the ones that are used worldwide. These standards and guidelines also undergo constant review and revision. The purpose of mentioning these standards in this section is to make the reader understand the depth of knowledge on information security and to make a point that it would be unfair to expect all employees to know and understand this vast knowledge.

1.6 Information security laws and regulations

The vastness of information security does not end with knowing just the standards and guidelines. These standards and guidelines are often always used to develop policies in conjunction with various information security laws and regulations. The laws which primarily affect users within the UK organisations are as below:

Data protection ACT 2018 (UK)

Data protection act 2018 which was updated post Brexit talks. Previously most organisations within the UK followed the General Data Protection Regulation (GDPR) which is a European Union (EU) regulation to protect, use and transfer of personal information.

Privacy and Electronic Communications Regulation (PECR)

This regulation is used in conjunction with the Data protection Act and the GDPR and gives people rights in relation to communication over electronic mediums. There are rules for the use of emails, text, fax, calls etc.

Computer misuse Act

This is one of the most cited Act in all policy documents. As such the purpose of this act is to define the legislation for dealing with cyber-crimes.

1.7 Organisational Security behaviour

In information security, research on organisational security behaviour primarily focusses the organisations security culture and human (end user) behaviour. It is believed that organisational Information security behaviour cultivates its information security culture (Da Veiga & Eloff, 2010). While information security behaviour itself is influenced by the information security components. According to Willcoxson et al (Willcoxson & Millett, 2000) culture is defined by group parameters such as language, concepts ideology, and by normative criteria involving authority, rewards, punishments etc. The need to change organisational security culture has been identified within research (Ashenden, 2008). The role of top management in improving organisational culture has also been emphasized (Hu, Dinev, Hart, & Cooke, 2012). Though there is some research on policymakers attitude towards users (Reinfelder et al., 2019), there is also a study focussing on the relationship between the mindsets of security professionals and users against their organisational security efforts(Posey, Roberts, Lowry, & Hightower, 2014). I could not find any research focussing on their perceptions of security policy and comparing it with the perceptions of users.

1.8 User Security behaviour

There is research showing why users behave insecurely rather than carelessly (Albrechtsen & Hovden, 2009) and there is research showing user behave in the way they behave because most security designs are not user centric (Adams & Sasse, 1999). There is once again little research in trying to capture their perceptions and comparing them with the perceptions of policymakers to identify the differences and see if this could be affecting compliance in any way. In most case it is generalised that users do not understand (Adams & Sasse, 1999) or what should be done to help them better understand (Höne & Eloff, 2002). The importance of understanding how to persuade

employees to adopt protective behaviour has also been emphasised (Orazi, Warkentin, & Johnston, 2019). Research on how employees behave securely on their own accord when it becomes difficult to follow policies and procedures implemented by organisations has also been brought to attention (Kirlappos et al., 2014).

1.9 Research questions

This research focusses on the following research questions, mainly focusing on highlighting the differences in perceptions of policymakers and employees from different organisations with varying security levels, viz. low, medium and high security organisations. At the end of each question the chapters they will be addressed in is mentioned in brackets.

1) How do policymakers and employees perceive organisational security policy? (Chapter 3)
2) Are there any differences in their perceptions? (Chapter 3 and 4)
3) Could they lead to employee non-compliant security behaviour? (Chapter 3)
4) How can compliance with the security policy be improved? (Chapter 3 and 5)
5) Can we find solution that works with both policymakers and employees? (Chapter 3 and 5)
6) What would make an effective Tailored policy? (Chapter 5)
7) Can we develop a generalised model of enhanced PMT in relation to security compliance? (chapter 5)
8) Can this model be tested for its application to both policymakers and employees? (Chapter 5)
9) Is this model a generalised model for organisations with varying security levels? (Low, medium and high security organisations) (Chapter 5)
10) Are there any moderation effects of a Tailored policy on the relationships between the constructs of PMT? (Chapter 5)
11) Can a tailored policy be used to improve organisational security behaviour? (Chapter 5)

1.10 Research methods

1.10.1 Objectives of research

The key objective of any research is to find answers to questions through scientific procedures (C.R.Kothari, 2004). Depending on the research study, their objective can vary. They can be

exploratory or formulative, they could be descriptive or diagnostic. Exploratory and formulative research is when you try to gain new insights into a subject. Descriptive study is when you are describing the characteristics of something that already exists. And diagnostic research is when you try to find associations of the studied subjects with something else.

1.10.2 Types of research

1.10.2.1 Descriptive vs Analytical

Descriptive research aims to understand the nature of something (Jarvinen, 2000) meaning the researcher has no control over the variables (C.R.Kothari, 2004). Analytical research aims to build a theory for something. Meaning the researcher must rely on facts and information already available.

1.10.2.2 Applied vs fundamental

Applied research is when you try to find an solution that can applied to an immediate existing problem (C.R.Kothari, 2004). Fundamental research is just pure basic research where it is mainly concerned with generalisation and theory building.

1.10.2.3 Quantitative and qualitative

Quantitative research is based on the measurement of quantity (C.R.Kothari, 2004). According to Choy (Choy, 2014) qualitative research does not focus on a specific research but explores the theoretical paradigm.

1.10.3 Research approach

With a multitude of research methodologies present and based on the research focus, a mixed method research approach was considered. For my research questions 1) How do policymakers and employees perceive organisational security policy? 2) Are there any differences in their perceptions? and 3) Could they lead to employee non-compliant security behaviour? we need to delve deeper into their perception and understand their thought process. This can only be achieved with open ended questions where the participants give descriptive answer. Hence for Study 1 a Qualitative approach with semi structured Interviews was considered as the most appropriate method for initial data collection.

To answer my research question, 4) How can compliance with the security policy be improved? 5) Can we find solution that works with both policymakers and employees? and 6) What would make an effective Tailored policy? we need the reliability of statistical data to establish the findings. Hence for study 2 a quantitative approach was decided in order to facilitate Structural equation modelling. The data from the survey was analysed using 2-way cross tabulation method to highlight individual differences between the perceptions of policymakers and employees.

1.10.4 Structural Equation Model

To statistically answer research questions, 4) How can compliance with the security policy be improved? 5) Can we find solution that works with both policymakers and employees? 6) What would make an effective Tailored policy? 7) Can we develop a generalised model of enhanced PMT in relation to security compliance? 8) Can this model be tested for its application to both policymakers and employees? 9) Is this model a generalised model for organisations with varying security levels? (Low, medium and high security organisations) 10) Are there any moderation effects of a Tailored policy on the relationships between the constructs of PMT? and 11) Can a tailored policy be used to improve organisational security behaviour? structural equation modelling is used.

Chin (Chin, 1998) believes Structural equation modelling provides techniques to perform covariance based and component based analysis. He adds, SEM based procedures have various advantages over previous techniques, like principal component analysis, factor analysis, discriminant analysis, and multiple regressions. This is because with SEM you can model relationship among multiple predictors (Chin, 1998), construct unobservable latent variables (LV's), model errors in measurements for observed variables and statistically test established theories. Contrary to this many researchers have found issues with the method such as Item parcelling issues (Bandalos, Finney, & Finney, 2001), which according to Bandolas is basically averaging two items and using this average as the basis of analysis, Causation issues (Bullock, Harlow, & Mulaik, 1994) addressing issues with forming causal statements and robustness issues (Satorra, 1990). However use of estimation methods such as maximum likelihood (ML) generalised least square (GLS) and weighted least squares (WLS) can be used to address the robustness issues (Satorra, 1990) (Olsson, Foss, Troye, & Howell, 2000).

1.11 Contributions

1. Provided a comparison of policymakers and employees perceptions of their organisational security policies. Thereby adding to the small existing literature on differences between security perceptions of policymakers and employees.
2. Identified differences between security perceptions of policymakers and employees, across different organisations with varying security levels, viz. low, medium and high security organisations.
3. Developed a new extended PMT model by creating new constructs and showing their relationships with the existing constructs of PMT.
4. Demonstrated usability of a tailored policy.
5. Demonstrated that the model can be generalised for both policymakers and employees from organisations with varying security levels and different industries. A concept that fits all.
6. Demonstrated that information security compliance behaviour can be improved through a tailored security policy. By showing covariance between usability of a tailored policy and actual behaviour of participants.

1.12 Structure of this thesis

Chapter 1 begins with an introduction to the core principles of and within information security. Before we even begin to understand people, who practice these principles it is necessary to understand the depth of knowledge pertaining information security. This chapter aims to provide the reader just that an introduction to information security and therefore only contains definitions and brief descriptions.

Chapter 2, reviews existing literature and divides it in to two main categories, research conducted from management perspective and research conducted from employee perspective. These in turn are further divided in to three subcategories, assessment, approach to implementation and outcomes of implementation. Research conducted from management perspective has been classified into assessment of organisational information security requirements, approach taken to implement pertinent security control mechanisms and the outcomes from the implementation of those control mechanisms. In terms of research from employee perspective, assessments of

employee perspective towards security, approach suggested to implement the control mechanisms to address these perspectives and the outcomes from these implemented control mechanisms have been put together. The purpose behind categorising the existing literature in this way is to identify the pattern of research conducted from both management and employee perspectives to attempt to find the key research gap and to see if studying the differences between the two perspectives would lead to better information security compliance research. Further a review of all the existent theories used for predicting or studying user security behaviour are presented. Following literature review the research gap has been highlighted.

Chapter 3 covers Study 1 and its analysis. This study is a qualitative study by conducting interviews with open ended semi structured questions. In his study Ray Galvin (Galvin, 2015) suggested that after 12 interviews data becomes saturated. This agreed by Baker et.al, (Baker & Edwards, n.d.) they believe for postgraduate students 12 interviews is sufficient to gain the experience of planning and structuring interviews, conducting, transcribing, and generating quotes for the writeup. For this study 14 interviews were conducted. Participants were recruited from 7 low security organisations such as academic institutions across England. For each organisation one academic and one non-academic staff was interviewed. The interview was structured in to 5 sections namely, 1) Understanding of Information security, 2) Organisational participation with security interventions, 3) Employee participation in security interventions, 4) Issues following the organisational security policies, 5) How can employees be a part of the solution. Thematic analysis was employed for the analysis of interview data, to identify key themes that originated from the interviews. The study confirmed a few existing themes from previous studies, communication (Yeniman Yildirim, Akalp, Aytac, & Bayram, 2011), accountability (Posthumus & von Solms, 2005), interdependence (Beautement et al., 2016), responsibility (Tsai et al., 2016), awareness (Stanton, Stam, Mastrangelo, & Jolton, 2005), duty (Leach, 2003)(Posthumus & von Solms, 2005), relevance of information within the policies (Jones, McDavid, Derthick, Dowell, & Spyridakis, 2012) however now with a clear distinction between policymakers and employees thereby addressing the gap identified in literature. This study also contributed new ideas to previously studied themes such as commitment (Muthuveloo & Rose, 2005) (Höne & Eloff, 2002), Visibility of policy (Weidman & Grossklags, 2018). The study finally provided with a novel theme of a tailored policy that both policymakers and employees felt could work.

Study 2 has been covered in two chapters. Chapter 4 covers Study 2 and its first analysis. This study was a quantitative study and reports the findings from the survey and separates it into only

highlighting the differences in perceptions of employees and policymakers. The survey instrument was created on Qualtrics and administered through a market research agency. Sample size of over 500 is considered very good as it provides adequately stable factor solutions that closely approximate the population factors (Hogarty, Hines, Kromrey, Perron, & Mumford, 2005). A total of 624 samples were collected out of which 513 complete and engaged (Guin, Baker, Mechling, & Ruyle, 2012) responses were used for data analysis. A statistical analysis of the constructs is presented using cross tabs analysis, highlighting how participants feel about certain items and how this relates to their opinions about items in other constructs. Samples are collected over multiple industries through varying levels of security within their respective organisations. The theme of a tailored policy was further explored in this study as in verifying its effectiveness efficiency and user satisfaction.

Chapter 5 Uses the data from study 2 to create a structural equation model with the aim to enhance the PMT model relating to security compliance behaviour. Its application to both policymakers and employees is tested. Following the successful creating of the model moderation effects of a tailored policy was tested on the relationships between the constructs of PMT and the constructs created for the purpose of this research study, 1. Perception of information security and 2. Perception of organisational interventions. Whether this model is for all types of organisations is also tested using data for low security, medium security, and high security organisations as controls. There by proving that this model is applicable across organisations with varying security levels. Further the usability of a tailored policy is verified and its effects on each pathway between the constructs are studied.

Chapter 6 provides conclusions and discussion. It also highlights novel contributions, limitations and future research directions.

2 CHAPTER 2 LITERATURE REVIEW

2.1 Introduction

This chapter reviews literature from both management and end-user perspective. From management perspective, research conducted within organisational information security requirements, organisational approach to implementation of control methods such as awareness programs, training programs, various forms of communication and security policy, and finally the outcomes in terms of end-user behaviour from such implemented methods has been reviewed. From end-user perspective, research relevant to their own perspective of organisational information security, its relevant behaviour, employee approach to the organisational control methods, and the resultant outcome from the methods has been reviewed. Later, extant theories used to measure end-user security behaviour have been reviewed identifying the most relevant theory that is used for this PhD research. After this a brief discussion on the identified research gap is addressed. And in the final section how a conceptual model was developed for this study has been articulated.

2.2 Literature review of research from Management perspective

This section covers research conducted from management perspective and is divided in to three sub sections, which would primarily keep the focus on compliance relevant research. These sub sections are based on how organisations assess their organisational security requirements and based on these assessments the organisations develop and implement security control mechanisms. Finally, the outcomes of these control mechanisms as found the literature have been put together. Fig 1. Shows the framework for literature review based on research done from management perspective. This framework is based on the ISMS (Information Security Management Systems) Framework. This framework was first devised in BS7799, a standard written by United Kingdom Governments Department of Trade and Industry (DTI) and was later revised to ISO/IEC 17799 in 2002 and most recent restructured into the ISO 27000 series of security standards. ISMS is also called as the Plan, Do, Check, Act model, first introduced in BS 7799 part 2, later revised to ISO/IEC 27001 is most commonly and widely used standard for developing and implementing information security policies and controls. The policies are intended

to provide guidance on implementing effective compliance strategies and control to facilitate effective compliance.

Figure 1 ISMS Framework

Plan-Do-Check-Act (PDCA) model: In this model what organisations do in each phase varies from organisation to organisation which is based on their respective organisational aims and objectives. However, the key purpose for each phase remains the same. The Plan phase objective is the come up with the actual policy document where in policymakers define the policy, define the scope of ISMS, perform Risk assessment and Risk management, select controls to be implemented and prepare the statement of applicability document. The Do phase objective involves implementing and operating the control. The Check phase objective is to evaluate the efficiency and effectiveness of the ISMS. And the Act phase objectives include making changes if necessary, to improve the efficiency and effectiveness of the ISMS. This will again be a part of the planning process and the cycle continues.

2.2.1 Assessment of information security requirements

Assessment of information security requirements falls under the planning phase of the PDCA model. Where in organisations perform risk assessment and identify the key assets (Information) which need to be protected. The risk associated with loss of such assets, the threats (Insider threat-employees / outsider threat - hackers) to those assets meaning who could try to target or cause damage to the asset, and the vulnerability of the assets, as in how likely the asset is to be targeted.

Along with risk assessment, while developing the policies, organisations also must consider internationally recognised standards and guidelines. The ones written by ISO/IEC and CoBIT are the most commonly and widely used standards. With the increasing importance of compliance laws and regulations such as the Sarbanes-Oxley, Graham-Leach-Bliley, and Basel II, organisations have become aware of the increasing importance of legal compliance and the obligations that arise with the laws (Gerber & von Solms, 2008).

2.2.2 Approach to implementation of control methods

Most industry standards such as the ISO/IEC series and CoBIT, emphasize the importance of educating employees and creating information security awareness programs. However, it has been found that awareness programs aren't very effective as the employees retain the knowledge from the program for a certain period after which they return to finding quicker ways of performing their complex daily job-related tasks. It has been suggested to have regular awareness programs, however having multiple programs at regular intervals result in intrinsic costs (Kruger & Kearney, 2006). While adhering to the standards and legal obligations it is also important for an organisation to perform a cost benefit analysis to identify the extent of expenditure and the benefits from these expenses related to implementing security controls which would then improve compliance. For these reasons technical security controls have been found to be the most effective way of implementing information security compliance. Organisations invest huge sums of money into technical controls such as smart cards, physical security control, CCTV systems etc. as these systems provide longevity, reliability and are easy to implement, monitor and control.

2.2.3 Outcomes from implemented methods

Reviewing and monitoring the implemented controls becomes the part of the Check phase of the PDCA model. Where in organisations review the effectiveness and efficiency of implemented security policies and control mechanisms. In terms of our research the measurement is in terms of security assessment, compliance and non-compliance. Reviewing and monitoring of user (employee) compliance, relevant to technical controls are relatively easier as this can be done from a central computer. What the organisations find difficult to monitor, control and measure is user behaviour with IT systems within the organisation. Depending on the security level of the organisation, usually in the low to medium security organisation, the action taken is to compromise the depth and intensity of the security policies and develop an Acceptable Use Policy (AUP), which is then implemented in conjunction with the primary organisation security policies.

These AUP's are intended to have a simpler language compared to the main security policy and to highlight and define the key aspects of organisational IT systems and conduct and behaviour expected from employees. Employees are informed about what is acceptable and unacceptable behaviour with regards to compliance with the main security policy.

Organisations with high level of security, usually end up enforcing the policies and taking a carrot and a stick approach. Meaning good security behaviour or compliance is rewarded (carrot) and bad / unacceptable security behaviour or noncompliance are punished (stick) (Herath & Rao, 2009). The effectiveness of this approach has been studied from employee perspective (next section). According to Self Determination Theory (SDT) (Padayachee, 2012), extrinsic motivation is regulated by four factors, external regulation, introjection, identification and integration. External regulations are intended to ensure behaviours are satisfied by applying external demands that include deterrent controls, rewards and sanctions. Actions performed by management such as, policies, monitoring, technical controls, sanctions, rewards, play a significant role when acting as external regulators. The effects of these actions from user (employee) perspective are discussed in the next section. From management perspective these actions are intended to improve security compliance. These actions however are seen to act as external motivators which affect user security behaviour in a positive way and seem to improve user security behaviour (Padayachee, 2012)(Aurigemma & Panko, 2012). How significant is this improvement, has been explained in research conducted from employee perspective (next section)?

Researchers have found that the involvement of top management officials and management practices play an important role in creating organisational culture (Leach, 2003) which in turn has a significant impact on user security behaviour (Hu et al., 2012)(Puhakainen & Siponen, 2010). Organisational security culture is formed when security practices and behaviours are passed down from top management (CEO, CSO, CTO) to middle management (regional or plant managers), from middle management to lower management (team leaders / assistant managers) and then to employees. In the studies conducted by Puhakainen and Siponen, they found that when the top officials changed their attitude towards promoting organisation information security and became actively involved in information security issues, the security behaviour of users also showed improvement. It has also been found that management plays an important role in imparting information to employees [What they are told] and thus be a part of the cognitive process of the employees which affects their attitude towards security (Adams & Sasse, 1999). Qing believes despite abundance of literature in management and information security studies, the significant

influences of top management on employee behaviour has not been adequately studied (Hu et al., 2012). Despite several suggestions within compliance standards - ISO/IEC and CoBIT, several researchers (Adams & Sasse, 1999)(Kirlappos et al., 2014) have identified the importance and absence of management participation. The process of developing and implementing policies still has a top down approach with no involvement of employees and it is evident that this is not because of lack of interest or intention from employees (Adams & Sasse, 1999)(Kirlappos et al., 2014).

2.3 Literature review of research from End user perspective

The effectiveness of ISP is measured in terms of employee's reaction towards implemented security policies and controls, positive reaction would lead to compliance and negative reaction to noncompliance. And hence magnitude of research conducted from end user perspective is done with a primary focus to their security behaviour within the organisation and the factors which directly or indirectly affect their security behaviour. This section will address these factors which have been used to assess their perspective. Later how what approaches have been taken to address these factors have been explained and finally the outcomes from these approaches are consolidated.

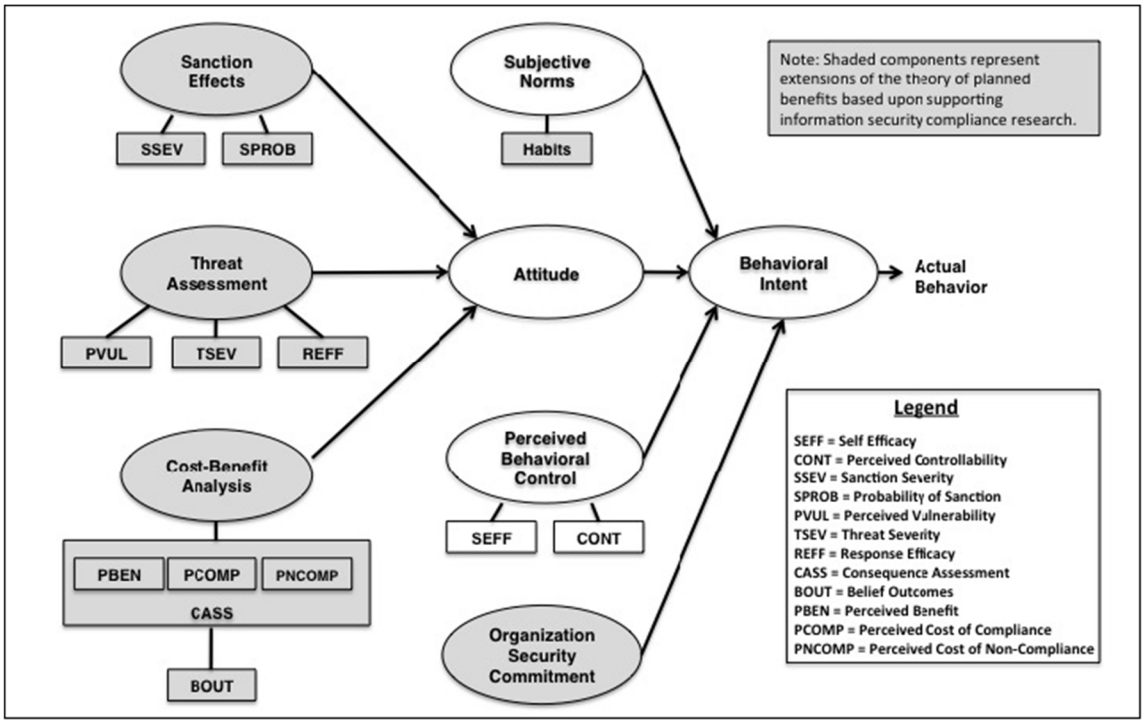


Figure 2 Lit review from end-user perspective

Fig 2. Shows the framework for literature review based on research done from end user perspective. For the sake of clarity and understanding only the key arrows are indicated however research indicates that the existing body of literature is extremely intricate and there are interdependencies between multiple factors. This framework is a composite framework based on Theory of Planned behaviour (Ajzen, 1991), attitude system (Zimbardo & Leippe, 1991), and a composite ISP behavioural compliance framework suggested by Aurigemma and Panko (Aurigemma & Panko, 2012). The use of Theory of Planned Behaviour (TPB) in ISP behavioural compliance studies is well established (Aurigemma & Panko, 2012). In TPB, Ajzen researched human behaviour using empirical data and using statistical analysis and explained how, human behavioural intention to perform a certain action is directly guided by subjective norms, attitude towards the behaviour, and perceived behavioural control. In attitude system, Zimbardo explained the different aspects involved in determining how an individual will behave in each situation, and posited that cognitions and emotions have a significant effect on a person's attitude, intention and behaviour. Aurigemma and Panko further drawing on TPB in terms of ISP behavioural compliance, explained the key factors directly influencing the attitude, subjective norms and perceived behavioural controls and thus influencing user security behaviour. It also incorporates a framework suggested by Leach (Leach, 2003) who focusses on the factors affecting the

cognition of users and describes user security behaviour based on what employees know (previous knowledge), what they see (subjective norms) and what they are told (policies, procedures, awareness etc).

2.3.1 Assessment of employee perspective

Assessment of employee perspective primarily focusses on the factors affecting their security behaviour, such as their intent to comply (and factors affecting it), their attitude (generally towards ISP's, security controls and their effects, and compliance), Cognition (ideas, belief, and knowledge) and perceptions about threat, vulnerability, cost of compliance and noncompliance etc.

Drawing on TPB, Zimbardo explains that the key aspects such as, attitude of an individual, their behavioural intentions, cognitions and their affective responses, are directly responsible for an individual's behaviour. This is supported by Thomson (Thomson & Solms, 1998) who suggested use of the attitude system to improve information security awareness programs. However, it has been observed that awareness programs aren't very effective, primarily because employees retain the knowledge from the program for a certain period after which they revert to finding alternate quicker ways of performing their daily tasks. This act is considered as a part of the subjective norms (Bulgurcu, Cavusoglu, & Benbasat, 2010)(Johnston & Warkentin, 2010)(Ng, Kankanhalli, & Xu, 2009)(Mikko Siponen, Adam Mahmood, & Pahnila, 2014) the employees are exposed to whist in their work environment. The key norms found to influence an employee's behavioural intent are habits (Aurigemma & Panko, 2012) - which the employees develop due to prolonged years of work experience at their organisations, commitment – another rule of society instilled at an early age, e.g. if you commit to do something you ensure that you do your best to carry it out (Zimbardo & Leippe, 1991), reciprocity – it refers to the characteristic that people will want to return a favour, obedience (Zimbardo & Leippe, 1991) – to authority could come due to fear, or devotion or innate nature, conformity – peer pressure such as "everyone else is doing it" , and group think (Asch 1952) – similar to conformity but specifically focusses on individuals experiencing peer pressure even when they feel other are wrong. Employees perceived social pressure on whether to follow an ISP or not, reflects their normative beliefs and social influence.

Aurigemma and Panko (Aurigemma & Panko, 2012) posited that Perceived behavioural control (PBC) (Zhang, Reithel, & Li, 2009) is another factor which influences an employee's behavioural intent. They devised the framework for ISP behavioural compliance using PBC and supporting

variable such as self-efficacy and perceived controllability. Using TPB as the core of their study the framework was designed using various constructs. The selection criteria for use of constructs for their framework was based only on empirical studies published in peer reviewed journals and conferences. And using only those construct's that were empirically evaluated in at least a third of the foundational papers and found to be significant in a majority of those (Aurigemma & Panko, 2012). Self-efficacy refers to the person's belief about their own capability to perform a task. In this case refers to their belief about their skills and abilities to perform the tasks within the ISP. Perceived controllability refers to the person's perception of whether the person is in control of their actions or if external entities are controlling their actions. A similar concept to locus of control as was explained by Rotter (Rotter, 1966).

Another factor which strongly influences the end users (employees) behavioural intent is their attitude towards security which in turn is influenced through various means such as, threat analysis, sanction effects, and cost benefit analysis (Aurigemma & Panko, 2012). Protection motivation theory (Rogers, 1975) consists of two main processes, threat assessment and coping appraisals. Herath and Rao tested their theoretical model through surveying 312 participants from 77 organisations and found that, threat assessment (Herath & Rao, 2009) is where the employee (end user) is actually concerned with a security breach and based upon the magnitude of the threat (perceived threat severity), susceptibility to the threat (perceived threat vulnerability), And based on the perceived threat severity and perceived threat vulnerability users assess the effectiveness of countermeasures (response efficacy) (Johnston & Warkentin, 2010)(Ng et al., 2009)(Zhang et al., 2009) implemented by the organisation. This is supported by tests conducted by researchers (Johnston & Warkentin, 2010)(Ng et al., 2009; Workman, Bommer, & Straub, 2008) who tested employees' perception about potential damage caused by a security threat and their perception about likelihood of them actually encountering a security threat (Bulgurcu et al., 2010)(Johnston & Warkentin, 2010)(Ng et al., 2009). Coping appraisal refers to the appraisal of the threat and the coping responses which result in the intention to comply or not to comply with the actions associated with the fear of performing that action, this could very well be the actions specified in the polices.

Cognition (Thomson & Solms, 1998) refers to a person's ideas beliefs and knowledge through which a person performs a cost benefit analysis about how one should behave when facing a situation. Leach (Leach, 2003) believes cognition is influenced from what the employees are told about security, what the employees see being practised by others around them (norms within the

organisation) and what they know about security which they could have gained from personal experiences. Intrinsic and extrinsic motivations (Padayachee, 2012) are other factors which a person considers while conducting cost benefit analysis. Cost benefit analysis (Aurigemma & Panko, 2012)(Bulgurcu et al., 2010) is where a person acquires affective and cognitive behaviour through personal experience where in a person basically performs a consequence assessment (consequences they might face) (Bulgurcu et al., 2010) based on perceived benefit of compliance, unfavourable consequence of compliance and unfavourable consequence of non-compliance. Benefits of compliance could lead to rewards (Padayachee, 2012) and consequences of non-compliance could lead to sanctions.

Sanctions also play a major role on influencing (Bulgurcu et al., 2010) the attitude of a person and its effects are based on the General Deterrence Theory (GDT). The main hypothesis of GDT is that people weigh costs and benefits when deciding whether to commit a crime, in this case whether to comply with the ISP or not (Aurigemma & Panko, 2012). Keshnee (Padayachee, 2012) also believes sanctions have a negative effect on the employees' attitude however how strong this influence is depends on the severity of the sanction and the probability of sanction being carried out. Self-efficacy and response efficacy have been found to have a positive effect on the attitude of employees.

2.3.2 Approach to implement control methods

From end user or employee perspective the most widely suggested control methods are a multitude of behaviour change methods which are intended to incline employees towards behaving more securely and thus improve compliance. These methods include stronger interventions in awareness programs in which it is suggested to involve communication and employee participation. And behaviour changing methods include direct behaviour change through instrumental learning, be it operant learning or behaviour shaping and indirectly bring about behaviour change by changing their attitude towards security and using methods of persuasion.

Communications has been identified as a significant factor to influence security behaviour. In the survey conducted by Yildirim (Yeniman Yildirim et al., 2011), their objective was to find the factors affecting information security within small and medium enterprises in Turkey. In their key findings they suggested improvement in communications leads to improvements in organisational and personal security. The limitation of this study however was that communication suggested, was limited to what should be done during the awareness programs and who the staff were

supposed to report to when they came across a security incident. Albrechtsen and Hovden (Albrechtsen & Hovden, 2010) also suggested that dialogue, participation and collective reflection would help improve security awareness and behaviour, however they suggested these actions be performed during awareness programs or training programs. This again leads to the fact that awareness programs are only effective when they are repeated as posited by Hagen (Merete Hagen et al., 2008). Which again leads to the fact that repeating awareness programs, increases intrinsic costs associated with conducting awareness programs (Kruger & Kearney, 2006). Intrinsic costs include financial costs and costs associated with taking staff away from production line during awareness programs.

Operant learning is a process in which the behaviour is modified through reinforcement and punishment as the core tools. These tools are often defined by the effect (either positive or negative) they have on the individual's behaviour. Positive reinforcement occurs when a response behaviour is followed by a stimulus which is rewarding, and negative reinforcement is when a response behaviour is followed by removal of the negative stimulus. Positive punishment also termed as "punishment "occurs when response behaviour is followed by an aversive stimulus which results in reduction of that behaviour. Negative punishment also terms as "penalty" occurs when a response behaviour is followed by removal of a positive stimulus which also results in reduction of that behaviour. In terms of ISP behavioural compliance, we have already seen the use of rewards and sanction as external motivator. When users show compliant behaviour, they are rewarded (Positive reinforcement), in case of non-compliance employees are punished (sanctions), e.g. monitory fines (positive punishment) Internet surfing/ web browsing rights taken away / loss of job (negative punishment). The severity of sanctions defines if it is a positive punishment or negative punishment.

The method of behaviour shaping also known as successive approximations primarily focusses on managing and rewarding appropriate behaviour in small steps. This is achieved by initially setting lower standards and as the person's abilities to achieve those improve the standards are gradually increased (Thomson & Solms, 1998). In terms of ISP compliance, it means awarding small tokens as rewards to employees showing desired behaviour. It is also suggested that these rewards must be earned and not just given out, and this act must be visible to other employees thereby motivating them to improve their own behaviour. It has been found that a person's behaviour changes when their attitude changes (Zimbardo & Leippe, 1991). We have seen various factors affecting a person's attitude (section 3.2.2). It is not an easy process to change someone's attitude towards

something. However, factors such as self-efficacy, intrinsic and extrinsic motivations (section 3.2.3) have been found to have a positive impact on changing a person's attitude toward security compliance (Padayachee, 2012).

Russo et al (Russo & Chaxel, 2010) posited through an experiment they conducted in which they applied process-based order effect to persuasion and showed that persuasive messages can influence behaviour without awareness. Process-based order relies on the concept that, the effects of early information is such that later information is subjectively distorted to support the opinion formed up to that point. In this experiment they observed how consumer's choice and buying behaviour is affected by TV commercials, without them having an awareness about the actual product information. In terms of ISP compliance, it is suggested that certain criteria's must be met to persuade the employee to comply with ISP's. It is considered important that employees are exposed to relevant information, the information is useful and new so that it captures the employee's attention (Thomson & Solms, 1998). Complex information should be provided in printed format and less complex information is to be broadcasted or spoken (Greenberg, J. and Baron, 1993) and hence can be easily comprehended by the employees. This also emphases the importance of quality of information provided to employees. Once comprehended this information can then be retained for longer periods of time (Zimbardo & Leippe, 1991).

2.3.3 Outcome from implemented methods

This section primarily covers research literature on effectiveness of organisational security methods from employee perspective. In the experiment conducted by Hagen et al (Merete Hagen et al., 2008) participants, or employees made a subjective assessment of the effectiveness of their respective organisational security measures in comparison to other similar organisations within the sector. They found an inverse relationship between implementation and effectiveness of the security measures. Meaning the most effective security measure (awareness programs) was also the least implemented. And the least effective security measure (security policy) was mostly implemented. The security measures compared were awareness programs, tools and methods, procedures and controls and policy.

Deterrent controls such as policies, technical controls, rewards, sanctions, which form the external regulatory (SDT) part of extrinsic motivators, have varying effects on employee attitude towards security. Rewards have a positive effect and encourages compliance whereas sanction seems to have a negative effect and found to discourage compliance. Management practices such as their

participation, organisational commitment, awareness programs, training programs, quality of information and response efficacy, also work as external motivators and have a positive effect on employee attitude. Self-efficacy which refers to people's beliefs about their own capabilities to carry out information security tasks has given birth to a new concept of "Shadow security" (Kirlappos et al., 2014). Self-efficacy, their own commitment towards the organisation, obedience to authority, have a positive effect as intrinsic motivators. Employees have also indicated that employee participation be a part of the policy development process in a form that their suggestions and feedback be considered (Adams & Sasse, 1999).

2.4 Extant theories

Tough there are a multitude of theories from social psychology, some of the key theories used in literature to understand user security behaviour are mentioned below.

2.4.1 Theory of planned behaviour (TPB)

The theory of planned behaviour is the most commonly cited theoretical model (Ajzen, 2011). It is also the most commonly used model used for predicting human behaviour. According to Ajzen (Ajzen, 1991), Theory of planned behaviour is an extension of his previous theory, Theory of reasoned actions. TPB states that an individual's behaviour is dependent on their intention to perform that behaviour. Their intention in return is dependent on their attitude towards the behaviour, the subjective norm and their perceived behavioural control (PBC). Subjective norm is defined by Ajzen as the perceived social pressure to perform a behaviour or not. And he defines perceived behavioural control as the individual's perception of their ability to perform the said behaviour. TPB has been widely used in medical and health research (Collins, Witkiewitz, & Larimer, 2011).

2.4.1.1 Theory of planned behaviour in Information security

TPB has also been used to study user's behaviour in the information security context, particularly with compliance of information security policies. In their study, Perugini and bagozzi (Perugini & Bagozzi, 2001), posited that desires have a causal effect on intentions and that the constructs attitude, subjective norm and PBC affect intentions through desires. In another study conducted by Bulgurcu et al (Bulgurcu et al., 2010) they posited that a user's intention to comply with a security policy is strongly influenced by their attitude, normative beliefs, and self-efficacy to

comply. They also posited that the users' attitude is influenced by their information security awareness, benefit of compliance, cost of compliance and cost of non-compliance.

The primary assumption of theory of planned behaviour is that an individual's behaviour can be predicted, when the individual has complete understanding of the said behaviour (Ajzen, 1991). However, this is not true for users within the information security context. Mainly because research indicates users do not understand security behaviour (Adams & Sasse, 1999).

2.4.2 Protection motivation theory

The second most popular theory for predicting user behaviour is Protection motivation Theory (PMT) (Herath & Rao, 2009)(Puhakainen & Siponen, 2010). PMT proposed that the three components of fear appeal, severity of threat, probability of occurrence and the effectiveness of coping with the event have a strong influence on the individuals intention to behave (Rogers, 1975). Perceived threat severity is defined as the individual's perception of the seriousness of the threat. Rogers posited that if the patients understood the health threat information they would adopt a health communicators recommendation (Rogers, R. W., & Prentice-Dunn, 1997).

2.4.2.1 Protection motivation theory in information security

Liang et al (Liang, Xue, & Pinsonneault, 2019) have provided a very good summary of PMT being use in IS research. They found PMT has been applied in the threat context of, internet security attacks, where it was found that constructs of PMT influence protective action and this effect was moderated by espoused culture (Y. Chen, Fatemeh, & Zahedi, n.d.). In the context online security (Tsai et al., 2016), where the researchers posited that coping appraisals increase intention but threat appraisal have no effect. In another study Tu et al (Zhiling Tu, Adkins, Yu Zhao, Zhiling, & Yu, 2019) used PMT in the context of BYOD policy compliance. PMT posits that the intention of an individual to perform a behaviour is dependent on their threat appraisal and coping appraisal. Threat appraisal has two sub constructs, threat severity, threat vulnerability (Aurigemma & Panko, 2012) and threat susceptibility (Zhiling Tu et al., 2019). Threat severity as mentioned earlier concerns the user's perception of threat. Threat vulnerability concerns user's perception of how likely a vulnerability will be attacked. Coping appraisal consists of two sub constructs. Response efficacy and self-efficacy. Response efficacy is the user's perception of how effective the response mechanism is. And self-efficacy concerns user's perception of their own capability to perform the behaviour.

2.4.3 Why PMT was used for this PHD study?

PMT has been extensively used in health relevant behaviour studies (Rajendran & Shenbagaraman, n.d.) and information security research (Johnston & Warkentin, 2010). The key reason for its widespread use is because it provides a clear distinction between threat, its severity and its efficacy (Orazi et al., 2019). It also provides a platform for researchers to individually study the effects of the different elements of threat appraisals and coping appraisals on users' behavioural intentions. In PMT fear appeal is used as a persuasive message with the intent to motivate individuals to comply with the recommended security behaviours(Johnston & Warkentin, 2010). Ajzen (Ajzen, 2011) confirms that persuasive communications are an effective method for modifying human attitudes intentions and behaviours. Rogers (Rogers, 1975) also confirms that higher the threat severity, the users intention to comply with the recommended actions is also stronger. Therefore, improving the efficacy of the security policies would increase the users understanding of threats associated with their organisations and the respective coping mechanisms implemented by the organisation.

2.4.4 Social Cognitive Theory

Social cognitive theory is another example of explaining human behaviour (Ifinedo, 2014). SCT primarily focusses on an individual's belief about their own capability also called as self-efficacy and locus of control (Workman et al., 2008). Locus of control is the degree to which and individual believes that they are in control of their actions.

2.4.4.1 Social Cognitive Theory in information security

In their study in context with system breaches, Workman et al (Workman et al., 2008) posited that Treat appraisal, coping appraisal, locus of control and self-efficacy influence the omissive behaviour of users. They emphasize that when fear appeals become chronic and extreme, people will adopt fatalistic attitude about the outcome and not take any action. Effect of locus of control and self-efficacy on users intention was supported by Ifinedo (Ifinedo, 2014).

2.5 Research gap

Even though management participation in improving organisational security has been widely established their own perceptions about information security policies or difficulties when designing policies with themselves acting as users or employees has not been extensively

researched. In their study of the impact of perceived technical protections on security behaviour Zang et al (Zhang et al., 2009) suggested that risk compensation theory, which states that people will take less cautious behaviours when they feel they are more protected, is applicable in information security context as well and posited that high security controls negatively affect employee's intention to comply and leads to less cautious behaviour. They also suggested that existence and effectiveness of technical support improves policy compliance by employees, however they did not take into consideration how these controls could affect their daily work and could negatively affect user's intention to comply.

Throughout literature review it has been identified (Kirlappos et al., 2014) that the end user does not fully understand the security polices and at the same time it is claimed that it is not possible to spell out the documentation unambiguously (Leach, 2003). Users have also noted that the policies are difficult to follow, it has not been researched as to what extent and in what way do these policies cause hindrance to their daily tasks. Despite this, users have shown the intention to follow security on their own accord, also termed as shadow security (Kirlappos et al., 2014), where users implement certain precautionary measures and mechanism themselves. Majority of research focusses on end user security behaviour from various aspects, however their perception about their own understanding of the ISP's has not been adequately explored. Research strongly indicates that bad / unacceptable user behaviour is due to misinterpretations of information received by employees. And this is based on their reasoning which is the effect of differences in their impressions and ideas about security. This begs the questions of how compliance can be improved when the users don't understand the security policies themselves. Posey et al (Posey et al., 2014) in their study provided a general comparison between information security professionals and internal employees to capture the differences in the mindset about threat perception. The classification between the two groups was done based on their knowledge and experience within the field of information security and not based on their participation in policy making. This PhD study however makes a clear distinction between policymakers and ordinary employees based on their participation in the development of their organisational information security policy. Some researchers (Blythe, Coventry, & Little, 2015) suggest that within ISP compliance different security actions are motivated by different factors hence to improve security policy compliance, research focus should move away from the usual ISP compliance paradigm and target specific behaviours however others (Beautement et al., 2016) argue that for a policy to be effective it must be targeted at specific business divisions within the organisations.

For this purpose, it is essential to understand the user's perceptions about a security policy, and how it is different from that of the policy makers. When we address this difference(s) we can find common factors which could then be used to create a framework which can be used by policymakers when designing policies. Considering recent literature, it might prove to be the most cost-effective way tackle poor compliance behaviour. Hence, part of this PhD research focusses on such targeted policies as such generalisable policies which works with both policymakers and employees would be immediately beneficial to both security researchers and information security policy makers and can be implemented to provide an immediate real world impact (Beautement et al., 2016).

2.6 Introduction to concepts developed for the purpose of this PhD research

For simplicity of understanding the overall research model is broken down into two models and presented below in order to ascertain the relationships between constructs created for study one and constructs from protection motivation theory (Rogers, 1975). The following relationships are tested through the two sub-models

1. Relationship between constructs of employee perception of security policy and those of PMT
2. Relationship between constructs of employee perception of security policy and their intent to behave securely and their actual security behaviour

2.6.1 Constructs used to enhance PMT

Leach (Leach, 2003) confirms that the users understanding of which security behaviours are expected of them, are formed by what they are told (communicated by others) what they see (behaviour practised by colleagues) and what they know (from their own past experiences). Generally, the expected security behaviours within the organisation are primarily communicated via the security policies, awareness programmes and training programmes. Therefore it is necessary to have effective interventions as Rogers (Rogers, 1975) believed that if the contents of the communication are describing unfavourable consequences it may result in failure to adopt the communicators recommended actions. Whether its new staff or existing staff people are strongly affected by the behaviour of their peers (Leach, 2003). Herath and Rao (Herath & Rao, 2009) also confirm that social pressures within organisations also act as external motivators and affect user behaviour. This is an extension to the effects of organisational citizenships (Ifinedo, 2014).

Therefore, it is important to understand the employee's perception of their organisational citizenship. The quality of information with the policy document itself has been questioned as it was found to be extremely ambiguous (Adams & Sasse, 1999). But does the perception of quality of the current policy documents add to users fear appeal need to be verified. Also, as a security policy is one of the primary means of communication within the organisation, participants perceptions of security policy document has been used as a construct. Staff make most of their decisions pertaining a security behaviour in a critical or a non-critical situation (Adams & Sasse, 1999) based on information acquired from methods above and also based on what they have experienced either in this current job role or previous job roles. Therefore, how their own perceptions either from past experiences or new experiences inform their fear appeals has been used as a construct. Effects of four constructs, employee perception of information security and its pertaining policies, employee perception of organisational interventions, employee's perception of organisational citizenship and employee perception of the current quality of policy document itself, on constructs of PMT are studied.

2.6.2 EPOS-PMT MODEL

This model focusses on effects of employee perception of security policy on their protection motivation. Employee perception of security policy is measured in terms of 1) their own understanding of the security policy, 2) their perception of organisational interventions, as in what efforts (Workman et al., 2008) (Coventry, Briggs, Blythe, & Tran, 2014) do they think their organisation has made to expose them to the importance of information security and security policy, compliance of those policies, and pertinent threats of non-compliance of those policies, and if they desire (Perugini & Bagozzi, 2001) these interventions. 3) employees organisational citizenship, as in what initiatives have they themselves taken (Kirlappos et al., 2014), and 4) their perception of the quality of the policy document itself (Jones et al., 2012). These constructs are measured in relation to constructs from protection motivation as in threat appraisal (Rogers, 1975) and coping appraisal (Zhiling Tu et al., 2019).

2.6.2.1 Constructs and variables description:

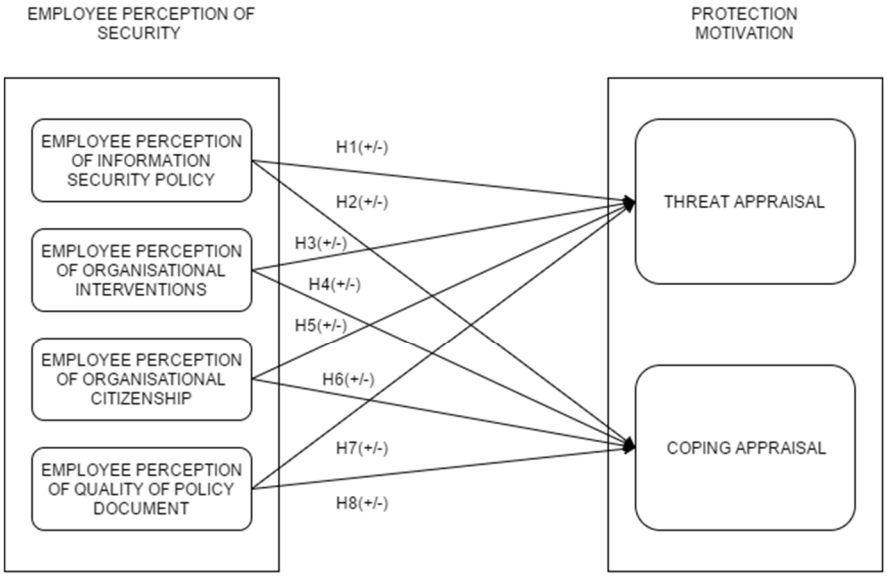
Measurement of *Employee perception of Information security (abbreviated as POIS)* is done by capturing their perception on variables such as, what information security is about, why is it relevant, how is it relevant and what does the security policy intend to protect. *Employee perception of organisational* interventions (abbreviated as POOI) (Workman et al., 2008) are

measured in terms of means organisations use to make their employees aware of their organisational goals and objectives (Muthuveloo & Rose, 2005), such as awareness programs, training programs, communication from management and policies (in this case the security policy). *Employee perception of organisational citizenship (POC)* is measured in terms of their feeling of allegiance towards the purpose of implementing the security policy, who is responsible for protecting the information, and employees own efforts (Kirlappos et al., 2014) in trying to make themselves aware of the security situation. *Employee perception of the quality of the policy document* (QOP) is measured in terms of visibility of the policy as in how easy or difficult is it to locate the document in case of need or for general understanding, the language used within the policy, the content of the policy and the length or the amount of information present within the policy.

Threat appraisal (TA) is measured in terms of *threat severity* - which is how severe is the threat of non-compliance of security policies, *threat vulnerability* (Farn, Lin, & Fung, 2004)– which is what targets would be affected in case the organisational security is compromised and *threat susceptibility* (Aurigemma & Panko, 2012)– which is the likelihood of the organisational security to be compromised.

Coping appraisal (CA) is measured in terms of the response efficacy (Tsai et al., 2016) – which is their belief on whether compliance of a security policy will avoid a threat, self-efficacy (Bandura, 1989) – which is their belief in their own ability to comply with the policies, and the response cost (Tsai et al., 2016) – which is what are the costs associated with either compliance or non-compliance of security policies.

Figure below shows the EPOS – PMT model.



MODEL 1: EPOS-PMT MODEL

2.6.3 EPOS-INTENT-BEHAVIOUR MODEL

For the purpose of easier representation, the models have been divided in to two models. This model focusses on effects of employee perception of security policy on their intention to comply with the security policy (Ifinedo, 2014) (Zhiling Tu et al., 2019) and their actual security behaviour (Kirlappos et al., 2014).

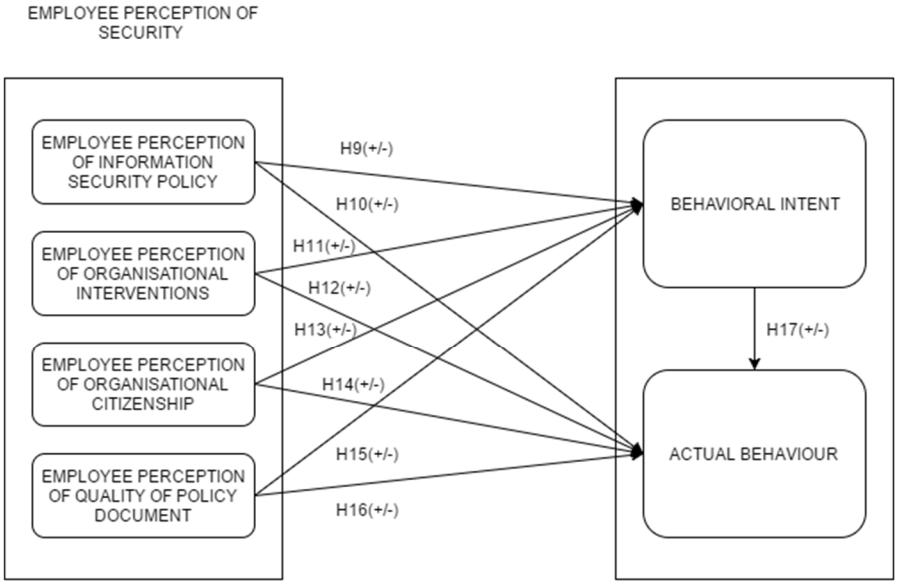
2.6.3.1 Constructs and variables description:

The constructs from employee perception of security policy are the same as mentioned above in the previous model.

In behavioural intent (BI), employee's perception of their intention to comply with the security policies is captured and measured, as in how they feel about compliance itself, what are their intentions towards acquiring security knowledge and understanding organisational security.

Their actual behaviour (AB) is captured by understanding how they behave in the organisation. As in how they regulate or motivate themselves and others to follow the security policy. Whether they follow all policies or specific policies is captured.

The figure below shows EPOS – Intent – Behaviour model.



MODEL 2: EPOS-Intent-Behaviour MODEL

2.6.4 The Novel concept of a tailored policy

Organisations generally have a centralised information security policy (Beautement et al., 2016) as such Beautement et al suggested that a policy cannot be effective unless it aligns with the goals and capabilities of employees. In their study they presented a methodology to gather large scale data on employee behaviour and their attitudes by applying scenario-based surveys and posited that organisational security interventions should be targeted according to the various business divisions. A similar notion was suggested few of the interviewees during study 1. The concept of having a tailored policy. In which they suggested that if a shorter policy with a few instructions which were relevant to their job roles was provided, it could be easy to follow it. Following up on this in study 2 usability of a tailored policy is measured in terms of its effectiveness, efficiency, and employee satisfaction (Chapter 4). Greenberg and Baron (Greenberg, J. and Baron, 1993), in their study of behaviour of employees in organisations suggested that complex information should always be given to employees in printed format so that it can be revisited and referred to whenever required and less complex information should be provided through broadcast (or spoken). This however has been implemented at an organisation level in the form of policies and awareness programs. However, we have seen that these methods aren't effective as the policies in fact include

more complex and comprehensive information. Combining this suggestion however with the requirement of employees of a tailored policy, organisational information security can most certainly be improved by providing less but relevant information accompanied by multi layered awareness programs and with multi layered awareness programs should be aimed at faculty level. In their study to design for residential heating policies, Yuan et.al. (Yuan & Choudhary, 2020) suggested that by understanding different behavioural patterns assists policy makers to better allocate their resources. Participatory policy making is a new concept which even tough has been addressed in other fields, has not yet been applied to the field of information security. In his study of relationships between citizens and governments from citizen's perspective, A Michels (Michels & De Graaf, 2010) conducted a study to find the level of involvement of citizens in the process of local municipal policy making. He concluded that it increases public engagement, encourages people to listen to a diversity of opinions, and contributes to more legitimacy of decisions. In another study T Holmes (Holmes & Scoones, 2000) applied the same study to the field of environmental policies and the participation of citizens in the policy making process. They concluded the same questioning the depth of participation involved. Meaning not all relevant groups and interests are represented and that such methods may be appropriate in some settings but not others. Papadopoulos and Warin (Papadopoulos & Warin, 2007) conducted a study to gauge the effectiveness of such participatory methods and addressed the questions of openness and access (input-legitimacy); questions regarding the quality of deliberation (throughput); questions of efficiency and effectiveness (output-legitimacy); and the issue of their insertion into the public space (questions of transparency and accountability). Almost all the studies pertaining participatory policy making have been studied in the setting of governmental organisations and citizens. Though it is understandable that such a level participation may not always be feasible or effective on a nationwide setting tough it can be achieved with lesser difficulty at an organisational level. This was confirmed by one of the participants in this study that such methods have recently been adopted. Though the effectiveness of such methods was yet to be confirmed.

3 CHAPTER 3 FINDINGS AND ANALYSIS STUDY ONE

3.1 Introduction

While exploring the relationship between organisational culture and information security culture, Lim Chang Maynard and Ahmed (Lim, Chang, Maynard, & Ahmad, 2009) posited that the organisational information security culture has an influence on employees actions and behaviours. Schlienger and Teufel (Schlienger & Teufel, 2003), define security culture as socio cultural measures that support technical security measures to improve employee behaviour. Ruighaver, Maynard and Chang (Ruighaver, Maynard, & Chang, 2007) propose security culture should also focus on the role of management, instead of only focussing on the end user perspective. As management is also made up of people it is first necessary to understand how they perceive organisational security when compared to other employees. Policymakers are expected to have the technical knowledge and skills to implement an effective information security management system (Farn et al., 2004). This however cannot be expected for all employees. There will be some employees with a lot more technical knowledge than other employees. When talking about security policies it is therefore best to distinguish groups of people as those involved in making security policies or policymakers and the rest who are expected to follow these policies as employees. To improve security culture, it is necessary to make employees aware of security threats. Better awareness, leads to changes in security culture definitively (Schlienger & Teufel, 2003). Research has identified three levels of security awareness, Perception, Comprehension, and projection (Shaw, Chen, Harris, & Huang, 2009). This study therefore tries to understand the perceptions of policymakers and employees the differences in their perceptions and if these differences could be addressed to improve organisational security behaviour.

This study addresses the following research questions:

1) How do policymakers and employees perceive organisational security policy?
2) Are there any differences in their perceptions?
3) Could they lead to employee non-compliant security behaviour?
4) How can compliance with the security policy be improved?
5) Can we find solution that works with both policymakers and employees?

3.2 Research Methodology

The main goal of this study is to create a theoretical foundation for the entire PhD study. For this we need to capture differences between two groups policymakers and employees. A total of 14 interviews were conducted. For this study only low security organisations such as academic institutions have been considered. Participants were contacted from 7 different universities from northern and southern part of England. Since the security policies of respective universities were collected from a public domain, such as the publicly available university websites, participants were contacted directly. Participation for the interview is voluntary and hence all participants were given information about the research and the researcher in advance and respective consent forms were signed before beginning the interview process. For sake of variety of data, participants are selected from different departments from within the universities. An effort has been made to recruit equal number of participants from academic departments (n=8) and administrative roles (n=6). Recruiting participants in such a way gives a better insight into the security culture of different groups that may have been formed within the different departments within their respective universities. At the same time participants selected were deemed to have varying knowledge of Information security, IT systems and handled different types of information in their daily course of work (Policymakers=4, employees=10). This approach is referred to as 'maximum variation' sampling strategy and provides heterogeneity which common patterns among groups (Posey et al., 2014). Table below summarises interviewees by their participation in policymaking viz policymakers or employees, job role, age, gender and years of experience within the organisation. Academic participants included researchers and teaching staff. Administrative participants included human resource staff, and general student support and wellbeing staff.

Table 2 Participant Demographic Information

PARTICIPANT REPRESENTATION	JOB ROLE Academic / Administrative	AGE	GENDER	YEARS IN THIS ORGANISATION	Previous Info-Sec Knowledge	PARTICIPATION IN POLICY-MAKING Policymaker/Employee
P1	Academic	32	Female	4	Yes	Employee
P2	Academic	30	Male	3	Yes	Employee
P3	Administrative	31	Female	1	No	Employee
P4	Academic	33	Female	3	No	Employee
P5	Academic	34	Male	3	No	Employee
P6	Administrative	36	Female	7	No	Employee
P7	Academic	38	Male	4	No	Employee
P8	Academic	36	Male	3	No	Employee

P9	Administrative	48	Female	4	No	Employee
P10	Academic	38	Female	5	No	Employee
PM11	Academic	52	Male	15	Yes	Policymaker
P12	Academic	45	Male	6	No	Employee
PM13	Academic	49	Male	8	Yes	Policymaker
P14	Administrative	33	Male	2	No	Employee

The interview was structured in to 5 sections namely, 1) Understanding of Information security, 2) Organisational participation, 3) Employee participation, 4) Issues following the policies, 5) How employees can be a part of the solution. Each section has approximately 5 to 6 questions with a total of 25 open ended semi-structured questions. Depending on replies from participants additional questions were asked to better understand their opinion and to probe further. These questions were created based on the concept provided by Leach(Leach, 2003) in understanding employees past and present knowledge and experiences. The first section is expected to gain an understanding of participants existing knowledge of Information security. Second section is gathering information about their opinion about organisational participation in implementing organisational security. Third section is aimed to gather their opinion about their personal involvement and about general employee involvement in implementing compliance of information security policies and procedures. For the fourth section the participants were shown their respective organisational information security and IT policies and were asked about their impression and opinion about the policies. They were also asked about the issues with complying with their respective policies. In the final section participants opinion about how, the employees could be a part of improving the organisational information security and their expectations from their organisations to facilitate this participation has been targeted.

Recruitment emails (sample in Appendix) were sent to several potential participants from different departments within different universities. The interviews were conducted in person by the author by travelling to meet the participants who agreed to be interviewed. At the beginning of the interview, participants were provided with an information sheet, which provided information about the purpose of the interview and other information about secure storage and usage of interview data, and finally the process for participant withdrawal from the project. They were asked to sign the consent forms which included their consent for participation in the interview and for recording the audio for the interview. Along with this an initial survey instrument was developed and provided before the interview, which basically collected key demographic information such as gender, age, education years of work experience, functional area of work,

number of years in this position, awareness of respective organizations information security policy and amount and purpose of usage of both organisational and personal computing devices.

For thematic analysis, the five step procedure (Srivastava et al., 2009) was used. These steps include, 1) Familiarising, where the researcher is immersed in the data by transcribing and re-reading transcripts. 2) identifying a thematic framework and emergent themes from the data, 3) indexing the data, where data is arranged according to the themes in the framework, 4) Charts are used to arrange the data identified in the previous stage and 5) mapping and interpretation, where a schematic diagram is developed. This method has been successfully used by other researchers (Blythe et al., 2015). In this study however only four of the five steps were used. The interviews were transcribed, and the author began analysis of the contents of the transcripts. Since all participants were asked the same primary questions, each section within all 14 interviews were compared with each other to identify common themes and were grouped together. Only those themes which were mentioned by more than one participant were considered. These themes were identified based on existing literature on these specific themes. The analysis and description of these themes is given below.

3.3 Findings and analysis

Information security in its simplicity can be said to address three aspects of protecting information(Farooq, Waseem, & Khairi, 2015), Confidentiality – means, ensuring all information that is protected is kept confidential and cannot be accessed by unauthorised user, Integrity – means, ensuring all protected information cannot modified by unauthorised users, and Availability – meaning, all protected information can always be access by authorised users only. The findings from the study are summarised below.

Interview participants were asked about their perceptions of information security, its need or necessity. They were asked if they felt it was necessary or important to their organisation or themselves in any way. They were also asked about the type of information they worked with and if they had experienced any security incidents. In the data collected participants showed varied level of understanding of information security. Even though none showed complete understanding, some participants showed partial or minimal understanding of information security. When participants were asked what they thought information security was about, most displayed knowledge to an extent it was about protecting information or data with no knowledge of how it was to be protected. Only one participant showed concern from external threats and said

data was to be protected from outside people, implying people not working within the organisation.

P2 "… What is information security… umm… information security I guess at a very high level is trying to maintain your information safe from outside people…"

Survey conducted by PWC-US (2018) shows information security is not just about protecting information from outside threats but insider threats as well where current employees contribute to 30% of the total security incidents. Chinchani Et Al. (Chinchani, Iyer, Ngo, & Upadhyaya, 2005) define insider threats as legitimate users who maliciously leverage their system privileges, and familiarity and proximity to their computational environment to compromise valuable information or inflict damage.

When probed further participants also showed some level of misunderstanding about information security. They thought information security was only related to IT or people working in IT and that information security behaviour is common sense.

P4 "… so this is very specific to I would say to IT and not putting things on your computer that aren't licensed and that they monitor everything, but yes I have never seen anything as specific, looks quite complicated, it's got a lot of sections, this one seems pretty technical, I would probably think it was specifically for people working in IT…"

Al-Omari Et.al (Al-Omari, Deokar, El-Gayar, Walters, & Aleassa, 2013) posit that all users, must be aware of their roles and responsibilities in protecting information assets and of how to respond to any potential threats. To this Wilson et.al. (Wilson et al., 2009) add that users should understand individual accountability and applicable governing documents such as the Computer Security Act, Computer Fraud and Abuse Act, Copyright Act and Privacy Act. Summarising, anyone who uses IT resource of an organisation should be responsible for its safe use and protection.

P5 "…I think most people will use common sense rather than thinking like having a policy in mind that they are following…"

P3 "… actually they are talking about what you should do and what you shouldn't do, which is a bit of common sense…"

Even though users might think it is common sense, John Leach (Leach, 2003) argues that it is the lack of common sense that increases the internal security threat.

The most common interventions an organisation can put in place to implement organisation wide information security are awareness programs, these can be individual or group sessions, training programs – these can be personal or online, and an information security policy which all management and non-management employees alike must adhere to (Wilson et al., 2009). During the interview, participants where asked questions to gauge their perceptions about which interventions they think their organisation implements. It is surprising that none of the participants were even aware that their organisation implemented awareness programs and had an information security policy, which they were expected to comply with (Boss, Kirsch, Angermeier, Shingler, & Boss, 2017). Though there is multitude of research (Albrechtsen & Hovden, 2009) (Broderick, 2006) present which emphasize on the need for an awareness programme, all participants replied there were no information security awareness programs within their organisations. Most awareness and training programs have budgetary constraints (Furnell, Gennatou, & Dowland, 2002), from a business perspective, Van Niekerk and Von Solms (Van Niekerk & Von Solms, 2010) report that any solution would be adequate as long as it is cost effective. The participants acknowledged the existence of training programs, however the topics covered within these training programs only related to their daily job tasks and not to information security at all. Eminagaoglu et.al. (Eminağaoğlu, Uçar, & Eren, 2009) in their study support the importance of effective training programs by positing the positive outcomes of having information security topics within the training programs.

Surely people now a days are more aware about password protection, computer viruses and spam emails, which was also evident from the interviews as these are the three thing's participants mentioned when asked about their experiences with security threats or events. But then again, they showed poor knowledge about password protection policies and how to handle spam emails as one participant pointed out.

P12 "…So I know every service I subscribe to I have to keep a separate password, so I know I have to do that and I came out with a system, but it's just way to complicated so I give it up, so when I know something, and I am even not doing it for myself I am not doing this for my work also. I wouldn't do it because I would just think there is no point it's not that my information even

if it's leaked would cause any trouble to me so it's ok… Many of the things are like common sense but people are not doing it, like using a different password for every different service…"

Eminagaoglu et.al. (Eminağaoğlu et al., 2009) conducted a study in a Turkish company with over 2900 employees, focussing on training programs which included password usage, password quality and measured the outcome of the training program with compliance of employees with the password policies of the company. Their result showed a positive effectiveness and impact of the training program on employee awareness.

When asked about computer viruses, they said it is the IT department who basically looks in to it and the employees are occasionally informed via email, about a rouge spam email or a computer virus moving around the network, however employees were never educated in terms of what they are supposed to do in such security events. Participants pointed that they were not exclusively made aware of any such password protection policies and spam reporting mechanisms and hence exercised their own caution and self-judgement on addressing these issues.

P1 "…I know that they put a lot of information on the IT websites and things I think, I have never read any of it but in terms of offering any course or training to let staff know why those things are in place, I've never been on one, I don't know if that's me not paying attention, yeah I don't think that there's anything that they've specifically setup…"

Confirming the ineffectiveness of these methods of posting information on IT websites or sending security emails, Kumaraguru et.al (Kumaraguru et al., 2007) in their study found that an embedded training email system which teaches employees phishing attempts, works better than the current practice of sending security notices. This is further supported by Shaw et.al. (Shaw et al., 2009) who posit on the information richness of information security training programs, that participants with better understanding of information security awareness training material perform better in their security behaviour.

P1 "…so when it first started my instinct was to contact IT and say this is a lot of spam a lot of things that have been saying click on here and flashing boxes and that was their advice to just delete things. But now I try and just assess what's really dodgy and what seems like a legitimate work email. IT do send out periodic email saying this is fishing or this is spam or this is a virus and they send that to all staff, but normally its two days after all the emails have come through

and everybody has had them. So my policy is now to just try and work it out myself and delete things that look bad…"

P2 "…I am quite sensible with the things that I open though… I received any spams you mean… oh well yeah I have about like 50 a day, phishing emails as well I would say about 2 a day but I have not fallen for them,…"

In their study, Kirlappos et.al. (Kirlappos et al., 2014) confirmed these behaviours of employees and coined the term *"Shadow Security"*. They posited that employees who are security conscious, take it on themselves to behave securely creating an alternative to the practices created by the organisation's official security staff.

These interviews were conducted within universities across UK, based on extant research and the observed security culture, it was assumed that these are low security organisations, and the information that needed to be protected was personal information of all employees and students. Personal information was expected to include research data, student information, staff payroll data, and biographic information of all home and international staff and students. As this kind of information is the most common target for Identity thefts (K. B. Anderson et al., 2008). During the interview questions were asked to ascertain what type of data the participants thought needed to be protected. Researchers strongly emphasised protecting their research data and the participant information they use for their own research, mentioning they were bound by the university ethics approval policies and hence had to protect such information,

P2 "…I work with participant data, results from studies that I have set, so in that case I don't know why anyone would generally want to get that kind of information and if they did I am not sure how useful it would be unless if were my competitor so to speak in the same field, but in out information sheets and so on, when we collect the data, we say that only the researchers will have access to it, so if it were to leak then it would be in breach of that, yeah but it's not like losing credit card numbers or anything like that…"

Whereas teaching and administrative staff thought protecting their organisational data, such as student data or exam data was very important.

P14 "…students record, student performance their evaluations and things that shouldn't be shared and also extenuating circumstances where the students have health concerns and things like that should be protected…"

Though quite surprisingly not one participant mentioned that their personal information held within the university needs to be protected as well. It is quite clear that the participants lacked a sense of risk or consequences associated with loss of personal information. Li, Sarathy and Xu (Li, Sarathy, & Xu, 2011) validate that disclosure of personal information inevitably implies the potential loss of control or risk of personal information.

P10 "…So I know every service I subscribe to I have to keep a separate password, so I know I have to do that and I came out with a system, but it's just way to complicated so I give it up, so when I know something and I am even not doing it for myself I am not doing this for my work also. I wouldn't do it because I would just think there is no point it's not that my information even if it's leaked would cause any trouble to me so it's ok…"

Most companies use simple information such as a date of birth as a method of account holder verification process (K. B. Anderson et al., 2008), getting access to this harmless information could potentially lead to getting access to more personal information which could then be used for malicious purposes.

There also were participants who were totally unaware of what information security was all about and said they never thought about it or didn't care about it.

P3 "…I never thought of it. And I really don't know. So, what is it?..."

P8 "…I think the answer is that I wouldn't know what to do, let me explain with an example from somewhere else, we are hired as lecturers and teachers and we are told you are now in charge of that course, that's what we are told, no one says you have to lecture in that way, you just lecture, so for the most important thing that we are doing even our research is the same, we are not really told by our boss how to do it, I was not told how to teach, I was not told what to do with information security…"

This shows that the employees don't realise that when they are working for an organisation along with their job responsibilities they are also bound by the organisational policies which they are expected to adhere to (Wilson et al., 2009).

On the other hand, when policymakers were asked what they thought about information security and the kind of information they needed to protect. They perceive information security is about protecting organisational data (Albrechtsen & Hovden, 2009) and more importantly the organisational information security policy was a means to protect the organisational reputation and resources (Bulgurcu et al., 2010) against any litigation from students or collaborators industrial funded research projects.

Pm11 "…primarily it's about protecting the organisations data so protecting its reputation against sort of litigation from primarily these days from students or collaborators we have on industrial funded research projects…"

3.3.1 Themes affecting compliance

Ten themes emerged from the data analysis. The table below provides a brief description of the themes.

Themes	Brief Description
1) Awareness	Assessment of current security awareness level characterised by presence of awareness and training programs
2) Accountability	Assessed by how compliance is percieved within the organisation
3) Visibility of policy	Assessment of accessibility of organisational security policies
4) Relevance of information	Perception of information within the policies in terms of language and content
5) Duty	Assessment of obligation of compliance

6) Commitment	Assessment of commitment shown by employees towards organisations and organisational commitment towards employees
7) Responsibility	Assessment of acceptance of liability
8) Interdependence	
9) Communication	Assessment of communication between management and employees in terms of its importance, its presence or its need.
10) Tailored policy	Finding a common ground which both policymakers and employees can agree to.

These themes were found to have considerable differences between policymakers and employees which are discussed below.

3.3.1.1 Awareness and accountability

This study was conducted within education providing institutes, so it is obvious that majority of the staff hired were teaching or research staff. For sake of gathering diverse opinion, staff from within administrative roles such as HR and student advisory and support roles were also recruited for this study. Like teaching and research staff, they expressed their concern for protecting student data, mostly emphasising on student grades and exam data.

P14 "…students record, student performance their evaluations and things that shouldn't be shared and also extenuating circumstances where the students have health concerns and things like that should be protected…"

They knew that this information needed to be protected, however they didn't have a clear understanding of why this information was to be protected or what other information needed to be protected (Albrechtsen, 2007). From their responses it seemed that they were simply following

their job description as to what was expected from them by their managers in terms of their daily job tasks. Participants from student advisory roles working with student's personal information said they had been trained in data protection but not information security.

P6 "…no the training is like fire safety, health and safety, fraud, and it's all on our online system and annually you get reminders to do it, but I don't think there is one that is specifically related to IT awareness or security…frauds like data protection, like a module on data protection and its online, and I am sure it relates to the data protection act, and if people make like a subject access request or a freedom of information all that kind of area, so we have an online training on that, and we have to go through it annually…"

This clearly shows that even if employees are trained in information security they are not aware that they have been trained in information security or what this training was about.

Of course, in this case the quality of the training program can be questioned (Shaw et al., 2009), however this clearly displays the state of awareness of information security within employees and employee's perception about information security within an educational environment such as universities. Policy makers expressed their concerns about the level of information security awareness within their organisation and said this was the battle they were still fighting (Albrechtsen, 2007).

Pm13 "…yes I think so, I think the first battle is to raise people's awareness, second battle is to make secure behaviour sort of second nature to people and it would be difficult for me to put my hand on that and say that we have actually gone on to that second stage with everyone here at the college by now but it something to work towards I would say…"

They confirmed the existence of information security awareness programs and online training programs but added they were not mandatory to all staff, particularly to research and teaching staff. They mentioned the policy and the training programs were online and perceived that the level of security awareness of staff to be quite high, quite contrary to what their employees perceived that the policy or the training program was not visible enough to be categorised as something important for example as a health and safety training program. Participants displayed lack of understanding of security issues (Albrechtsen, 2007), no awareness of security events and said they did not know what they were supposed to do in case of a security incident or who they are supposed to get in touch with to notify a security breach. Chen Shaw and Yang (C. C. Chen,

Shaw, & Yang, 2006) suggest for an effective Information Security Awareness System (ISAS), its need to have the capabilities both for the users to report security events, and the management to act upon them. They further suggest that management needs to document lessons learned each time issues are resolved, and such security events are documented along with their solutions. A clear gap within the perception levels of employees and policy makers is evident here which needs to be addressed if the organisational information security compliance level is to be improved.

3.3.1.2 Visibility of policy

Participants were asked what efforts they have made to make themselves aware of and understand their organisational information security and its pertaining policies. Since all participants claimed they had never even seen their organisational information security policies as it was not clearly made visible by the management, either in person or on the university website, hence each participant was handed their respective organisational information security policies by the interviewer and asked to skim through the policy document. Responses were recorded in the form of their live commentary about their opinion/impression of their respective organisational information security policies. These policy documents were easily available on the university websites in a public domain to whoever wished or tried to review them. The interviewer knew exactly which document to look for hence it was easy to locate the policy documents, however this could not be said to be true for the employees who didn't even know such a policy existed.

P3 "…maybe I have heard of some of them, but I have never seen this page (webpage which shows all the policies listed on the university website) I am aware of some of the policies, but I am not aware of this list, where did you find this…"

On the other hand policymakers believe that the policies are freely available online on the university websites.

Pm11 "…, I mean these are available online so these are always available to go and look at in detail…"

3.3.1.3 Relevance of information

When asked why no effort was made to make themselves aware of this policy, most replied they didn't know about this policy, and surprisingly some said they didn't care about information security as it was not relevant to them. Albrechtsen and Hovden (Albrechtsen & Hovden, 2009)

in their study, also noticed the lack of visibility of the policy document. They reported the document was either not readily available or difficult to find. When shown their respective policies, participants found the policy document to be extremely lengthy, there were to many documents and they normally wouldn't want to waste their time going through them. This is supported by Hone and Eloff (Höne & Eloff, 2002) in their review of What makes an effective Information security policy. They reported users claims of the policy being too long or too technical, and that the users did not see the relationship between the policy and their daily tasks, and see it as a nuisance.

P2 "…I guess they just have to read it properly, ITS TOO LONG, who has the time to read all this? I mean look at this 5.2, 5.2.1, 5.2.2, 5.2.3 up until 8, 5.8.1. 5.8.2, 6.1, 6.2, 6.2.1, who has the will or the time or the motivation to go through this…"

P10 "…This basically is 16 17 pages, if you read it quickly it maybe takes you 15 mins, if you want to read it carefully, and you really want to understand everything, for me it would probably take close to an hour, to read it really really carefully and even if you read it carefully after half a year you have forgotten it, so I think if the head of the department decided to send it around to everyone and asked to do it then, they would probably decide not to do it as because they think spending an hour more on the research has potentially some benefit but there is hardly any benefit from this…"

After skimming the policy document, participants found a variety of issues with following the document. Apart from being too lengthy and too many, they perceived the information within the documents to be irrelevant to them. Hone and Eloff (Höne & Eloff, 2002), in their review suggest that to be fully effective, the policy needs to incorporate both the users needs for accurate and reliable information, as well as the business's needs for achieving its strategic objectives. The appearance or the layout of the policy document was regarded as very unattractive and not very appealing. Albrechtsen and Hovden (Albrechtsen & Hovden, 2009) agree that the tone of the documentation is admonitory and puts people off.

P9 "…This is not designed to educate someone, this looks more like a database…"

The language used within the policy document was found to be complicated, too technical and difficult to understand (Albrechtsen & Hovden, 2009). It seems most employees simply presume that they are expected to do their job and everything else is not allowed. This even though makes

them more efficient and productive at work, however does not necessarily make them aware of information security or the implications associated with non-compliance of a security policy. As one policy-maker pointed, employees read the policy only when they get in to some sort of trouble.

Pm11 "…I agree like many institutional are written kind of pseudo legal sense and not very easy to understand and navigate they are certain not something that people would refer to possibly on a daily basis unfortunately they will too often will only be referred to when there has been a breach of policy and there has been some kind of a disciplinary proceedings going on as a result…"

There were a few other themes which were also identified during data analysis. Some participants showed trust on the people within the organisational management. Albrechtsen and Hovden (Albrechtsen & Hovden, 2009) identified that even though users trust in their security managers and the technology to take care of security, the managers did not trust the users. Kirlappos and Sasse (Kirlappos & Sasse, 2014) support this by saying that current focus on designing security systems are to restrict user actions. They argue that an important but often neglected aspect of compliance is trusting employees to do what is right for security.

P10 "…Not knowing in detail what it all says, I am not sure whether I can answer. I think it's certainly possible to follow, those people are sensible people who made this policy, they wouldn't have come up with a policy which you cannot follow…"

3.3.1.4 Duty

Participants do realise to some extent that they are bound by some organisational policies, such as HR policies, and perceive information security policy is not one of them and that information security is something the organisation should be responsible for and claimed it was the organisations duty to protect their personal information,

P4 "…of course they have our personal information, so they have the duty to protect our personal information…"

A certain sense of lack of attachment with the organisation can also be seen from some responses where participants feel employees usually change jobs after a certain duration and hence they cannot be bothered with compliance of information security where they would rather be doing what they were hired to do in the first place. Ifinedo (Ifinedo, 2014) in his research tried to

establish a relationship between Attachment and attitude towards ISP compliance how ever did not find substantial results.

P10 "…We are in a world, I don't know, where many people stay for three years four years and then they move on, I don't think when they start, they would be bothered to read all kinds of things … everyone thinks it's not really helping to do what we are supposed to be doing which is teach well and publish well…"

3.3.1.5 Commitment

Commitment is another theme which originated from data analysis where employees thought the organisation is not thinking about employees when designing these policies. They thought the policy was not to protect the employees, which was also confirmed by one of the policymakers that the primary purpose of the policy is to protect the organisation. Ifinedo (Ifinedo, 2014) in his study found commitment has a positive effect on attitude towards ISP compliance.

P1 "…I very much feel that a lot of these things are to protect the university and cover certain rules that they've got to obey reading these sorts of things like breaches and this would be investigated, I don't think that's to protect me or my data…"

3.3.1.6 Responsibility and interdependence

It seems lack of sense of protection directly leads to self-protection and results in both parties starting to play the blame game, where the employees blame the organisation for not complying with their own policy (Albrechtsen & Hovden, 2009).

P1 "…but also these things about physical security, all equipment must be physically secured and locked, honestly our door has been broken for almost two months, so all of our equipment isn't secured and safe, but that to me that's the universities fault, not mine if a computer gets stolen. We have reported the issue…"

And the management blames the employees for not following the policy, and it is their responsibility to find out what information or policy is relevant to them.

Pm11 "…I would say that that guidelines are probably more important the general policies for the staff to find out what's important to them, I mean these are available online so these are always available to go and look at in detail… unfortunately they will too often will only be referred to

when there has been a breach of policy and there has been some kind of a disciplinary proceedings going on as a result…"

It is a common notion that compliance also causes hindrances to employee's daily job tasks due to technical security procedures in terms of time spent complying with the policy and disruption to work flow, as a couple of the participants pointed, This was also noted by Hone and Eloff (Höne & Eloff, 2002) in their study stating that users found complying with security policy as a nuisance.

P1 "…it because every time you have to get something downloads you can't do it but you have to have these updates otherwise you have an out of date piece of software…"

P9 "…So here this policy states that I should not use my personal email address for work, So on this occasion my assistant sent me some files on my university email address, but for some reason, I don't know what , I couldn't open it on my computer, so then I asked her to send it on my personal email, and this time again for some reason I don't know why it worked, I also use my private skype to talk to the head of the department and students, so if I had to open a new account in order to do that I think its inconvenient and it's not efficient, so I guess there would be things which probably would be sensible to do, but my assistant trying to send me a file and not working, it doesn't justify spending time trying to figure out a way just to get this across to me. So, I think there would be some inconveniences if you were to follow this entirely…"

P10 "…I do want to maximise my time doing research, everything that takes time away from my research, I am not very happy about that. So, improving this kind of thing has nothing to do with me, I am not gonna get promoted because of that, I am not very interested…"

Employees feel complying with the policy is always not efficient and may not always be the sensible thing to do. Kirlappos and Sasse (Kirlappos et al., 2014) agree that security restrictions led to disruptions of employee tasks.

Near the end of the interview participants were asked their views about employees being a part of improving organisational information security, in what capacity could the employees help, and what the organisation could do help the employees to improve compliance. Most common responses identified feedback, communication and a tailored policy to be something that would certainly improve employee compliance of information security policies.

3.3.1.7 Feedback and communication

It has been acknowledged in research that feedback from employees could in fact help improve the design process of policies and thus improve compliance. However, it has also been acknowledged that employees' feedback is widely ignored (Kirlappos et al., 2014). During this study as well, employees expressed the need of some sort employee involvement either in terms of an employee forum or feedback system which would enable the management to understand how things are done at employee level.

P1 "…But actually if someone came in to our office and saw how we worked and saw how we store data and saw how we communicated they could perhaps learn something and to understand why things might go wrong…"

To this a policymaker replied communication is not always easy. Adams and Blandford (Adams & Blandford, 2005) argue that open communication about security requirement helps the community understand security risks while increasing motivation to adhere to changes in work practices. They also add that poor communication from IT department about security mechanisms provoked their misuse by some employees.

P13 *"…I think that's a difficult one I think communications always a problem, we have had lengthy debates about what's the best way to actually communicate these issues to the general staff, we have a college sort of release paper which comes out three times a term, and some point last year I think they featured issues around cyber security to actually point people to the course to what ICT would do, but certainly thinking about the academic community who maybe see hundreds of emails a day for them maybe emails isn't the most effective way of communicating it's one of a different group of communication mechanisms and hope one of them will get through…"*

Feedback systems are also not without its pitfalls, as one participant identified, people would simply make unjustified requests, which may not necessarily be in the interest of improving organisational information security.

P1 "…everybody will say that I don't want a password I want to able to download whatever I want I realise that these things are in place to stop people doing silly things in the workplace…"

3.3.1.8 Tailored policy

The researcher did not find any evidence in existing literature to support the existence of this method of having a tailored Security policy to improve organisational security behaviour. The researcher decided to pursue this theme anticipating a novel contribution to existing research.

A more common solution which both employees and the policy-makers agreed, was a tailored information security policy. Tailored in the sense that employees are being given policies which tell them what is relevant to them and to their job roles. All participants expressed this was something they would be encouraged to comply with. They expected the policies to be short with fewer instructions– one or two pages and the information within the policies should be relevant to them.

P2 "…it would definitely help. Yeah so. As I said a lot of those (pointing to policy) didn't apply to me, maybe just get told you know in a user-friendly way, "this is what YOU have to do", yeah that would be a good thing…"

P4 "…yes that would be easier to follow and that would be also more interesting to read…"

P10 "…It would be better if it would one or two pages. And also, something that I don't already know…"

Participants feel if the policy was tailored it would be easy to follow as different departments have different ways of functioning,

P5 "…yes if the policy was tailored to what your role is that way you could access it quicker whereas now there are sections in there that aren't remotely relevant, then it looks like a harder way to get through and or probably not gonna refer to it…"

P1 "…yeah I mean a lot of this (pointing to the policy) is university wide but actually there are different issues with different programs that psychologists will use, different bits of equipment they have to use, different spaces they have to access, different things they need to download, so yeah something more tailored to what people are doing day to day rather than, 'these are all the rules follow them' it would be better yeah…"

To this one policymaker replied this however would increase the amount of effort on the policymaker's part, simultaneously as policies exist for different faculties it would certainly be possible to develop tailored information security policies.

Pm11 "…I think there sort of are issue clearly in terms of the effort involved in developing those policies but at the same time if we look at other areas of college's business we at least have policies which are specific to different faculties, so there are presidents of the college to develop bespoke policies certainly for different faculties in the college, so doing so for different job families shouldn't be too much of a challenge, I don't think so…"

3.4 Limitations of this study

This study focusses on low security organisations such as academic institutions, there is a strong possibility that the participants may not have already read the organisational security policies, in which case the findings may not be substantial enough to develop a model. It is therefore essential to conduct further studies to get a comprehensive understanding of perceptions of employees working in medium and high security organisations as well. This will enable to formulate a more generalised measurement model which can be implemented in any type of organisation.

3.5 Summary and Conclusion

Perception means, the way in which something is regarded, understood or interpreted. To understand something, we must first gain or acquire knowledge about said something. Acquiring knowledge of a skill or something is also termed as learning. Cognitive psychologists believe that four stages of information processing are used in learning: input, integration, storage, and output. Input referring to taking in all the information that is present basically analysis of the stimuli, stimuli is usually through our 5 senses, sight, hearing, touch, taste, and smell. Integration means processing the information, where we use our brains to process the information and prepare and appropriate response to the stimuli. Storage of information again takes place within our brain where we confirm the information we have already known and add new information which we have learnt, and finally output which refers to output behaviour that was decided after we have processed the information. To comply with the policy, one must first read and understand the policy. One must understand what behaviour - that which is mentioned in the policy, is expected of the individual to facilitate good organisational security behaviour. The stimuli here being the policy, input is reading the policy and making sense of it. Integrations is processing the

information within the policy, understanding the information, and storing it in your memory and then the output is the user security behaviour.

Now if the very first step of the learning process is flawed or incomplete, i.e., the employees have not clearly understood or misunderstood information security and/or its pertaining policies, the information integrated and stored by the employees could be a misinterpretation of info sec and thus lead to bad or unacceptable info sec behaviour. Since the employees lack a clear understanding of info sec, they are themselves not aware that such behaviour is unacceptable. So, if the users do not understand information security, they will by default not know how to behave with information securely. The alternative to 'behaving securely through understanding info sec', is to 'rely on someone else's understanding of info sec', which is first, to follow how others (colleagues or supervisors) within the organisation are behaving (What they see), second, to follow instructions provided by supervisors (what they are told) instructions could be in the form of policies procedures, awareness and training programs, and third, when the user believes they have learnt what they need to know, use common sense on how to behave securely (based on what they know or acquired knowledge). These alternatives themselves have many issues associated with them, e.g. There is no guarantee or assurance that the colleagues are themselves well informed about information security and are behaving in a secure way, so simply following what they are doing may not necessarily lead to better security compliance behaviour, instructions provided by supervisors or higher officials are not always easily understandable and often difficult to follow, here again the usability of information provided by supervisors and upper management is questionable, and finally research clearly shows that information security behaviour is not common sense, if it was in fact common sense we would not have compliance issues. The two main problems that make perception difficult are that either there is 'too much information' or there is 'not enough information'. From employee perspective we have seen both to be present, in case of compliance with policies. Employees believe there is too much information within the policies and not enough relevant information within the policies. So, the question that needs to be asked is how we can provide minimal yet necessary information to employees which can also be easily understood by them and help them to comply with information security policies thus improving organisational information security compliance. The solution from both employee's perspective and policymaker's perspective seems to be participatory policy generation methods and tailored policies.

The table below shows how the identified themes where grouped together to form the constructs created for enhancing PMT.

Table 3 Themes grouped within the created constructs

Constructs	Themes
Information security Awareness	Security Awareness
Organisational Interventions	Awareness Programs
	Communication
	Training Programs
Organisational Citizenship	Duty
	Commitment
	Responsibility
	Interdependence
	Accountability
Quality of Policy documents	Visibility of policy
	Relevance of information in the policy
Tailored policy	Common grounds

In the following chapter the effects of these constructs on constructs of PMT are measured. The items within the survey instrument were created using these themes.

Based on data analysis clear differences in perception levels of employees and policymakers were observed which have been summarised in a tabular format below along with the factors which affect compliance have been identified. However due to a small sample size this cannot be considered as it would be applicable generally. However, this can used as a basis for designing a further study to substantiate the findings.

Table 4 Differences in perceptions of policy makers and employees

Differences in perception of policymakers and employees			
S. No	Factors affecting compliance	Employee's perception	Policymakers' perception
1	Awareness	No awareness programs	Awareness programs in place but not mandatory
2	Accountability	Compliance not part of my job description	Employees bound by policy

3	Visibility of policy	Policy Not visible	Policy available online
4	Relevance of information in the policy	Too much info, irrelevant info,	Following guidelines, pseudo legal language
5	Duty	Organization's duty to protect my info	Employees refer to policy only when in trouble, it's their duty to follow policies
6	Commitment	Policy is not to protect us	Policy to protect the organization
7	Responsibility	Not my responsibility	Staff should find out what's important to them
8	Interdependence	Organization should tell us what to do	Rely on employees to follow policy
9	Communication	Want communication	Communication is difficult
10	Common grounds	Want a tailored policy	Requires increased effort, however, can be done.

Factors such as allegiance, accountability communication gap, relevance of information within the policy document, visibility of the policy, interdependence of organisation and employees to comply with the ISP, responsibility, awareness, and duty were found to be the key factors where differences of perception between employees and policymakers was observed. However, this was observed in employees from low security organisations. We need to find if this is true for medium and high security organisations. In this chapter we have identified a solution to our research questions 4 and 5 where participants claimed a tailored policy may improve security policy compliance. However this need further exploration and a statistical justification which is provided in chapters 5.

So, going forward we will assess the individual effects of each construct in Table 3, viz. Information security awareness, Organisational interventions, Organisational commitment, and quality of policy documents on the constructs of PMT viz. Threat Appraisal, Coping appraisal and behavioural intent. We will also assess if having a tailored policy has any effect on the relationships between these constructs. This is done by creating a survey instrument and administering it to a wide variety of audience to cater to our attempt of finding a framework that works for all types of organisations and all types of employees. This is then followed by creating

a structural equation model using the data from the survey. Here we will verify this framework using multi group analysis for two groups viz policymakers and employees. We will also use tailored policy as a moderator and test its moderation effects on the pathways between constructs. All of this will be done using the security level of the organisations viz. low security, medium security and high security, as controls.

4 CHAPTER 4 EMPLOYEES VS POLICYMAKERS – Study Two (Survey)

4.1 Introduction

The findings from this study are separated in to two parts. This chapter focusses on the first part and reports the findings from the survey and forms a comparative description of differences in perceptions of employees and policymakers. In the previous chapter we identified several themes which were used to create item statements for the following survey instrument (In Appendix).

This chapter focusses on addressing the following research question:

1) Are there any differences in the perceptions of policymakers and employees?

Though we addressed the first three questions in the previous chapter and study however that was done only for low security organisations. To develop an effective generalised model these questions, need to be addressed again for all types of organisations with varying levels of security. So, for this study organisations with low, medium, and high security levels are considered. A statistical analysis of the constructs is presented using cross tabs analysis, highlighting how participants feel about certain items and how this relates to their opinions about items in other constructs. Constructs related to protection motivation theory are reported in the structural equation model chapter. The structure begins with a report of the participants demographic information followed by the analysis of this information. Only key demographics relevant to this research are analysed, such as security level of the organisation, type of information handled on the job by participants and analysed against their involvement in designing / implementing their organisational security policies, i.e. policymaker's vs employees.

4.2 Research methodology

It is difficult to get accurate measurements of attitudes and emotions (Al-Omari et al., 2013). Al Omari et al also reviewed that self-reporting via surveys, questionnaires and interviews are a very common way of gathering data in almost all of social sciences. They also suggest people are expected to be able to report their internal states such as attitudes and perceptions. Therefore, based on literature review and findings from previous study an initial survey instrument was developed.

4.2.1 Item development

A total of 100 item statements were created. 13 item statements were used to collect demographic information of participants. Demographics inform was to include, current employment status, age, education, total work experience, number of years worked in the current organisation, department working within the organisation, job position. Further questions were asked to get their perception of their organisational security level, how they would rate their organisations security procedures, what sort of information they handled on the job, are they involved in designing organisational security policies, their current knowledge about IT systems, and their current knowledge about information security. 72 item statements were created for the measurement of core constructs, Knowledge of information security (12 item statements), Perception of organisational interventions (13 item statements), their perception of organisation citizenship (9 item statements), and their perception of current quality of policy documents (12 item statements). 32 items were created for all the constructs from Protection motivation theory. 9 item statements for Threat Appraisal, 11 item statements for Coping appraisal, 6 items statements for their intent to follow a security policy, 6 item statements to measure their actual security behaviour

4.2.2 Data collection

For the purpose of administering the survey, and online survey tool, Qualtrics, was used. Qualtrics has been recommended (Barnhoorn, Haasnoot, Bocanegra, & van Steenbergen, 2014) as a very good online survey tool. Researchers (Benton, Pappas, & Pappas, 2011) (Boas, Christenson, & Glick, 2018) often use Qualtrics to find participants from all across the world in order get a diversified opinion. In this research we used Qualtrics to find users primarily from across UK. As in the previous study one, this time we focussed on finding participants from low medium and high security organisations. We also used participation in policy making as one of the selection panel for the survey. This was in order to capture separate opinions and differentiate between policymakers and employees. Sector to which the organisation belonged was not used as a panel, as we hoped to find participants from various organisations from diverse sectors. This was so that we can generalise the opinions and not restrict us to a particular sector or organisation.

At the end of the survey a total of 624 samples were collected. Out of which only 513 complete surveys were selected. The primary selection criteria for participants was that they were employed full time and over the age of 18 years. The distribution of participants over different age ranges is as follows-

Employment status	Age Range								
	Under 18	18-25	26-30	31-35	36-40	41-45	46-50	50+	Total
Full time	0	34	59	73	67	64	72	144	513

Table 3 Employment Status of participants

Additional demographic information was also collected such as participants level of education, total work experience, no. of years employed at the current organisation, the department they were working in the organisation, and their job position at the organisation. The breakdown of participants based on their level of education is as follows-

#	Answer	%	Count
1	(Undergraduate)	53.22%	273
2	(Bachelors)	30.60%	157
3	(Masters)	12.67%	65
4	(Doctorate)	3.51%	18
	Total	100%	513

Table 4 Education Level of participants

Breakdown of participants based on the total work experience they have in years is as follows-

#	Answer	%	Count
1	(0-5)	6.43%	33
2	(5-10)	14.62%	75
3	(10-15)	13.26%	68
4	(15-20)	14.42%	74
5	(20+)	51.27%	263
	Total	100%	513

Table 5 Work Experience of Participants

Number of participants based on total number of years they have worked in their current organisation is as follows-

#	Answer	%	Count
1	(0-5)	33.53%	172
2	(5-10)	25.15%	129
3	(10-15)	16.18%	83
4	(15-20)	9.75%	50
5	(20+)	15.40%	79
	Total	100%	513

Table 6 Work experience of participants in their current organisation

Classification of participants based on the departments they worked in is as follows-

#	Answer	%	Count
1	HR-(Manage current organizations human resource)	6.24%	32
2	Finance-(Manage current organizations finance)	9.55%	49
3	Specialist-(focusing on current organizations products or services)	14.42%	74
4	IT-(Manage current organizations IT systems)	13.06%	67
5	Management-(Manager or management of overall organization)	19.69%	101
6	others (Please Specify)	37.04%	190
	Total	100%	513

Table 7 Departments the participants are currently working in their current organisation

These departments were selected for classifications mainly because in majority of organisations and from information security perspective, these departments are the ones which often deal with sensitive information. Other departments participants specified accounts, administration, customer service, data management, education, sales, secretary, supervisor, teaching.

Classification of participants based on their job position within the organisation is as follows-

#	Answer	%	Count
1	Junior role - (First line)	30.21%	155
2	Senior role - (Second line)	29.63%	152
3	Team Leader/Manager	22.81%	117
4	Senior Manager/Dept Head	12.87%	66
5	Top Management	4.48%	23
	Total	100%	513

Table 8 Participants current job role in their current organisation

One of the primary criteria of this research is to capture opinions of participants from organisations with different levels of organisational security operations, thus being classified as low security organisation, medium security organisation and high security organisation depending on the Threat level.

The opinion of participants of how they feel their organisations should be classified in terms of security, based on the type of information it deals with, the nature of services provided and the sector it falls under, is as follows-

#	Answer	%	Count
1	(Low Security)	18.13%	93
2	(Medium Security)	43.86%	225
3	(High Security)	38.01%	195
	Total	100%	513

Table 9 Security level of participants current organisation

Participants perceptions about their organisation's overall security procedures in terms of their organisations effort in securing company assets is as follows-

#	Answer	%	Count
1	Terrible	1.17%	6
2	Poor	3.12%	16

3	Average	27.49%	141
4	Good	45.42%	233
5	Excellent	22.81%	117
	Total	100%	513

Table 10 Participant's perception of their current organisational security procedures

The second important criteria of this research is to understand the differences in perceptions of policymakers and employees. Hence for the purpose the classification of participants is based on their participation in their own organisational policymaking, including designing, developing and/or implementing their organisational security policies is as follows-

#	Answer	%	Count
1	Yes (Full or Partial contribution)	37.62%	193
2	No (No contribution at all)	62.38%	320
	Total	100%	513

Table 11 Participation in policymaking - Policymakers vs Employees

Participants who responded 'yes' implies that they have full or some contribution in designing and developing their organisational security policies and hence considered as policymakers. While participants who are not involved in the design or development of policies are classified as regular employees.

Before we begin to understand their perception of information security it is essential to understand the depth of knowledge, they possess about the type of information they deal with daily. At the same time, it is also essential to capture their own understanding of IT systems and information security. This in turn will assist in analysing their perception of self-efficacy when complying with policies.

Participant perception of the type of information they deal with daily-

#	Answer	%	Count
1	Non - confidential	6.63%	34
4	Low - (e.g. General work-related information)	16.18%	83

2	Medium - (e.g. personal information, employee information)	39.18%	201
3	Highly Confidential - (e.g. company data, financial information etc.)	38.01%	195
	Total	100%	513

Table 12 Level of confidentiality of information directly handled by participants

Classification of participants based on how they perceive their knowledge about IT systems is as follows-

#	Answer	%	Count
1	(None)	8.58%	44
2	(Low)	16.18%	83
3	(Average)	39.96%	205
4	(Above average)	27.88%	143
5	(Expert)	7.41%	38
	Total	100%	513

Table 13 Participant's knowledge of IT systems

Participant's perception of the knowledge they possess about information security is as follows-

#	Answer	%	Count
1	(None)	8.77%	45
2	(Low)	17.54%	90
3	(Average)	40.94%	210
4	(Above average)	25.73%	132
5	(Expert)	7.02%	36
	Total	100%	513

Table 14 Participant's knowledge of information security

Out of the total 513 participants we had 193 policymakers, and 320 employees. Out of the 193, 8.8% were from low security organisation. 48.2% from medium security organisation and 43 from high security organisation. Out of the 320 employees, 23.8% were from low security organisation, 41.3% were from medium security organisation, and 38% were from high security organisation.

See table below for participant distribution.

Policymaker_Employee * Sec_Level Crosstabulation

			Sec_Level			
			(Low Security)	(Medium Security)	(High Security)	Total
Policymaker_Employee	Yes (Full or Partial contribution)	Count	17	93	83	193
		% within Policymaker_Employee	8.8%	48.2%	43.0%	100.0%
	No (No contribution at all)	Count	76	132	112	320
		% within Policymaker_Employee	23.8%	41.3%	35.0%	100.0%
Total		Count	93	225	195	513
		% within Policymaker_Employee	18.1%	43.9%	38.0%	100.0%

Table 15 Distribution of policymakers and employees based on the security level of their organisation

Distribution for participants based on the type of information they handled is as follows. Out of the 193 participant policymakers, 2.1% handled non-confidential information, 8.8% handled low confidential information e.g. general work-related information, 44.6% handled medium confidential information such as personal or employee information, 44.6% dealt with highly confidential information such as company data or financial information.

Out of the 320 participant employees, 9.4% handled non-confidential information, 20.6% handled low confidential information e.g. general work-related information, 35.9% handled medium confidential information such as personal or employee information, 34.1% dealt with highly confidential information such as company data or financial information.

Policymaker_Employee * Info_Handled Crosstabulation

			Info_Handled				
			Non - confidential	Low	Medium	High	Total
Policymaker_Employee	Yes (Full or Partial contribution)	Count	4	17	86	86	193
		% within Policymaker_Employee	2.1%	8.8%	44.6%	44.6%	100.0%

	No (No contribution at all)	Count	30	66	115	109	320
		% within Policymaker_Employee	9.4%	20.6%	35.9%	34.1%	100.0%
Total		Count	34	83	201	195	513
		% within Policymaker_Employee	6.6%	16.2%	39.2%	38.0%	100.0%

Table 16 Distribution of policymakers and employees based on level of confidential information directly handled by them

4.3 Data Analysis

Perception of Security (Employees vs policymakers)

This is measured in terms of their perception of information security itself, their perception of organisational interventions, their perception of organisational interventions, perceptions of organisational commitment (in terms of protecting information, personal and organisational) – organisations commitment towards employees and employee's commitment towards organisation and their perception of quality of the policy document. These constructs are further analysed against constructs from protection motivation theory, viz. threat appraisal, coping appraisal, behavioural intent, and actual behaviour. Items causing singularity in the co-relation matrix were deleted and are not reported. Items which were cross loading in pattern matrix were also deleted to get uniform factors. As such out of the 87 item statements only the key 37 item statements which align with the constructs created and which reflect the differences in perceptions of policymakers and employees are reported. The rest are moved in Appendix C.

4.3.1 Perception of information security

As discussed in chapter 1, information security is a very vast subject area. It would be unfair to expect everyone to have all or even considerable amount of knowledge about information security. It was evident from study 1 that not all participants had enough knowledge as is. Though it is difficult to define enough knowledge, for this research, it is considered that they should at least have a basic understanding of the differences between information security, cyber security, data protection and have some understanding of the risks associated with non-compliance of security policies.

4.3.1.1 Knowledge of information security

Is there a clear distinction between, data protection, Cyber security, and Information Security? Data protection only deals with personal information of individuals, be it in physical form or digital form. Cyber security focusses only on security of digital information. Whereas Information security deals with security of all types of information, be it physical or digital. It can be said that cyber security and data protection are subsets of Information security.

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	Information security is different from data protection	24.37%	35.09%	29.24%	8.77%	2.53%
2	Information security is different from cyber security	21.64%	38.21%	29.63%	7.41%	3.12%

Table 17 Response distribution (in%) for knowledge of information security

59 % of participants agreed to some extent that information security is different from data protection. However, 32% of participants were not aware of the distinction. While information security deals confidentiality, integrity and availability of information, data protection deals with privacy aspect of information security. Of the 193 participant policymakers, 70% agreed with the statement, showing 30% of the total were either unsure of, or disagreed with the distinction. This is concerning as Wilson et. al (Wilson et al., 2009) suggest that due to the increase in severity of threats and privacy concerns, proper solutions can only be implemented by professionals with expertise in systems and information protection. Of the 320 participant employees, 53% agreed with the statement, showing 47% of the total number of employees, were either unsure or unaware of the distinction. Out of the total number of employees who agreed with the distinction (169), 88% employees claimed to have adequate to expert, knowledge of IT and Information Security. 8% of the remaining claimed, it was their organisations responsibility to protect their information, and did not follow security policy at work.

60 % of participants agreed to some extent that information security is different from data protection. However, 40% of participants were not aware of the distinction. Von Solms et. al (Von Solms & Van Niekerk, 2013) agree that information security and cyber security are in fact different. They posit that in information security, reference to human factors relates to their role in the security process, however cyber security identifies humans as potential targets of cyber-

attacks. Of the 193 participant policymakers, 69% agreed with the statement, showing 31% of the total were either unsure of, or disagreed with the distinction. Of the 320 participant employees, 54% agreed with the statement, showing 46% of the total number of employees, were either unsure or unaware of the distinction. Out of the total number of employees who agreed with the distinction (173), 92% employees claimed to have adequate to expert, knowledge of IT and Information Security. 2% of the remaining claimed, it was their organisations responsibility to protect their information, but did follow the organisational security policy.

4.3.1.2 Appreciation of non-compliance and threats

There are a multitude of risks associated with non-compliance of security policies. To name a few risks for the organisations - financial loss, confidential information loss, legal penalties for not acting in accordance with industry or government laws and regulation. Risks for employees – legal proceedings, imprisonment, loss of employment, identity theft, loss of confidential information etc. It would be impossible to assess policymakers and employee's perception of their overall understanding of the all the risks associated with non-compliance. Hence for this research purpose, their awareness of the existence of risks associated with non-compliance is measured. Along with this their understanding of the two most common issues faced by organisations and employees is measured. As such what we measure from this section is that the participants understand why security policies are implemented and what do these security policies protect us from.

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	There are risks associated with non-compliance of policies	46.98%	30.60%	20.27%	1.95%	0.19%
2	There are risks associated with a security policy breach	51.85%	29.04%	16.37%	2.34%	0.39%
3	I understand how a spam email could potentially hurt me or my organization	55.36%	27.68%	14.42%	1.95%	0.58%
4	I understand how an identity theft could potentially hurt me or my organization	62.77%	21.64%	13.06%	1.75%	0.78%

Table 18 Response distribution for participant's understanding of risks with noncompliance and threats

77% of participants agreed to some extent that there are risks associated with non-compliance of security policies. However, 23% of participants were not aware of the associated risks. There are risks associated with noncompliance of security policies, whether they are from intentional or unintentional user activities (Warkentin & Willison, 2009). It is imperative that users understand that their actions and behaviours while handling their organisational systems, are directly connected with the compliance and noncompliance of the organisational policies. Of the 193 participant policymakers, 81% agreed with the statement, showing 18% of the total were either unsure of, or disagreed that there are any associated risks. Of the 320 participant employees, 75% agreed with the statement, showing 25% of the total number of employees, were either unsure or unaware of the distinction. Out of the total number of employees who agreed with the distinction (241), 88% employees claimed to have adequate to expert, knowledge of IT and Information Security. 6% of the remaining claimed, it was their organisations responsibility to protect their information.

79% of participants agreed to some extent that there are risks associated with a security policy breach. However, 21% of participants were not aware of the associated risks. Of the 193 participant policymakers, 84% agreed with the statement, showing 16% of the total were either unsure of, or disagreed there were risks. Of the 320 participant employees, c % agreed with the statement, showing d % of the total number of employees, were either unsure or unaware of the distinction. Out of the total number of employees who agreed with the distinction (243), 91% employees claimed to have adequate to expert, knowledge of IT and Information Security. 7% of the remaining claimed, it was their organisations responsibility to protect their information.

83% of participants agreed to some extent that a spam email could potentially hurt them or their organisation. However, 17% of participants were not aware of how a spam email was harmful. Emails are one of the fastest and economical means of communications (Sumecki, Chipulu, & Ojiako, 2011) (Youn & McLeod, 2007). Management of emails still remains a challenge to organisations (Sumecki et al., 2011). A spam email is an unsolicited email as such only adding to the volume of emails handled by the organisations email servers (Youn & McLeod, 2007). However, in their study Sumecki et al (Sumecki et al., 2011) claim that technological solutions may have rendered the impact of spam emails. Of the 193 participant policymakers, 84% agreed with the statement, showing 16% of the total were unaware of how spam could hurt the individual or the organisation. Of the 320 participant employees, 82% agreed with the statement, showing

18% of the total number of employees, were either unsure or unaware of the harm. Out of the total number of employees who agreed with the distinction (263), 88% employees claimed to have adequate to expert, knowledge of IT and Information Security. 7% of the remaining claimed, it was their organisations responsibility to protect them.

84% of participants agreed to some extent with the severity of identity theft. However, 16% of participants were not aware of the harm. Identity threat involves, acquiring enough data about another person's account and pretending to be that person (K. B. Anderson et al., 2008). One purpose of identity theft would be where the thief, acquires goods while attributing the charge to another person's account. Identity theft is known to cause financial damage to consumers, creditors, establishments and the economy as a whole (Hoofnagle, 2007). Of the 193 participant policymakers, 85% agreed with the statement, showing 15% of the total were unaware of the harm. Of the 320 participant employees, 84% agreed with the statement, showing 16% of the total number of employees, were either unsure or unaware of the harm. Out of the total number of employees who agreed with the distinction (268), 87% employees claimed to have adequate to expert, knowledge of IT and Information Security. 7% of the remaining claimed, it was their organisations responsibility to protect them.

4.3.2 Perception of organisational interventions

For this research purpose, organisational interventions for implementing or improving organisational security such as awareness programs, training programs, any form of communication and the security policy itself, are considered. This is further measured through two subcategories, current organisational interventions and the desire for organisational interventions. Through this section the differences in perceptions of policymakers and employees are noted.

4.3.2.1 Current organisational interventions

In this section awareness of policymakers and employees about the awareness programs, training programs, forms of communication and security policy is measured.

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	I know our organization has made us aware of our security policy	45.03%	30.21%	17.54%	5.07%	2.14%
2	I know our organization provides training on compliance of our security policy	36.26%	25.73%	23.20%	10.33%	4.48%
3	My organization tells me if compliance of security policy is important to my job role	39.57%	29.24%	22.61%	6.04%	2.53%
4	My organization asks me if I could do anything to improve organizational security policy compliance behavior	26.51%	25.93%	26.90%	10.33%	10.33%
5	I know our organization has an organizational security policy	43.27%	25.73%	23.00%	5.65%	2.34%

Table 19 Response distribution of participant's perception of their current organisational interventions

4.3.2.1.1 Awareness programs

75% of participants agreed to some extent know that their organisation has made them aware of the security policy. However, 25% of participants disagreed. Lack of awareness of security policies and procedures are the root cause of users mistakes (Sohrabi Safa et al., 2016). A traditional employee awareness program utilises a one size fits all approach (Valentine, 2006) and are often considered ineffective (Leach, 2003). Of the 193 participant policymakers, 80% agreed with the statement, showing 20% of the total disagreed or thought an awareness program was not there. Of the 320 participant employees, 72% agreed with the statement, showing 16% of the total number of employees, claimed they were not made aware.

4.3.2.1.2 Training programs

For item statement, *I know our organisation provides training on compliance of security policy* 62% of participants agreed that they were aware of training programs. However, 38% of participants disagreed. Eminagaoglu et al (Eminağaoğlu et al., 2009) perceive that effective compliance can be achieved through security training of employees. However the quality of

presenter or authors of the training programs are questioned (May, 2008). Clifford May also suggests having different training materials for different audiences. Of the 193 participant policymakers, 74% agreed with the statement, showing 26% of the total disagreed or thought a training program was not there. Of the 320 participant employees, 54% agreed with the statement, showing 46% of the total number of employees, claimed they were not made aware.

4.3.2.1.3 Communication

69% of participants agreed to some extent know that their organisation told them about compliance. However, 31% of participants thought the organisation did not communicate. Continuous communication is required to improve users IS security policy compliance (Puhakainen & Siponen, 2010). Adams and Sasse (Adams & Sasse, 1999) believe users are forced to circumvent security measures due to lack of communications between the security departments and users. They further posit that users do not understand security issues while the security departments do understand users' perceptions, tasks and needs. Of the 193 participant policymakers, 75% agreed with the statement, showing 25% of the total disagreed or thought that the communication was not there. Of the 320 participant employees, 65% agreed with the statement, showing 35% of the total number of employees, claimed they were not made aware.

53% of participants agreed to some extent know that their organisation asked them about compliance improvement. However, 47% of participants thought the organisation did not ask them. It has been emphasised that employee participation could improve their security awareness and behaviour (Albrechtsen & Hovden, 2010). This study identifies lack of communication between organisation and its employees. Of the 193 participant policymakers, 70% agreed that the organisation asks employees for participation, showing 30% of the total disagreed or thought that this communication was not there. Of the 320 participant employees, 42% agreed with the statement, showing 58% of the total number of employees, claimed there was no communication in this regard.

4.3.2.1.4 Security policy

For item statement, *I know our organisation has an organisational policy*, 69% of participants agreed to be aware of the existence of a security policy. However, 31% of participants thought the organisation did not know if a security policy existed. Siponen et al (Mikko Siponen, Pahnila, & Mahmood, 2010) in their study posited that visibility of security policies have a significant effect on employees intention to comply with those policies. Of the 193 participant policymakers, 80%

agreed that the organisation asks employees for participation, showing 20% (39) of the total disagreed or thought that there was no security policy. Of these 39, 38 were up to the senior manager job position level within their organisation and 1 from Top management. Of the 320 participant employees, 62% agreed that a policy existed, showing 38% of the total number of employees, claimed they didn't know, or a policy didn't exist.

4.3.2.2 Desire for organisational interventions

Perugini and Bagozzi (Perugini & Bagozzi, 2001) in their study suggested that desires have a strong mediating effect of users attitude on their intention and behaviour. In this section, differences in perception of the desire of policymakers and employees for the awareness programs, training programs, forms of communication and security policy to exist, is measured.

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	My organization ought to / should make us aware of our security policy	48.15%	25.15%	21.44%	3.90%	1.36%
2	My organization ought to / should provide training on how to comply with our security policy	44.25%	28.27%	21.83%	3.90%	1.75%
3	My organization should tell me if compliance of security policy is important to my job role	45.03%	30.41%	18.71%	3.90%	1.95%
4	My organization ought to / should have an organizational security policy	44.05%	28.46%	23.78%	1.95%	1.75%

Table 20 Response distribution for participants desire for organisational interventions

4.3.2.2.1 Awareness programs

73% of participants agreed that their organisation should have awareness programs. However, 27% of participants were not sure or disagreed. Of the 193 participant policymakers, 82% agreed that awareness programs should be implemented, showing 18% (35) of the total disagreed. Of these 35, 33 were up to the senior manager job position level within their organisation and 2 from

Top management. Of the 320 participant employees, 68% agreed that they should have the programs, showing 21% of the total number of employees, were not sure and 5% didn't want them.

4.3.2.2.2 Training programs

72% of participants agreed the organisation should have a training program. However, 28% of participants disagreed. Of the 193 participant policymakers, 80% agreed to have the programs, showing 20% (38) of the total disagreed or thought that training was not needed. Of these 38, 36 were up to the senior manager job position level within their organisation and 2 from Top management. Of the 320 participant employees, 68% agreed that a policy existed, showing 26% of the total number of employees, claimed they were not sure, and 6% didn't need a training program.

4.3.2.2.3 Communication

75% of participants agreed that their organisation should inform them. However, 25% of participants were not sure or didn't want to know. Of the 193 participant policymakers, 78% agreed that the organisation should tell their employees, showing 22% (42) of the total disagreed or thought that there was no need. Of these 42, 40 were up to the senior manager job position level within their organisation and 2 from Top management. Of the 320 participant employees, 74% agreed that the organisation should inform them, showing 20% of the total number of employees, were not sure, and 6% didn't want this to be communicated.

4.3.2.2.4 Security policy

72% of participants agreed they should have a security policy. However, 24% of participants were not sure and 4% didn't want it. Of the 193 participant policymakers, 80% agreed that the organisation should have a security policy, showing 20% (39) of the total disagreed or thought that there was no security policy. Of these 39, 38 were up to the senior manager job position level within their organisation and 1 from Top management. Of the 320 participant employees, 68% agreed that a policy existed, showing 26% of the total number of employees, were not sure, 6% didn't want the organisation to have one.

4.3.3 Perception of organisational commitment

During study 1 the researcher found that participant questioned the commitment or organisations towards their employees, as in whether these polices existed to protect the employees or just the

organisation itself. The researcher felt it was worth asking this question to the masses through this study. Hence in this section commitment from and towards the organisation has been measured.

4.3.3.1 Commitment from organisation

In this section, employee's (and policymaker's) perception of commitment from the organisation towards its employees is measured. Meyer et al (Meyer, Allen, & Gellatly, 1990) have shown that organisational dependability improves employees affective commitment. They define affective commitment as an attitude that centres on emotional identification with the values and goals of the organisation (O'Driscoll & Randall, 1999).

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	My organizational policies are made to protect me and my information	44.83%	33.53%	18.13%	2.53%	0.97%
2	My organizational policies are made to protect the organization and its information	52.83%	30.21%	15.01%	1.36%	0.58%

Table 21 Participant's perceived commitment from their organisation

78% of participants agreed that the security policies were to protect the employees and their information. However, 18% of participants were not sure and 4% disagreed. Of the 193 participant policymakers, 84% agreed that the security policy protects their employees, showing 18% of the total were not sure or thought it did not. Of the 320 participant employees, 75% agreed that the security policy protects them, showing 22% of the total number of employees, were not sure, 4% didn't agree.

83% of participants agreed that the security policies were to protect the employees and their information. However, 15% of participants were not sure and 2% disagreed. Of the 193 participant policymakers, 88% agreed that the security policy protects their employees, showing 12% of the total were not sure or thought it did not. Of the 320 participant employees, 80% agreed that the security policy protects the organisation, showing 18% of the total number of employees, were not sure, 2% didn't agree.

4.3.3.2 Commitment towards organisation

In this section, employee's (and policymaker's) own perception of their commitment towards their organisation is measured. Safa et al (Sohrabi Safa et al., 2016) in their findings have shown using social bond theory that commitment towards organisations policies and plans have a strong effect on employees' attitude towards compliance.

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	I will change organizations in a few years, so security compliance is not my concern	15.79%	15.40%	23.59%	15.01%	30.21%

Table 22 Participants perceived commitment towards their organisation

This item is reverse coded for SEM analysis and as such the ideal answer should incline strongly towards "disagree" and less towards "agree". The table below shows the participants actual commitment, meaning the table is derived from straight coding. 31% of participants agreed with the statement. 23% of participants were not sure and 45% disagreed. Muthuveloo et al (Muthuveloo & Rose, 2005) identify that employees intention to stay with an organisation is one of the two dominant conceptualisations of organisational commitment in sociological literature. The other being employee's loyalty towards their organisation. This was surprising to note that of the 193 participant policymakers, 44% agreed that they are going to leave the organisation and compliance was not their concern showing lack of commitment towards their organisation, whereas 17% of the total were not sure and 38% disagreed with the statement. On the other hand of the 320 participant employees, 23% agreed with the statement, 27% of the total number of employees, were not sure, and 49% didn't agree, showing higher commitment towards their organisation compared to their peer policymakers.

4.3.4 Perception of responsibility

To have effective security compliance behaviour it is imperative that someone or a body is responsible for that security behaviour. Hence in the following section employee's and policymaker's perception of responsibility to protect personal and organisational information is measured. This perception is measured in terms of who is responsible and who should make the effort. It is the organisations responsibility to protect their and employee information (Posthumus

& von Solms, 2005). Postumus and Von Solms also suggest it is employee's responsibility as well, to protect their and their organisations information.

4.3.4.1 Organisation's responsibility to protect

This section aims to see if the policymaker's and employees think it's the organisations responsibility to protect employee and organisational information.

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	It is my organizations responsibility to protect my personal information and organizational information	44.64%	31.97%	18.71%	3.12%	1.56%
2	My organization should tell me what security procedures are relevant to my job role	47.17%	32.55%	19.49%	0.58%	0.19%

Table 23 Participant's perception of organisational responsibility

76% of participants agreed that it is their organisations responsibility to protect them and their information. However, 24% of participants were not sure or disagreed. Of the 193 participant policymakers, 82% agreed it is their organisations responsibility, showing 16% of the total were not sure or thought it is not. Of the 320 participant employees, 73% agreed that the security policy protects the organisation, showing 21% of the total number of employees, were not sure, 6% didn't agree.

80% of participants agreed that their organisation should make the effort to promote secure behaviour. However, 19% of participants were not sure and 1% disagreed. Of the 193 participant policymakers, 84% agreed that the organisation should make the effort, with 16% of the total were not sure or thought it shouldn't. Of the 320 participant employees, 77% agreed that their organisation should make the effort to promote security, with 21% of the total number of employees, were not sure, 1% didn't agree.

4.3.4.2 Self-responsibility to protect

This section aims to see if the policymaker's and employees think it is their own responsibility to protect their and organisational information.

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	It is my responsibility to protect my and organizational information	48.54%	31.97%	15.20%	3.12%	1.17%
2	I should find out what security procedures are relevant to my job role	42.69%	33.33%	20.66%	2.34%	0.97%

Table 24 Participant's perception of self-responsibility

80% of participants agreed that it is their responsibility to protect their and organisational information. However, 15% of participants were not sure and 5% disagreed. Of the 193 participant policymakers, 89% agreed that employees should protect their and organisational information, with 9% of the total were not sure and 2% thought they shouldn't. Of the 320 participant employees, 75% agreed that they should be responsible for protecting their and organisational information, with 19% of the total number, were not sure, 6% didn't agree.

76% of participants agreed that they should find the information relevant to their job role. With 21% of participants were not sure and 3% disagreed. Of the 193 participant policymakers, 86% agreed that they should make the effort to find out what security procedures are relevant to their job role, with 14% of the total were not sure or disagreed. Of the 320 participant employees, 70% agreed, they should find the relevant security procedures, with 26% of the total number of employees, were not sure and 4% didn't agree.

4.3.4.3 Accountability

It is important for employees to understand that compliance of security policies or general policies, is a part of their job description, even if it is not explicitly mentioned in their job descriptor. Boss et al (Boss et al., 2017) pointed that employees do not find policies and procedures to be mandatory and hence do not comply with them. They posit that the perception of mandatoriness is effective to motivate employees to take security precautions.

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	I am bound by an organizational information security policy	46.20%	26.90%	19.88%	4.48%	2.53%
2	Complying with Information security policy is relevant to me or my job role	43.86%	28.27%	20.47%	4.87%	2.53%

Table 25 Participants perception of accountability

73% of participants agreed with the statement. With 20% of participants were not sure and 7% disagreed. Of the 193 participant policymakers, 78% agreed that they are bound by their organisational security policies, with 22% of the total were not sure or disagreed. Of the 320 participant employees, 70% agreed, they are bound by their organisational policies, with 21% of the total number of employees, were not sure and 9% didn't agree.

72% of participants agreed that it is relevant to their job role. With 21% of participants were not sure and 7% disagreed. Of the 193 participant policymakers, 81% agreed that security policy is relevant to their job role, with 19% of the total were not sure or disagreed. Of the 320 participant employees, 66% agreed, security policies are relevant to their job roles, with 23% of the total number of employees, were not sure and 11% didn't agree.

4.3.5 Quality of policy documents

From study 1 it was identified that for a good quality of a policy document, its visibility, language of text within the document, relevance of information and length of the document were found to be vital. And as such in the following sections the perceptions of policymaker's and employees about the 4 sub constructs is measured. Visibility gave a very low alpha hence has not been included in the structural equation model.

4.3.5.1 Language

It was established from study 1 that most security policies are written in pseudo legal language and can tend to be filled with a lot of legal and technical information. It is also a fact that not all employees are experts in technology and as such if it is expected for all employees to understand and follow the security policies, the language should not be jargon heavy. Jones et al (Jones et al., 2012) agree that plain language affects the comprehension and perceptions of readers of policy

documents. In most policies the language is found to be vague (Nicholson, Coventry, & Briggs, 2019) and difficult to understand (Höne & Eloff, 2002).

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	The language within the policies is vague and ambiguous	11.89%	22.42%	33.33%	21.25%	11.11%
2	The language within the policies is mostly legal and difficult to understand	12.48%	23.00%	31.19%	19.88%	13.45%

Table 26 participants perception of language used in their current organisational security policies

36% of participants agreed the language was legal and difficult to understand. With 31% of participants were not sure and 33% disagreed. Of the 193 participant policymakers, 45% agreed that security policies are difficult to understand, with 22% of the total were not sure and 33% disagreed. Of the 320 participant employees, 30% agreed with the statement, 37% of the total number of employees, were not sure and 33% didn't agree.

4.3.5.2 Relevance of Information

It is common practice to consolidate all information regarding organisations IT security on to a single document. This makes the content of the document jargon heavy. Too technical and filled with legal information about compliance and data security procedures, standards and regulations. On top of this there could be other documents complementing the primary security policy, e.g. acceptable use policy. Employees can find all this information overwhelming (Jones et al., 2012) and think all of it might not be relevant to them or their job role.

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	My organizational information security policy has information which is relevant to my job role	36.45%	31.77%	24.17%	4.87%	2.73%
2	The organizational security policy is made using industry standard guidelines	27.29%	34.50%	32.75%	3.31%	2.14%

3	Policies mostly include legal information	21.44%	30.60%	34.50%	10.33%	3.12%

Table 27 Participant's perception of relevance of information within their current organisational security policies

68% of participants agreed that the policies have information relevant to their job roles. With 24% of participants were not sure and 8% disagreed. Of the 193 participant policymakers, 80% agreed that content within security policies is relevant to their job roles, with 17% of the total were not sure and 3% disagreeing. Of the 320 participant employees, 61% agreed, content within security policies to be relevant, with 29% of the total number of employees, were not sure and 10% didn't agree.

62% of participants agreed that the security policies are made using industry standard guidelines. With 33% of participants were not sure and 5% disagreed. According to Whitman et al (Whitman, Townsend, & Aalberts, 2001) policies are in fact made using standard guidelines. Of the 193 participant policymakers, 76% agreed that security policies are made using standard guidelines, with 21% of the total were not sure and 3% disagreeing. Of the 320 participant employees, 53% agreed, content within security policies is made using guidelines, with 40% of the total number of employees, were not sure and 7% didn't agree.

4.3.5.3 Length

As mentioned previously, most security policies contain consolidated information about security for the entire IT systems within the organisation. This makes the polices very long, and time consuming to read and comprehend. The length of the policy documents have been considered to cause ambiguity with users in understanding the document (Karlsson, Hedström, & Goldkuhl, 2017) because of the lengthy texts.

#	Question	Strongly agree	Somewhat agree	Neither agree nor disagree	Somewhat disagree	Strongly disagree
1	My organizational policies are of average length	13.06%	32.94%	41.91%	9.94%	2.14%
2	My organizational policies are short and concise	10.33%	23.39%	39.38%	17.93%	8.97%

Table 28 participant's perceived length of their current organisational security policy documents

46% of participants think their organisational policies of average length. With 42% of participants were not sure and 12% disagreed. Of the 193 participant policymakers, 60% agreed that security policies are average length, with 29% of the total were not sure and 11% disagreeing. Of the 320 participant employees, 37% agreed that security policies are average length, with 50% of the total number of employees, were not sure and 13% didn't agree.

On the other hand, 34% of participants think that their organisational security policies are short and concise. With 39% of participants were not sure and 27% disagreed. Of the 193 participant policymakers, 50% agreed that security policies are short and concise, with 28% of the total were not sure and 22% disagreeing. Of the 320 participant employees, 24% agreed that security policies are short and concise, with 46% of the total number of employees, were not sure and 30% didn't agree.

4.4 Discussion and Conclusion

In this study we set out to find differences in perceptions of policymakers and employees. We addressed the limitation of our previous study one by incorporating participant data from different types of industries with varying levels of security. The study found substantial differences in participants perceptions of information security, their perception of organisational interventions their perceptions of organisational citizenship and the quality of policy documents. Responses that align with the survey item statements were considered good and those that didn't align were considered bad. E.g. policymakers are expected to have strong knowledge of information security and its policies and procedures. So when asked if information security is the same as cyber security, the accurate answer is that they should disagree, as cyber security is a subset of information security and they are not the same. Meaning Information security deals with security of all types of data, be it in digital format or physical. Cyber security only deals with security of digital data. Therefore, agreeing with statement is incorrect and hence shows poor knowledge of information security. Participants who disagreed with this statement show good knowledge of information security. In the table below the average of all good and poor responses is noted. The novel differences are noted in blue coloured text.

4.4.1 Perception of information security

It was noted that 30% of policymakers displayed poor understanding of information security. Ideally this should be closer to 100% if organisations are to implement stronger security measures. On the other hand, for employees there was even split between good and poor understanding of

information security. This was primarily because employees who claimed to have average to expert knowledge of IT systems displayed better understanding security. Both policymakers and employees showed good appreciation of non-compliance and understanding of threats that affected their organisations. There were some policymakers and employees who displayed poor understanding. Ideally all policymakers and employees should have a strong understanding of issues with non-compliance and threats that could harm them or their organisations.

4.4.2 Perception of organisational interventions.

Policymakers showed good awareness of present interventions, in the form of awareness programs, training programs, and security policy. They also claimed that there was communication from the organisation to make employees aware of such interventions. They also displayed a strong desire for better organisational security interventions. Employees were split 60-40 in favour of existing interventions. But they also showed a considerable desire for organisational interventions. It is of concern that about 40% of employees had poor awareness.

SUMMARY OF DIFFERENCES IN PERCEPTIONS					
		Policymakers		**Employees**	
		Good	**Poor**	**Good**	**Poor**
Perception of information security	Knowledge of information security	69.95%	30.05%	53.44%	46.56%
	Appreciation of non-compliance and threats	83.81%	16.19%	79.30%	20.70%
Perception of organizational interventions	Existing organizational interventions	75.75%	24.25%	59.31%	40.69%
	Desire for Organisational interventions	80.05%	19.95%	69.45%	30.55%
Perception of organizational commitment	From organization towards employees	86.53%	13.47%	77.19%	22.81%
	From employees towards organization	38.86%	61.14%	49.06%	50.94%
	Organisational responsibility	82.90%	17.10%	75.31%	24.69%
	Self-responsibility	87.56%	12.44%	72.66%	27.34%
	Compliance a part of Job description	79.53%	20.47%	68.44%	31.56%
	Language	30.31%	69.69%	34.38%	65.63%

Quality of policy document	Relevance of information	73.92%	26.08%	52.81%	47.19%
	Length	55.18%	44.82%	30.63%	69.38%

4.4.3 Perception of organisational commitment

Most noticeable information was observed for perception of organisational commitment. Even though both policymakers and employees claimed they observed commitment from organisation in some form, commitment from employees and policymakers alike showed a cause of concern. It is surprising that 61% of policy makers claimed that they would leave the organisation in a few years hence security compliance was not their concern. Similarly, 51% of employees claimed the same. This was surprising to note that participant policymakers, agreed that they are going to leave the organisation and compliance was not their concern showing lack of commitment towards their organisation. On the other hand of the employees, showed higher commitment towards their organisation compared to their peer policymakers. Both policymakers and employees displayed a sense of responsibility to protect their and their organisations information. Security behaviour within and organisation is not just the organisations responsibility, but also its employees. Though policymakers were strongly aware that complying with security policies is a part of their job description, 31% of employees were not aware of the fact.

4.4.4 Quality of policy documents

In terms of the quality of the security policy document itself, both policymakers and employees had similar concerns with regards to the language used within the policies and the length of the document. They confirmed that the language was mostly legal, difficult to understand and the policies were long. In terms of relevance of information, the policymakers felt that the information was mostly relevant, about 47% employees thought it contained no-relevant information.

In the next chapter we look at the second part of analysis of study two.

5 CHAPTER 5 STRUCTURAL EQUATION MODELLING

5.1 Introduction

This chapter focusses on the second part of analysis of study two. In this chapter we describe generalised solution that works for all types of organisations with varying levels of security and the same time works for all types of employees including policymakers. Viz a tailored policy.

This chapter addresses the following research questions

1) How can compliance with the security policy be improved?
2) Can we find solution that works with both policymakers and employees?
3) What would make an effective Tailored policy?
4) Can we develop a generalised model of enhanced PMT in relation to security compliance?
5) Can this model be tested for its application to both policymakers and employees?
6) Is this model a generalised model for organisations with varying security levels? (Low, medium, and high security organisations)
7) Are there any moderation effects of a Tailored policy on the relationships between the constructs of PMT?
8) Can a tailored policy be used to improve organisational security behaviour?

This chapter focusses on Structural equation modelling and the constructs and the item statements within. Item statements which were deemed to be more relevant to the constructs and for this SEM were selected, the remaining were discarded and are not reported in this chapter. This was a part of the screening process of data to be used in structural equation model. Items were deleted based on how they were affecting the Cronbach's α value or reliability of the construct. Any item deemed to lower the α value below 0.7 were deleted. It is posited that an instrument cannot be valid unless its reliable (Tavakol & Dennick, 2011). Higher value of alpha show a good shows good internal consistency of the items in the measurement scale (Gliem & Gliem, 2003). We start with screening the data for missing data in the survey and unengaged responses. This is followed by exploratory factor analysis (EFA) (Al-Omari et al., 2013) in order to obtain a clean pattern matrix. We then input the data in AMOS and do the confirmatory factory analysis (CFA) (Liang et al., 2019)to check for model fit.

We have done multi group CFA analysis (Xu & Tracey, 2017) for the model to ensure the model does not have measurement invariances (Byrne, 2004). In this research's case the multi group is policymakers and employees. This method was successfully used by Chambal et al (Chambel, Castanheira, & Sobral, 2016) in their study of temporary agency and permanent workers as one group, and call centres and manufacturing sectors as the second group. We have also attempted to understand the mediation and moderation effects of the core constructs on the constructs of protection motivation theory (PMT). Mediation and moderation are effects caused my one construct on two or more other constructs, thereby helping us understand the causal relationships between them (Wu & Zumbo, 2008). Assume there are two constructs A and B. Construct A is an independent variable and construct B is a dependent variable. Construct A has some causal effect on Construct B. So the mediator is a third construct which links to this causal effect (Wu & Zumbo, 2008). According to Wu and Zumbo a mediator explains how construct A causes Construct B. While a moderator affects the causal effect of construct A on Construct B, either to strengthen or weaken the effect.

5.2 SEM:

5.2.1 Conceptual model

The researcher intents to posit on:

Part 1: Multi Group Analysis: Policymakers vs employees, for moderating effects on the relationships in PMT

Part 2: If the constructs of Employee perception of Security (EPOS), namely, Perception of information security, Perception of organisational intervention, Perception of organisational citizenship, viz. Perception of organisational commitment and Perception of responsibility, and Perception of quality of policy document, have meditation effects or moderation effects on the relationships of Protection motivation theory (PMT), viz, Threat appraisal, coping appraisal and behavioural intent, and actual behaviour.

Part 3: Usability of a tailored policy: To test the moderation effects of a tailored policy

Part 4: All the while using type of security in organisation viz. Low security, medium security, high security, as controls.

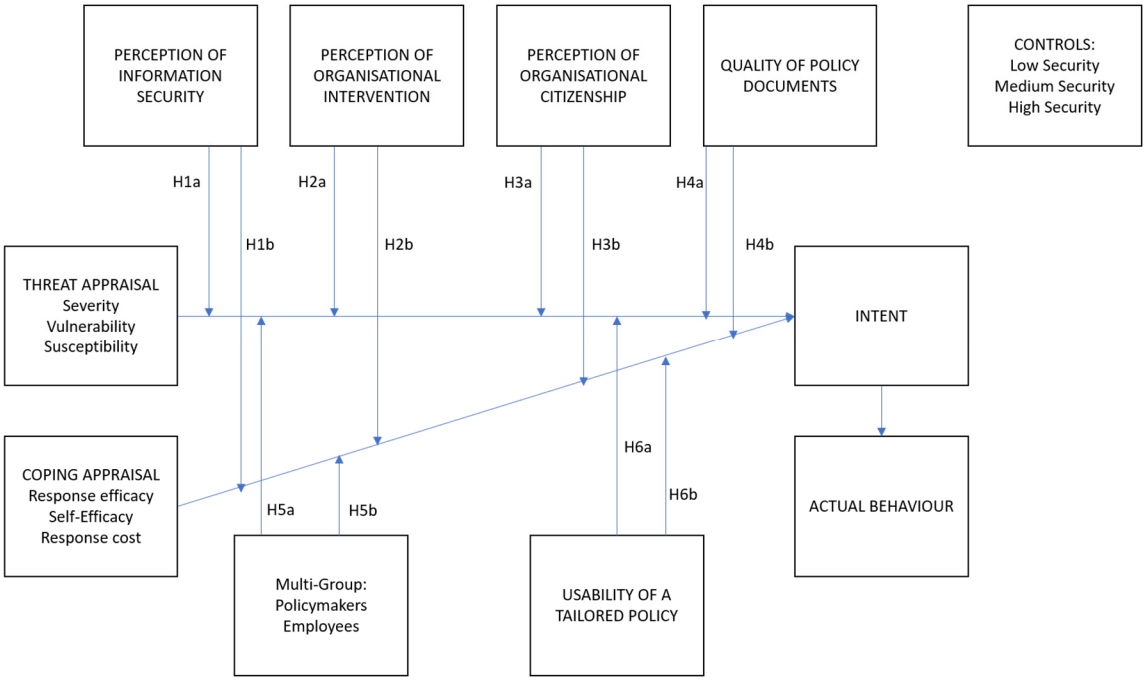


Figure 3 SEM Conceptual Model.

5.2.2 Part 1: Tested hypothesis

Logic: In their study of end user security behaviour of password management, Stanton et al (Stanton et al., 2005) posited that users who possess technical knowledge showed better security behaviour. And users with poor technical knowledge showed poor password creation behaviour. So, if you have stronger knowledge about Information security, it will be easier for you to understand vulnerabilities within your IT systems, and associated threats. And thus, understand Threat severity of an attack. This understanding of severity will lead to better security behaviour intention and thus better security behaviour.

H1a: Perception of information security positively moderates the positive effect of Threat appraisal on Behavioural intent.

Logic: If you have stronger knowledge of information security, it will be easier for you to understand the recommended behaviours (Orazi et al., 2019). This will improve self-efficacy (Rhee, Kim, & Ryu, 2009), thereby increasing the chances of effective response efficacy (Orazi

et al., 2019). Easier understanding of recommended behaviour will make the behaviour easier to perform and thus reduce response costs.

H1b: Perception of information security positively moderates the positive effect of Coping appraisal on Behavioural intent.

Logic: Organisational interventions are there to make you aware of what needs to be protected. Stronger perceptions of these interventions would mean, the organisation has implemented effective interventions (Workman et al., 2008). Being effective means providing better understanding of which vulnerabilities to prioritise and their associated threat severity levels. Thus, improving security behavioural intention.

H2a: Perception of organisational interventions positively moderates the positive effect of Threat appraisal on Behavioural intent.

Logic: Interventions should educate you about threat severity and vulnerability. Effectiveness of these interventions will create stronger perceptions (Zhiling Tu et al., 2019), effective awareness programs will help to assess effectiveness of recommended behaviour (response efficacy), effective training programs will improve self-efficacy, better communications to increase awareness of response costs (Eminağaoğlu et al., 2009).

H2b: Perception of organisational interventions positively moderates the positive effect of Coping appraisal on Behavioural intent.

Logic: Stronger organisational citizenship means stronger commitment and a stronger sense of responsibility to protect (Kirlappos et al., 2014). Hence increasing the intention to protect. Therefore, you will make stronger efforts to understand your organisational vulnerabilities and the threats involved. Because of fear of threat severity, response efficacy can be affected negatively (Mikko Siponen et al., 2014). However if you are information security conscious, you will make stronger effort to learn the recommended behaviour (Safa et al., 2015). And a stronger sense of responsibility will lead to stronger self-efficacy and in turn increase response efficacy.

H3a: Perception of organisational citizenship positively moderates the positive effect of Threat appraisal on behavioural intent.

H3b: Perception of organisational citizenship positively moderates the positive effect of Coping appraisal on behavioural intent.

Logic: An information security policy is something the users can identify and see what is expected from them (Höne & Eloff, 2002). Better documentation will provide better referencing in case of an emergency.

H4a: Quality of policy documents positively moderates the positive effect of Threat appraisal on their Behavioural intent.

H4b: Quality of policy documents positively moderates the positive effect of Coping appraisal on their Behavioural intent.

5.2.3 Part 2: Multi-group Hypotheses

Logic: Policymakers are expected to have stronger information security knowledge (Wilson et al., 2009), hence stronger positive effect. As a policymaker, participant will decide the recommended behaviour hence have a better understanding of coping mechanisms. Employee participation has been found effective in improving general sense of responsibility and improving participants behaviour (Michels & De Graaf, 2010).

H5a: Participation in policymaking positively moderates the effect of Threat appraisal on Behavioural intent such that, the effect is stronger for policymakers than employees

H5b: Participation in policymaking positively moderates the effect of Coping appraisal on Behavioural intent such that, the effect is stronger for policymakers than employees

5.2.4 Part 3: Usability of a tailored policy

Logic: I found no research on usability tailored policy. Though the importance of making the security policy effective has been identified (Höne & Eloff, 2002) implying an effective policy will affect behavioural intent. Usability of a policy is measured in terms of its effectiveness, efficiency and satisfaction (Bevan & Macleod, 1994). Hence, we will try to establish this trough SEM and survey data analysis. A tailored policy should adequately provide users information about information security and security practices within the organisation. It should also inform users about existing resources and interventions offered by the organisation to practice acceptable security behaviour (Doherty, Anastasakis, & Fulford, 2011). The policy should inform users about

the threats associated with their job role and how to address these threats. Based on these following hypotheses can be made.

H6a: Usability of a tailored policy strengthens the positive relationship between Perception of information security on Threat Appraisal

H6b: Usability of a tailored policy strengthens the positive relationship between Perception of Organisational Interventions on Threat Appraisal.

H6c: Usability of a tailored policy strengthens the positive relationship between Perception of information security on Coping Appraisal.

H6d: Usability of a tailored policy strengthens the positive relationship between Perception of Organisational Interventions on Coping Appraisal.

H6e: Usability of a tailored policy strengthens the positive relationship between Perception of information security on Behavioural intent.

H6f: Usability of a tailored policy strengthens the positive relationship between Perception of Organisational Interventions on Behavioural intent.

H6g: Usability of a tailored policy strengthens the positive relationship between Perception of information security on Actual Behaviour.

H6h: Usability of a tailored policy strengthens the positive relationship between Perception of Organisational Interventions on Actual Behaviour.

H6i: Usability of a tailored policy strengthens the positive relationship between Threat appraisal on Behavioural intent.

H6j: Usability of a tailored policy strengthens the positive relationship between Coping Appraisal on Behavioural intent.

H6k: Usability of a tailored policy dampens the negative relationship between Threat appraisal on Actual Behaviour.

H6l: Usability of a tailored policy strengthens the positive relationship between Coping appraisal on Actual Behaviour.

5.3 SEM 1st Run – Unsuccessful (Issues with run)

It seems I had started the entire process of SEM incorrectly. I had not cleaned my data properly. Firstly, I had not removed unengaged responses from my SPSS data. This caused issues to standard deviation as for most unengaged responses SD is 0. For cleaning the data properly all responses with standard deviation less than 0.3 were removed. Then, it seems I had not done the exploratory factor analysis properly. I did the principal component analysis with individual constructs. Because of this for my first run all my components in the first run showed a determinant value over .00001 for all constructs which indicates good correlation. But by doing this I was corelating all the individual items within the construct. It was later obvious that these will correlate. Because of this I was also getting excellent reliability for all constructs. But when I loaded up all the items from all the constructs in AMOS the factor loadings seemed reasonable but not great. I realised that there might be some issues with the item's selection. Particularly items in the construct Quality of policy documents. Though some items are loading nicely on the construct itself, the overall correlation with other constructs was not so great. I also realised that you cannot correlate errors values from different construct. My values were improving slightly because of this but this was another incorrect step. Deleting items in AMOS was not improving results. Analysis was simply not progressing ahead. I decided a complete overhaul was deemed necessary. After speaking with a few AMOS experts, they suggested I should still report this run as this is an important part for showing how I reached satisfactory results. All the mistakes I corrected in the second run are mentioned in their respective place in their respective steps below.

5.4 Preparing for SEM 2nd Run (Successful)

5.4.1 Conceptual model

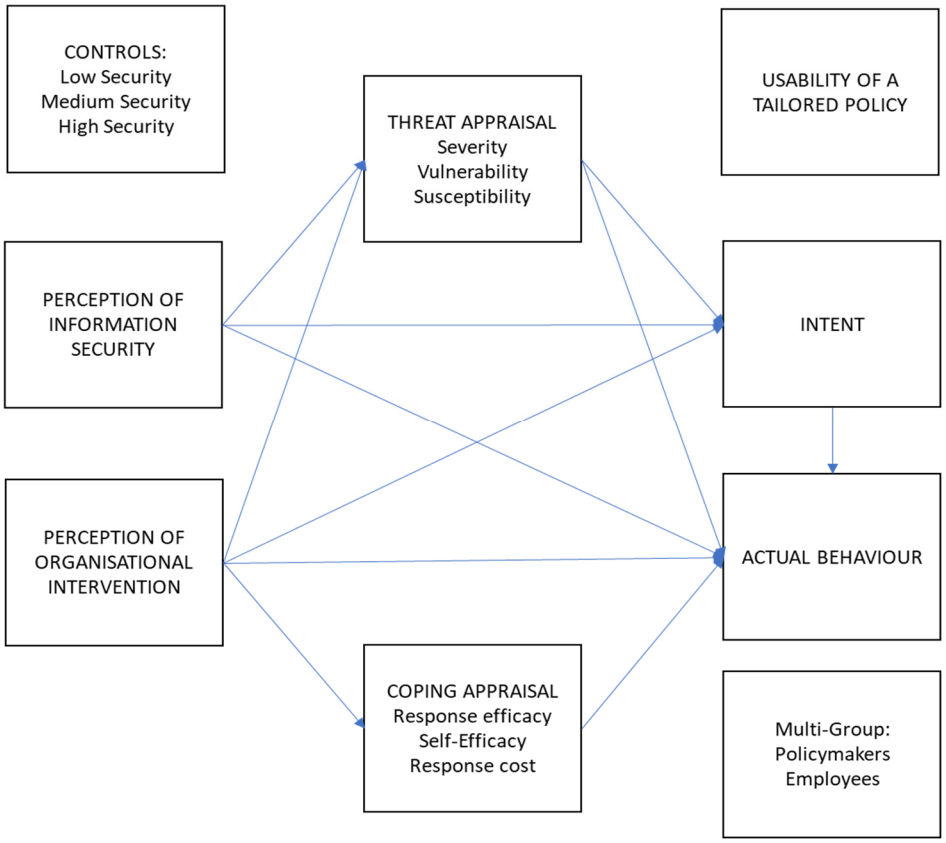


Figure 4: Conceptual Model developed through SEM

5.4.2 Screening data

Data screening basically making sure your data is clean for further analysis. This means to check the data for any missing data, outliers and normality. It has been found in research that screening SPSS data by addressing missing values, outliers unengaged responses and normality R squared value is increased (Odom & Henson, 2002).

5.4.2.1 Missing Data

Occasionally you may have missing data, where the participant has not missed to respond or simply left the survey incomplete. With missing values EFA and CFA analysis won't work. Care was taken before administering the survey. All questions must be answered, or the survey won't move forward and only completed surveys were recorded. This survey collected 624 samples

however only 513 complete samples are selected for analysis. Hence with research data there are no missing values. Missing data causes inaccurate estimates (Odom & Henson, 2002). This process involves checking for any item statements case by case, where the respondent has not answered. For this survey this was not an issue as participants were not allowed to proceed ahead without giving a response. This was achieved by displaying a message on screen, indicating that it is expected of the participant that they answer the question.

5.4.2.2 Unengaged Responses

There are various methods for identifying unengaged responses from participants (Guin et al., 2012). One particularly used method is finding standard deviation (Hone & El Said, 2016). We deleted 27 participant responses, they had standard deviation 0. And 15 other participant responses with standard deviation std. < 0.3 (Hone & El Said, 2016).

5.4.2.3 Outliers

Outliers are present on only on continuous variable (Norman, 2010). An outlier is a variable which can take any value. Presence of outliers has been found to impact Cronbach's alpha (Liu & Zumbo, 2007). However, it is highly unlikely to have outliers on a 5-point Likert scale.

5.4.2.4 Normality

We check normality to ensure data is normally distributed. This is done by checking Skewness and Kurtosis (Groeneveld & Meeden, 1984). Ideal value for Skewness is between +2 and -2. According to published thresholds anything outside of 2.2 gives errors. The kurtosis for a standard distribution is 3. We had no skewness or only From_3 showed slight Kurtosis. We would have had to delete the item statement if the kurtosis was very high.

Statistics

	N		Skewness	Std. Error of Skewness	Kurtosis	Std. Error of Kurtosis
	Valid	Missing				
AC_BEHAVE_1	471	0	1.200	0.113	0.984	0.225
AC_BEHAVE_2	471	0	1.215	0.113	1.185	0.225
AC_BEHAVE_3	471	0	0.614	0.113	-0.526	0.225
AC_BEHAVE_4	471	0	0.948	0.113	0.329	0.225
TSEV_1	471	0	0.700	0.113	-0.065	0.225
TSEV_2	471	0	0.783	0.113	0.293	0.225

TSEV_3	471	0	0.750	0.113	0.223	0.225
TSUS_1	471	0	0.889	0.113	0.263	0.225
TSUS_2	471	0	1.052	0.113	0.762	0.225
TVUL_1	471	0	0.862	0.113	0.330	0.225
TVUL_2	471	0	1.014	0.113	0.456	0.225
TVUL_3	471	0	0.996	0.113	0.611	0.225
AWARENESS_2	471	0	1.210	0.113	0.984	0.225
COMMUNICATION_1	471	0	0.931	0.113	0.229	0.225
COMMUNICATION_3	471	0	0.503	0.113	-0.797	0.225
EFFECTIVENESS_1	471	0	0.864	0.113	0.435	0.225
EFFECTIVENESS_2	471	0	0.918	0.113	0.628	0.225
EFFICIENCY_2	471	0	0.916	0.113	0.223	0.225
SATISFACTION_2	471	0	0.628	0.113	-0.172	0.225
SATISFACTION_3	471	0	0.937	0.113	0.499	0.225
SEC_POLICY_2	471	0	0.962	0.113	0.209	0.225
TRAINING_2	471	0	0.726	0.113	-0.460	0.225
RESC4R	471	0	0.485	0.113	-1.029	0.225
RESC5R	471	0	0.447	0.113	-0.963	0.225
RESC_1R	471	0	0.209	0.113	-1.305	0.225
AWARENESS_3	471	0	1.085	0.113	0.567	0.225
COMMUNICATION_2	471	0	1.201	0.113	1.106	0.225
FROM_1	471	0	1.454	0.113	2.096	0.225
FROM_3	471	0	1.839	0.113	3.502	0.225
SEC_POLICY_3	471	0	1.031	0.113	0.782	0.225
SEFF_1	471	0	0.567	0.113	-0.386	0.225
SEFF_2	471	0	0.866	0.113	0.486	0.225
SEFF_3	471	0	0.600	0.113	-0.216	0.225
TRAINING_3	471	0	1.048	0.113	0.619	0.225
WHAT_1	471	0	0.545	0.113	-0.223	0.225
WHAT_2	471	0	0.637	0.113	0.096	0.225
WHY_1	471	0	0.887	0.113	0.063	0.225
WHY_3	471	0	1.220	0.113	1.124	0.225
INTENT_2	471	0	0.527	0.113	0.081	0.225
INTENT_3	471	0	0.599	0.113	-0.026	0.225
REFF_1	471	0	1.076	0.113	0.583	0.225
REFF_2	471	0	1.019	0.113	0.530	0.225
REFF_3	471	0	1.032	0.113	0.590	0.225

5.4.3 Exploratory Factor Analysis (EFA)

Exploratory Factor Analysis or EFA (Al-Omari, El-Gayar, & Deokar, 2011), is used to determine corelated factors. This was done to ensure we have a clean pattern matrix. This was also done to improve Cronbach's Alpha (Tavakol & Dennick, 2011). Cronbach's alpha for all constructs was found to be above 0.7 as shown in the pattern matrix table. Hence the measurement instrument showing strong reliability.

5.4.3.1 Rotation types

There are different types of rotations that can be used to clearly differentiate the factor loading. Orthogonal, such as Varimax, and Oblique, such as Promax. Either method is affective, however Promax has been found to be preferable due to faster computation and larger datasets (Finch, 2006). For the factor analysis direct oblima or Oblique Rotation is used as the investigator presumes the constructs are correlated.

5.4.3.2 Principle component analysis (PCA)

We have used Maximum likelihood Principal component analysis for extracting factors. Use of estimation methods such as maximum likelihood (ML) generalised least square (GLS) and weighted least squares (WLS) can be used to address the robustness issues (Satorra, 1990) (Olsson et al., 2000). Plus this is the same algorithm AMOS uses for CFA which we are going to do.

Pattern Matrix[a]										
	Factor									
	1	2	3	4	5	6	7	8	9	10
CRONBACH'S ALPHA	**0.901**	**0.874**	**0.814**	**0.852**	**0.71**	**0.858**	**0.734**	**0.85**	**0.903**	**0.823**
TVUL_1	0.862									
TVUL_3	0.831									
TSEV_2	0.792									
TSEV_1	0.771									
TVUL_2	0.735									
TSEV_3	0.650									
TSUS_1	0.624									
TSUS_2	0.523									
TRAINING_2		0.909								
SEC_POLICY_2		0.711								
COMMUNICATION_1		0.696								

AWARENESS_2		0.693								
COMMUNICATION_3		0.692								
EFFECTIVENESS_2			0.877							
EFFECTIVENESS_1			0.820							
EFFICIENCY_2			0.811							
SATISFACTION_2			0.713							
SATISFACTION_3			0.563							
RESC4R				1.038						
RESC5R				0.871						
RESC_1R				0.665						
AWARENESS_3					0.830					
TRAINING_3					0.820					
SEC_POLICY_3					0.781					
COMMUNICATION_2					0.505					
SEFF_3						0.854				
SEFF_1						0.733				
SEFF_2						0.722				
WHY_1							0.636			
WHY_3							0.606			
WHAT_2							0.487			
FROM_3							0.487			
FROM_1							0.481			
WHAT_1							0.476			
AC_BEHAVE_1								0.947		
AC_BEHAVE_2								0.920		
AC_BEHAVE_4								0.579		
AC_BEHAVE_3								0.476		
REFF_2									0.854	
REFF_3									0.803	
REFF_1									0.788	
INTENT_2										1.026
INTENT_3										0.608

Extraction Method: Maximum Likelihood.
Rotation Method: Promax with Kaiser Normalization.

a. Rotation converged in 8 iterations.

5.4.3.3 Appropriateness of data

Appropriateness of data is measured using Kaiser-Mayer-Olkin (KMO) statistics (Kaiser, 1970), and Bartlett's Sphericity test (Bartlett, 1937) (Tobias & Carlson, 1969). Both showing good values, hence confirming appropriateness of data. Goodness of Fit (T. W. Anderson & Darling, 1954) test shows a Chi-Square 1361.034 and degrees of freedom 518 and significance of .000

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.922
Bartlett's Test of Sphericity	Approx. Chi-Square	13025.610
	df	903
	Sig.	.000

Goodness-of-fit Test

Chi-Square	df	Sig.
1361.034	518	.000

Low communalities have influence on the quality of factors (Hogarty et al., 2005), hence items with communalities less than .2 are removed.

Communalities[a]

	Initial	Extraction
AC_BEHAVE_1	.787	.869
AC_BEHAVE_2	.781	.834
AC_BEHAVE_3	.513	.479
AC_BEHAVE_4	.603	.570
AWARENESS_2	.632	.633
COMMUNICATION_1	.563	.559
COMMUNICATION_3	.581	.564
FROM_1	.540	.456
SEC_POLICY_2	.693	.681
TRAINING_2	.670	.729
WHY_1	.527	.557
WHY_3	.505	.541
AWARENESS_3	.511	.574

SEC_POLICY_3	.576	.617
TRAINING_3	.576	.653
EFFECTIVENESS_1	.680	.700
EFFECTIVENESS_2	.693	.744
EFFICIENCY_2	.632	.676
SATISFACTION_2	.535	.485
SATISFACTION_3	.606	.546
TSEV_1	.553	.502
TSEV_2	.679	.568
TSUS_1	.665	.595
TSUS_2	.617	.533
TVUL_1	.604	.600
TVUL_2	.655	.640
TVUL_3	.675	.686
REFF_1	.721	.762
REFF_3	.693	.724
SEFF_1	.630	.634
SEFF_2	.693	.728
SEFF_3	.657	.755
RESC5R	.666	.698
TSEV_3	.539	.384
INTENT_2	.584	.999
INTENT_3	.587	.546
WHAT_2	.415	.222
RESC4R	.718	.896
RESC_1R	.486	.495
REFF_2	.757	.816
COMMUNICATION_2	.549	.547
WHAT_1	.435	.205
FROM_3	.530	.460

Extraction Method: Maximum Likelihood.

a. If one or more communality estimates greater than 1 were encountered during iterations. The resulting solution should be interpreted with caution.

In total variance explained (Howe, 2003) we look at Cumulative % in extracted sums of squared loadings. The cumulative % greater than 50 is considered good. Over 60 is better. For this research it is 61.546

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
Factor	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	14.343	33.356	33.356	4.374	10.171	10.171	11.376
2	3.506	8.153	41.509	10.655	24.780	34.951	7.949
3	2.655	6.175	47.683	2.964	6.893	41.843	7.995
4	1.968	4.577	52.260	2.222	5.168	47.012	4.563
5	1.725	4.011	56.271	1.443	3.356	50.367	8.153
6	1.538	3.576	59.847	1.105	2.569	52.937	5.993
7	1.240	2.885	62.731	1.100	2.558	55.495	6.016
8	1.153	2.681	65.412	0.924	2.149	57.644	9.566
9	1.070	2.488	67.900	0.803	1.867	59.511	8.990
10	1.014	2.359	70.258	0.875	2.035	61.546	4.470
11	0.946	2.201	72.459				
12	0.808	1.878	74.338				
13	0.781	1.816	76.154				
14	0.635	1.477	77.631				
15	0.624	1.452	79.082				
16	0.581	1.351	80.433				
17	0.544	1.266	81.699				
18	0.520	1.208	82.908				
19	0.495	1.151	84.059				
20	0.463	1.076	85.135				
21	0.459	1.067	86.202				
22	0.430	0.999	87.201				
23	0.406	0.945	88.146				
24	0.395	0.918	89.064				
25	0.371	0.863	89.927				
26	0.354	0.822	90.749				
27	0.344	0.799	91.548				
28	0.328	0.763	92.311				
29	0.304	0.706	93.017				
30	0.297	0.690	93.707				

31	0.283	0.658	94.365				
32	0.281	0.653	95.018				
33	0.264	0.614	95.632				
34	0.248	0.578	96.209				
35	0.239	0.556	96.765				
36	0.226	0.526	97.291				
37	0.209	0.487	97.778				
38	0.195	0.453	98.231				
39	0.175	0.406	98.637				
40	0.166	0.385	99.022				
41	0.157	0.366	99.388				
42	0.140	0.325	99.712				
43	0.124	0.288	100.000				

Extraction Method: Maximum Likelihood.

a. When factors are correlated, sums of squared loadings cannot be added to obtain a total variance.

5.4.3.4 Convergent Validity

As evidenced from the pattern matrix we have all values above 0.5. Some items from Knowledge of information security and 1 item from actual behavior is showing values under 0.5. Deleting these items causes the pattern matrix to collapse or creates various cross loadings. Meaning these items are helping to distinguish the factor loadings. However, we are going to keep these items as they are not far off 0.5 and their reliability is above 0.7 also it is highly likely that these values may go up during CFA in AMOS.

5.4.3.5 Discriminant Validity

As evidenced from the pattern matrix we have no cross loadings. Another evidence of discriminant validity is to see that none of the non-diagonal values are above 0.7, as this would indicate sharing a majority of variance.

Factor Correlation Matrix										
Factor	1	2	3	4	5	6	7	8	9	10
1	1.000	0.533	0.500	0.423	0.588	0.453	0.544	0.641	0.661	0.411
2	0.533	1.000	0.353	0.080	0.499	0.547	0.194	0.580	0.346	0.311
3	0.500	0.353	1.000	0.185	0.461	0.374	0.467	0.542	0.574	0.367
4	0.423	0.080	0.185	1.000	0.260	-0.051	0.300	0.400	0.480	0.047
5	0.588	0.499	0.461	0.260	1.000	0.331	0.413	0.541	0.542	0.429

6	0.453	0.547	0.374	-0.051	0.331	1.000	0.177	0.447	0.272	0.345
7	0.544	0.194	0.467	0.300	0.413	0.177	1.000	0.383	0.542	0.201
8	0.641	0.580	0.542	0.400	0.541	0.447	0.383	1.000	0.582	0.320
9	0.661	0.346	0.574	0.480	0.542	0.272	0.542	0.582	1.000	0.302
10	0.411	0.311	0.367	0.047	0.429	0.345	0.201	0.320	0.302	1.000

Extraction Method: Maximum Likelihood.
Rotation Method: Promax with Kaiser Normalization.

5.4.3.6 Reliability

Cronbach's Alpha has been added to the pattern matrix table to show all values above 0.7.

5.4.4 Confirmatory Factor Analysis (CFA)

5.4.4.1 Getting a cursory model fit. Checking for validity.

The first step is to bring the model to a rough fit also termed Cursory model fit, and then check for validity.

In AMOS, analysis properties for output we selected, standardised estimates, modification indices with a threshold of 20. Looking the initial model, we have an inflated Chi Square 2485.847, this is expected because our sample size is 471.

CMIN

Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	112	2485.847	834	0	2.981
Saturated model	946	0	0		
Independence model	43	13459.956	903	0	14.906

Baseline Comparisons					
Model	**NFI**	**RFI**	**IFI**	**TLI**	**CFI**
	Delta1	rho1	Delta2	rho2	
Default model	0.82	0.8	0.87	1	0.868
Saturated model	1		1		1
Independence model	0	0	0	0	0

RMSEA				
Model	**RMSEA**	**LO 90**	**HI 90**	**PCLOSE**
Default model	0.07	0.062	0.07	0
Independence model	0.17	0.169	0.18	0

After bringing the model to a cursory fit,

CMIN					
Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	119	1987.111	827	0	2.403
Saturated model	946	0	0		
Independence model	43	13459.956	903	0	14.906

Baseline Comparisons					
Model	NFI	RFI	IFI	TLI	CFI
	Delta1	rho1	Delta2	rho2	
Default model	0.85	0.839	0.91	0.899	0.908
Saturated model	1		1		1
Independence model	0	0	0	0	0

RMSEA				
Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	0.055	0.052	0.06	0.007
Independence model	0.172	0.169	0.18	0

5.4.4.2 Metric invariance

We did a metric invariance test by constraining the two models to be equal and did a chi square difference test between the fully constrained and unconstrained models and found them to be invariant (p-value = 0.862).

	Chi-square	**df**	**p-val**	**Invariant?**
Overall Model				
Unconstrained	3065.9	1654		
Fully constrained	3125	1726		

Number of groups		2			
Difference	59.1	72	0.862		YES

5.4.4.3 Configural, metric and scalar variance tests.

This method is necessary to report if I am going to a multi group causal model. (Policymakers vs Employees) For this we create the groups we are going to sue for our multi groups analysis.

CMIN					
Model	NPAR	CMIN	DF	P	CMIN/DF
Default model	238	3065.876	1654	0	1.854
Saturated model	1892	0	0		
Independence model	86	14531.064	1806	0	8.046

Baseline Comparisons					
Model	NFI	RFI	IFI	TLI	CFI
	Delta1	rho1	Delta2	rho2	
Default model	0.789	0.77	0.89	0.879	0.889
Saturated model	1		1		1
Independence model	0	0	0	0	0

RMSEA				
Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	0.043	0.04	0.05	1
Independence model	0.123	0.121	0.12	0

Standardised RMR: 0.0745 (Threshold 0.08)

We did a configural invariance test and found an adequate goodness of fit when analysing a freely estimated model across two groups, policymakers, and employees. (CFI-0.889, SRMR-0.0745, RMSEA-0.043)

5.5 Findings

5.5.1 Model description

Stanton et al (Stanton et al., 2005) posited that users who possess technical knowledge showed better security behaviour. If you have stronger knowledge about Information security, it will be easier for you to understand vulnerabilities within your IT systems, and associated threats. And thus, understand Threat severity of an attack. This understanding of severity will lead to better security behaviour intention and thus better security behaviour (Adams & Sasse, 1999). If you have stronger knowledge of information security, it will be easier for you to understand the recommended behaviours (Orazi et al., 2019). This will improve self-efficacy (Rhee et al., 2009), thereby increasing the chances of effective response efficacy (Orazi et al., 2019). Easier understanding of recommended behaviour will make the behaviour easier to perform and thus reduce response costs. Stronger perceptions of organisational interventions would mean, the organisation has implemented effective interventions (Workman et al., 2008). Being effective means providing better understanding of which vulnerabilities to prioritise and their associated threat severity levels. Thus, improving security behavioural intention. Stronger organisational citizenship means stronger commitment and a stronger sense of responsibility to protect (Kirlappos et al., 2014). Therefore, you will make stronger efforts to understand your organisational vulnerabilities and the threats involved. This in turn will result in a stronger sense of responsibility which leads to stronger self-efficacy and in turn increase response efficacy. While carrying out EFA to understand corelated factors it was found that quality of policy documents did not fit the model. This could be due to the fact that the item statements were focussed on current policy documents and could mean that the current quality of policy documents does not facilitate better understanding of threats their severity and does not make the coping mechanisms clearly understandable. After deleting the item statements from during EFA, the resulting factors were found to provide a more stable pattern matrix. To successfully acquire a model in AMOS, it is important for the factors to correlate as shown in the model as if they do not correlate AMOS would simply not execute the model. To understand how participation in policymaking affected this model the participants were divided in to two groups, policymakers and employees and this model was then used for a multi group analysis. Usability of a tailored policy was used as a moderator to see how it affected the pathways between constructs.

CMIN					
Model	NPAR	CMIN	DF	P	CMIN/DF

Default model	26	1.402	2	0.496	0.701
Saturated model	28	0	0		
Independence model	7	2071.125	21	0	98.625

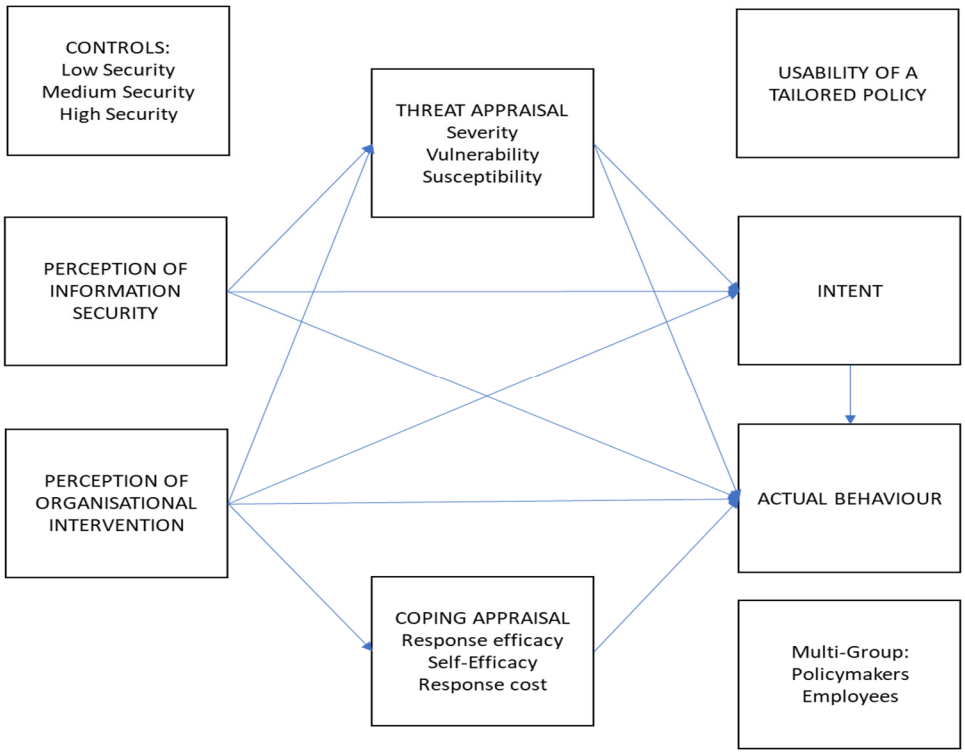
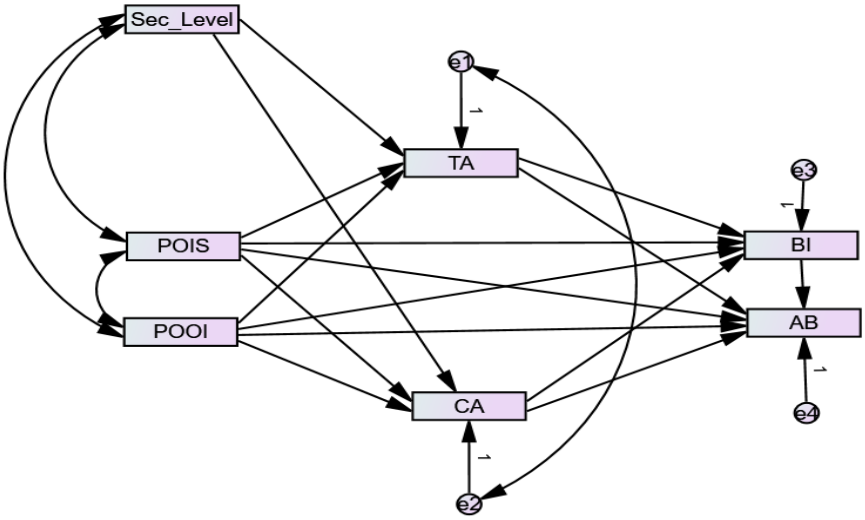


Figure 5 Conceptual model aquired from AMOS

Model acquired from AMOS

Baseline Comparisons					
Model	NFI	RFI	IFI	TLI	CFI
	Delta1	rho1	Delta2	rho2	
Default model	0.999	0.993	1	1.003	1
Saturated model	1		1		1
Independence model	0	0	0	0	0

RMSEA				
Model	RMSEA	LO 90	HI 90	PCLOSE
Default model	0	0	0.082	0.78
Independence model	0.456	0.439	0.472	0



5.5.2 Regression Weights

Table 3 below shows unstandardised regression weights on the pathways between the constructs along with their p value. Table 4 below shows the beta regression coefficients. It shows strong and positive corelation between Perception of information security (POIS) and constructs of PMT viz Threat appraisal (TA), and Coping appraisal (CA), and between perception of Organisational interventions (POOI) and constructs of PMT viz Threat appraisal (TA), and Coping appraisal (CA). We also see a strong and positive correlation between Threat appraisal (TA) and behavioural intent (BI). This is confirmed by PMT. The effect of users Perception of information security (POIS) on Threat appraisal (TA) is statistically significant with beta coefficient of 0.54

(p<0.001). The effect of Perception of information security (POIS) on Coping appraisal (CA) is statistically significant with beta coefficient of 0.61(p<0.001). The effect of users' perception of their organisational interventions (POOI) on Threat appraisal (TA) was strong and significant with beta coefficient of 0.48(p<0.001). The effect of Perception of organisational interventions (POOI) on Coping appraisal (CA) was statistically significant with a beta coefficient of 0.28(p<0.001). The effect of Threat appraisal (TA) on behavioural intent (BI) was statistically significant with a beta coefficient of 0.41(p<0.001). The effect of Coping appraisal (CA) on behavioural intent (BI) was more significant with a beta coefficient of 0.17(p<0.01)

			Estimate	S.E.	C.R.	P	Label
CA	<---	POOI	.196	.024	8.027	***	
TA	<---	POIS	1.710	.083	20.711	***	
TA	<---	Sec_Level	.001	.022	.066	.948	
TA	<---	POOI	.317	.019	17.021	***	
CA	<---	POIS	2.059	.108	19.029	***	
CA	<---	Sec_Level	-.002	.028	-.084	.933	
BI	<---	POIS	-.247	.238	-1.039	.299	
BI	<---	POOI	.066	.043	1.523	.128	
BI	<---	TA	.502	.097	5.154	***	
BI	<---	CA	.192	.074	2.587	.010	
AB	<---	BI	.006	.037	.177	.859	
AB	<---	POIS	-.161	.188	-.857	.391	
AB	<---	POOI	.399	.034	11.558	***	
AB	<---	TA	.215	.079	2.706	.007	
AB	<---	CA	.416	.059	7.017	***	

*Table 29 Regression Weights without the effect of Tailored policy *** p<0.001, **p<0.01, *p<0.05*

			Estimate
CA	<---	POOI	.283
TA	<---	POIS	.536
TA	<---	Sec_Level	.002
TA	<---	POOI	.483
CA	<---	POIS	.612
CA	<---	Sec_Level	-.003
BI	<---	POIS	-.065
BI	<---	POOI	.084
BI	<---	TA	.419
BI	<---	CA	.169
AB	<---	BI	.006
AB	<---	POIS	-.038
AB	<---	POOI	.456
AB	<---	TA	.161
AB	<---	CA	.330

Table 30 Standardised Regression Weights (Beta)

Other noticeable effects were of Perception of organisational interventions (POOI) on Actual behaviour was statistically significant with a beta coefficient of 0.46(p<0.001) and effect of coping

appraisal (CA) on actual behaviour (AB) was statistically significant with a beta coefficient of 0.33($p<0.001$) The effect of Threat appraisal (TA) on Actual behaviour (AB) was more significant with a beta coefficient of 0.16($p<0.01$).

5.5.3 Part 1: Tested Hypotheses

5.5.3.1 Supported hypothesis

We found a positive and a significant relationship between perception of information security and threat appraisal, and between perception of information security and coping appraisal. Which means as your perception of information security increases your appraisal of threat increases and it also increases your understanding of coping mechanisms suggested by your organisation. We know from literature and also found from this study a positive and significant relationship of threat appraisal and coping appraisal with behavioural intent (Rogers, R. W., & Prentice-Dunn, 1997). Therefore, it can be said that perception of information security moderates the positive effect of threat appraisal and coping appraisal on behavioural intent.

H1a: Perception of information security positively moderates the positive effect of Threat appraisal on Behavioural intent.

H1b: Perception of information security positively moderates the positive effect of Coping appraisal on Behavioural intent.

From this study we found a positive and significant relationship of users' perception of organisational interventions with threat appraisal and coping appraisal. Which means that with increased awareness and training users' appreciation threats associated with their job roles and the responses they need to enact also increases. Based on this it can be said that users' perception of organisational interventions strongly and positively moderates the effects threat appraisal and coping appraisal on behavioural intent.

H2a: Perception of organisational interventions positively moderates the positive effect of Threat appraisal on Behavioural intent.

H2b: Perception of organisational interventions positively moderates the positive effect of Coping appraisal on Behavioural intent.

5.5.3.2 Unsupported (null) hypothesis

H3a: Perception of organisational citizenship positively moderates the positive effect of Threat appraisal on behavioural intent.

H3b: Perception of organisational citizenship positively moderates the positive effect of Coping appraisal on behavioural intent.

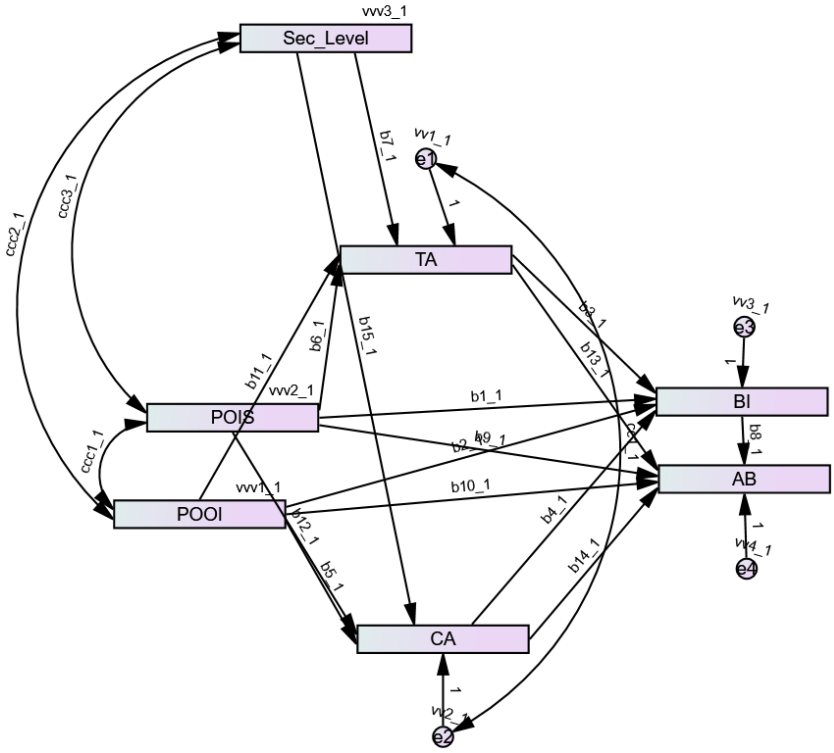
H4a: Quality of policy documents positively moderates the positive effect of Threat appraisal on their Behavioural intent.

H4b: Quality of policy documents positively moderates the positive effect of Coping appraisal on their Behavioural intent.

These preceding hypotheses can be considered as null hypothesis for this study as they provided no statistical relationships or significance with the constructs, perception of information security, perception of organisational interventions and the constructs of protection motivation theory. The possible reasons for this could be as found in previous analysis, there was a lot of confusion between policymakers and employees regarding responsibility and commitment. During the survey participants were asked about the current quality of the existing security policies. Therefore, is also possible that the current security policies are not efficient enough to adequately inform users' about the threats and the respective coping behaviours.

5.5.4 Part 2: Multi Group Hypotheses

SEM model used for multi group



We did a chi squared difference test across two groups Policymakers and employees. And found the following values. The p-value proves the model is invariant across both groups.

Model	DF	CMIN	P	NFI Delta-1	IFI Delta-2	RFI rho-1	TLI rho2
Structural weights	15	14.802	.466	.007	.007	.006	.006

H5a: Participation in policymaking positively moderates the effect of Threat appraisal on Behavioural intent such that, the effect is stronger for policymakers than employees

We reject this hypothesis. By Constraining the path between TA and BI, we did a chi square difference test and found that the path was stronger for employees than for policymakers. However, the p-value was not statistically significant.

H5b: Participation in policymaking positively moderates the effect of Coping appraisal on Behavioural intent such that, the effect is stronger for policymakers than employees

We reject this hypothesis. By Constraining the path between CA and BI, we did a chi square difference test and found that the path was stronger for policymakers than for employees. However, the p-value was not statistically significant.

5.5.4.1 Noticeable paths

TA → AB

By Constraining the path between TA and AB, we did a chi square difference test and found that the path was stronger for employees than for policymakers. However, the p-value was not significant.

POOI → CA

By Constraining the path between POOI and CA, we did a chi square difference test and found that the path was stronger for employees than for policymakers. However, the p-value was not significant.

5.5.5 Part 3: Usability of a tailored policy

The following section discusses the interaction paths between constructs and the moderation effect of a tailored policy on these paths

H6a: Usability of a tailored policy strengthens the positive relationship between POIS on TA.

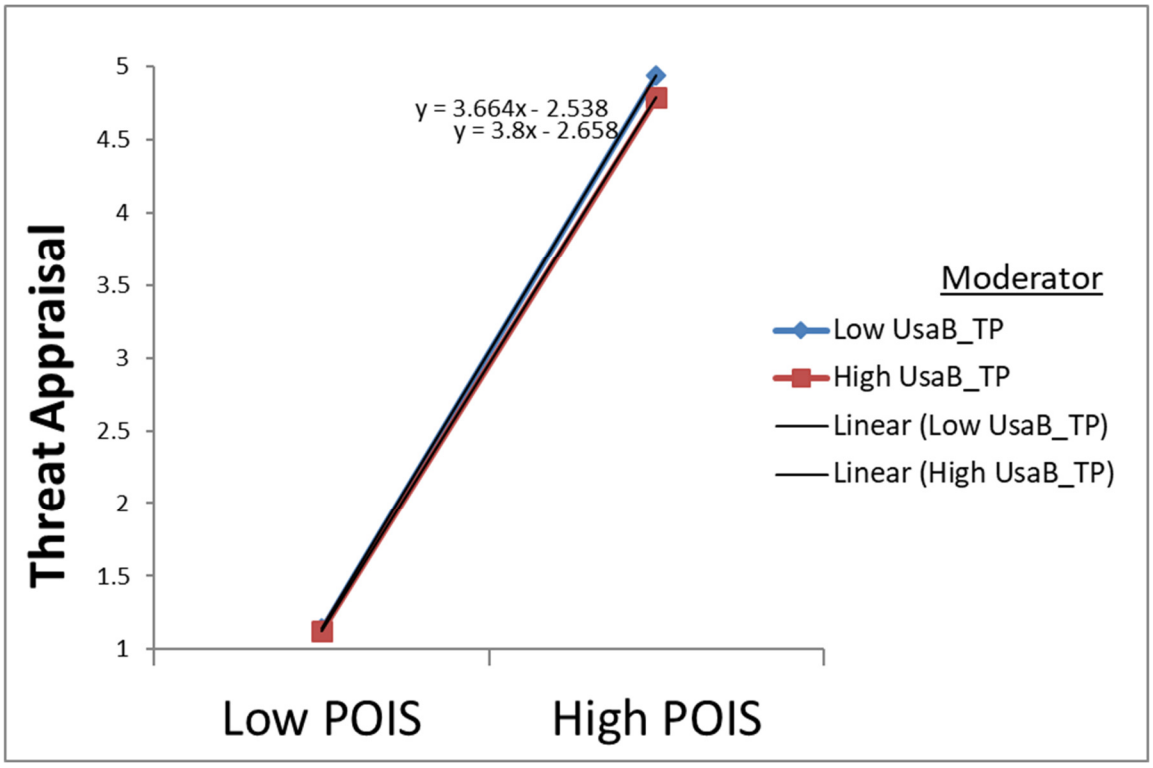


Figure 6 Interaction plot showing effect of Tailored policy on users' perception of information security and Threat appraisal

Interaction summary

Independent variable:	POIS
Moderator:	UsaB_TP
Dependent variable	Threat Appraisal

Unstandardized Regression Coefficients:

Independent variable:	1.866
Moderator:	-0.042
Interaction:	-0.034

Outcome: Use of a tailored policy dampens the positive relationship between perception of information security and threat appraisal. High usability of a tailored policy will reduce threat appraisal even when perception of information security is high.

H6b: Usability of a tailored policy strengthens the positive relationship between POOI on TA.

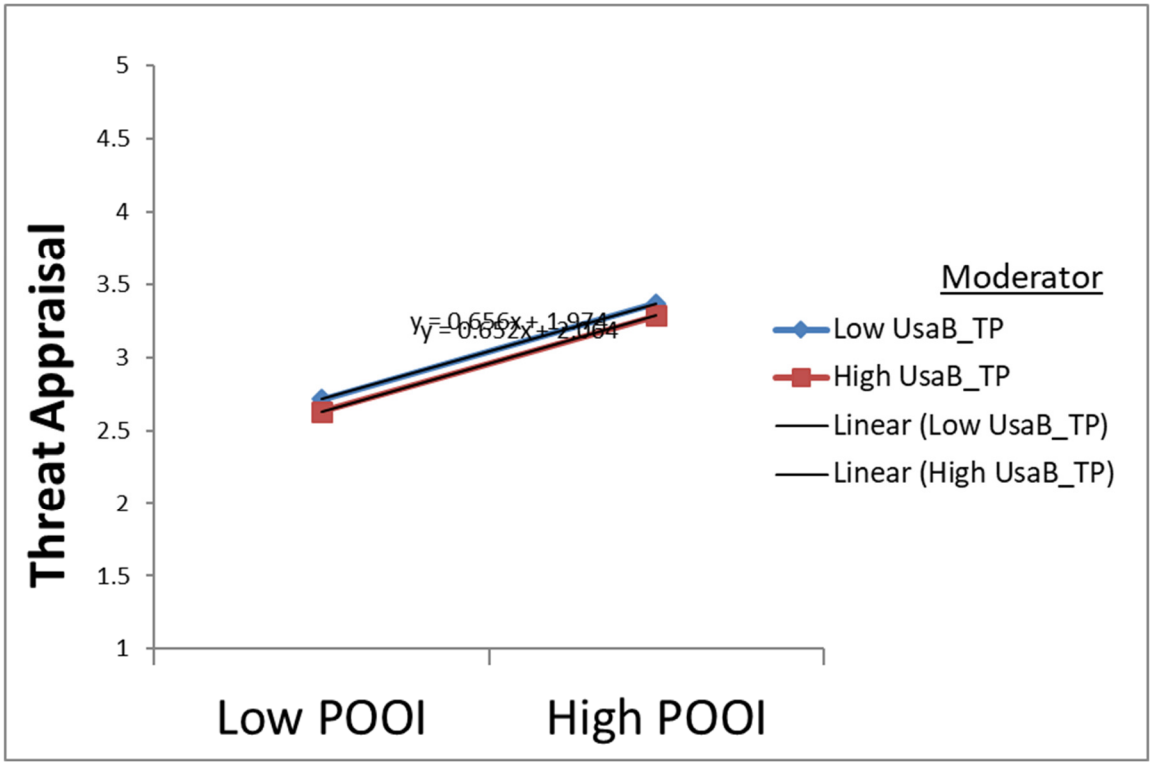


Figure 7 Interaction plot showing effect of Tailored policy on users' perception of organisational intervention and Threat appraisal

Interaction summary

Independent variable:	POOI
Moderator:	UsaB_TP
Dependent variable	Threat Appraisal

Unstandardized Regression Coefficients:

Independent variable:	0.327
Moderator:	-0.042
Interaction:	0.001

Outcome: Use of a tailored policy strengthens the positive relationship between perception of organisational interventions and threat appraisal.

H6c: Usability of a tailored policy strengthens the positive relationship between POIS on CA.

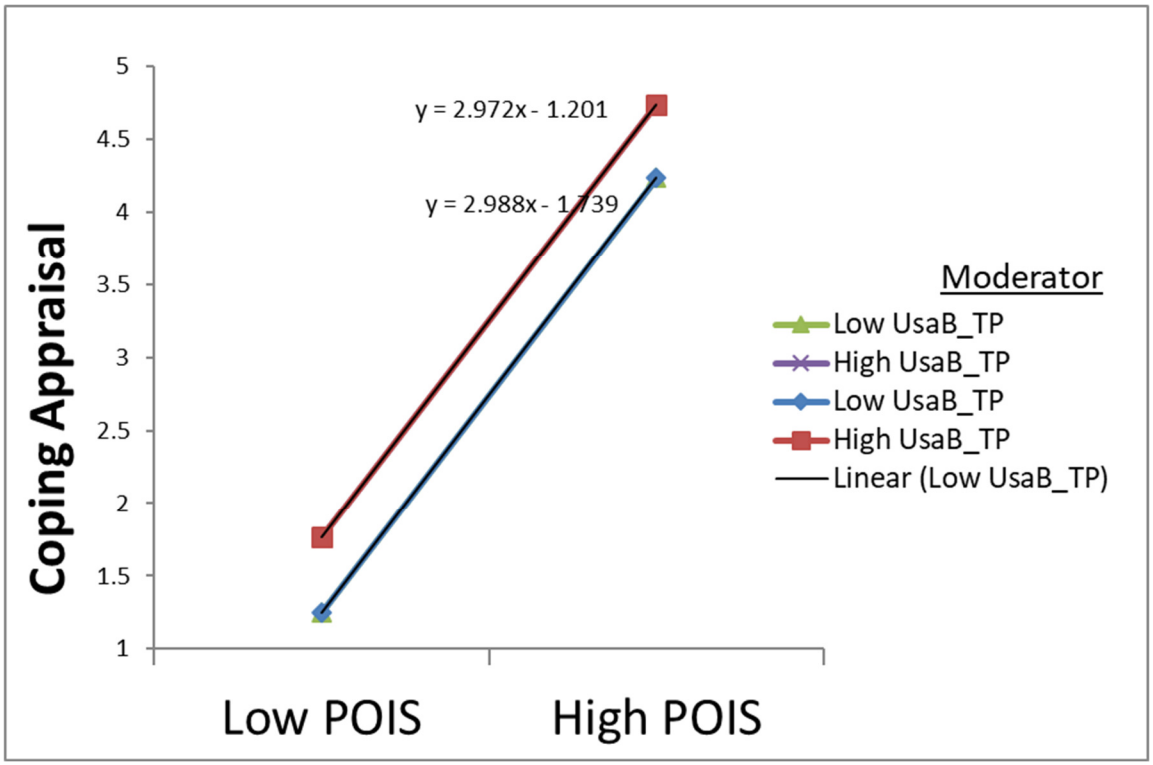


Figure 8 Interaction plot showing effect of Tailored policy on users' perception of information security and Coping appraisal

Interaction summary

Independent variable:	POIS
Moderator:	UsaB_TP
Dependent variable	Coping Appraisal

Unstandardized Regression Coefficients:

Independent variable:	1.490
Moderator:	0.257

Interaction: -0.004

Outcome: Use of a tailored policy dampens the positive relationship between perception of information security and coping appraisal.

H6d: Usability of a tailored policy strengthens the positive relationship between POOI on CA.

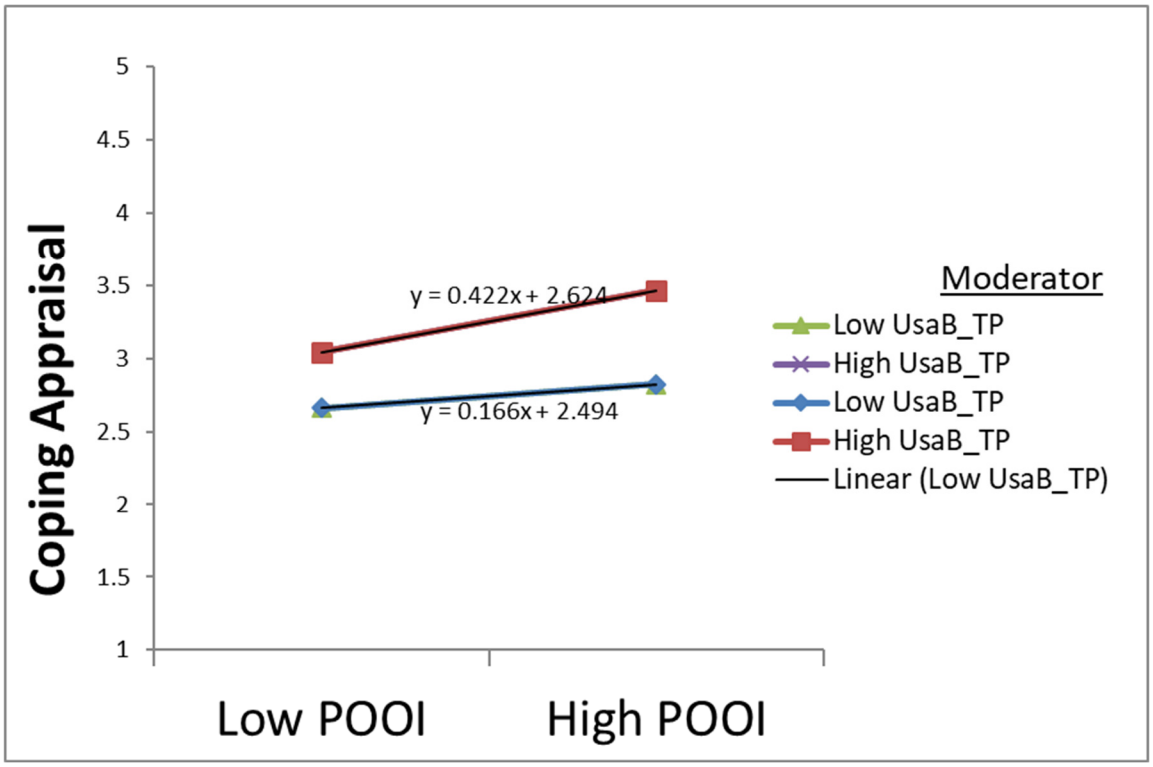


Figure 9 Interaction plot showing effect of Tailored policy on users' perception of organisational interventions and Coping appraisal

Interaction summary

Independent variable: POOI

Moderator: UsaB_TP

Dependent variable Coping Appraisal

Unstandardized Regression Coefficients:

Independent variable: 0.147

Moderator: 0.257

Interaction: 0.064

Outcome: use of a tailored policy strengthens the positive relationship between perception of organisational interventions and coping appraisal.

H6e: Usability of a tailored policy strengthens the positive relationship between POIS on Behavioural intent.

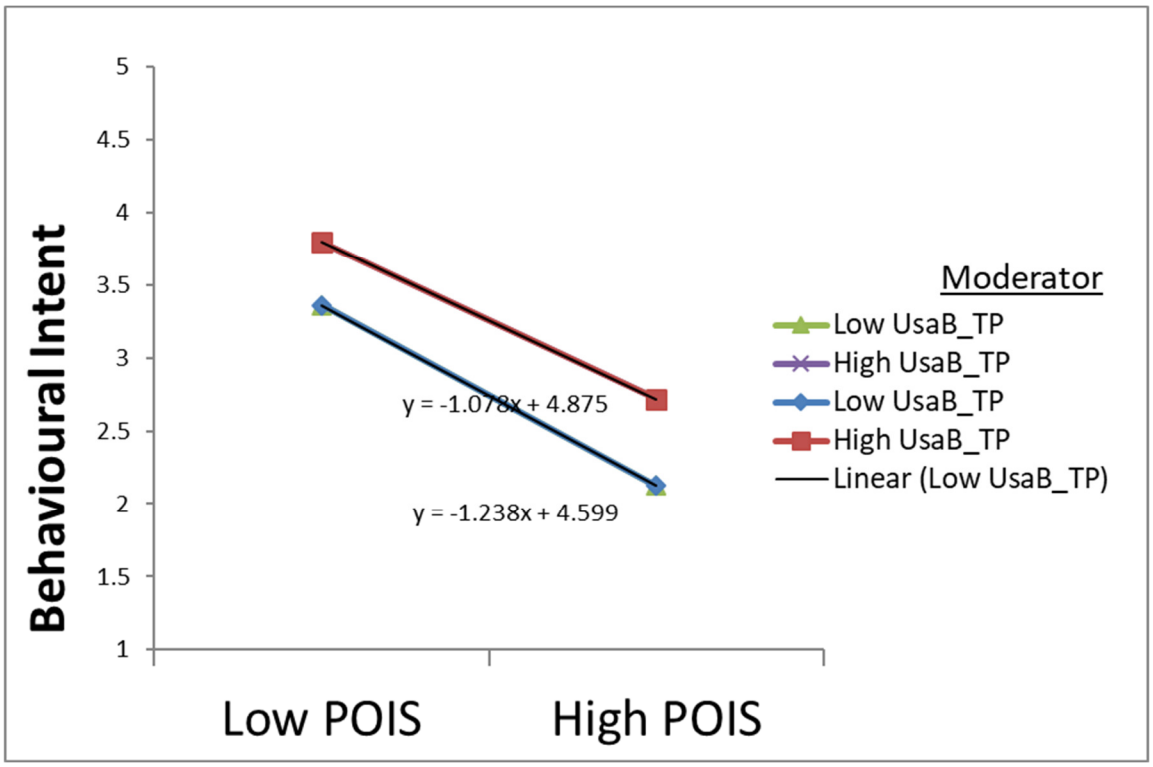


Figure 10 Interaction plot showing effect of Tailored policy on users' perception of information security and Behavioural Intent

Interaction summary

Independent variable: POIS

Moderator: UsaB_TP

Dependent variable Behavioural Intent

Unstandardized Regression Coefficients:

Independent variable: -0.579

Moderator: 0.258

Interaction: 0.040

Outcome: Use of a tailored policy dampens the negative relationship between perception of information security and behavioural intent.

H6f: Usability of a tailored policy strengthens the positive relationship between POOI on Behavioural intent.

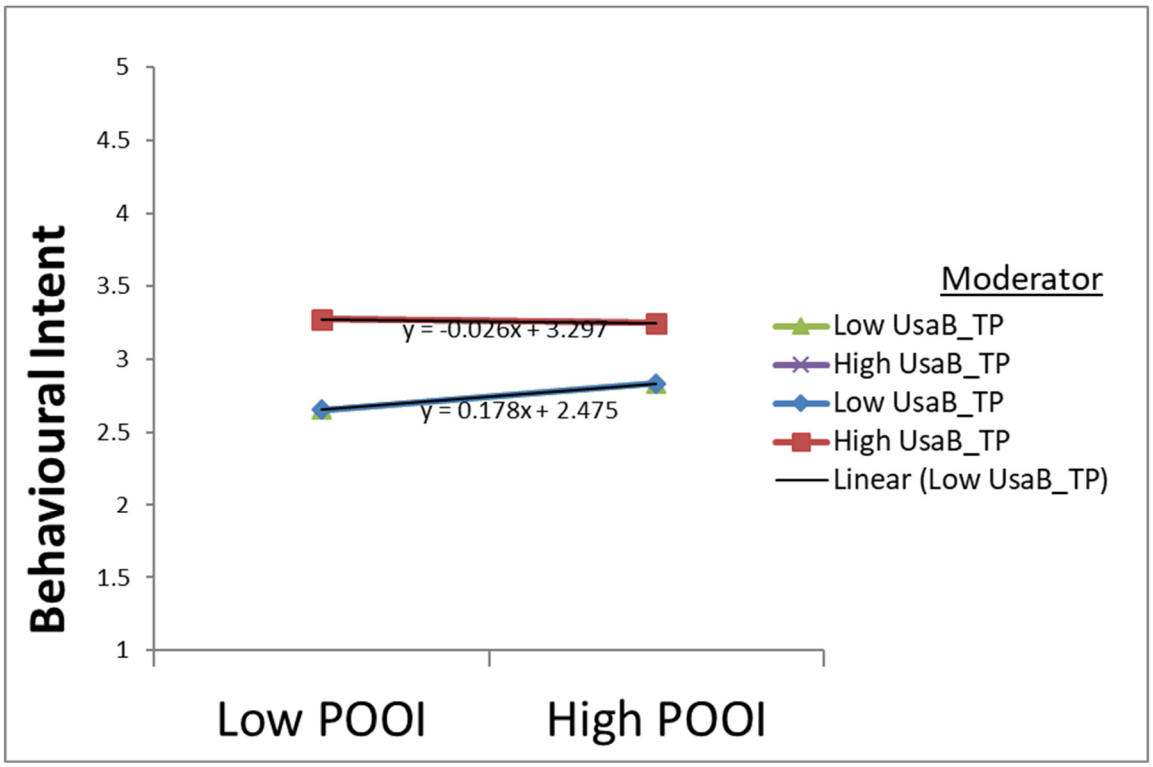


Figure 11 Interaction plot showing effect of Tailored policy on users' perception of organisational interventions and behavioural intent

Interaction summary

Independent variable: POOI

Moderator:	UsaB_TP
Dependent variable	Behavioural Intent

Unstandardized Regression Coefficients:

Independent variable:	0.038
Moderator:	0.258
Interaction:	-0.051

Outcome: Use of a tailored policy dampens the positive relationship between perception of organisational interventions and behavioural intent.

H6g: Usability of a tailored policy strengthens the positive relationship between POIS on Actual Behaviour.

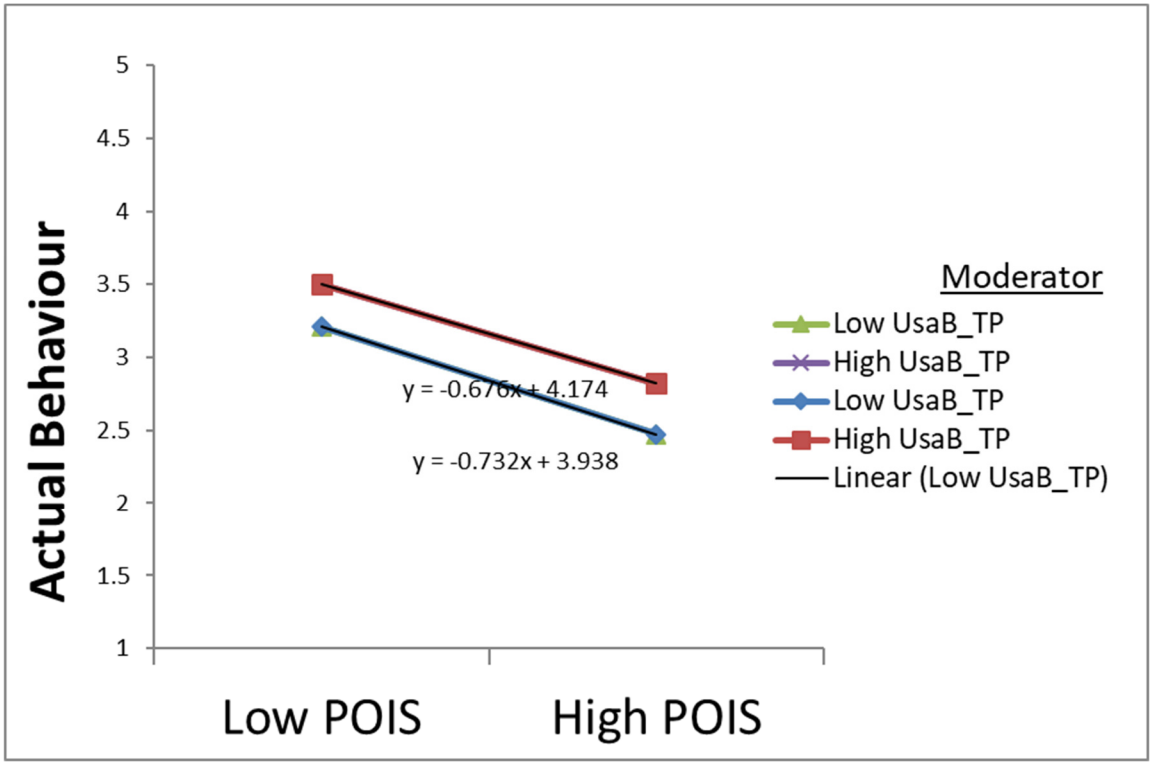


Figure 12 Interaction plot showing effect of Tailored policy on users' perception of information security and actual behaviour

Interaction summary

Independent variable:	POIS
Moderator:	UsaB_TP
Dependent variable	Actual Behaviour

Unstandardized Regression Coefficients:

Independent variable:	-0.352
Moderator:	0.160
Interaction:	0.014

Outcome: use of a tailored policy dampens the negative relationship between perception of information security and actual behaviour.

H6h: Usability of a tailored policy strengthens the positive relationship between POOI on Actual Behaviour.

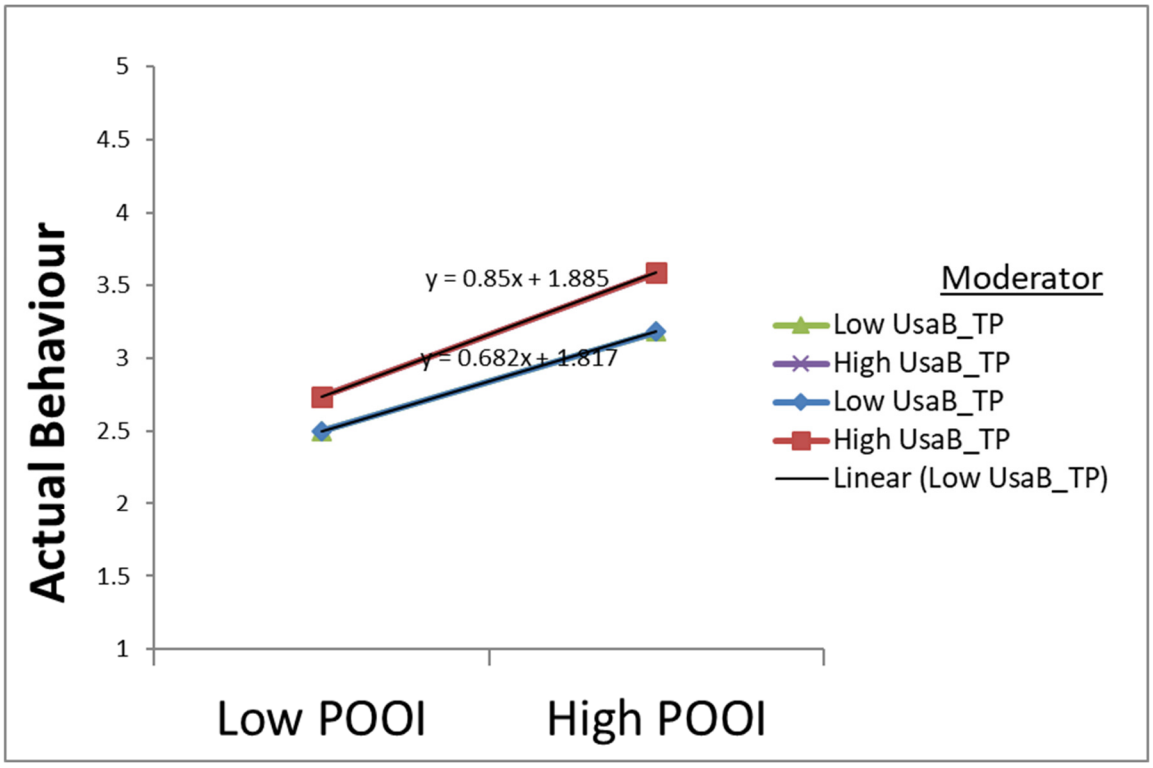


Figure 13 Interaction plot showing effect of Tailored policy on users' perception of organisational interventions and actual behaviour

Interaction summary

Independent variable:	POOI
Moderator:	UsaB_TP
Dependent variable	Actual Behaviour

Unstandardized Regression Coefficients:

Independent variable:	0.383
Moderator:	0.160
Interaction:	0.042

Outcome: Use of a tailored policy strengthens the positive relationship between perception of organisational interventions and actual behaviour.

H6i: Usability of a tailored policy strengthens the positive relationship between Threat appraisal on Behavioural intent.

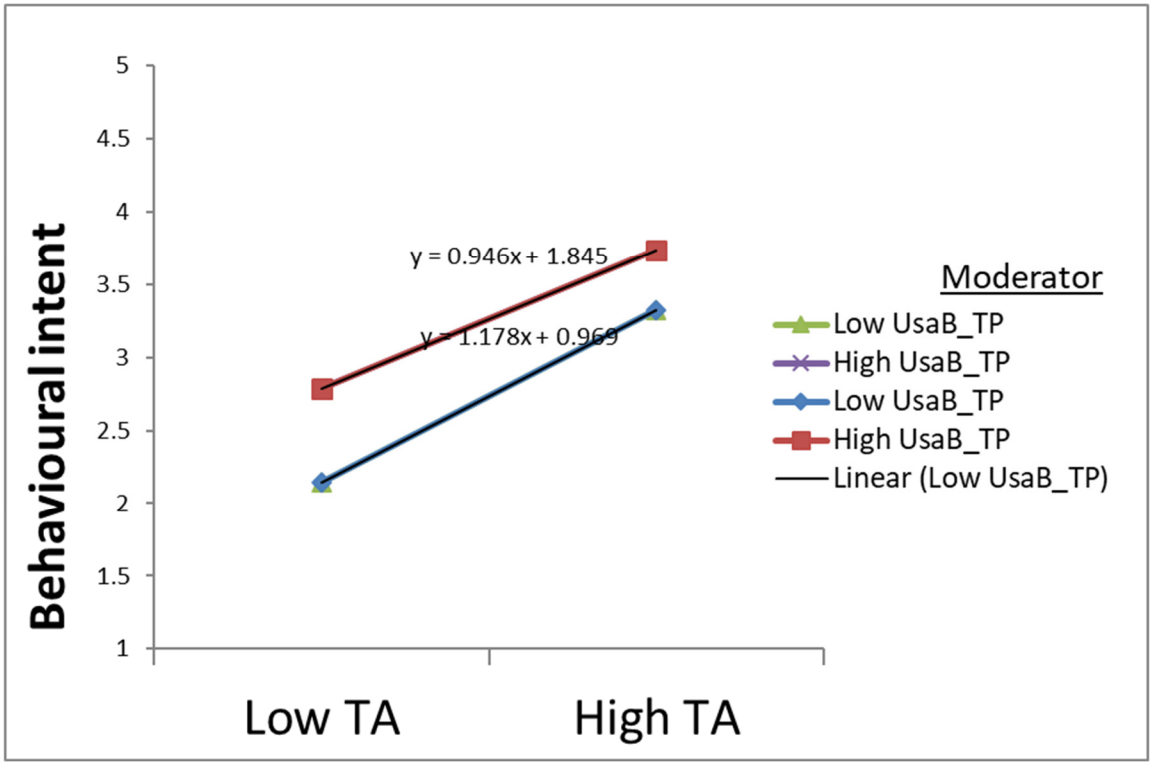


Figure 14 Interaction plot showing effect of Tailored policy on users' perception of Threat appraisal and behavioural intent

Interaction summary

Independent variable:	TA
Moderator:	UsaB_TP
Dependent variable	Behavioural intent

Unstandardized Regression Coefficients:

Independent variable:	0.531
Moderator:	0.264
Interaction:	-0.058

Outcome: Use of a tailored policy dampens the positive relationship between threat appraisal and behavioural intent

H6j: Usability of a tailored policy strengthens the positive relationship between CA on Behavioural intent.

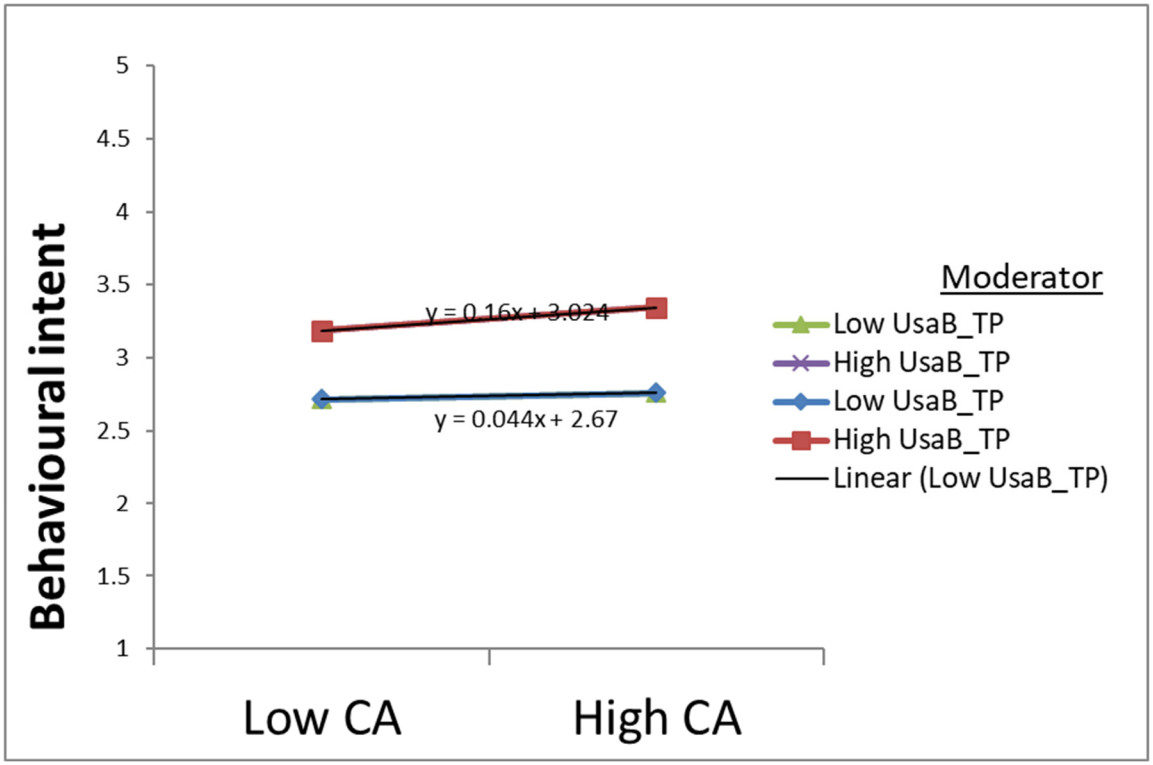


Figure 15 Interaction plot showing effect of Tailored policy on users' perception of coping appraisal and behavioural intent

Interaction summary

Independent variable:	CA
Moderator:	UsaB_TP
Dependent variable	Behavioural intent

Unstandardized Regression Coefficients:

Independent variable:	0.051

Moderator: 0.264

Interaction: 0.029

Outcome: Use of a tailored policy strengthens positive the relationship between coping appraisal and behavioural intent.

H6k: Usability of a tailored policy dampens the negative relationship between Threat appraisal on Actual Behaviour.

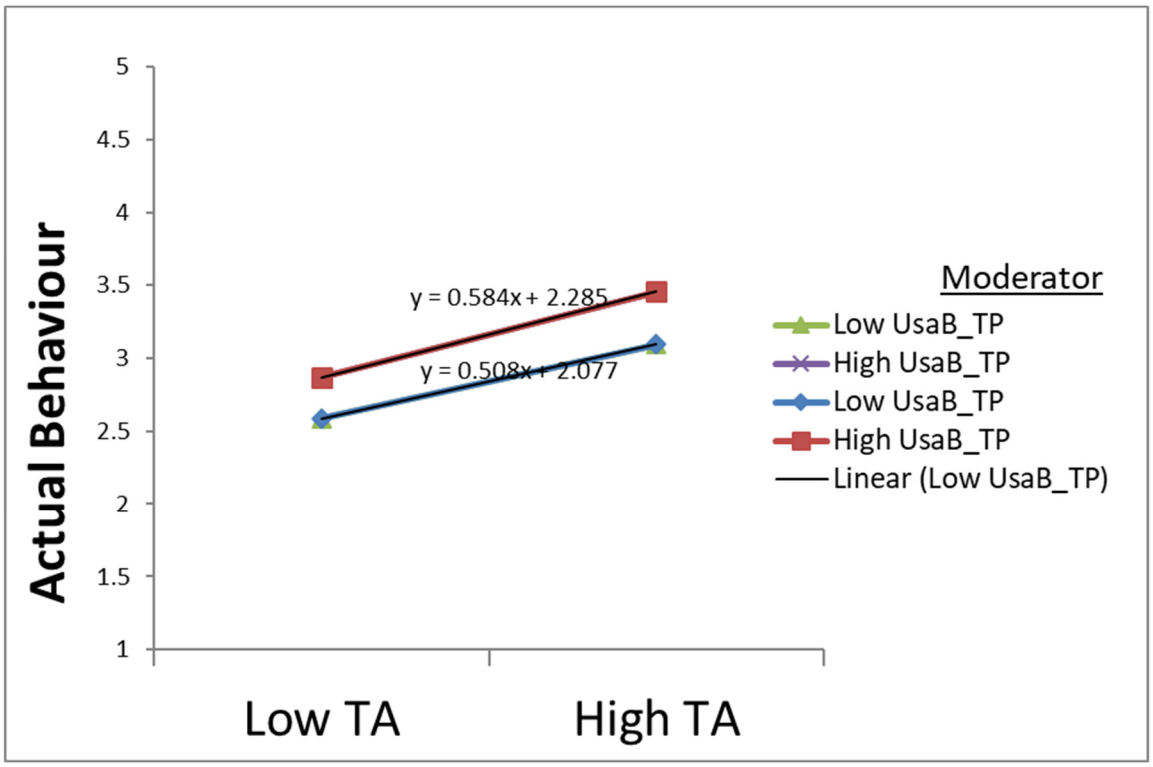


Figure 16 Interaction plot showing effect of Tailored policy on users' perception of threat appraisal and actual behaviour

Interaction summary

Independent variable: TA

Moderator: UsaB_TP

Dependent variable Actual Behaviour

Unstandardized Regression Coefficients:

Independent variable: 0.273

Moderator: 0.161

Interaction: 0.019

Outcome: Use of a tailored policy strengthens the positive relationship between threat appraisal and actual behaviour.

H6l: Usability of a tailored policy strengthens the positive relationship between Coping appraisal on Actual Behaviour.

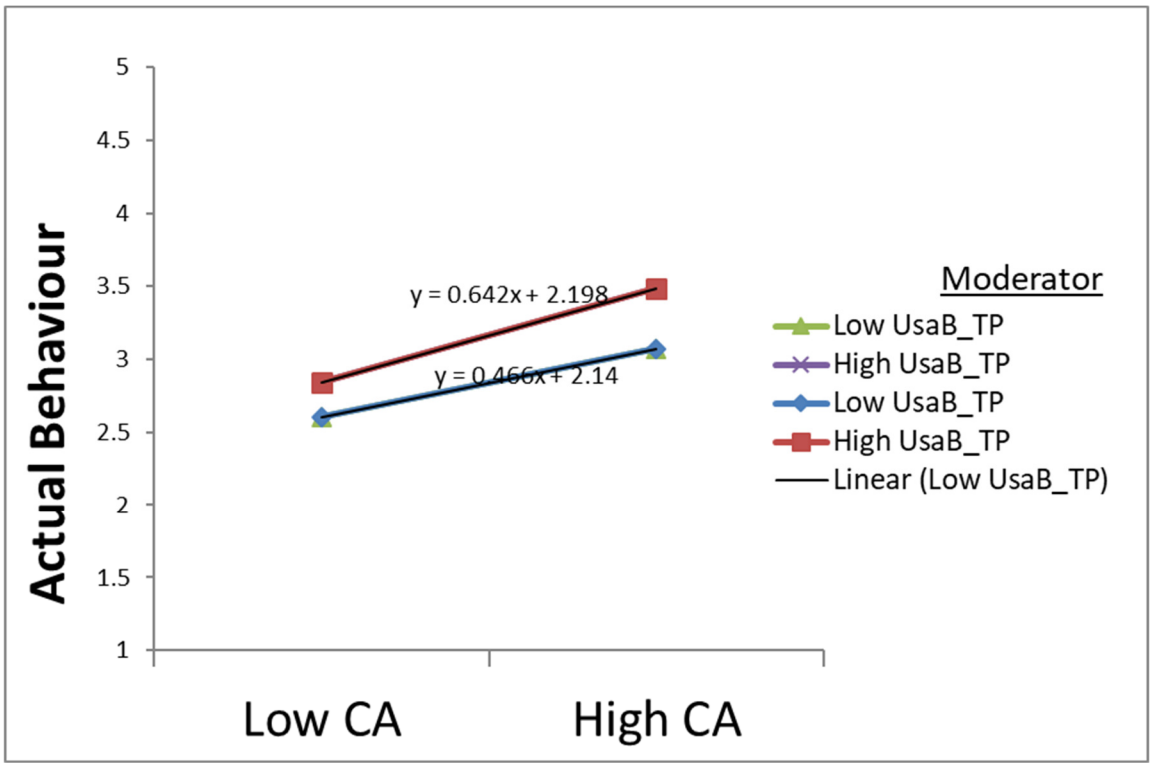


Figure 17 Interaction plot showing effect of Tailored policy on users' perception of coping appraisal and actual behaviour

Interaction summary

Independent variable: CA

Moderator:	UsaB_TP
Dependent variable	Actual Behaviour
Unstandardized Regression Coefficients:	
Independent variable:	0.277
Moderator:	0.161
Interaction:	0.044

Outcome: use of a tailored policy strengthens the positive relationship between Coping Appraisal and Actual behaviour.

5.6 Discussion

This study empirically investigates the factors that could improve compliance of organisational information security policies. It examines users' perceptions to find a solution that works for both policymakers and employees. This study also examines a novel method of improving compliance viz a tailored policy. It studies the moderation effects of a tailored policies on the various relationships between the constructs used in this model. The results of the data analysis are used to develop a generalised model of enhanced PMT which works for both policymakers and employees from different organisations within different industries with varying levels or their organisational security. Employee's compliance intention is significantly affected by their threat appraisal which consists of perceived vulnerability and perceived severity and their coping appraisal which consists of self-efficacy, response cost and response efficacy. We found that users perceptions of information security and organisational interventions have insignificant direct effect on their intent to behave. However, their perceptions of information security and organisational interventions have a positive and significant effect on their perceptions of threat appraisal and coping appraisal, therefore have a strong indirect effect on their behavioural intent. Though perception of information security doesn't have a significant effect on their actual behaviour it was found that their

perception of their organisational interventions had a strong effect on their actual behaviour. This study also found that use of a tailored policy improves their knowledge of information security and their organisational interventions by increasing their understanding of threats and associated coping mechanisms. This comes with a surprising finding, as their understanding of threats increases their intent to behave securely should also increase. However, if a tailored policy is used for this purpose even if their intention to behave securely decreases, their actual security behaviour improves. This implies that a tailored policy should actively enable employees to behave securely as management's intentions are made clear from the policy.

Constructs		Relationship	Significance	Effect of tailored policy on this relationship
POIS	TA	+ ve	Significant	dampens
POOI	TA	+ ve	Significant	strengthens
POIS	CA	+ ve	Significant	dampens
POOI	CA	+ ve	Significant	strengthens
POIS	BI	- ve	Non-Significant	dampens
POOI	BI	+ ve	Non-Significant	dampens
POIS	AB	- ve	Non-Significant	dampens
POOI	AB	+ ve	Significant	dampens
TA	BI	+ ve	Significant	dampens
CA	BI	+ ve	Significant	strengthens
TA	AB	+ ve	Significant	strengthens
CA	AB	+ ve	Significant	strengthens

Table 31 SEM Summary, POIS - perception of information security, POOI - Perception of orgaisational interventions, TA - Threat appraisal, CA - Coping appraisal, BI - Behavioural intent, AB - Actual behaviour

6 CHAPTER 6 DISCUSSION AND CONCLUSION

6.1 Introduction

You cannot talk about information security, without talking about confidentiality integrity and availability. These are the three pillars information security was built on. Also called at the CIA triad (Wilson et al., 2009), these three are the core principles all information systems are based on. Confidentiality emphasises on ensuring that the no information is accessible to persons who are not authorised to see it. Integrity ensures, that no information is modified by any person, who is not authorised. While availability ensures that all information is available to those who are authorised to use it.

With role of computing becoming ubiquitous (Von Solms & Van Niekerk, 2013), information has gained monitory value and therefore protecting it has become ever so important. Information security has three main aspects which most people confuse with. Information security itself, Cyber security, and data protection. Information security is protecting all types of information. Be it in digital form or physical (paper). Cyber security and data protection are subsets of information security dealing with different aspects of information. Cyber security only deals with digital information. This could be information on your computer, or on the internet. Data protection deals with keeping personal identifying information secure.

The process of designing and implementing information security within an organisation is called information security governance. There are various guidelines and industry standards which the organisations must strictly adhere to, or they could face legal sanctions. The process of information security governance is carried out through a process called information security management systems. To implement information security organisations, create security policies to inform all employees, procedures on how to deal with a security breach and control to ensure those breaches do not occur.

There is a magnitude of technical controls which do more than half the job of securing the organisation. The rest falls on the employees. Employees are considered the weakest link in the security chain of the organisation; this is primarily because they are the easiest to compromise. This could be due to external motivators, such as become a victim of social engineering or

personal emotional motivators, such a disgruntled employee. It is most often the case that an employee gets blamed for a security breach.

6.2 Research questions and research objectives

A lot of research has been conducted to reinforce the notion that employees are not to be blamed (Adams & Sasse, 1999). Security researchers feel that most of the security mechanisms are not user centric (Adams & Sasse, 1999)(Albrechtsen, 2007) and the upper management should be responsible implementing security. While other researchers believe management has a negative perception of employees and cannot trust employee behaviour and hence they should not be blamed either (Reinfelder et al., 2019).

The purpose of this PhD study is to attempt to address this gap between the policymakers and employees. Hence for the purpose of understanding their individual story the following research questions were formulated.

1. How do policymakers and employees perceive organisational security policy? (Chapter 3)
2. Are there any differences in their perceptions? (Chapter 3 and 4)
3. Could they lead to employee non-compliant security behaviour? (Chapter 3)
4. How can compliance with the security policy be improved? (Chapter 3 and 5)
5. Can we find solution that works with both policymakers and employees? (Chapter 3 and 5)
6. What would make an effective Tailored policy? (Chapter 5)
7. Can we develop a generalised model of enhanced PMT in relation to security compliance? (chapter 5)
8. Can this model be tested for its application to both policymakers and employees? (Chapter 5)
9. Is this model a generalised model for organisations with varying security levels? (Low, medium and high security organisations) (Chapter 5)
10. Are there any moderation effects of a Tailored policy on the relationships between the constructs of PMT? (Chapter 5)
11. Can a tailored policy be used to improve organisational security behaviour? (Chapter 5)

The key objective of any research is to find answers to questions through scientific procedures (C.R.Kothari, 2004). Depending on the research study, their objective can vary. They can be exploratory or formulative, they could be descriptive or diagnostic. Our key objective was to address the issue of noncompliance of security policies and to find an immediate method to implement. For this we first had to explore the current situation and understand how the organisational security policies and procedures a currently perceived by both those who make the policies (policymakers) and those who are expected to follow these policies (employees). And as such find a method which can be approved by both groups. Keeping this in mind the following objectives were formulated.

- Identify the key differences in perceptions of policymakers and employees.
- Developing a generalised model of enhanced PMT in relation to security compliance
- Examine the validity of this model for different groups viz policymakers and employees, for different industries and for varying levels of organisational security
- Explore the effects of a tailored policy on this model to facilitate improvement in the organisational security behaviour.

6.3 Identify the key differences in perceptions of policymakers and employees.

The first research question is aimed to understand and establish a baseline for achieving this objective. Only after understanding how the two key groups who are responsible for effective compliance of an organisational security policy, perceive their organisational security policies, we can then identify the key differences in their perceptions. Study 1 and study 2 was used to achieve this objective. Both studies to answer research questions 1 and 2. Study 1 answers the research question 3. Both studies are once again used to identify the solution to answer the research questions 4 and 5. However the answer to these questions is provided through the analysis of findings from study 2 in chapter 5.

6.3.1 Study 1 (Chapter 3)

To comply with the policy, one must first read and understand the policy. One must understand what behaviour - that which is mentioned in the policy, is expected of the individual to facilitate good organisational security behaviour. In chapter 2 we established that the employees have not clearly understood or misunderstood information security and/or its pertaining policies, the

information integrated and stored by the employees could be a misinterpretation of info sec and thus lead to bad or unacceptable info sec behaviour. Since the employees lack a clear understanding of info sec, they are themselves not aware that such behaviour is unacceptable. So, if the users do not understand information security, they will by default not know how to behave with information securely. By applying Leach's framework for how information about security behaviour is acquired, semi structures open-ended interview questions were developed for this purpose. Responses reflecting the participants understanding of Information security itself, their perception of their organisational interventions, commitment towards and from their organisation, and quality of the policy document, was analysed and reported in chapter 3. From this thematic analysis ten themes emerged pertinent to how compliance with organisational information security policy compliance behaviour was influenced.

This study was conducted within education providing institutes, so it is obvious that majority of the staff hired were teaching or research staff. They knew that this information needed to be protected, however they didn't have a clear understanding of why this information was to be protected or what other information needed to be protected (Albrechtsen, 2007). It seemed that they were simply following their job description as to what was expected from them by their managers in terms of their daily job tasks. The findings clearly display the lacking state of awareness and accountability of and with information security within employees and employee's perception about information security within an educational environment such as universities. The policymakers confirmed the existence of information security awareness programs and online training programs but added they were not mandatory to all staff, particularly to research and teaching staff. The employees on the other were unable to easily access this information confirming visibility and quality of such organisational interventions to be an issue. The quality of security policy document which is one of the key interventions that informs all employees about their organisational expectations with regards to security compliance, was found to be ineffective in terms of its length, the language used within these documents and its content, as most participants found the information not relevant to their job role thereby causing more of a hindrance. These themes were consistent with the extant literature along with other themes such as the need for feedback and communication.

The key finding from this study was a novel concept of a tailored policy. Participants felt if the policy was tailored to their job role it would be easy to follow as different departments have different ways of functioning. All participants expressed this was something they would be

encouraged to comply with. They expected the policies to be short with fewer instructions– one or two pages and the information within the policies should be relevant to them. Policymakers agreed that though this would be difficult and time consuming it would certainly be possible to develop and implement such policies.

6.3.2 Study 2 Cross Tabulation Analysis (Chapter 4)

The findings from previous study led to the beginnings of the thematic framework that was developed for the purpose of this study. The previous study was carried out in a low security organisational environment and with a small number of participants. Therefore, there was a need to validate these findings on a larger scale and incorporate participants from medium and high security organisations. We grouped the findings from the previous studies in to constructs such as Perception of information security, Perception of organisational interventions, perception of organisational citizenship and Quality of Policy documents. For this study a survey instrument was created and administered via online survey tool, Qualtrics. Qualtrics has been recommended (Barnhoorn, Haasnoot, Bocanegra, & van Steenbergen, 2014) as a very good online survey tool. Researchers (Benton, Pappas, & Pappas, 2011) (Boas, Christenson, & Glick, 2018) often use Qualtrics to find participants from all across the world in order get a diversified opinion. This study aimed to find users primarily from across UK. As in the previous study one, this time it focussed on finding participants from low medium and high security organisations. Participation in policy making was also used as one of the selection panel for the survey. This was done to differentiate between policymakers and employees and capture their separate opinions. Sector to which the organisation belonged was not used as a panel, as we hoped to find participants from various organisations from diverse sectors. This was so that we can generalise the opinions and not restrict us to a particular sector or organisation. Cross tabulation analysis was used to highlight key differences in perceptions of policymakers and employees and providing statistical data as evidence.

As discussed in chapter 1, information security is a very vast subject area. It would be unfair to expect everyone to have all or even considerable amount of knowledge about information security. It was evident from study 1 that not all participants had enough knowledge as is. Though it is difficult to define enough knowledge, for this research, it is considered that they should at least have a basic understanding of the differences between information security, cyber security, data protection and have some understanding of the risks associated with non-compliance of security

policies. It was noted that 30% of policymakers displayed poor understanding of information security. Ideally this should be closer to 100% if organisations are to implement stronger security measures. On the other hand, for employees there was even split between good and poor understanding of information security. This was primarily because employees who claimed to have average to expert knowledge of IT systems displayed better understanding security. Both policymakers and employees showed good appreciation of non-compliance and understanding of threats that affected their organisations. Policymakers showed good awareness of present interventions, in the form of awareness programs, training programs, and security policy. They also claimed that there was communication from the organisation to make employees aware of such interventions. However about 40% of participant employees were unaware of these interventions. It was surprising to note that employees showed higher levels of commitment towards their organisation than policymakers. It was mutually agreed by both groups that the quality of the policy documents did in fact needed work to make them more effective.

Study 2 provided a new instrument to measure perceptions of participants with respect to their understanding of security procedures in their own workplace. The validation of this instrument is provided in chapter 5. Though the instrument was not completely used for the development of the framework presented in chapter 5, it was validated for specific measurement of participants perceptions of their organisational information security policies and procedures. The study also validated the instrument for the measurement of participants perceptions of organisational commitment from the organisation towards employees and from employees towards their respective organisations. These are some of the key contributions from this study in terms of an instrument. More contributions are mentioned in the following sections.

6.4 Developing a generalised model of enhanced PMT in relation to security compliance

Theory of planned behaviour (TPB) which is one of the most widely used theories in security research for predicting human behaviour, could not be used, as this theory relies on the primary assumption that the behaviour of an individual can be predicted if that individual completely understands the said behaviour. We know that some employees understand security behaviour thereby practise something called as shadow security(Adams & Sasse, 1999), however it is also established in chapter 2 that not all employees understand security behaviour as such this theory cannot be used for a generalised model. Protection Motivation Theory was the next best to study security behaviours given its two key constructs of threat appraisal and coping appraisal.

Therefore, the constructs previous developed form study 1 were incorporated with the constructs from PMT to develop this generalised model of enhanced PMT particularly focussing on compliance of organisational security policies. This section answers research question 7.

6.4.1 Study 2 Structural Equation Model (Chapter 5)

Chin (Chin, 1998) believes Structural equation modelling provides techniques to perform covariance based and component based analysis. He adds, SEM based procedures have various advantages over previous techniques, like principal component analysis, factor analysis, discriminant analysis, and multiple regressions. This is because with SEM you can model relationship among multiple predictors (Chin, 1998), construct unobservable latent variables (LV's), model errors in measurements for observed variables and statistically test established theories. Running through EFA it was found that the constructs, Perception of organisational citizenship and Quality of policy documents did not covariate with the constructs of PMT. Even though individually they were giving a strong Cronbach's alpha over 0.7. they did not fit with the model. The figure below shows the conceptual model obtained by SEM.

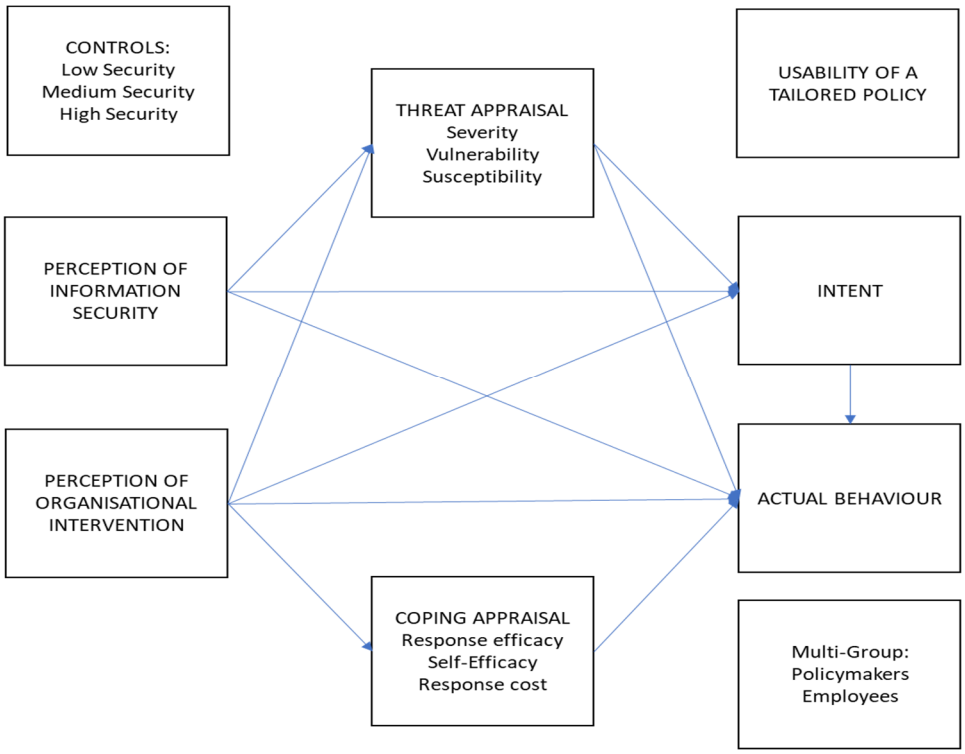


Figure 18 Conceptual Model developed in SEM

The key contributions from this study are that both Perceptions of information security and Perceptions of organisational interventions have a positive and significant effect core constructs of PMT viz Threat appraisal and coping appraisal. We know from existing literature on PMT that threat appraisal and coping appraisal have a positive and significant effect on behavioural intent. This was once again validated by this model. Even though the direct effect of Perception of information security is negative it was non-significant. This means that the knowledge of information security can have a positive effect on the behavioural intent of employees only if that information pertains to the threats associated with the job and that it provides appropriate coping mechanisms against these threats. Similarly, the direct effect of employee's perception of organisational interventions was non-significant however it was a positive effect. This implies that if organisational interventions are tailored around specific threats and respective coping mechanisms their indirect effect on behavioural intent are expected to have positive results. This can be posited because the model validated that there is a significant and positive effect of perceptions of organisational interventions, threat appraisal and coping appraisal on actual behaviour.

6.5 Examine the validity of this model for different groups viz policymakers and employees, for different industries and for varying levels of organisational security

This part of the study addresses research questions 8 and 9. To achieve this objective, the survey instrument was administered via an online tool Qualtrics. At the end of the survey a total of 624 samples were collected. Out of which only 513 complete surveys were selected. The primary selection criteria for participants were that they were employed full time and over the age of 18 years. The second important criteria of this research is to understand the differences in perceptions of policymakers and employees. Hence for the purpose the classification of participants is based on their participation in their own organisational policymaking, including designing, developing and/or implementing their organisational security policies Classification of participants was also based on the departments they worked in. These departments were selected for classifications mainly because in majority of organisations and from information security perspective, these departments are the ones which often deal with sensitive information viz HR, Finance, IT, Management and Others. For the classification 'Other' departments, participants specified accounts, administration, customer service, data management, education, sales, secretary, supervisor, teaching. Participants perceptions about their organisation's overall security

procedures in terms of their organisation's effort in securing company assets was used to classify the security levels within the organisation. The analysis was done using multi group analysis in SEM. With the groups being policymakers and employees.

6.5.1 Study 2 SEM – Multi group Analysis and Control Group (Chapter 5)

The analysis was done using multi group analysis in SEM. With the groups being policymakers and employees. This involves verifying the model by checking the regression weights on each pathway between constructs. This means the model was checked using responses from the 193 policymakers and 320 employees separately. The model was fit for both groups however there was no significant difference in beta weights for the pathways. This validates that the model is fit for both policymakers and employees however their participation in policymaking does not have a significant effect on the strength of the pathways.

6.6 Explore the effects of a tailored policy on this model to facilitate improvement in the organisational security behaviour.

This part of the study address research questions 4, 5, 6, 10, and 11. In study 1 a novel concept was suggested by participants. In which they suggested that if a shorter policy with a few instructions which were relevant to their job roles was provided, it could be easy to follow it. It was also agreed upon by policymakers interviewed in this study, they however expressed concerns about additional work and management of numerous smaller documents. Following up on this this was further explored in study 2. Usability of a tailored policy is measured in terms of its effectiveness, efficiency, and employee satisfaction (Chapter 4). Further to this it was also necessary to find if the tailored policy will have any effect on end-user behaviour. For this the moderation effect of a tailored policy on each of the relationships mentioned in our model was measured. It was found that the tailored policy in fact did moderate the relationships to provide a theoretical proof that end-user behaviour can be improved (Chapter 5).

6.6.1 Study 2 SEM – Moderation Effect of Tailored policy (Chapter 5)

To achieve the objective 6.6, the moderation effect of a tailored policy on each of the constructs in the proposed model and their pathways was studied. It was noted that a tailored policy dampens the positive relationship between perception of information security and threat appraisal and coping appraisal. This is expected as your knowledge of information security, threats and their

respective coping mechanisms are associated with your job role, as provided in the tailored policy it might make you oblivious to other threats and how to cope with them. A typical example would be threat of social engineering. The use of a tailored policy strengthens the positive relationship between perception of organisational interventions and threat appraisal and coping appraisal. Meaning a tailored policy informs all employees about their organisations expectations from them in the event of a threat and how to cope with such said threats. We also noted that use of a tailored policy dampens the positive relationship between threat appraisal and behavioural intent. This is expected as once you know what threats are and which threats affect your job role, this might make you aware of the susceptibility of a threat happening. This may keep you alert if there is a high likelihood of a threat. However, if there is a reduced likelihood of a threat the employees might get complacent. But this is where the key benefit of having a tailored policy comes in. The results showed that the use of a tailored policy strengthens the positive relationship of treat appraisal and coping appraisal with employee's actual behaviour, implying that even if there is a reduced intent, it does not affect the actual security behaviour of the employee rather strengthens it.

6.7 What makes an effective tailored policy?

After studying the effects of a tailored policy on the constructs and relationships of the model a general idea of an effective tailored policy can be summarised. A tailored policy should provide knowledge about information security keeping in mind not to overwhelm the employees. A tailored policy will make the employees aware of threats associated with an employee's job role and the coping mechanisms put in place, including support from their organisation in terms of awareness programmes, training programmes, communication, and feedback procedures. While developing such policies it should be kept in mind to keep the policy easy to read understand and follow. Participants believed that a tailored policy will be tailored to their job role and will tell them exactly what they need to do. If such a policy is developed, they firmly believe, that a tailored policy can be regularly followed and will improve policy compliance as the employees will be more inclined and happier to follow this policy.

6.8 Implications

As described in chapter 2 majority of the research is conducted within the field of information security is either from management perspective or employee perspective. Research areas are

further broken down to understand underlying parameters of each perspective. Though the existing literature contributes extensively to the overall subject of information security and human security behaviour, thereby increasing our understanding of the deeper meaning behind every action, it does not provide an immediate solution that can built on. There was a need for a study that incorporates perspectives of both policymakers and employee and addresses this gap between their perceptions of security in a single study. This thesis has designed and theoretically tested an immediate solution to a real-life situation of noncompliance of security policies. The result of this research is a new type of intervention that can be used alongside previous interventions such as awareness programmes, training programmes and even their comprehensive security policies. This research therefore has direct implications to real life situations and can be utilised by policymakers within any industry or within any organisation with any level of security. This research provides the policymakers a starting point for designing developing and implementing effective security policies. The survey instrument was proven to have excellent reliability for all individual constructs and as such proves to be an effective tool to measure progress made within each areas or information security governance. This can be used to measure if each implemented intervention is effective or not.

6.9 Limitations

The first qualitative study was done only in low security organisations. As such the views and opinions expressed in the interviews were from employees from such organisations. It would be beneficial to conduct qualitative interviews within medium and high security organisations to assess if the views and opinions of their employees are similar to the ones from low security organisations. Considering the sensitivity of the research it was however not possible to gain access to said medium and high security organisations. Secondly, the participants in the qualitative study were all from different organisations. So even though this research addresses the differences in perceptions of policymakers and employees, it does so between policymakers and employees from different organisations. It would be beneficial to conduct this study within a few organisations involving policymakers and employees from the same organisation. This would help us understand the differences in perceptions of policymakers an employee's operating within the same organisational culture. Attempt was made to address this issue with the second study; however, this limitation persists there as well. Another limitation of this study is the concept of a tailored policy. Though item statements were created to measure usability of a tailored policy, the statements provide as a mere general guideline on what to expect from a tailored policy. It is

possible that participants may have had a completely different perception of a tailored policy. All participants for study 1 and 2 are from with England only consequently the generalizability of the model may be limited to this country. Individual or organisations from different countries or with different organisational cultures may have different perceptions.

6.10 Future research

This research also has implications to information systems research. This thesis has developed a theoretical model to identify factors that moderate user's security behaviours with regards to following their organisational security policies. It extends the protection motivation theory in researching security behaviour of employees in terms of compliance with security policies. All constructs were empirically verified for validity and reliability. PMT framework is extensively used in security research as such the results provide empirical evidence that a tailored policy affects each of the relationships. This can used for further research focussing on security behaviour change methodologies. This research relied on self-reporting measures which means individuals report themselves about how things are to be done. This good when capturing perceptions and therefore the survey instrument tools can be used to measure changes in perceptions. The concept of a tailored policy is vast particularly when designing them for individuals or individual departments. As such this will require further research with recruiting organisations, then designing and implementing these tailored policies and then measuring changes in perceptions and or security behaviours. This research provides an excellent basis for longitudinal research to assess whether a tailored policy will work in a real-life scenario.

7 APPENDIX A

7.1 PARTICIPANT INFORMATION SHEET – STUDY ONE

The purpose of this information sheet is to provide you with sufficient information so that you can then give your informed consent. It is thus very important that you read this document carefully, and raise any issues that you do not understand with the investigator. This study has received full ethical approval from the Faculty of Health & Life Sciences Ethics Committee.

1. What is the purpose of the project?

Organisations continue to actively use technology and put in place policies and practices to protect their information technology. Whilst there is a need for more research to investigate the factors that affect employees' ability to behave securely and their attitudes towards security, it is also important to find ways to make the employees aware of the importance of designing effective security policies that can generate good levels of compliance. The purpose of this project is to therefore investigate employees' knowledge, attitudes and behaviour towards information security.

2. Why have I been selected to take part?

It is important that we assess as many people as possible to capture a more generalised opinion and point of view and you have indicated that you are interested in taking part in this study, and that you are employed and an adult aged 18 and above.

3. What will I have to do?

Your participation will start with a briefing session where you will be allowed to ask any questions concerning the project. After signing a consent form, the investigator will ask you to complete a short questionnaire requesting some biographical information (e.g. gender, age etc.). You will then be asked to take part in an interview, led by a researcher, who will ask a few questions around your knowledge and attitudes to your work security policy. E.g. what do you think information security is about or what it should be about? Or how it is relevant to you or your organisation? After you have completed the interview the investigator will give you a debrief sheet explaining

the nature of the research, how you can find out about the results, and how you can withdraw your data if you wish. It is estimated that the total time to complete this study will be approximately 30 - 45 minutes.

4. What are the exclusion criteria (i.e. are there any reasons why I should not take part)?

Participation in this study is entirely voluntary. If you choose to participate, you can withdraw from the study at any time during the interview without giving a reason.

5. How will confidentiality be assured and who will have access to the information that I provide?

All information will be stored anonymously. Any information and data gathered during this research study will only be available to the research team identified in the information sheet. Paper records will be stored in a locked filing cabinet and electronic information (audio/video) will be stored on a password-protected computer. All data will be treated in accordance with the Data Protection Act. Should the research be presented or published in any form, all data will be anonymous (i.e. your personal information or data will not be identifiable). The interview will be transcribed and any identifiable data (e.g., names, locations) will be removed during transcription. Transcripts will be analysed by the researcher.

6. How will my information be stored / used in the future?

All identifiable paper records will be stored in a locked filing cabinet, accessible only to the research team and all electronic information will be stored on a password-protected computer. All of the information you provide will be treated in accordance with the Data Protection Act. This information will be destroyed 7 years after completion of the project. During that time the data may be used by members of the research team only for purposes appropriate to the research question, but at no point will your personal information or data be revealed.

7. How can I withdraw from the project?

The research you will take part in will be most valuable if few people withdraw from it, so please discuss any concerns you might have with the investigators. During the study itself, if you do decide that you do not wish to take any further part then please inform one of the research team member(s) as soon as possible, and they will facilitate your withdrawal and discuss with you how you would like your data to be treated in the future. After you have completed the research you

can still withdraw your data by contacting one of the research team, give them your participant number or if you have lost this give them your name so we can identify and destroy your data (be it in paper or electronic form).

For further information:

For questions regarding the study or protocol or to withdraw data please contact the researcher at amit.naik@northumbria.ac.uk or their supervisor at p.briggs@northumbria.ac.uk

If you have any concerns or worries concerning this research or if you wish to register a complaint, please direct it to the Chair of Ethics, Dr Nick Neave: nick.neave@northumbria.ac.uk

7.2 PARTICIPANT DEBRIEF SHEET – STUDY ONE

PARTICIPANT NUMBER

1. What was the purpose of the project?

Organisations continue to actively use technology and put in place policies and practices to protect their information technology. However, with stronger policies top management ends up enforcing the security policy, thereby making the policy difficult to follow and making the day to day job tasks of employees even more tedious. Or sometime due to a lenient policy the security of the organisation could be compromised. Whilst there is a need for more research to investigate the factors that affect employees' ability to behave securely and their attitudes towards security, it is also important to find ways to make the employees aware of the importance of designing effective security policies that can generate good levels of compliance. The purpose of this project is to therefore investigate employees' knowledge, attitudes and behaviour towards information security.

2. How can I find out about results?

The results will be available from July 2017. If you would like to know about the results, please email the researcher Amit Naik at amit.naik@northumbria.ac.uk at any time and he will happily provide you a general summary of the findings.

3. What will happen to the information that I have provided?

All information and data gathered during this research will be stored in line with the Data Protection Act and will be destroyed 6 months after completion of the project. If the research is published in a scientific journal it may be kept for up to 7 years before being destroyed. During that time the data may be used by members of the research team only for purposes appropriate to the research question, but at no point will your personal information or data be revealed. Insurance companies and employers will not be given any individual's information, samples, or test results, and nor will we allow access to the police, security services, social services, relatives or lawyers, unless forced to do so by the courts.

4. How will results be disseminated?

A generalised report will be written about the findings which will inform the development of a questionnaire. Data might be published in a scientific journal or may be presented at a conference, but the data will be generalised and personal information will not be identifiable.

5. Have I been deceived in any way during the project?

No, you have not been deceived at any point.

6. If I change my mind and wish to withdraw the information I have provided, how do I do this?

Your involvement in research is valuable, so please discuss any concerns you have with the researcher. During the study itself, if you decide that you do not wish to take part then please inform the researcher as soon as possible and they will help your withdrawal and discuss how you would like your data to be treated in the future.

After you have completed the research you can still withdraw your data by contacting the researcher (Amit Naik at amit.naik@northumbria.ac.uk), give your participant number or if you have lost this, your name. If, for any reason, you wish to withdraw your data please contact the researcher within a month of your participation. After this date, it may not be possible to withdraw

your individual data as the results may have been published. As all data is anonymised, your individual data will not be identifiable in any way.

NOTE: *If you have any concerns or worries concerning the way in which this research has been conducted, or if you have requested, but did not receive feedback from the principal investigator concerning the general outcomes of the study within a few weeks after the study has concluded, then please contact Chair of the Ethics Committee, Dr Nick Neave via email at nick.neave@northumbria.ac.uk*

7.3 INFORMED CONSENT

Participant Number	

Please tick where applicable

I have read and understood the Participant Information Sheet. ☐

I have had an opportunity to ask questions and discuss this study and I have received satisfactory answers. ☐

I understand I am free to withdraw from the study at any time, without having to give a reason for withdrawing, and without prejudice. ☐

I agree to take part in this study. ☐

I would like to receive feedback on the overall results of the study at the email address given below. (OPTIONAL) ☐

Email address……

I hereby confirm that I give consent for the following recordings to be made:

Recording	Purpose	Consent
Voice recordings	The interview will be tape recorded for later transcription	

I understand that the transcriptions from the recording(s) may be published in an appropriate journal/textbook or on an appropriate Northumbria University webpage. My name or other personal information will never be associated with the recording(s). I understand that I have the right to withdraw consent at any time prior to publication, but that once the recording(s) are in the public domain there may be no opportunity for the effective withdrawal of consent.

Participant
Name (please print) _____
Signed _____ Date _____

Researcher
Name (please print) Amit Naik
Signed _____ Date _____

7.4 DEMOGRAPHIC QUESTIONAIRE

Participant number:

1. **Please enter your age below:**

2. **Please tick your gender:**

   ☐ **Male**

   ☐ **Female**

3. **Please enter the type of sector your organization is:**

4. **Please enter how many years (or months) have you worked for the organization (approx.)?**

5. **Please enter your job title:**

6. **How many hours a day do you use a computer at work?**

   Less than 1 hour | 1-2 hours | 2-3 hours | 3-4 hours | 4 hours +

7. **Do you store personal data on your work computer (e.g. photos, non-work related files)?**

   ☐ **Yes**

   ☐ **No**

8. **Have you read your organization's information security policy?**

   ☐ **Yes**

   ☐ **No**

9. When was the last time you read your organization's information security policy?

Less than 1 month	1-6 months ago	6-12 months	More than 12 months ago	N/A

10. Do you use your personal devices (e.g. mobile phone, laptop, USB sticks) at work?

- ☐ **Yes**
- ☐ **No**

11. Do you do work-related tasks on your personal devices?

- ☐ **Yes**
- ☐ **No**

7.5 RECRUITMENT EMAIL

Subject: Information Security Compliance: Employee Security Behaviour

Dear ___,

My name is Amit Naik and I am a doctoral researcher from the Psychology and Communication Technology Lab at Northumbria University. Currently, I am conducting research into Information Security Policy Compliance in the workplace. In particular, I am investigating the psychological factors that influence the security behaviour of employees whilst understanding and adhering to the Organisations Information Security Policy; I intend to utilise this knowledge to design a framework in order to design an Information Security Policy which works best with both Policymakers and Employees (Users) there by promoting stronger security compliance behaviour.

I am currently recruiting individuals from organisations to participate in this research. This will involve one-to-one interviews with a sample of employees and a report can be produced to give an indication of employee's security behaviour within your workplace.

For an informal discussion about participating in this research, please contact me by email at amit.naik@northumbria.ac.uk or by phone (0191 2273716).

I look forward to hearing from you.

Kind Regards

Amit Naik

This study has received full ethical approval from the Faculty of Health and Life Sciences ethics board at Northumbria University.

7.6 INTERVIEW SCHEDULE

Greeting, and explain what is to follow.

Let the participant read the participant information sheet.

Tell the participant if there are any questions they should feel free to ask.

Get the consent form signed.

Start recording and begin interview.

A. Understanding Information security
    1. What do you think information security is about?
    2. Do you think it is necessary or important to your work place?
    3. Do you think it is important to you or your job role?
    4. How would you classify the information you work with? Sensitive, personal, not very important?
    5. Have you experienced any security events?
    6. How do you know what you are supposed to do in case of a security event? Has anyone told you what to do? Have you asked somebody? Or you do something yourself?
B. Organisational interventions
    1. Has your organisation provided you any awareness programs? What kind of awareness programs?

2. Has your organisation provided you with any training programs? What kind of training programs?
3. What kind of support or information do you get from your organisation with regards to information security?
4. How would you know about the security procedures put in place? From colleagues, your managers, or do you find it yourself?
5. Does your organisation ask for any sort of feedback / or your opinion about policies or procedures?
6. Do they test you in any way about your understanding of the policies?

C. Employee participations
1. Have you read your organisations security policy?
2. Did you or were you able to understand it? How easy or difficult was it to understand?
3. SHOW POLICY: This is your organisational security policy, which is available on your organisations website. Could you please go through this and give me your impression of it?

D. Issues following the policies.
1. Can you think of any issues with following this or these policies?
2. Do you think that following these policies would affect your daily job tasks in any way?
3. What do you think about the relevance of information within the policies? Do you feel they are relevant to you or your job role in any way?
4. How do you determine what information is relevant to you or your job role? Would you ask somebody?

E. Being a part of the solution.
1. How can your organisation help you with following these policies?
2. Would it be better if you were given a few instructions which you have to follow on a regular basis and are relevant to your job role rather than knowing or following the entire security policy? (Tailored policy). Why? How?
3. Do you think employees should be a part of improving the organisational security?
4. How do you think employees can help with improving organisational security behaviour?

Thank participant for their participation.

Stop recording.

Hand the debrief sheet to the participant.

8 Appendix B

STUDY TWO SURVEY INSTRUMENT

	Table one			
	Demographics		**Item no**	**Scale**
1	Age		1	(18-25)(26-30)(31-35)(36-50)(50+)
	Education		2	(Undergraduate)(Bachelors)(Masters)(Doctorate)
	Total No of years worked		3	(0-5)(5-10)(10-15)(15-20)(20+)
	No of years worked in current organisation		4	(0-5)(5-10)(10-15)(15-20)(20+)
2	Department working within the organisation		5	(HR-Manage current organisations human resource)(Finance-Manage current organisations finance)(Specialist-focussing on current organisations products or services)(IT-Manage current organisations IT systems)(Management-Manage overall organisation)
	Job Position		6	(First line)(Second line)(Team Leader/Manager)(Senior Manager/Dept Head)(Top Management)
	How would you rate your organisational security?		7	(Very Low)(Low)(Medium)(High)(Very High)
	How would you rate your organisation?		8	(Low Security)(Medium Security)(High Security)
	How would you rate the information you handle while on job?		9	(Not confidential)(Medium- personal information, employee information)(Highly Confidential-such as company data, financial information etc.)

	I am involved in designing/implementing organisational policies		10	(Yes)(No)
	How would you rate your knowledge about IT systems?		11	(None)(Adequate)(Average)(Above average)(Expert)
	How would you rate your knowledge about Information Security		12	(None)(Adequate)(Average)(Above average)(Expert)
	Table Two			
	Construct	**Variables**	**Item No.**	**Item Statement**
1	Employee perception of information security policy	What is it	1	Information security and data protection are not the same
			2	Information security is different from cyber security
			3	How I protect the information stored on my computer is common sense
		Why is it relevant	4	There are risks associated with non-compliance of policies
			5	There are risks associated with a security breach
			6	There are risks associated with a security policy breach
		How is it relevant	7	I am bound by an organisational information security policy
			8	Complying with Information security policy is relevant to me or my job role
			9	Information security policy is only relevant to people working in IT department
		Protection from	10	I understand how a spam email could potentially hurt me or my organisation

			11	I understand how a virus on my computer could potentially hurt me or my organisation
			12	I understand how an identity theft could potentially hurt me or my organisation
2	Employee perception of organisational interventions regarding security policy and its compliance	Awareness	13	I think our organisation has made us aware of our security policy
			14	I know our organisation has made us aware of our security policy
			15	My organisation ought to/should make us aware of our security policy
		Training	16	I think our organisation provides training on compliance of our security policy
			17	I know our organisation provides training on compliance of our security policy
			18	My organisation ought to/should provide training on how to comply with our security policy
		Communication	19	My organisation tells me if compliance of security policy is important to my job role
			20	My organisation should tell me if compliance of security policy is important to my job role
			21	My organisation asks me if I could do anything to improve organisational security policy compliance behaviour
			22	My organisation should ask me if I could do anything to improve organisational security policy compliance behaviour
		Security policy	23	I think our organisation has an organisational security policy
			24	I know our organisation has an organisational security policy
			25	My organisation ought to/should have an organisational security policy

3	Employee perception of organisational citizenship (towards compliance of security policy)	Allegiance	26	My organisational policies are made to protect me and my information
			27	My organisational policies are made to protect the organisation and its information
			28	I will change organisations in a few years so security compliance is not my concern
		Responsibility	29	It is my organisations responsibility to protect my personal information and organisational information
			30	It is my responsibility to protect my and organisational information
			31	Information security compliance is not a part of job decription
		Effort	32	My organisation should tell me what security procedures are relevant to my job role
			33	I should find out what security procedures are relevant to my job role
			34	My colleagues who have worked longer than me in the organisation should tell me what security procedures are relevant to my job role
4	Employee perception of quality of policy document	Visibility	35	My organisational information security policy is easily available for my reference
			36	I can find my organisational information security policy with some effort
			37	It is extremely difficult to find my organisational information security policy
		Language	38	Policies are written in layman language and easy to understand
			39	The language within the policies is vague and ambigious
			40	The language within the policies is mostly legal and difficult to understand
		Content	41	My organisational information security policy has information which is relevant to my job role

			42	The organisational security policy is made using industry standard guidelines
			43	Policies mostly include legal information information
		Length	44	My organisational polices are too long with many pages
			45	My organisational policies are of average length
			46	My organisational policies are short and concise
5	Threat Appraisal (Threat being non compliance)	Threat severity	47	Risks associated with non compliance of security policies are severe
			48	Risks associated with non compliance of security policies are serious
			49	Risks associated with non compliance of security policies are significant
		Threat Vulnerability	50	Non-compliance of a security policy affects me
			51	Non-compliance of a security policy affects my organisation
			52	Non-compliance of policies affects the security of the information I work with
		Threat Susceptibility	53	My organisation/me are at risk if I don't comply with the security policy
			54	It is likely that my organisation/me, are at risk if I don't comply with the security policy
			55	It is possible that my organisation/me, are at risk if I don't comply with the security policy
6	Coping appraisal (compliance with security policy)	Response efficacy	56	Complying with policies makes us (me/my organisation) and our information (personal/organisational) safer
			57	Complying with policies is effective to make us (me/ my orgnisation) and out information (personal / organisational) safer.

			58	Complying with policies is more likely to make us (Me/my organisation) and our information (personal and organisational) safer
		Self efficacy	59	I can identify a security breach of our organisational security policy
			60	I can identify when I am in breach of my organisational security policy
			61	I can identify when others are in breach of my organisational security policy
		Response cost	62	Compliance of information security policy is not mandatory in my organisation
			63	There are implications associated with breach of my organisational security policy
			64	Secure behaviour is rewarded in my organisation
			65	Following the security policy on a daily basis would be a waste of time
			66	Following policies would cause disruption to my work
7	Behavioural Intent (To comply with a security policy)	Complying with policy	67	I don't want to do anything about security policy compliance
			68	I would like to know about complying with our security policy
			69	I would like to understand our security policy
			70	I am likely to follow our security policy
			71	It is possible that I will follow our security policy
			72	I am certain I will follow our security policy
8	Actual Behaviour	Compliance with policies	73	I follow our security policy in my work place
			74	I follow our security policy on a daily basis
			75	I tell others to follow our security policy in the work place

			76	I comply with all our organisational policies
			77	I comply with policies that I think are relevant to my job role
			78	I comply with policies that I am told are relevant to my job role
9	Usability of a Tailored security policy	Effectiveness	79	A tailored policy will tell me exactly what I need to follow
			80	A tailored policy can be followed on a regular basis
			81	A tailored policy will improve policy compliance
		Efficiency	82	A tailored policy will be easy to read
			83	A tailored policy will be easy to understand
			84	A tailored policy will be easy to follow
		Satisfaction	85	I want our organisational security policies to be tailored to my job role
			86	I will be more inclined to follow a tailored policy
			87	I will be happy to follow a tailored policy

9 Appendix C

WHAT_1	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	136	37	20	70.47%	19.17%	10.36%
Employees	320	169	113	38	52.81%	35.31%	11.88%
Total	513	305	150	58	59.45%	29.24%	11.31%

WHAT_2	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	134	43	16	69.43%	22.28%	8.29%
Employees	320	173	109	38	54.06%	34.06%	11.88%
Total	513	307	152	54	59.84%	29.63%	10.53%

WHY_1	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	157	30	6	81.35%	15.54%	3.11%
Employees	320	241	74	5	75.31%	23.13%	1.56%
Total	513	398	104	11	77.58%	20.27%	2.14%

WHY_3	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	162	26	5	83.94%	13.47%	2.59%
Employees	320	243	58	19	75.94%	18.13%	5.94%
Total	513	405	84	24	78.95%	16.37%	4.68%

FROM_1	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	163	25	5	84.46%	12.95%	2.59%
Employees	320	263	49	8	82.19%	15.31%	2.50%
Total	513	426	74	13	83.04%	14.42%	2.53%

FROM_3	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	165	22	6	85.49%	11.40%	3.11%
Employees	320	268	45	7	83.75%	14.06%	2.19%
Total	513	433	67	13	84.41%	13.06%	2.53%

AWARENESS_2	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	155	28	10	80.31%	14.51%	5.18%
Employees	320	231	62	27	72.19%	19.38%	8.44%
Total	513	386	90	37	75.24%	17.54%	7.21%

TRAINING_2	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	143	30	20	74.09%	15.54%	10.36%
Employees	320	175	89	56	54.69%	27.81%	17.50%
Total	513	318	119	76	61.99%	23.20%	14.81%

COMMUNICATION_1	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A

Policymakers	193	145	34	14	75.13%	17.62%	7.25%
Employees	320	208	82	30	65.00%	25.63%	9.38%
Total	513	353	116	44	68.81%	22.61%	8.58%

COMMUNICATION_3	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	134	40	19	69.43%	20.73%	9.84%
Employees	320	135	98	87	42.19%	30.63%	27.19%
Total	513	269	138	106	52.44%	26.90%	20.66%

SEC_POLICY_2	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	154	29	10	79.79%	15.03%	5.18%
Employees	320	200	89	31	62.50%	27.81%	9.69%
Total	513	354	118	41	69.01%	23.00%	7.99%

AWARENESS_3	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	158	29	6	81.87%	15.03%	3.11%
Employees	320	218	81	21	68.13%	25.31%	6.56%
Total	513	376	110	27	73.29%	21.44%	5.26%

TRAINING_3	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	155	29	9	80.31%	15.03%	4.66%
Employees	320	217	83	20	67.81%	25.94%	6.25%
Total	513	372	112	29	72.51%	21.83%	5.65%

COMMUNICATION_2	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	151	31	11	78.24%	16.06%	5.70%
Employees	320	236	65	19	73.75%	20.31%	5.94%
Total	513	387	96	30	75.44%	18.71%	5.85%

SEC_POLICY_3	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	154	38	1	79.79%	19.69%	0.52%
Employees	320	218	84	18	68.13%	26.25%	5.63%
Total	513	372	122	19	72.51%	23.78%	3.70%

ALLEGIENCE_1	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	163	24	6	84.46%	12.44%	3.11%
Employees	320	239	69	12	74.69%	21.56%	3.75%
Total	513	402	93	18	78.36%	18.13%	3.51%

ALLEGIENCE_2	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	171	19	3	88.60%	9.84%	1.55%
Employees	320	255	58	7	79.69%	18.13%	2.19%
Total	513	426	77	10	83.04%	15.01%	1.95%

ALLEGIENCE_3R	Coding - Reverse						

	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	85	33	75	44.04%	17.10%	38.86%
Employees	320	75	88	157	23.44%	27.50%	49.06%
Total	513	160	121	232	31.19%	23.59%	45.22%

RESPONSIBILITY_1	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	158	29	6	81.87%	15.03%	3.11%
Employees	320	235	67	18	73.44%	20.94%	5.63%
Total	513	393	96	24	76.61%	18.71%	4.68%

EFFORT_1	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	162	30	1	83.94%	15.54%	0.52%
Employees	320	247	70	3	77.19%	21.88%	0.94%
Total	513	409	100	4	79.73%	19.49%	0.78%

RESPONSIBILITY_2	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	172	18	3	89.12%	9.33%	1.55%
Employees	320	241	60	19	75.31%	18.75%	5.94%
Total	513	413	78	22	80.51%	15.20%	4.29%

EFFORT_2	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	166	24	3	86.01%	12.44%	1.55%
Employees	320	224	82	14	70.00%	25.63%	4.38%
Total	513	390	106	17	76.02%	20.66%	3.31%

HOW_1	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	150	34	9	77.72%	17.62%	4.66%
Employees	320	225	68	27	70.31%	21.25%	8.44%
Total	513	375	102	36	73.10%	19.88%	7.02%

HOW_2	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	157	32	4	81.35%	16.58%	2.07%
Employees	320	213	73	34	66.56%	22.81%	10.63%
Total	513	370	105	38	72.12%	20.47%	7.41%

LANGUAGE_2R	Coding - Reverse						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	90	50	53	46.63%	25.91%	27.46%
Employees	320	86	121	113	26.88%	37.81%	35.31%
Total	513	176	171	166	34.31%	33.33%	32.36%

This item is reverse coded in structural equation model. Analysis for this section is done from their straight responses.

LANGUAGE_3R	Coding - Reverse						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	87	42	64	45.08%	21.76%	33.16%
Employees	320	95	118	107	29.69%	36.88%	33.44%
Total	513	182	160	171	35.48%	31.19%	33.33%

This item is reverse coded in structural equation model. Analysis for this section is done from their straight responses.

CONTENT_1	Coding - Straight						

	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	155	32	6	80.31%	16.58%	3.11%
Employees	320	195	92	33	60.94%	28.75%	10.31%
Total	513	350	124	39	68.23%	24.17%	7.60%

CONTENT_2	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	147	41	5	76.17%	21.24%	2.59%
Employees	320	171	127	22	53.44%	39.69%	6.88%
Total	513	318	168	27	61.99%	32.75%	5.26%

CONTENT_3	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	126	44	23	65.28%	22.80%	11.92%
Employees	320	141	133	46	44.06%	41.56%	14.38%
Total	513	267	177	69	52.05%	34.50%	13.45%

LENGTH_2	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	116	55	22	60.10%	28.50%	11.40%
Employees	320	120	160	40	37.50%	50.00%	12.50%
Total	513	236	215	62	46.00%	41.91%	12.09%

LENGTH_3	Coding - Straight						
	Participants (A)	Agree	Not Sure	Disagree	% agree of A	% Not Sure of A	% Disagree of A
Policymakers	193	97	53	43	50.26%	27.46%	22.28%
Employees	320	76	149	95	23.75%	46.56%	29.69%
Total	513	173	202	138	33.72%	39.38%	26.90%

10 Appendix D

10.1 Normality with all items

Statistics

	N			Std. Error of		Std. Error of
	Valid	Missing	Skewness	Skewness	Kurtosis	Kurtosis
from3	513	0	1.466	.108	1.720	.215
responsibility2	513	0	1.124	.108	.940	.215
from1	513	0	1.178	.108	.897	.215
allegience2	513	0	1.087	.108	.776	.215
responsibility1	513	0	.990	.108	.617	.215
communication2	513	0	1.013	.108	.569	.215
awareness2	513	0	1.030	.108	.506	.215
allegience1	513	0	.933	.108	.504	.215
ac_behave2	513	0	1.002	.108	.481	.215
how1	513	0	1.004	.108	.402	.215
tsus2	513	0	.892	.108	.356	.215
efficiency3	513	0	.841	.108	.299	.215
sec_policy3	513	0	.854	.108	.295	.215
how2	513	0	.946	.108	.293	.215
ac_behave1	513	0	.983	.108	.278	.215
why3	513	0	.989	.108	.270	.215
seff2	513	0	.745	.108	.239	.215
effort2	513	0	.817	.108	.235	.215
training3	513	0	.880	.108	.193	.215
tvul3	513	0	.830	.108	.183	.215
intent4	513	0	.870	.108	.148	.215
content1	513	0	.778	.108	.125	.215
awareness3	513	0	.906	.108	.094	.215
content2	513	0	.473	.108	.017	.215
what2	513	0	.542	.108	.014	.215
effectiveness2	513	0	.738	.108	.007	.215
tvul1	513	0	.717	.108	.003	.215
communication1	513	0	.800	.108	-.016	.215
satisfaction3	513	0	.762	.108	-.016	.215
intent2	513	0	.428	.108	-.036	.215
tvul2	513	0	.837	.108	-.041	.215

sec_policy2	513	0	.823	.108	-.064	.215
reff3	513	0	.847	.108	-.075	.215
length2	513	0	.146	.108	-.110	.215
effectiveness1	513	0	.694	.108	-.112	.215
reff2	513	0	.848	.108	-.117	.215
reff1	513	0	.894	.108	-.124	.215
tsev3	513	0	.603	.108	-.141	.215
intent3	513	0	.493	.108	-.170	.215
tsev2	513	0	.635	.108	-.180	.215
ac_behave4	513	0	.772	.108	-.205	.215
tsus1	513	0	.727	.108	-.210	.215
efficiency1	513	0	.718	.108	-.227	.215
efficiency2	513	0	.744	.108	-.248	.215
what1	513	0	.468	.108	-.280	.215
seff3	513	0	.518	.108	-.282	.215
tsev1	513	0	.561	.108	-.371	.215
effectiveness3	513	0	.648	.108	-.375	.215
seff1	513	0	.507	.108	-.381	.215
satisfaction2	513	0	.506	.108	-.392	.215
content3	513	0	.308	.108	-.422	.215
why1	513	0	.711	.108	-.455	.215
length3	513	0	.099	.108	-.477	.215
training2	513	0	.649	.108	-.509	.215
effort1	513	0	.662	.108	-.541	.215
ac_behave3	513	0	.543	.108	-.548	.215
satsfaction1	513	0	.385	.108	-.671	.215
communication3	513	0	.478	.108	-.728	.215
language2r	513	0	-.023	.108	-.758	.215
resc3	513	0	.060	.108	-.797	.215
language3r	513	0	-.056	.108	-.865	.215
resc5	513	0	-.363	.108	-.981	.215
resc4	513	0	-.390	.108	-1.060	.215
allegience3r	513	0	.215	.108	-1.268	.215

10.2 Perception of Information Security

Correlation Matrix[a]

		what1	what2	why1	why3	from1	from3
Correlation	what1	1.000	.606	.248	.196	.187	.219
	what2	.606	1.000	.242	.249	.206	.241
	why1	.248	.242	1.000	.677	.548	.501
	why3	.196	.249	.677	1.000	.545	.552
	from1	.187	.206	.548	.545	1.000	.709
	from3	.219	.241	.501	.552	.709	1.000
Sig. (1-tailed)	what1		.000	.000	.000	.000	.000
	what2	.000		.000	.000	.000	.000
	why1	.000	.000		.000	.000	.000
	why3	.000	.000	.000		.000	.000
	from1	.000	.000	.000	.000		.000
	from3	.000	.000	.000	.000	.000	

a. Determinant = .091

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.737
Bartlett's Test of Sphericity	Approx. Chi-Square	1222.697
	df	15
	Sig.	.000

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	3.044	50.734	50.734	3.044	50.734	50.734	2.910
2	1.331	22.189	72.922	1.331	22.189	72.922	1.855
3	.621	10.346	83.269				
4	.405	6.749	90.017				
5	.327	5.450	95.467				
6	.272	4.533	100.000				

Extraction Method: Principal Component Analysis.

a. When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

Pattern Matrixa

	Component	
	1	2
what1		.903
what2		.887
why1	.799	
why3	.830	
from1	.863	
from3	.832	

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 3 iterations.

10.3 Perception of Organisational interventions

Correlation Matrix[a]

		awareness2	training2	communication1	communication3	sec_policy2	awareness3	training3	communication2	sec_policy3
Correlation	awareness2	1.000	.663	.614	.456	.710	.359	.442	.451	.386
	training2	.663	1.000	.659	.630	.682	.277	.421	.428	.355
	communication1	.614	.659	1.000	.516	.616	.306	.411	.493	.382
	communication3	.456	.630	.516	1.000	.564	.196	.286	.334	.314
	sec_policy2	.710	.682	.616	.564	1.000	.327	.441	.514	.497
	awareness3	.359	.277	.306	.196	.327	1.000	.648	.480	.626
	training3	.442	.421	.411	.286	.441	.648	1.000	.603	.636

	communication2	.451	.428	.493	.334	.514	.480	.603	1.000	.624
	sec_policy3	.386	.355	.382	.314	.497	.626	.636	.624	1.000
Sig. (1-tailed)	awareness2		.000	.000	.000	.000	.000	.000	.000	.000
	training2	.000		.000	.000	.000	.000	.000	.000	.000
	communication1	.000	.000		.000	.000	.000	.000	.000	.000
	communication3	.000	.000	.000		.000	.000	.000	.000	.000
	sec_policy2	.000	.000	.000	.000		.000	.000	.000	.000
	awareness3	.000	.000	.000	.000	.000		.000	.000	.000
	training3	.000	.000	.000	.000	.000	.000		.000	.000
	communication2	.000	.000	.000	.000	.000	.000	.000		.000
	sec_policy3	.000	.000	.000	.000	.000	.000	.000	.000	

a. Determinant = .006

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.885
Bartlett's Test of Sphericity	Approx. Chi-Square	2595.191
	df	36
	Sig.	.000

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	4.884	54.271	54.271	4.884	54.271	54.271	4.239
2	1.442	16.020	70.291	1.442	16.020	70.291	3.725
3	.561	6.230	76.521				
4	.512	5.690	82.210				
5	.431	4.785	86.995				
6	.363	4.032	91.027				

7	.307	3.409	94.437				
8	.265	2.949	97.386				
9	.235	2.614	100.000				

Extraction Method: Principal Component Analysis.

a. When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

Pattern Matrixa

	Component	
	1	2
awareness2	.762	
training2	.899	
communication1	.781	
communication3	.832	
sec_policy2	.792	
awareness3		.909
training3		.832
communication2		.666
sec_policy3		.842

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 5 iterations.

10.4 Perception of responsibility

Correlation Matrix[a]

		responsibility1	effort1	responsibility2	effort2	how1	how2
Correlation	responsibility1	1.000	.510	.538	.425	.321	.330
	effort1	.510	1.000	.556	.554	.374	.380
	responsibility2	.538	.556	1.000	.538	.490	.526
	effort2	.425	.554	.538	1.000	.406	.447
	how1	.321	.374	.490	.406	1.000	.711
	how2	.330	.380	.526	.447	.711	1.000
Sig. (1-tailed)	responsibility1		.000	.000	.000	.000	.000
	effort1	.000		.000	.000	.000	.000
	responsibility2	.000	.000		.000	.000	.000

	effort2	.000	.000	.000		.000	.000
	how1	.000	.000	.000	.000		.000
	how2	.000	.000	.000	.000	.000	

a. Determinant = .088

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.822
Bartlett's Test of Sphericity	Approx. Chi-Square	1238.015
	df	15
	Sig.	.000

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.377	56.286	56.286	3.377	56.286	56.286
2	.941	15.688	71.975			
3	.572	9.530	81.505			
4	.426	7.100	88.605			
5	.400	6.660	95.266			
6	.284	4.734	100.000			

Extraction Method: Principal Component Analysis.

Component Matrixa

	Component
	1
responsibility1	.685
effort1	.750
responsibility2	.819
effort2	.750
how1	.734
how2	.757

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

10.5 Quality of Policy document

Correlation Matrix[a]

		language2r	language3r	content1	content2	content3	length2	length3
Correlation	language2r	1.000	.726	.038	-.084	-.272	-.122	-.291

	language3r	.726	1.000	.080	-.097	-.395	-.106	-.231
	content1	.038	.080	1.000	.531	.320	.363	.162
	content2	-.084	-.097	.531	1.000	.532	.354	.129
	content3	-.272	-.395	.320	.532	1.000	.242	.169
	length2	-.122	-.106	.363	.354	.242	1.000	.507
	length3	-.291	-.231	.162	.129	.169	.507	1.000
Sig. (1-tailed)	language2r		.000	.195	.028	.000	.003	.000
	language3r	.000		.035	.014	.000	.008	.000
	content1	.195	.035		.000	.000	.000	.000
	content2	.028	.014	.000		.000	.000	.002
	content3	.000	.000	.000	.000		.000	.000
	length2	.003	.008	.000	.000	.000		.000
	length3	.000	.000	.000	.002	.000	.000	

a. Determinant = .108

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.640
Bartlett's Test of Sphericity	Approx. Chi-Square	1133.207
	df	21
	Sig.	.000

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	2.597	37.101	37.101	2.597	37.101	37.101	2.146
2	1.685	24.078	61.179	1.685	24.078	61.179	1.990
3	1.113	15.896	77.075	1.113	15.896	77.075	1.736
4	.534	7.635	84.709				
5	.445	6.356	91.065				
6	.381	5.444	96.509				
7	.244	3.491	100.000				

Extraction Method: Principal Component Analysis.

a. When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

Pattern Matrixa

Component		
1	2	3

language2r		.874	
language3r		.918	
content1	.733		
content2	.876		
content3	.737		
length2			.796
length3			.885

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 6 iterations.

10.6 Threat Appraisal

Correlation Matrix[a]

		tsev1	tsev2	tsev3	tvul1	tvul2	tvul3	tsus1	tsus2
Correlation	tsev1	1.000	.645	.528	.580	.530	.546	.601	.539
	tsev2	.645	1.000	.713	.562	.596	.606	.572	.522
	tsev3	.528	.713	1.000	.422	.451	.503	.492	.477
	tvul1	.580	.562	.422	1.000	.646	.694	.609	.529
	tvul2	.530	.596	.451	.646	1.000	.698	.618	.582
	tvul3	.546	.606	.503	.694	.698	1.000	.665	.597
	tsus1	.601	.572	.492	.609	.618	.665	1.000	.725
	tsus2	.539	.522	.477	.529	.582	.597	.725	1.000
Sig. (1-tailed)	tsev1		.000	.000	.000	.000	.000	.000	.000
	tsev2	.000		.000	.000	.000	.000	.000	.000
	tsev3	.000	.000		.000	.000	.000	.000	.000
	tvul1	.000	.000	.000		.000	.000	.000	.000
	tvul2	.000	.000	.000	.000		.000	.000	.000
	tvul3	.000	.000	.000	.000	.000		.000	.000
	tsus1	.000	.000	.000	.000	.000	.000		.000
	tsus2	.000	.000	.000	.000	.000	.000	.000	

a. Determinant = .006

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.906
Bartlett's Test of Sphericity	Approx. Chi-Square	2589.561
	df	28
	Sig.	.000

Total Variance Explained

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	5.072	63.401	63.401	5.072	63.401	63.401
2	.776	9.705	73.106			
3	.562	7.019	80.126			
4	.472	5.895	86.021			
5	.343	4.284	90.306			
6	.279	3.491	93.796			
7	.255	3.191	96.987			
8	.241	3.013	100.000			

Extraction Method: Principal Component Analysis.

Component Matrixa

	Component
	1
tsev1	.779
tsev2	.818
tsev3	.711
tvul1	.795
tvul2	.808
tvul3	.838
tsus1	.833
tsus2	.781

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

10.7 Coping Appraisal

Correlation Matrix[a]

		reff1	reff2	reff3	seff1	seff2	seff3	resc3	resc4	resc5
Correlation	reff1	1.000	.816	.781	.237	.417	.305	-.033	-.313	-.270
	reff2	.816	1.000	.793	.286	.465	.376	.001	-.256	-.250
	reff3	.781	.793	1.000	.243	.447	.351	.007	-.245	-.246
	seff1	.237	.286	.243	1.000	.644	.677	.430	.155	.175
	seff2	.417	.465	.447	.644	1.000	.741	.248	-.049	-.024

	seff3	.305	.376	.351	.677	.741	1.000	.313	.045	.101
	resc3	-.033	.001	.007	.430	.248	.313	1.000	.493	.431
	resc4	-.313	-.256	-.245	.155	-.049	.045	.493	1.000	.807
	resc5	-.270	-.250	-.246	.175	-.024	.101	.431	.807	1.000
Sig. (1-tailed)	reff1		.000	.000	.000	.000	.000	.225	.000	.000
	reff2	.000		.000	.000	.000	.000	.493	.000	.000
	reff3	.000	.000		.000	.000	.000	.441	.000	.000
	seff1	.000	.000	.000		.000	.000	.000	.000	.000
	seff2	.000	.000	.000	.000		.000	.000	.135	.295
	seff3	.000	.000	.000	.000	.000		.000	.152	.011
	resc3	.225	.493	.441	.000	.000	.000		.000	.000
	resc4	.000	.000	.000	.000	.135	.152	.000		.000
	resc5	.000	.000	.000	.000	.295	.011	.000	.000	

a. Determinant = .003

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.782
Bartlett's Test of Sphericity	Approx. Chi-Square	2927.763
	df	36
	Sig.	.000

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings[a]
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total
1	3.647	40.520	40.520	3.647	40.520	40.520	3.199
2	2.612	29.024	69.543	2.612	29.024	69.543	2.420
3	1.028	11.422	80.965	1.028	11.422	80.965	2.969
4	.551	6.125	87.090				
5	.331	3.673	90.763				
6	.251	2.790	93.553				
7	.225	2.501	96.054				
8	.196	2.174	98.228				
9	.159	1.772	100.000				

Extraction Method: Principal Component Analysis.

a. When components are correlated, sums of squared loadings cannot be added to obtain a total variance.

Pattern Matrixa

	Component		
	1	2	3
reff1	.938		
reff2	.921		
reff3	.932		
seff1			-.879
seff2			-.850
seff3			-.902
resc3		.640	
resc4		.946	
resc5		.914	

Extraction Method: Principal Component Analysis.

Rotation Method: Oblimin with Kaiser Normalization.

a. Rotation converged in 6 iterations.

10.8 Behavioural Intent

Correlation Matrix[a]

		intent2	intent3	intent4
Correlation	intent2	1.000	.719	.424
	intent3	.719	1.000	.524
	intent4	.424	.524	1.000
Sig. (1-tailed)	intent2		.000	.000
	intent3	.000		.000
	intent4	.000	.000	

a. Determinant = .349

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.642
Bartlett's Test of Sphericity	Approx. Chi-Square	537.575
	df	3
	Sig.	.000

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.120	70.675	70.675	2.120	70.675	70.675
2	.610	20.344	91.019			

3	.269	8.981	100.000			

Extraction Method: Principal Component Analysis.

Component Matrixa

	Component 1
intent2	.863
intent3	.903
intent4	.749

Extraction Method: Principal Component Analysis.

a. 1 components extracted.

10.9 Actual Behaviour

Correlation Matrix[a]

		ac_behave1	ac_behave2	ac_behave3	ac_behave4
Correlation	ac_behave1	1.000	.866	.564	.714
	ac_behave2	.866	1.000	.554	.702
	ac_behave3	.564	.554	1.000	.469
	ac_behave4	.714	.702	.469	1.000
Sig. (1-tailed)	ac_behave1		.000	.000	.000
	ac_behave2	.000		.000	.000
	ac_behave3	.000	.000		.000
	ac_behave4	.000	.000	.000	

a. Determinant = .076

KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.797
Bartlett's Test of Sphericity	Approx. Chi-Square	1311.803
	df	6
	Sig.	.000

Total Variance Explained

	Initial Eigenvalues			Extraction Sums of Squared Loadings		
Component	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	2.955	73.883	73.883	2.955	73.883	73.883
2	.575	14.380	88.263			

3	.336	8.395	96.658			
4	.134	3.342	100.000			

Extraction Method: Principal Component Analysis.

Component Matrixa

	Component 1
ac_behave1	.927
ac_behave2	.921
ac_behave3	.731
ac_behave4	.845

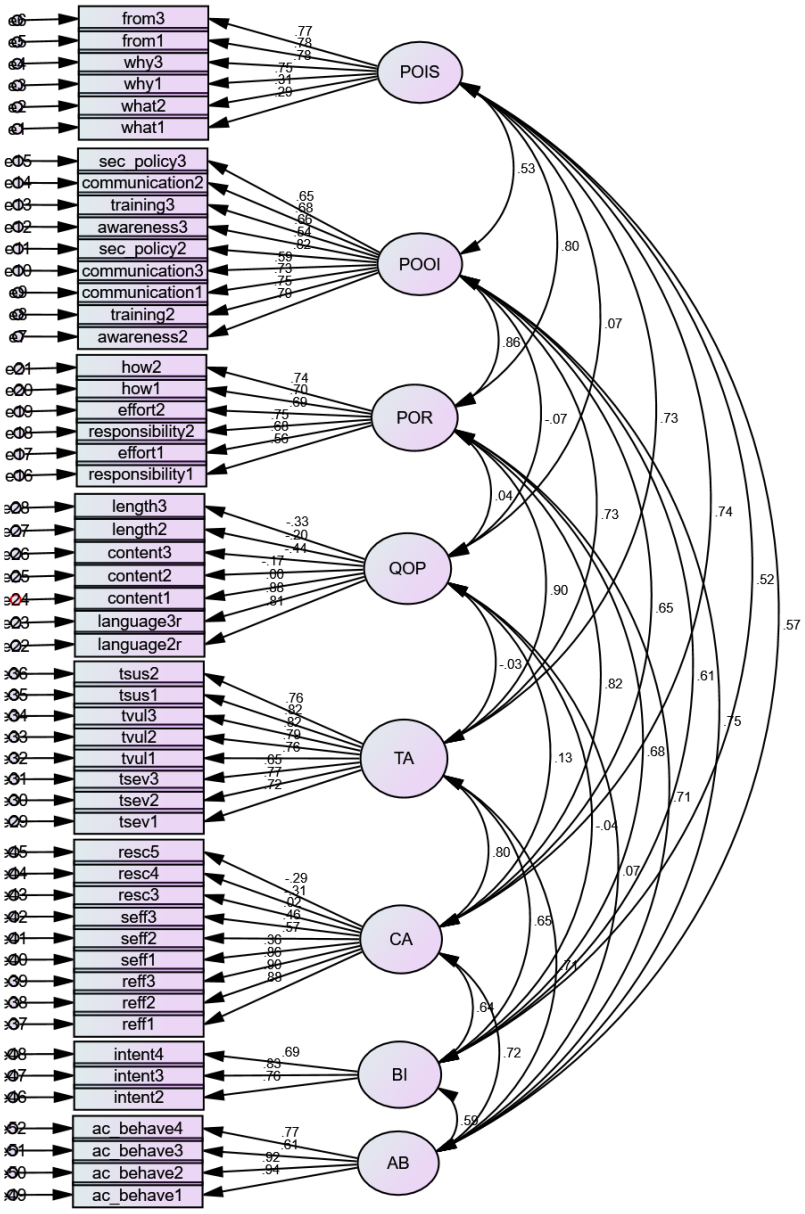
Extraction Method: Principal Component Analysis.

a. 1 components extracted.

10.10 Confirmatory Factor Analysis (CFA) (Failed)

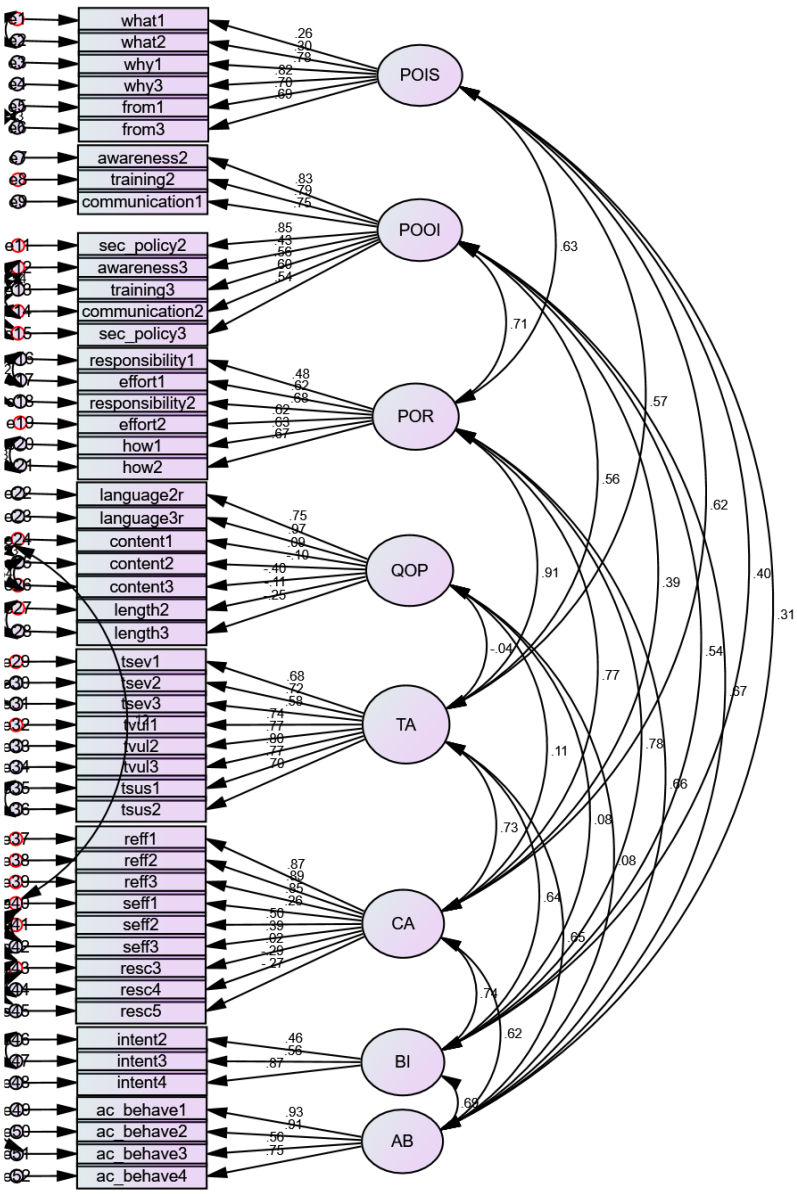
Getting a cursory model fit. Checking for validity.

Initial loading



CFI and RMSEA values outside of threshold.

After further iterations,



CFI Value 0.851 RMSEA value 0.067 showing satisfactory model fit.

Chi-square = 3849.638

Degrees of freedom = 1173

These values are expected as our sample size is quite high.

References

Adams, A., & Blandford, A. (2005). Bridging the gap between organizational and user perspectives of security in the clinical domain. *International Journal of Human-Computer Studies*, *63*(1–2), 175–202. https://doi.org/10.1016/J.IJHCS.2005.04.022

Adams, A., & Sasse, M. A. (1999). USERS ARE NOT THE ENEMY. *Communications of the ACM*, *42*(12), 40–46. https://doi.org/doi:10.1145/322796.322806

Ajzen, I. (1991). The theory of planned behavior. *Orgnizational Behavior and Human Decision Processes*, *50*, 179–211. https://doi.org/10.1016/0749-5978(91)90020-T

Ajzen, I. (2011, September). The theory of planned behaviour: Reactions and reflections. *Psychology and Health*, Vol. 26, pp. 1113–1127. https://doi.org/10.1080/08870446.2011.613995

Al-Omari, A., Deokar, A., El-Gayar, O., Walters, J., & Aleassa, H. (2013). Information security policy compliance: An empirical study of ethical ideology. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3018–3027. https://doi.org/10.1109/HICSS.2013.272

Al-Omari, A., El-Gayar, O., & Deokar, A. (2011). Security policy compliance: User acceptance perspective. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3317–3326. https://doi.org/10.1109/HICSS.2012.516

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computers and Security*, *26*(4), 276–289. https://doi.org/10.1016/j.cose.2006.11.004

Albrechtsen, E., & Hovden, J. (2009). The information security digital divide between information security managers and users. *Computers and Security*, *28*(6), 476–490. https://doi.org/10.1016/j.cose.2009.01.003

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. *Computers and Security*, *29*(4), 432–445. https://doi.org/10.1016/j.cose.2009.12.005

Anderson, K. B., Durbin, E., & Salinger, M. A. (2008, March). Identity theft. *Journal of Economic*

Perspectives, Vol. 22, pp. 171–192. https://doi.org/10.1257/jep.22.2.171

Anderson, T. W., & Darling, D. A. (1954). A Test of Goodness of Fit. *Journal of the American Statistical Association*, *49*(268), 765–769. https://doi.org/10.1080/01621459.1954.10501232

Ashenden, D. (2008). Information Security management: A human challenge? *Information Security Technical Report*, *13*(4), 195–201. https://doi.org/10.1016/j.istr.2008.10.006

Aurigemma, S., & Panko, R. (2012). A composite framework for behavioral compliance with information security policies. *Proceedings of the Annual Hawaii International Conference on System Sciences*, 3248–3257. https://doi.org/10.1109/HICSS.2012.49

Baker, S. E., & Edwards, R. (n.d.). *How many qualitative interviews is enough? Expert voices and early career reflections on sampling and cases in qualitative research*.

Bandalos, D. L., Finney, S. J., & Finney, S. J. (2001). *Item Parceling Issues in Structural Equation Modeling*. 289–316. https://doi.org/10.4324/9781410601858-15

Bandura, A. (1989). Human Agency in Social Cognitive Theory. *American Psychologist*, *44*(9), 1175–1184. https://doi.org/10.1037/0003-066X.44.9.1175

Barnhoorn, J. S., Haasnoot, E., Bocanegra, B. R., & van Steenbergen, H. (2014). QRTEngine: An easy solution for running online reaction time experiments using Qualtrics. *Behavior Research Methods*, *47*(4), 918–929. https://doi.org/10.3758/s13428-014-0530-7

Bartlett, M. S. (1937). The Statistical Conception of Mental Factors. Retrieved December 15, 2019, from ritish Journal of Psychology.General Section, 28(1), 97. website: https://search.proquest.com/docview/1293463650?pq-origsite=gscholar

Beautement, A., Becker, I., Parkin, S., Krol, K., Sasse, A., & Sasse, M. A. (2016). *Productive Security: A Scalable Methodology for Analysing Employee Security Behaviours*. Retrieved from www.usenix.org/conference/soups2016/technical-sessions/presentation/beautement

Benton, M. C., Pappas, J., & Pappas, E. (2011). *Association for Information Systems AIS Electronic Library (AISeL) WordPress+Qualtrics: A Plugin Supporting Research and New Pedagogy to Develop Personal Sustainability via 360° Evaluation Recommended Citation*

WordPress+Qualtrics: A Plugin Supporting Research and New Pedagogy to Develop Personal Sustainability via 360° Evaluation. Retrieved from http://aisel.aisnet.org/amcis2011_submissions/113

Bevan, N., & Macleod, M. (1994). Usability measurement in context. *Behaviour and Information Technology*, *13*(1–2), 132–145. https://doi.org/10.1080/01449299408914592

Blythe, J. M., Coventry, L., & Little, L. (2015). Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. *SOUPS 2015 - Proceedings of the 11th Symposium on Usable Privacy and Security*.

Boas, T. C., Christenson, D. P., & Glick, D. M. (2018). Recruiting large online samples in the United States and India: Facebook, Mechanical Turk, and Qualtrics. *Political Science Research and Methods*. https://doi.org/10.1017/psrm.2018.28

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2017). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems*, *18*(2), 151–164. https://doi.org/10.1057/ejis.2009.8

Broderick, J. S. (2006). ISMS, security standards and security regulations. *Information Security Technical Report*, *11*(1), 26–31. https://doi.org/10.1016/j.istr.2005.12.001

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, *34*(3), 523–548. https://doi.org/10.1093/bja/aeq366

Bullock, H. E., Harlow, L. L., & Mulaik, S. A. (1994). Causation Issues in Structural Equation Modeling Research. *Structural Equation Modeling: A Multidisciplinary Journal*, *1*(3), 253–267. https://doi.org/10.1080/10705519409539977

Byrne, B. M. (2004). Testing for multigroup invariance using AMOS graphics: A road less traveled. *Structural Equation Modeling*, *11*(2), 272–300. https://doi.org/10.1207/s15328007sem1102_8

C.R.Kothari. (2004). Research Methodology: Methods and Techniques - C. R. Kothari - Google Books. In *New age international*. https://doi.org/10.1007/s11274-011-0813-4

Chambel, M. J., Castanheira, F., & Sobral, F. (2016). Temporary agency versus permanent workers: A multigroup analysis of human resource management, work engagement and organizational commitment. *Economic and Industrial Democracy*, *37*(4), 665–689. https://doi.org/10.1177/0143831X14550695

Chen, C. C., Shaw, R. S., & Yang, S. C. (2006). Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System. *Information Technology, Learning, and Performance Journal*, *24*(1). Retrieved from http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.5945&rep=rep1&type=pdf

Chen, Y., Fatemeh, M., & Zahedi, S. B. (n.d.). *INDIVIDUALS' INTERNET SECURITY PERCEPTIONS AND BEHAVIORS: POLYCONTEXTUAL CONTRASTS BETWEEN THE UNITED STATES AND CHINA Appendix A Literature Review on Security Behaviors in Non-Work Settings*. Retrieved from www.cert.org

Chen, Y., Ramamurthy, K. (Ram), & Wen, K.-W. (2015). Impacts of Comprehensive Information Security Programs on Information Security Culture. *Http://Dx.Doi.Org/10.1080/08874417.2015.11645767*, *55*(3), 11–19. https://doi.org/10.1080/08874417.2015.11645767

Chin, W. W. (1998). Commentary Issues and Opinion on Structural Equation Modeling. *MIS Quarterly*, *22*(1), vii-xvi CR-Copyright © 1998 Management Inf. https://doi.org/10.2307/249674

Chinchani, R., Iyer, A., Ngo, H. Q., & Upadhyaya, S. (2005). Towards a Theory of Insider Threat Assessment. *2005 International Conference on Dependable Systems and Networks (DSN'05)*, 108–117. https://doi.org/10.1109/DSN.2005.94

Chou, N., Ledesma, R., Teraguchi, Y., & Mitchell, J. C. (2004). Client-side defense against web-based identity theft. *Computer Science Department, Stanford University. Available: Http://Crypto. Stanford. Edu/SpoofGuard/Webspoof. Pdf.* Retrieved from www.ebaymode.com

Choy, L. T. (2014). The Strengths and Weaknesses of Research Methodology: Comparison and Complimentary between Qualitative and Quantitative Approaches. In *IOSR Journal Of*

Humanities And Social Science (IOSR-JHSS (Vol. 19). Retrieved from www.iosrjournals.org

Collins, S. E., Witkiewitz, K., & Larimer, M. E. (2011). The theory of planned behavior as a predictor of growth in risky college drinking. *Journal of Studies on Alcohol and Drugs*, *72*(2), 322–332. https://doi.org/10.15288/jsad.2011.72.322

Colwill, C. (2009). Human factors in information security: The insider threat – Who can you trust these days? *Information Security Technical Report*, *14*(4), 186–196. https://doi.org/10.1016/J.ISTR.2010.04.004

Coventry, L., Briggs, P., Blythe, J., & Tran, M. (2014). Using behavioural insights to improve the public ' s use of cyber security best practices improve the public ' s use of cyber. In *Project Report. Government Office for Science*.

Da Veiga, A., & Eloff, J. H. P. (2010). A framework and assessment instrument for information security culture. *Computers and Security*, *29*(2), 196–207. https://doi.org/10.1016/j.cose.2009.09.002

Doherty, N. F., Anastasakis, L., & Fulford, H. (2011). Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy. *International Journal of Information Management*, *31*(3), 201–209. https://doi.org/10.1016/J.IJINFOMGT.2010.06.001

Eminağaoğlu, M., Uçar, E., & Eren, Ş. (2009). The positive outcomes of information security awareness training in companies – A case study. *Information Security Technical Report*, *14*(4), 223–229. https://doi.org/10.1016/J.ISTR.2010.05.002

ENISA. (2006). *Risk Management : Implementation principles and Inventories for Risk Management / Risk Assessment methods and tools*. Retrieved from https://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/files/deliverables/risk-management-principles-and-inventories-for-risk-management-risk-assessment-methods-and-tools

Farn, K., Lin, S., & Fung, A. R. (2004). A study on information security management system evaluation—assets, threat and vulnerability. *Computer Standards & Interfaces*, *26*(6), 501–

513. https://doi.org/10.1016/j.csi.2004.03.012

Farooq, M. U., Waseem, M., & Khairi, A. (2015). A Critical Analysis on the Security Concerns of Internet of Things (IoT). In *International Journal of Computer Applications* (Vol. 111). Retrieved from http://www.pcporoje.com/filedata/592496.pdf

Finch, H. (2006). Comparison of the performance of varimax and promax rotations: Factor structure recovery for dichotomous items. *Journal of Educational Measurement*, *43*(1), 39–52. https://doi.org/10.1111/j.1745-3984.2006.00003.x

Furnell, S. M., Gennatou, M., & Dowland, P. S. (2002). A prototype tool for information security awareness and training. *Logistics Information Management*, *15*(5/6), 352–357. https://doi.org/10.1108/09576050210447037

Gadd, S., Keeley, D., Balmforth, H., Health and Safety Laboratory (Great Britain), Great Britain, & Health and Safety Executive. (2003). Good practice and pitfalls in risk assessment.–Health & Safety Laboratory. In *Research Report 151.–HSE Book*. Health & Safety Laboratory.

Galvin, R. (2015). How many interviews are enough? Do qualitative interviews in building energy consumption research produce reliable knowledge? *Journal of Building Engineering*, *1*, 2–12. https://doi.org/10.1016/J.JOBE.2014.12.001

Gerber, M., & von Solms, R. (2008). Information security requirements – Interpreting the legal aspects. *Computers & Security*, *27*(5), 124–135. https://doi.org/10.1016/j.cose.2008.07.009

Gliem, J. A., & Gliem, R. R. (2003). *Midwest Research to Practice Conference in Adult, Continuing, and Community Education*.

Greenberg, J. and Baron, R. A. (1993). Behavior in Organisations. In *Allyn and Bacon Boston MA*.

Groeneveld, R. A., & Meeden, G. (1984). Measuring Skewness and Kurtosis. *The Statistician*, *33*(4), 391. https://doi.org/10.2307/2987742

Guin, T. D. Le, Baker, R., Mechling, J., & Ruyle, E. (2012). Myths and realities of respondent engagement in online surveys. *International Journal of Market Research*, *54*(5).

https://doi.org/10.2501/ijmr-54-5-613-633

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems*, *47*(2), 154–165. https://doi.org/10.1016/j.dss.2009.02.005

Hogarty, K. Y., Hines, C. V., Kromrey, J. D., Perron, J. M., & Mumford, A. K. R. (2005). The quality of factor solutions in exploratory factor analysis: The influence of sample size, communality, and overdetermination. *Educational and Psychological Measurement*, *65*(2), 202–226. https://doi.org/10.1177/0013164404267287

Holmes, T., & Scoones, I. (2000). Participatory environmental policy processes : experiences from North and South. In *IDS working paper* (Vol. 113). Retrieved from http://bases.bireme.br/cgi-bin/wxislind.exe/iah/online/?IsisScript=iah/iah.xis&src=google&base=REPIDISCA&lang=p&nextAction=lnk&exprSearch=4179&indexSearch=ID

Höne, K., & Eloff, J. H. P. (2002). What makes an effective information security policy? *Network Security*, *2002*(6), 14–16. https://doi.org/10.1016/S1353-4858(02)06011-7

Hone, K. S., & El Said, G. R. (2016). Exploring the factors affecting MOOC retention: A survey study. *Computers and Education*, *98*, 157–168. https://doi.org/10.1016/j.compedu.2016.03.016

Hoofnagle, C. J. (2007). Identity Theft: Making the Known Unknowns Known. *Harvard Journal of Law & Technology*, *21*. Retrieved from https://heinonline.org/HOL/Page?handle=hein.journals/hjlt21&id=101&div=7&collection=journals

Howe, D. A. (2003, January 22). *Total variance explained [in frequency stability]*. 1093–1099. https://doi.org/10.1109/freq.1999.841512

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing Employee Compliance with Information Security Policies: The Critical Role of Top Management and Organizational Culture. *Decision Sciences*, *43*(4), 615–660. https://doi.org/10.1111/j.1540-5915.2012.00361.x

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management. *Information Security Technical Report*, *13*(4), 247–255. https://doi.org/10.1016/j.istr.2008.10.010

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79. https://doi.org/10.1016/J.IM.2013.10.001

ISACA. (2018). *About ISACA*. Retrieved from https://www.isaca.org/about-isaca/Pages/default.aspx

ISO/IEC. (2013). ISO/IEC 27002:2013(E) Information technology — Security techniques — Code of practice for information security controls. In *Iso/Iec 27002:2013(E)*. Retrieved from https://www.iso.org/standard/54533.html

Jarvinen, P. H. (2000). *Research Questions Guiding Selection of an Appropriate Research Method*. Retrieved from http://aisel.aisnet.org/ecis2000/26

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. *MIS Quarterly*, *34*(3), 549–566.

Jones, N., McDavid, J., Derthick, K., Dowell, R., & Spyridakis, J. (2012). Plain language in environmental policy documents: An assessment of reader comprehension and perceptions. *Journal of Technical Writing and Communication*, *42*(4), 331–371. https://doi.org/10.2190/TW.42.4.b

Kaiser, H. F. (1970). A second generation little jiffy. *Psychometrika*, *35*(4), 401–415. https://doi.org/10.1007/BF02291817

Karabacak, B., & Sogukpinar, I. (2006). A quantitative method for ISO 17799 gap analysis. *Computers and Security*, *25*(6), 413–419. https://doi.org/10.1016/j.cose.2006.05.001

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security*, *67*, 267–279. https://doi.org/10.1016/J.COSE.2016.12.012

Kirlappos, I., Parkin, S., & Sasse, M. A. (2014). Learning from “Shadow Security”: Why

understanding non-compliant behaviors provides the basis for effective security. *Usec '14*, (February), 1–10. https://doi.org/10.14722/usec.2014.23<007>

Kirlappos, I., & Sasse, M. A. (2014). What usable security really means: Trusting and engaging users. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *8533 LNCS*, 69–78. https://doi.org/10.1007/978-3-319-07620-1_7

Knapp, K. J., Franklin Morris, R., Marshall, T. E., & Byrd, T. A. (2009). Information security policy: An organizational-level process model. *Computers & Security*, *28*(7), 493–508. https://doi.org/10.1016/j.cose.2009.07.001

Kruger, H. A., & Kearney, W. D. (2006). A prototype for assessing information security awareness. *Computers and Security*, *25*(4), 289–296. https://doi.org/10.1016/j.cose.2006.02.008

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L. F., Hong, J., & Nunge, E. (2007). Protecting people from phishing. *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems - CHI '07*, 905. https://doi.org/10.1145/1240624.1240760

Leach, J. (2003). Improving user security behaviour. *Computers and Security*, *22*(8), 685–692. https://doi.org/10.1016/S0167-4048(03)00007-5

Li, H., Sarathy, R., & Xu, H. (2011). The role of affect and cognition on online consumers' decision to disclose personal information to unfamiliar online vendors. *Decision Support Systems*, *51*(3), 434–445. https://doi.org/10.1016/J.DSS.2011.01.017

Liang, H., Xue, Y., & Pinsonneault, A. (2019). WHAT USERS DO BESIDES PROBLEM-FOCUSED COPING WHEN FACING IT SECURITY THREATS: AN EMOTION-FOCUSED COPING PERSPECTIVE Appendix A Summary of Past IT Security Research on PFC and EFC. *MIS Quarterly*, *43*(2). Retrieved from https://www.misq.org/skin/frontend/default/misq/pdf/appendices/2019/V43I2Appendices/02_14360_RA_LiangXueAppendices.pdf

Lim, J., Chang, S., Maynard, S., & Ahmad, A. (2009). Exploring the Relationship between Organizational Culture and Information Security Culture. *Australian Information Security*

Management Conference. https://doi.org/10.4225/75/57b4065130def

Liu, Y., & Zumbo, B. D. (2007). The impact of outliers on Cronbach's coefficient alpha estimate of reliability visual analogue scales. *Educational and Psychological Measurement*, *67*(4), 620–634. https://doi.org/10.1177/0013164406296976

Mataracioglu, T., & Ozkan, S. (2011). Governing Information Security in Conjunction with COBIT and ISO 27001. *ArXiv:1108.2150*. Retrieved from http://arxiv.org/abs/1108.2150

May, C. (2008). Approaches to user education. *Network Security*, *2008*(9), 15–17. https://doi.org/10.1016/S1353-4858(08)70109-0

Merete Hagen, J., Albrechtsen, E., & Hovden, J. (2008). Implementation and effectiveness of organizational information security measures. *Information Management & Computer Security*, *16*(4), 377–397. https://doi.org/10.1108/09685220810908796

Meyer, J. P., Allen, N. J., & Gellatly, I. R. (1990). Affective and Continuance Commitment to the Organization: Evaluation of Measures and Analysis of Concurrent and Time-Lagged Relations. *Journal of Applied Psychology*, *75*(6), 710–720. https://doi.org/10.1037/0021-9010.75.6.710

Michels, A., & De Graaf, L. (2010). Examining Citizen Participation: Local Participatory Policy Making and Democracy. *Local Government Studies*, *36*(4), 477–491. https://doi.org/10.1080/03003930.2010.494101

Muthuveloo, R., & Rose, R. C. (2005). Typology of Organisational Commitment. *American Journal of Applied Science*, *2*(6), 1078–1081.

Ng, B. Y., Kankanhalli, A., & Xu, Y. (Calvin). (2009). Studying users' computer security behavior: A health belief perspective. *Decision Support Systems*, *46*(4), 815–825. https://doi.org/10.1016/j.dss.2008.11.010

Nicholson, J., Coventry, L., & Briggs, P. (2019). Introducing the Cybersurvival Task: Assessing and Addressing Staff Beliefs about Effective Cyber Protection. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, (ACM), 433. Retrieved from https://www.usenix.org/conference/soups2018/presentation/nicholson

Norman, G. (2010). Likert scales, levels of measurement and the "laws" of statistics. *Advances in Health Sciences Education*, *15*(5), 625–632. https://doi.org/10.1007/s10459-010-9222-y

O'Driscoll, M. P., & Randall, D. M. (1999). Perceived organisational support, satisfaction with rewards, and employee job involvement and organisational commitment. *Applied Psychology*, *48*(2), 197–209. https://doi.org/10.1080/026999499377619

Odom, L., & Henson, R. (2002). Data screening: Essential techniques for data review and preparation. *Southwest Educational Research Association*, 1–37.

Olsson, U. H., Foss, T., Troye, S. V., & Howell, R. D. (2000). The performance of ML, GLS, and WLS estimation in structural equation modeling under conditions of misspecification and nonnormality. *Structural Equation Modeling*, *7*(4), 557–595. https://doi.org/10.1207/S15328007SEM0704_3

Orazi, D. C., Warkentin, M., & Johnston, A. C. (2019). Integrating Construal Level Theory in the Design of Fear Appeals in IS Security Research. *Communications of the Association for Information Systems*. Retrieved from http://aisel.aisnet.org/cais/.

Padayachee, K. (2012). Taxonomy of compliant information security behavior. *Computers and Security*, *31*(5), 673–680. https://doi.org/10.1016/j.cose.2012.04.004

Papadopoulos, Y., & Warin, P. (2007). Are innovative, participatory and deliberative procedures in policy making democratic and effective? The context of the growth of participatory and deliberative procedures in policy making. *European Journal of Political Research*, *46*, 445–472. Retrieved from https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1475-6765.2007.00696.x

Perugini, M., & Bagozzi, R. P. (2001). The role of desires and anticipated emotions in goal-directed behaviours: Broadening and deepening the theory of planned behaviour. *British Journal of Social Psychology*, *40*(1), 79–98. https://doi.org/10.1348/014466601164704

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. *Information and Management*, *51*(5), 551–567. https://doi.org/10.1016/j.im.2014.03.009

Posthumus, S., & von Solms, R. (2005). A responsibility framework for information security. *IFIP Advances in Information and Communication Technology*, *193*, 205–221. https://doi.org/10.1007/0-387-31167-x_13

Puhakainen, P., & Siponen, M. (2010). Improving Employees' Compliance Through Information Systems Security Training: An Action Research Study. *MIS Quarterly*, *34*(4), 757. https://doi.org/10.2307/25750704

Rajendran, S., & Shenbagaraman, V. M. (n.d.). A Comprehensive Review of the Applications of Protection Motivation Theory in Health Related Behaviors. *Journal of Chemical and Pharmaceutical Sciences*, *10*(1). Retrieved from www.jchps.com

Reinfelder, L., Landwirth, R., & Benenson, Z. (2019). Security Managers Are Not The Enemy Either. *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 1–7. https://doi.org/10.1145/3290605.3300663

Rhee, H. S., Kim, C., & Ryu, Y. U. (2009). Self-efficacy in information security: Its influence on end users' information security practice behavior. *Computers and Security*, *28*(8), 816–826. https://doi.org/10.1016/j.cose.2009.05.008

Rogers, R. W., & Prentice-Dunn, S. (1997). Protection motivation theory. Retrieved December 12, 2019, from D. S. Gochman (Ed.), Handbook of health behavior research 1: Personal and social determinants website: https://psycnet.apa.org/record/1997-36396-006

Rogers, R. W. (1975). Protection Motivation Theory Fear Appeals.pdf. *The Journal of Psychology*, *91*(91(1)), 93–114.

Rotter, J. B. (1966). Generalized expectancies for internal versus external control of reinforcement. *Psychological Monographs: General and Applied*, *Vol 80(1)*, 1-28.

Ruighaver, A. B., Maynard, S. B., & Chang, S. (2007). Organisational security culture: Extending the end-user perspective. *Computers and Security*, *26*(1), 56–62. https://doi.org/10.1016/j.cose.2006.10.008

Russo, J. E., & Chaxel, A. S. (2010). How persuasive messages can influence behavior without awareness. *Journal of Consumer Psychology*, *20*(3), 338–342. https://doi.org/10.1016/j.jcps.2010.06.005

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers and Security*, *53*, 65–78. https://doi.org/10.1016/j.cose.2015.05.012

Saint-Germain, R. (2005). Information security management best practice based on ISO/IEC 17799. *Information Management Journal*, *39*(4), 60–66. https://doi.org/10.1055/s-0031-1297364

Satorra, A. (1990, November). Robustness issues in structural equation modeling: a review of recent developments. *Quality and Quantity*, Vol. 24, pp. 367–386. https://doi.org/10.1007/BF00152011

Schlienger, T., & Teufel, S. (2003). Analyzing information security culture: increased trust by an appropriate information security culture. *14th International Workshop on Database and Expert Systems Applications, 2003. Proceedings.*, 405–409. https://doi.org/10.1109/DEXA.2003.1232055

Shaw, R. S., Chen, C. C., Harris, A. L., & Huang, H.-J. (2009). The impact of information richness on information security awareness training effectiveness. *Computers & Education*, *52*(1), 92–100. https://doi.org/10.1016/j.compedu.2008.06.011

Siponen, M, & Willison, R. (2009). Information security management standards: Problems and solutions. *Information and Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Siponen, Mikko, Adam Mahmood, M., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information and Management*, *51*(2), 217–224. https://doi.org/10.1016/j.im.2013.08.006

Siponen, Mikko, Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64–71. https://doi.org/10.1109/MC.2010.35

Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, *56*, 70–82. https://doi.org/10.1016/J.COSE.2015.10.006

Srivastava, A., Thomson, S. B., Barnett-Page, E., Thomas, J., Carroll, C., Booth, A., … Firth, J. (2009). Framework Analysis : A qualitative methodology for applied policy research. *BMC Medical Research Methodology*, *4*(2), 72–79. Retrieved from https://papers.ssrn.com/abstract=2760705

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124–133. https://doi.org/10.1016/j.cose.2004.07.001

Sumecki, D., Chipulu, M., & Ojiako, U. (2011). Email overload: Exploring the moderating role of the perception of email as a "business critical" tool. *International Journal of Information Management*, *31*(5), 407–414. https://doi.org/10.1016/j.ijinfomgt.2010.12.008

Tavakol, M., & Dennick, R. (2011, June 27). Making sense of Cronbach's alpha. *International Journal of Medical Education*, *2*, 53–55. https://doi.org/10.5116/ijme.4dfb.8dfd

Thomson, M. E., & Solms, R. von. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security*, *6*(4), 167–173. https://doi.org/10.1108/09685229810227649

Tobias, S., & Carlson, J. E. (1969). Brief report: Bartlett's test of sphericity and chance findings in factor analysis. *Multivariate Behavioral Research*, *4*(3), 375–377. https://doi.org/10.1207/s15327906mbr0403_8

Tsai, H. Y. S., Jiang, M., Alhabash, S., Larose, R., Rifon, N. J., & Cotten, S. R. (2016). Understanding online safety behaviors: A protection motivation theory perspective. *Computers and Security*, *59*, 138–150. https://doi.org/10.1016/j.cose.2016.02.009

Valentine, J. A. (2006). Enhancing the employee security awareness model. *Computer Fraud and Security*, *2006*(6), 17–19. https://doi.org/10.1016/S1361-3723(06)70370-0

Van Niekerk, J. F., & Von Solms, R. (2010). Information security culture: A management perspective. *Computers and Security*, *29*(4), 476–486. https://doi.org/10.1016/j.cose.2009.10.005

Vithanwattana, N., Mapp, G., & George, C. (2017). Developing a comprehensive information security framework for mHealth: a detailed analysis. *Journal of Reliable Intelligent*

Environments 2017 3:1, *3*(1), 21–39. https://doi.org/10.1007/S40860-017-0038-X

Von Solms, R., Thomson, K. L., & Maninjwa, P. M. (2011). Information security governance control through comprehensive policy architectures. *2011 Information Security for South Africa - Proceedings of the ISSA 2011 Conference*. https://doi.org/10.1109/ISSA.2011.6027522

Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. *Computers and Security*, *38*, 97–102. https://doi.org/10.1016/j.cose.2013.04.004

Warkentin, M., & Willison, R. (2009, April). Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems*, Vol. 18, pp. 101–105. https://doi.org/10.1057/ejis.2009.12

Weidman, J., & Grossklags, J. (2018). What's in your policy? An analysis of the current state of information security policies in academic institutions. *26th European Conference on Information Systems: Beyond Digitization - Facets of Socio-Technical Change, ECIS 2018*.

Whitman, M. E., Townsend, A. M., & Aalberts, R. J. (2001). Information Systems Security and the Need for Policy. In *Information Security Management* (pp. 9–18). https://doi.org/10.4018/978-1-878289-78-0.ch002

Willcoxson, L., & Millett, B. (2000). The management of organisational culture. *Australian Journal of Management & Organisational Behaviour*, *3*(2), 91–99.

Wilson, M., de Zafra, D. E., Pitcher, S. I., Tressler, J. D., & Ippolito, J. B. (2009). Information Technology Security Training Requirements: A Role- and Performance-Based Model. In *NIST Special Publication 800-16*. Retrieved from https://apps.dtic.mil/docs/citations/ADA391650

Workman, M., Bommer, W. H., & 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), 2799–2816. https://doi.org/10.1016/j.chb.2008.04.005

Wu, A. D., & Zumbo, B. D. (2008). Understanding and using mediators and moderators. *Social Indicators Research*, *87*(3), 367–392. https://doi.org/10.1007/s11205-007-9143-1

Xu, H., & Tracey, T. J. G. (2017). Use of multi-group confirmatory factor analysis in examining measurement invariance in counseling psychology research. *The European Journal of Counselling Psychology*, *6*(1), 75–82. https://doi.org/10.5964/ejcop.v6i1.120

Yeniman Yildirim, E., Akalp, G., Aytac, S., & Bayram, N. (2011). Factors influencing information security management in small- and medium-sized enterprises: A case study from Turkey. *International Journal of Information Management*, *31*(4), 360–365. https://doi.org/10.1016/j.ijinfomgt.2010.10.006

Youn, S., & McLeod, D. (2007). A comparative study for email classification. *Advances and Innovations in Systems, Computing Sciences and Software Engineering*, 387–391. https://doi.org/10.1007/978-1-4020-6264-3_67

Yuan, M., & Choudhary, R. (2020). A two-step clustering framework for locally tailored design of residential heating policies. *Sustainable Cities and Society*, *63*, 102431. https://doi.org/10.1016/J.SCS.2020.102431

Zhang, J., Reithel, B. J., & Li, H. (2009). Impact of perceived technical protection on security behaviors. *Information Management and Computer Security*, *17*(4), 330–340. https://doi.org/10.1108/09685220910993980

Zhiling Tu, C., Adkins, J., Yu Zhao, G., Zhiling, C., & Yu, G. (2019). Complying with BYOD Security Policies: A Moderation Model Based on Protection Motivation Theory. *Journal of the Midwest Association for Information Systems* |, (1). https://doi.org/10.17705/3jmwa.000045

Zimbardo, P. G., & Leippe, M. R. (1991). *The psychology of attitude change and social influence.* New York, NY, England: Mcgraw-Hill Book Company.