

https://dspace.org/

User compliance with the organisation's information security policy: a deterrence theory study

Fachin, Dario

2016

http://hdl.handle.net/10539/21795

Fachin, Dario (2016) User compliance with the organisation's information security policy: a deterrence theory study, University of the Witwatersrand, Johannesburg <http://wiredspace.wits.ac.za/handle/10539/21795>

Downloaded from a DSpace repository. https://dspace.org/



User compliance with the organisation's Information Security Policy: a deterrence theory study

MCom Information Systems
Research report
2015

Submitted by:

Dario Fachin
9810203H

Supervisor:

Prof. Ray Kekwaletswe

ABSTRACT

In today's age of increasing cyber-attacks, with even national governments interests forming cyber warfare departments to defend their countries, there is no company globally which cannot be prepared for their critical infrastructure or information to be stolen, destroyed, manipulated or be made unavailable from various cyber-attacks. In most organisations, the user of the Information Systems is vital to ensuring that systems are protected by adhering to the Information Security Policy. Failure to comply with the Information Security Policy by end users exposes the company to the risk of the loss of sensitive information which could have major reputational, legal and financial impacts.

The study followed a positivist research philosophy using a hypothetical model to test various hypotheses. Through the lens of deterrence theory, using a survey method to gather the information, the hypotheses are tested and analysed to further understand user compliance with an organisation's Information Security Policy.

The findings reveal that some elements of the deterrence theory are strong predictors to ensuring user compliance within a large global mining firm. The certainty of being caught for end users and the celerity of not adhering to the Information Security policy are strong predictors to ensure user compliance. The awareness of severity for not complying with the Information Security Policy or the awareness of being monitored is reflected to not be strong predictors to ensure user compliance. The research is intended to further assist both academics and practitioners to further their understanding of user compliance to the Information Security Policy.

KEYWORDS: Information Security Policy, Deterrence Theory, Compliance, Information Security, Employee.

Contents

Chapter 1: Introduction and background 5
1.1 Introduction to the field of study 5
1.2 Background to the research problem 6
1.3 Study location and context 7
1.4 Problem statement 7
1.5 Goal and Objectives 8
1.6 Significance of the study 10
1.7 Summary of the chapter 10
Chapter 2: Literature Review 11
2.1 Information Security Policy Defined 11
2.2 Review of the literature 11
2.2.1 Neutralisation theory & Deterrence Theory 11
2.2.2 Deterrence theory & Deindividuation theory 12
2.2.3 The Theory of Cognitive Moral Development by Kohlberg and the Theory of Motivational Types of Values by Schwartz 12
2.2.4 Theory of planned behavior, Social bond theory, social cognitive theory and Rational choice theory 13
2.2.5 Deterrence Theory (GDT); Protection Motivation Theory (PMT); Theory of Planned Behavior (TPB); Decomposed Theory of Planned Behavior (DTPB) and Organisational Commitment (OC). 13
2.2.6 The concept of “mandatoriness” 14
2.2.7 Deterrence Theory Research Papers 15
2.2.8 Deterrence Theory & Compliance Theory 15
2.2.9 Summary of reviewed literature 16
2.3 Summary of the Literature Review 22
Chapter 3: Theoretical framework, hypotheses and research model 23
3.1 Theoretical Framework 23
Chapter 4: Research methodology and design 29
4.1 Research Paradigm and approach 29
4.2 Quantitative research approach 29
4.3 Research Strategy 29
4.4 Research Design 30

4.4.1 Unit of Analysis, Participants, Sampling & Data collection techniques 30
4.4.2 The research instrument 31
4.4.3 Data Analysis 33
4.5 Ethics 34
4.5.1 Informed consent 34
4.5.2 Right to privacy 34
4.5.3 Informed protection of harm (Emotional) 34
Chapter 5: Data analysis and discussion of findings 35
5.1 Convergent and Discriminant Validity Results 35
5.2 Validity Results 37
5.3 Model Analysis 40
5.4 Test of Research Method 42
Chapter 6: Interpretation of findings 44
6.1 Discussion of findings 44
6.2 Implications for practice 49
6.3 Limitations of the study 50
Chapter 7: Evaluation of the research and conclusion 52
7.1 Introduction 52
7.2 Overview of the research 52
7.3 Research questions revisited 53
7.4 Relevance of the research methodology 54
7.5 Relevance of deterrence theory to the study 55
7.6 Recommendations for further studies 55
7.7 Reflection on the research study 56
7.8 Conclusion 57
Appendix A - Questionnaire 58
Appendix B: Literature Source Questions 63
References 65

Chapter 1: Introduction and background

1.1 Introduction to the field of study

The core element for any Information Security manager is the ability to manage risk. This is no small task in today's organisations with Information flowing from laptops, servers, tablets, smartphones etc. to the cloud, personal devices or local data centers. Protecting all Information within an organisation has become practically impossible and as such one attempts to protect the "keys to the kingdom" and furthermore tries to protect that exceptionally well. Once risk assessments have been performed, controls are generated to mitigate risk and policy and procedures begin to govern the process to ensure the risk is continually mitigated. This continued cycle of risk identification continues as technology advances and as threats identify new vulnerabilities. Policies become living documents and adapt as the risk landscape evolves.

Verizon, (2014) in their latest data breach investigations report, which obtains annual reports on security incidents and breaches from over 50 global organisations, shows how espionage, hacking, malware and social tactics all have an upward trend over the past 10 years. Ponemon Institute, (2013) examined the costs incurred by 54 U.S. companies in 14 industry sectors after those companies experienced the loss or theft of protected personal data and estimated the average cost of a data breach to be $5.4 Million. As more and more breaches occur, companies are constantly trying to protect and secure their confidential information. The upward trend in data theft and the cost of a data breach means companies need to protect their information and a key element to achieving this is the Information Security policy. The Information Security policy defines what the Information Security controls for an organisation should be and this research is to further understand through the lens of deterrence theory how compliance to the Information Security policy can best be achieved.

1.2 Background to the research problem

Information Security managers are tasked with protecting key information within an organisation and are therefore constantly trying to identify the best strategies to ensure that Information Security risk exposure is tolerable as possible. Information Security just like the rest of an organisation has limited resources and budget constraints with Information in general growing at an exponential rate. The researcher has observed that there is a continuous balancing act of implementing controls versus the identified vulnerabilities. The use of risk matrices, which have likelihoods and impacts, assist risk owners on their primary focus areas for risk closure. Key areas as observed by the researcher, which are risks for all risk owners, will form part of the Information Security policy and will be governed accordingly.

Practitioners use the Information Security policy to govern the organisation, but at the end of the day if one does not bring a piece of paper and give it life by implementing it, it will not be adhered to and the company will be put at risk. The conceptual model below will aim to further strengthen deterrence theory through the use of empirical evidence.

Chen et al., (2012) mention that Information Security cannot be solved by technology alone, and requires people and processes. Legislation is also dictating that controls are in place. As of 26 November 2013 in South Africa, the Protection of Personal Information (POPI) Act which is similar in nature to the data protection act in the United Kingdom, specifies in condition seven that reasonable Information Security measures need to be adhered too, which means companies in South Africa if they have personal information need to ensure that they use reasonable measures. Reasonable measures can be defined as industry best practice, such as ISO 27001 mentioned above, which includes the use of an Information Security policy.

D'Arcy & Herath, (2011) states that deterrence theory predicts that criminal behavior can be controlled by "the threat of sanctions that are certain, severe, and swift". This research will identify if the threats of disciplinary actions that are certain, sever and swift will control individual's behavior to comply with the Information Security Policy.

1.3 Study location and context

The challenges and issues within launching an effective Information Security function to reduce risk for the organisation in today's age is extremely challenging as there are continuous vulnerabilities being identified and threats are continually reinventing themselves in order to gain access to confidential and sensitive information. The research will occur within a global mining firm. A global mining firm just like any organisation needs to reduce its overall risk and the Information Security Policy is the governance mechanism to achieve this. The challenge of course is how to make compliance to the Information Security policy as effective as possible to ensure that risk is properly mitigated. As Information Security is everyone's responsibility and the old adage of you are only secure as your weakest link, illustrates the important of compliance to the Information Security policy.

1.4 Problem statement

Deterrence theory is to be used as a lens to understand how compliance to the Information Security Policy is achieved. If end users do not comply with the Information Security policy then the company will be put at risk at achieving its overall strategic objectives which could have financial, legislative and reputational damage to a company. The need to comply therefore is to ensure the overall Information Security risk within the company is managed. Poor compliance to the Information Security policy will enable attackers to take advantage of multiple vulnerabilities, which they will exploit for their own gain. To understand how compliance to the Information Security policy is achieved is therefore of great interest to practitioners to understand how end users ensure they comply to the Information Security policy. It will also help practitioners continue to understand what is the best approach for ensuring risk is mitigated through compliance to the Information Security policy.

This study contribution from an academic perspective is based on general deterrence theory to understand compliance to the Information Security policy, thus reducing the overall risk for the company. There is a gap within literature as far as this, and this research extends the body of knowledge in that it shows how deterrence theory – that is, awareness of severity and the awareness of end users knowing the policy is being monitored – may be used to explain compliance. The

systematic review of literature reveals inadequate literature within the compliance to the Information Security Policy, especially within a global mining environment. Using deterrence theory as a lens the study further bridges that gap.

1.5 Goal and Objectives

The goal of this research thesis was to develop a research model and test the effects of compliance to the Information Security policy for end users based on deterrence theory. The scope is a global mining firm from which this research thesis will be used to further explore the relevance of deterrence theory.

The research objectives are as follows:

- To determine if the extent of the severity ensures compliance to the Information Security Policy
- To determine if awareness of severity ensures compliance to the Information Security Policy
- To determine if certainty of being caught ensures compliance to the Information Security Policy
- To determine if awareness about monitoring occurring of the Information Security Policy ensures compliance
- To analyse if the celerity (swiftness) of sanctions determines compliance to the Information Security Policy

The research objectives above were established through data gathering using quantitative methods and to analyse the data using inferential analysis to establish causality to the research questions below and to further strengthen the use of deterrence theory. The literature was reviewed, and previous research models on the phenomena reviewed. A research model was then developed and extended from current literature. The research model was tested through a hypothetical model based on a real life scenario, followed by a questionnaire based on the scenario. The variables hypothesized were operationilsed based on current literature with a relevant instrument developed. Pre-testing and pilot testing was incorporated to assist with ensuring that face validity and content validity of constructs were maintained. The research instrument was distributed to a sample frame within the

global mining environment, the data was analysed and inferences were deduced around the causality of the hypotheses.

The study answered the following research questions:

- How does the severity of the disciplinary action affect compliance to the Information Security Policy?
- How does the higher the certainty of being caught for breaching the Information Security Policy affect compliance to the Information Security Policy?
- What is the effect of the quicker the disciplinary action occurring from a breach of the Information Security Policy affect compliance to the Information Security Policy?
- How does the higher awareness about the severity of the Information Security Policy effect compliance to the Information Security Policy
- How does the higher the awareness that monitoring about the Information Security Policy is occurring affect the compliance to the Information Security Policy

1.6 Significance of the study

The research model aims to further the study and practice of Information Systems in two ways, both academically and also in practical use. For academic purposes it provides empirical evidence on a global mining firm using deterrence theory as a main basis for the model. Darcy & Herath, (2011) mention that celerity was not included in the operational definition of deterrence theory in any of the IS deterrence research papers that they reviewed. This research paper discusses celerity, which furthers the study around celerity within deterrence theory.

From a practical point of view, the research paper will provide valuable insights into deterrence theory supporting the various hypotheses to further understand how end-users comply with the Information Security policy.

1.7 Summary of the chapter

This Chapter discussed the field of study, background to the research problem, the study location and the problem statement. Further to that the research study goals and objectives, research questions and finally the significance of the research paper were discussed.

The rest of the research report is arranged as follows: Chapter 2 will further explore within the literature the various theories around compliance to the Information Security Policy; Chapter 3 discusses the theoretical framework, hypotheses and research model; Chapter 4 discusses the research methodology, the analysis of the data and discusses the findings; Chapter 5 provides the data analysis; Chapter 6 provides an interpretation of the findings and Chapter 7 evaluates the research and provides the overall conclusion.

Chapter 2: Literature Review

The following chapter discusses the definition of the Information Security Policy and the contributions and shortcomings of past research related to conforming to the Information Security policy. All research papers reviewed are sourced from high quality journals.

2.1 Information Security Policy Defined

ISO 27001 is the industry best practice for Information security and was developed for protecting the company's information assets. Disterer, (2013) as per ISO 27001 defines the Information Security policy as providing "management direction and support for information security in accordance with business requirements and relevant laws and regulations."

2.2 Review of the literature

This sub-chapter is broken down into the various theories that are related to the Information Security Policy and discuss various theories related to user compliance to the Information Security Policy. Each is broken down into what the researcher(s) main objective of the research paper was and the key findings. The research papers forming this review of the literature are then presented in a summary table of the theories used, methods used, variables examined and limitations of reviewed literature. Lastly a summary is provided that discusses the various research papers to deterrence theory.

2.2.1 Neutralisation theory & Deterrence Theory

Siponen & Vance, (2010) in their research paper describe how neutralisation theory as opposed to deterrence theory provides a compelling explanation for Information Systems security policy violations and also describes how employees explain this behavior. The purpose of their study was to extend the theory from the main theory of deterrence theory to neutralisation theory. Siponen & Vance, (2010) try to prove that violations of IS security policies might not always best be explained by fear of sanctions due to neutralisation techniques. Neutralisation theory & Deterrence

Theory were used in their study. Siponen & Vance, (2010) found the following four key findings, namely:

- Neutralisation is a predictor of employees' intention to bypass IS security policies.
- Informal sanctions predicts intention, in the presence of neutralization, the effect of informal sanctions on intention is insignificant.
- Formal sanctions do not predict IS security policy violations.
- The report of the most common and important IS security violations

2.2.2 Deterrence theory & Deindividuation theory

D'Arcy & Herath, (2011) in their research paper aimed to perform a review of deterrence theory within IS security to further understand the different results often obtained through the use of deterrence theory. The purpose of the study was to assist with further understandings of the IS security domain to advance security management strategies. D'Arcy & Herath, (2011) found that if researchers are using deterrence theory they need to be cognisant of various contingency factors, which may influence their findings. Researches also need to ensure that the sanction constructs have been measured and their treatment. (E.g. Even "Shame" should be inclusive when looking at deterrence theory from an informal sanction perspective.) Lastly, D'Arcy & Herath, (2011) found that researchers should be aware of using generalized measures of deterrence constructs across a range of behaviors that be represented differently in the mind of end users.

2.2.3 The Theory of Cognitive Moral Development by Kohlberg and the Theory of Motivational Types of Values by Schwartz

Myyry et al., (2009) proposed a theoretical model that explains noncompliance in terms of moral reasoning and values to Information Security rules. Myyry et al., (2009) attempt to present a new theoretical model to prove employee compliance to the IS policies. Myyry et al., (2009) found that the model explains employee adherence to information security policies in some instances. (E.g. if an employee was given another person's password). In summary, Myyry et al., (2009) found the

following:

- “preconventional moral reasoning is positively related to both hypothetical and actual compliance. “
- “preconventional moral reasoning is positively related to both hypothetical and actual compliance in the given information security context. “
- “respondents who prioritize Openness to Change values (to follow their own intellectual and emotional interests) were less likely to follow the information security policy“

2.2.4 Theory of planned behavior, Social bond theory, social cognitive theory and Rational choice theory

Bulgurcu et al., (2010) in their research paper attempts to identify the antecedents of employee compliance with the Information Security policy. The research paper shows a theoretical explanation with empirical evidence for the impact of an employee’s beliefs about the consequences of compliance and noncompliance with the Information Security policy. Bulgurcu et al., (2010) found attitude, normative beliefs and self-efficacy influences an employee's compliance to the information security policy. Bulgurcu et al., (2010) also found Information security awareness influences a person’s attitude to comply with the information security policy.

2.2.5 Deterrence Theory (GDT); Protection Motivation Theory (PMT); Theory of Planned Behavior (TPB); Decomposed Theory of Planned Behavior (DTPB) and Organisational Commitment (OC).

Herath & Rao, (2009) develop an Integrated Protection Motivation and Deterrence model of security policy compliance, which is empirically tested. The purpose of their study was to evaluate the effect of organisational commitment on employee security compliance intentions. Hearth & Rao, (2009) found the following:

- “perceptions about the severity of breach, response efficacy and self-efficacy are likely to have a positive effect on attitudes towards security policies“
- “social influence has a significant impact on compliance intentions“

- “resource availability is a significant factor in enhancing self-efficacy, which is a predictor of policy compliance intentions “
- “A dual role is played by organisational commitment by impacting intentions directly as well as promoting a belief that employee actions have an effect on an organisation’s overall information security. “

2.2.6 The concept of “mandatoriness”

Boss et al., (2009) try to introduce the idea of 'mandatoriness' and try to see how this affects compliance to the information security policy. The purpose of the study In order to explain individual information security precaution taking behavior a model was created and empirically tested. Boss et al., 2009) found the following hypotheses tested are supported by the empirical evidence:

- “Specification of a set of security policies will be positively associated with the individual’s perceived mandatoriness of that set of security policies. “
- “Evaluation of compliance with security policies will be positively associated with the individual’s perceived mandatoriness of the established set of security policies. “
- “Perceived mandatoriness of an information security policy will be associated with an increased likelihood that individuals will take security precautions. “

The following hypotheses was found to be not supported:

- “Reward for compliance with security policies and procedures will be positively associated with the individual’s perceived mandatoriness of the established set of security policies. “

The following hypotheses was found to be partially supported:
“Perceived mandatoriness of an information security policy will mediate the relationship between the control elements (specification, evaluation, and reward) and security precautions taken. “

2.2.7 Deterrence Theory Research Papers

D’Arcy et al., (2009) This paper presents an extended deterrence theory model that combines work from social psychology, criminology and information systems. D'Arcy et al., (2009) created a model that suggests that user awareness of security countermeasures directly influences the perceived certainty and severity of organisational sanctions associated with IS misuse. D'Arcy et al., (2009) found perception of sanctions is more valid than the actual sanctions themselves. It was also found, based on evidence, that one’s morality defines the impact of perceptions for imposed sanctions.

2.2.8 Deterrence Theory & Compliance Theory

Chen et al., (2013) The interactions between punishment and reward for complying to the Information Security policy is examined. Chen et al., (2013) propose a research model in which coercive control and remunerative control is seen to ensure individuals adhere to the Information Security policy. Chen et al., (2013) identified:
“(1) Incorporates both punishment and reward for enforcing IS security policy
(2) Brings more attention to reward as a plausible strategy in the field of IS security. “

2.2.9 Summary of reviewed literature

The following table for all papers reviewed above describes the theories used, methods used, variables examined and their limitations:

Reference	Theories Used	Methods Used	Variables Examined	Limitations
Journal: MIS Quarterly: Topic: Neutralization: New insights into the problem of employee information systems security policy violations. Siponen & Vance, (2010)	Neutralisation theory & Deterrence Theory	Model was empirically tested through a hypothetical scenario method and obtained 395 responses. Three scenarios were created of which an individual would only have received one.	The following are applicable for Neutralization: • Defense of Necessity • Appeal to higher loyalties • Condemn the condemners • Metaphor of the ledger • Denial of injury • Denial of responsibility The following is based on the Intention to violate IS security policy: • Formal sanctions • Informal sanctions • Shame	The limitation is the sample size being from only 3 Finnish organisations and as such the study might not extend to other organisations. There is also a culture limitation to this study. The dependent variable being the use of intention raises the question of if intention is indicative of actual behavior. The individual might have already committed an IS security policy transgression and could have used neutralisation to answer the scenario question. The cross-sectional design of the study could limit the findings.

Reference	Theories Used	Methods Used	Variables Examined	Limitations
Journal: European Journal of Information Systems Topic: A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings D'Arcy & Herath, (2011)	Deterrence theory & Deindividuation theory	D'Arcy et al., 2011 searched major IS journals, two IS conference proceedings & three studies from non IS-journals to identify IS deterrence studies. The deterrence studies are based on classic deterrence theory with a key focus on certainty and severity with very little focus on celerity due to most research papers not looking at this. They also looked at contingency variables, methodological issues and lastly additional	**Contingency Variable:** Self-control CSE Moral beliefs Virtual Status Employee position **Methodological Issues:** Operational definitions of deterrence theory Objective vs perceptual sanction measurement Self vs other-referenced perceived sanction measures Fixed vs open values for perceived severity of sanctions Conceptual overlap among deterrence constructs	Not specifically mentioned in research paper.

Reference	Theories Used	Methods Used	Variables Examined	Limitations
		substantive issues in order to obtain their review results.	**<u>Additional substantive issues:</u>** Positive vs negative outcome variable Benefit portion of the rational decision process Severity of the behavior Generalizability of deterrence theory constructs	
<u>Journal:</u> European Journal of Information Systems. <u>Topic:</u> What levels of moral reasoning and values explain adherence to information security rules? An	The Theory of Cognitive Moral Development by Kohlberg and the Theory of Motivational Types of Values by Schwartz	The model was empirically tested through a set of hypothesis based on hypothetical and actual information security compliance using two populations and one scenario.	Hypothetical and actual information security compliance models tested against the following constructs: • Preconventioal reasoning • Conventional reasoning • Postconventional reasoning • Openness to change • Conservation	The study used only two populations and also only used one scenario.

Reference	Theories Used	Methods Used	Variables Examined	Limitations
empirical study. Myyry et al., (2009)				
Journal: MIS QUARTERLY Topic: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness Bulgurcu et al., (2010)	Theory of planned behavior, Social bond theory, social cognitive theory, Rational choice theory.	464 employees from a diverse set of companies were given a survey to obtain empirical results.	Constructs: Attitude toward compliance with Information security policy Normative beliefs Self-efficacy to comply Intention to comply	Limitations include the selection of the participant. The data were collected via a cross sectional manner which means the statistical data could have provided correlation rather than causation. The Information Security awareness was perception based which also could be a limitation.
Journal: European Journal of Information Systems	General Deterrence Theory (GDT); Protection Motivation Theory (PMT);	Herath & Rao, (2009) empirically test the theoretical model with a data set representing the	Punishment severity Detection certainty Perceived probability of security breach Perceived severity of security breach	The study did not consider reward systems as a means to promote policy compliance. Habits and time needed for task completed was also not done in this study.

Reference	Theories Used	Methods Used	Variables Examined	Limitations
Topic: Protection motivation and deterrence: a framework for security policy compliance in organisations Herath & Rao, (2009)	Theory of Planned Behavior (TPB); Decomposed Theory of Planned Behavior (DTPB); Organisational Commitment (OC).	survey responses of 312 employees from 78 organisations.	Security breach concern level Response efficacy Response cost Security policy compliance intention Security policy attitude Self-efficacy Subjective norm Descriptive norm Resource availability Organisational commitment	Limited geographic of the study with it being limited to western new york.
Journal: European Journal of Information Systems Topic: If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security Boss et al., (2009)	Created a new research model based on the concept of "mandatoriness"	Using a field survey as the data instrument, the hypotheses are developed and tested.	Specification Evaluation Reward Mandatoriness Precautions taken	Limited to a specific industry (health-care industry).
Journal: *Information*	Deterrence Theory	The model is tested on 269 computer users from eight	User Awareness of: Security policies Security Education,	(D'Arcy et al., 2009) found the following limitations: a single source for both dependent and independent

Reference	Theories Used	Methods Used	Variables Examined	Limitations
Systems Research Topic: *User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach* D'Arcy et al., (2009)		different companies. The results suggest that three practices deter IS misuse: "user awareness of security policies; security education, training, and awareness (SETA) programs and computer monitoring. "	Training, and Awareness (SETA) Programs Computer Monitoring Perceived certainty of Sanctions Perceived Severity of Sanctions IS Misuse intention	variables (This could introduce common method bias.) The use of misusing IS intention instead of actual behaviors. The measurement of misusing IS is limited to the specific hypothetical scenarios.
Journal: Journal of Management Information Systems Topic: Organisations' Information Security Policy Compliance: Stick or Carrot Approach? Chen et al., (2013)	Deterrence Theory & Compliance Theory	A Web-based field experiment involving real-world employees in their natural settings was used to empirically test the model.	Punishment Reward Certainty of control These three variables then have hypotheses to compliance intention	Study was limited to two financial institutions. The data was collected in a cross-sectional manner and therefore common method bias could be a limitation.

2.3 Summary of the Literature Review

In summary for the above survey of the literature it shows there is various support for deterrence theory when it comes to compliance to the Information Security Policy. Siponen & Vance, (2010) finds neutralization theory to further explain areas where they feel deterrence theory is unable to explain why individuals do not adhere to the Information Security policy. Neutralisation according to Siponen & Vance, (2010) is a predictor of employees' intention to bypass IS security policies. D'Arcy et al., (2009) found perception of sanctions more valid than the actual sanctions themselves which strengthens the sanctions (severity) pillar of deterrence theory but specifically looks at the perceptions and not the actual sanctions itself.

Some of the studies extend past deterrence theory for example Chen et al., (2013) who look into reward (as opposed to the consequences factor) as does Boss et al., (2009). They try and investigate the other side of the coin and see how a positive approach to compliance is perceived. Hearth et al., (2009) bring in other elements such as the social influence to compliance and resource availability for enhancing self-efficacy, being a predicator of policy compliance intentions. The literature has elements of deterrence theory and also in other areas that extend over and above the remit of deterrence theory. An unexplored area identified within this research through examining the literature is extending this research within a global mining firm to see the relevance of deterrence theory. This research will also extend deterrence theory to the awareness of severity and the awareness of end users knowing that policy is being monitored and how these two items will have an effect on compliance to the Information Security Policy.

Chapter 3: Theoretical framework, hypotheses and research model

3.1 Theoretical Framework

Most studies from the existing literature on the phenomena on Information Security policy have used deterrence theory as the underpinning theory/theoretical framework, which aims at achieving deterrence through the use of sanctions.

Within the use of deterrence theory it has been established that there has been disparate findings. While trying to understand the disparate findings within the use of deterrence theory, D'arcy & Herath, (2011) state the use of certain contingency variables, methodological issues and additional substantive issues in order to assist researchers when using deterrence theory (Figure 1a) to make their research more compelling. Alternate theories to deterrence theory also exist and Siponen & Vance, (2010) clearly show that deterrence theory when an individual invokes neutralisation theory (a theory from criminology) makes the use (or threat) of sanctions irrelevant. Herath & Rao, (2009) also expand further on general deterrence theory to further understand compliance to Information Security policies through mainly the use of the theory of planned behavior. Boss et al., (2009) show that when people are being monitored and the idea of 'mandatoriness' occurs they are more likely to adhere to the Information Security policy and also that being rewarded would not necessarily make an end-user adhere to the Information Security policy. D'Arcy et al., (2009) further go on to show that Information Security awareness programmes also assist with compliance to the Information Security policy. Bulgurcu et al., (2010) concluded the same result about Information Security awareness increasing compliance to the Information Security policy. D'Arcy et al., (2009) also show that the perceived severity of sanctions is actually more effective than the actual sanctions themselves. Tell the reader how deterrence theory is appropriate for the study and how it has been used previously in IS studies

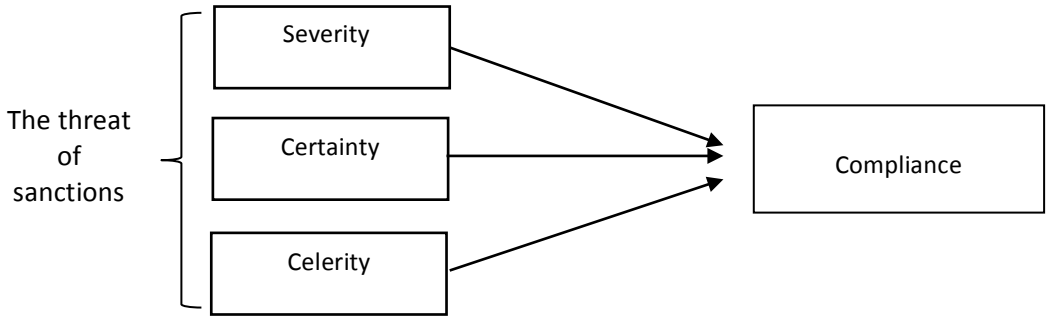


Figure 1a: Deterrence Theory

The conceptual model presented below (Figure 1) will be based on deterrence theory, as described by Ugrin & Pearson, (2010) and Herath & Rao, (2009). In order to govern the much needed security controls within an organisation, the Information Security policy is a key element to assist with the overall governance to provide guidance to employees, IT infrastructure teams and IT applications on what should and should not be allowed within the Information Security remit. As mentioned by Herath & Rao, (2009), trying to understand what issues relate to information security behaviors, for instance what motivates individuals to comply with security measures can be observed through the lens of theories borrowed from other disciplines, namely psychology, sociology, and criminology. An influence within deterrence theory is mentioned by Diiulio, (1959) cited from Bosworth, (2005), in which the general population would adhere to local laws through deterrence theory. In this instance the general population are the employees of the company and the local laws are defined in Information Security policy for the company. Ugrin & Pearson, (2010) also mention that from a criminological theory perspective it is suggested that deterrence mechanisms (e.g. sanctions and monitoring) can reduce overall illicit behavior.

Bosworth, (2005) mentions that “people choose to obey or violate the law after calculating the gains and consequences of their actions” and in the case of the Information Security policy, which is the law that governs Information Security within an organisation, it defines the lines of which an individual would have to debate if the gains of breaking the “law” would outweigh the proposed disciplinary actions (consequences) if using deterrence theory.

Bosworth, (2005) identified there to be three key components for deterrence theory as found from the early works of classical philosophers of which deterrence theory is based upon such as “Thomas Hobbes (1588–1678), Cesare Beccaria (1738–1794), and Jeremy Bentham (1748–1832)”. The three key components are severity, certainty and celerity of deterrence theory (Figure 1a). In an Information security context, this would mean for a rational individual there would have to be severe (I.e. Human Resources first warning, second warning and finally termination of the employee contract), you would have to be caught breaking the Information Security policy (certainty) and disciplinary action would have to be quick (celerity) in order to discourage an individual from breaking the “law” – namely the Information Security policy in this context.

The key constructs of this conceptual model will be based on these three key components from deterrence theory and it will be empirically tested within a global mining organisation to ascertain if the theory as per the identified hypotheses shows causality through empirical evidence.

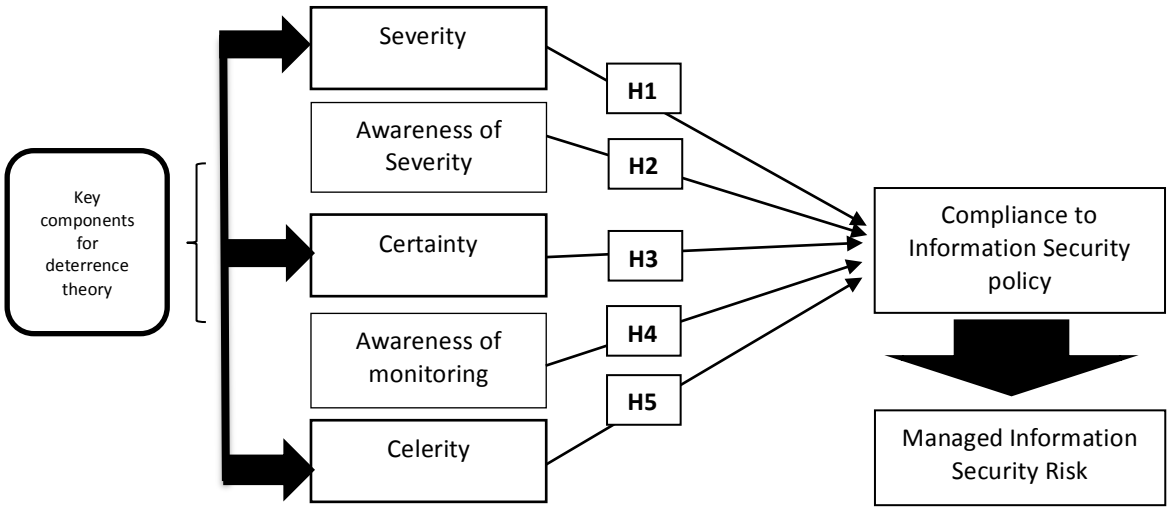


Figure 1: Conceptual Model

The above conceptual model (Figure 1) covers deterrence theory (Severity, Certainty and Celerity) and also provides an extension of the theory by empirically testing the conceptual model at a global mining organisation. The hypotheses

based on the conceptual model could all potentially be falsifiable and the empirical evidence will either prove strong causal reasoning which will either strengthen deterrence theory or prove otherwise. Awareness of severity and awareness of monitoring through empirical evidence will either further push the need for increased awareness of the severity if one does not adhere to the Information Security policy and also potentially the increased need for monitoring and the awareness that monitoring is occurring.

If, within the Information Security policy, it is clearly stated that confidential information must be encrypted before being sent out of the organisation then every rational employee would be aware that sending out unencrypted confidential information would be a breach of the Information Security policy and that to do so would mean that disciplinary actions (sanctions) would be imposed if caught. If every rational employee understands the policy and also realises that there will be disciplinary action, then they should be deterred from committing the breach of the policy.

H1: *The severity of the disciplinary action would be positively associated with an end-user complying with the Information Security policy.*

Organisations generally follow the disciplinary route of having a first and second warning before an official written warning is given which will then lead ultimately to dismissal. An Information Security policy might well be on the organisations portal but in most cases the disciplinary actions are not made publicly aware to all employees and the hypotheses here is to identify if the disciplinary actions are well known will there be a higher positive correlation with compliance to the Information Security policy.

H2: *The awareness of the severity would be positively associated with an end-user complying with the Information Security policy.*

H2 is supported by D'Arcy et al., (2009) who found perception of sanctions to be positively supported.

Deterrence theory is also quite clear that individuals would need to be well aware that if they commit a crime that they will be caught. If in the example above an end-user knows that they can send out confidential information and that nobody is watching or enforcing the Information Security policy, they will soon realise that they can get away with breaching the Information Security policy. This would mean that there would have to be a strong link to monitoring of the security policy to ensure it is enforced so that end-users are well aware that should they choose to breach the Information Security policy they will be reprimanded.

H3: *The certainty of an end-user breaching the Information Security Policy would be positively associated with an end-user complying to the Information Security Policy.*

As part of the certainty that an end-user would have to comply with the Information Security policy would also have to be directly linked to the awareness that an end-user would actually be fully aware of the fact that they are being continuously monitored to identify if they are indeed in breach of the Information Security policy.

H4: *The awareness of the certainty of an end-user breaching the Information Security policy would be positively associated with an end-user complying to the Information Security policy.*

Bulgurcu et al., (2010) found a positive relationship between Information security awareness influences a person's attitude to comply with the information security policy, which should support H4. Boss et al., (2009) also shows that when people are being monitored they are more likely to adhere to the Information Security policy, which should support H4.

Celerity, which is the swiftness of enforcing the policy and the proposed disciplinary action would ensure that individuals are deterred from breaching the Information

Security policy. If an end-user breached the policy and sent out a confidential document and immediately a data loss prevention tool flagged this to the end-user as a breach of policy and the Information Security manager to action a warning, they would have instant celerity that they had committed an offence.

H5: *The quicker the end-user is informed of the offence committed against the Information Security policy the more the positive association with an end user complying with the Information Security policy will be.*

Hu et al., (2011) tested celerity within their research paper and found no significant impact. Celerity in general within general deterrence theory and Information Security policy compliance has had limited testing in the field and this research paper will hopefully deepen the literature on this front.

Chapter 4: Research methodology and design

4.1 Research Paradigm and approach

Bhattacherjee, (2012) defines positivist research as using laboratory experiments or survey research in order to test theory through hypotheses. This research paper will follow the positivist research method as it aims to test theory through hypotheses. Bhattacherjee, (2012) further mentions that a positivist method uses a deduction approach, starting with theory and then testing the theory based on empirical data.

Lee, (1991) states the positivist approach "involves the manipulation of theoretical propositions using the rules of formal logic and the rules of hypothetico-deductive logic." For deductive testing of theories for MIS case studies Lee, (1989) describes the process that the proposed theory must be "(a) falsifiable, (b) logically consistent, (c) more predictive than other theories, and (d) not falsified by the tests it experiences." This method is the same scientific methodology as the natural sciences and the positivist approach will be the method applied to this research.

4.2 Quantitative research approach

This research was used to test deterrence theory using quantitative methods and inferential analysis. As per Bhattacherjee, (2012) inferential analysis is the statistical testing of hypotheses.

4.3 Research Strategy

As per Siponen & Vance, (2010), Myyry et al., (2009) and Chen et al., (2013) a hypothetical model based on a scenario was used to test the above hypotheses. Siponen & Vance, (2010) state that this is also known as a vignette or policy capturing method. The vignettes "present subjects with written descriptions of realistic situations and then request responses on a number of rating scales that measure the dependent variables of interest" as cited by Trevino (1992) from Siponen & Vance, (2010).

4.4 Research Design

The research design followed was a hypothetical scenario method using a survey design following a similar approach to the research design to Siponen & Vance, (2010) while using a hypothetical model based on scenarios Siponen & Vance, (2010).

4.4.1 Unit of Analysis, Participants, Sampling & Data collection techniques

The population or unit of analysis for this research was an individual (the employees) within a global mining firm. The sampling frame (participants) was a list of employees (448) with contact information within a global mining firm. As this is a global mining firm, multi-stage sampling was used, namely cluster sampling and then simple random sampling. Cluster sampling was initially used in order to cluster the areas first into geographic areas. Once the areas were clustered into geographic areas, in this case the geographic areas were per country followed by simple random sampling. Bhattacherjee, (2012) defines simple random sampling as having all possible subsets of the sampling frame being given an equal probability of being selected. This means that for each country (from the cluster sampling), the sample frame (list of employees) will all have had an equal probability of being chosen. The cluster sampling was limited to three countries on different continents and the simple random sampling per cluster was limited, so in total the sample frame was 448 individuals of which 121 were the final amount of respondants. Bhattacherjee, (2012) defines sampling as the statistical process of selecting a sample of a population of interest for making observations and statistical inferences about that population. This sample was then used to generalise about the rest of the organisation and the mining industry in general. The sample frame completed an online questionnaire upon which the data was collected and analysed.

4.4.2 The research instrument

The research instrument was therefore a cross-sectional structured questionnaire based on specific hypothetical scenarios (See Appendix A). The questionnaire used closed-ended structured questions (See Appendix A). Scale items were used from previous research papers as far as possible as they would have been pre-validated. Content validity Bhattacherjee, (2012) being an assessment of how well a set of scale items matches with the domain of the construct was ensured for constructs where scale items have already been used. The proposed measurements occurred on an 11-point scale from 0 to 10 and operationalised all variables Siponen & Vance, (2010) in the conceptual model. Celerity, was a new construct that did not have previous scale items and also used an 11-point scale to keep it consistent with the other.

The compliance to the Information Security policy, being the dependent variable, was measured using a single item based on Siponen & Vance, (2010) which they adapted from Paternoster & Simpson, (1996). The single item would be, “What is the chance that you would do what the individual in the described scenario did?” This measurement would still occur on an 11-point scale, ranging from 0 (no chance at all) to 10 (100% chance). Siponen & Vance, (2010) identified a reliability threat using this single measure through Cook & Campbell, (1979) but Siponen & Vance, (2010) also found through Straub et al., (2004) in some cases a single measure is the most appropriate and thus the same was used in this research.

Weber, (1992) states in citing Cavanagh & Fritzsche, (1985) that to use complex, multidimensional issues that reflect real world decision making, scenarios are a preferable choice. This compelling evidence in the literature has further strengthened the use of a scenario for this research.

In order to identify if the scenario appears to be based on a potential real life scenario, an added question was added to see if individuals feel that the scenario in question could be a potential real situation. This is important to ensure the validity of the scenario. Respondents who found the scenario to be unrealistic were removed from the study as individuals would probably not respond correctly to the questions as per Paternoster & Simpson, (1996).

Following Chen et al., (2012) control variables have been chosen namely age, location, gender, and education. Employee position D'arcy & Herath, (2011), which has been identified as relevant to complying with the Information Security Policy, was also included. D'arcy & Herath, (2011) include employee position, in furthering deterrence theory research papers, mentioning that based on an individual's role within the organisation will mean different reactions to sanctions. The random assignment in the sampling frame will ensure bias can be eliminated as much as possible. The scenario and items based on the constructs below were taken directly from the source cited (Appendix B), except for the celerity construct. The questionnaire that will be used can be found below in Appendix A.

Pre-testing of the questionnaire was given to a convenience sample limited to academics and also to two Information Security managers to ensure face validity. At this point some adjustments were made to the final questionnaire (See Appendix A). This pretesting as stated by Bhattacherjee, (2012) was able to uncover ambiguity, lack of clarity and biases in the wording of the questions. All items identified were adjusted before the sample frame was administered with the final questionnaire. Once the pre-testing of the questionnaire was completed, a pilot test occurred. The pilot test would have detected any issues with the research design and the instrumentation Bhattacherjee, (2012). The pilot test further ensures that the measurement instruments are reliable and valid measurements of the constructs. The pilot sample was a small subset of the target population Bhattacherjee, (2012) and was therefore limited to one geographic region of eight random individuals. The pilot then proceeded with no issues identified. The pre-testing and pilot test ensured that face validity and content validity of constructs were valid and was ready for deployment to the rest of the sample frame. The remaining sample frame once the pilot was completed and found to be successful received the questionnaire for completion and was submitted to over 448 respondents over three countries of which 121 individuals responded which was a sufficient amount of individuals for this research.

4.4.3 Data Analysis

In order to understand the methods and statistical techniques used for demonstrating scale reliability, convergent validity and discriminant validity one needs to first understand the definitions of the terms mentioned. A construct is an abstract concept such as a person's height or a set of related concepts such as person's attitude, which could have several underlying concepts such as culture, personality, education etc. If we were looking at a person's height then the scale reliability would mean that the scale we would be using would need to be consistent or dependable to ensure that scale reliability is achieved. The use of a tape measure would ensure that consistently a person's height would be correct. Bhattacherjee, (2012) defines convergent validity as "the closeness with which a measure relates to (or converges on) the construct that it is purported to measure" and mentions that discriminant validity is "the degree to which a measure does not measure (or discriminates from) other constructs that it is not supposed to measure."

Scale reliability for each constructs measurement would be assessed using Cronbach's α (ensuring internal consistency) and convergent and discriminant validity will be assessed using principal components analysis Siponen & Vance, (2010). In the pre-test phase measurement items with unacceptably low Cronbach's α will be rephrased or disregarded.

All scales will be kept to the original scales already found to be valid and reliable in past research papers. Celerity, however, is a new variable and will not have been tested for reliability and will therefore be tested using Cronbach's α and will be tested to ensure the alpha values exceeds the recommended minimum value of 0.7. Nunnally, (1978).

The theoretical model will be analysed using partial least squares (PLS) which was the same approach used by Siponen & Vance, (2010) outlined by Gefen & Straub, (2005). As per Siponen & Vance, (2010) an additional test of convergent validity used by Fornell & Larcker, (1981) is that the "average variance extracted (AVE), which is a measure of variance explained by a latent construct for the variance observed in its measurement items, should be at least .50 or higher". This test will

assist with establishing convergent validity.

4.5 Ethics

4.5.1 Informed consent

The selected individuals (identified as the sample frame) were invited to participate through completion of a web-based survey via a one page introductory e-mail.

4.5.2 Right to privacy

The letter explained the purpose of their participation and respondents were assured of the confidentiality and anonymity of their responses and that the data are purely to be used for academic research and will not impact their work in any manner.

4.5.3 Informed protection of harm (Emotional)

No individual is mentioned in this final research report and the results are reported in aggregate. Potential respondents were informed that participation is voluntary, that they could withdraw from participating at any time and lastly that there is no gain or loss of benefits should they choose not to participate. Individuals who did not respond were sent a follow-up e-mail to invite them to participate or contacted telephonically. Ethics approval was obtained for this research proposal.

Chapter 5: Data analysis and discussion of findings

5.1 Convergent and Discriminant Validity Results

In order to understand the methods and statistical techniques used for demonstrating scale reliability, convergent validity and discriminant validity one needs to first understand the definitions of the terms mentioned.

Bhattacherjee, (2012) defines reliability as “the degree to which the measure of a construct is consistent or dependable.” A construct is an abstract concept such as a person’s height or a set of related concepts such as person’s attitude, which could have several underlying concepts such as culture, personality, education etc. If we were looking at a person’s height then the scale reliability would mean that the scale we would be using would need to be consistent or dependable to ensure that scale reliability is achieved. The use of a tape measure would ensure that consistently a person’s height would be correct. Bhattacherjee, (2012) defines convergent validity as “the closeness with which a measure relates to (or converges on) the construct that it is purported to measure” and mentions that discriminant validity is “the degree to which a measure does not measure (or discriminates from) other constructs that it is not supposed to measure.” As per Siponen & Vance, (2010), convergent validity is illustrated when all indicators load significantly on their latent construct.

	Awareness of Monitoring	Awareness of Severity	Celerity	Certainty	Compliance to the Information Security Policy	Realism	Severity
AOM1	0.8466						
AOM2	0.8569						
AOM3	0.8071						
AOM4	0.84						
AOM5	0.7144						
AOM6	0.6415						
AOM7	0.738						
AOS1		0.8761					
AOS2		0.9264					
AOS3		0.716					
C1			0.6808				
C2			0.9147				
C3			0.9236				
CE1				0.7969			
CE2				0.8119			
CE3				0.8892			
CISP1					0.8983		
CISP2					0.8974		
CISP3					0.8278		
R1						1	
SE1							1

Figure 2: Outer Loadings Results

Convergent and discriminant validity was assessed using principal components analysis Siponen & Vance, (2010). Items far below < 0.6 were removed (e.g. SE2 and SE3) and the model was rerun. As per Figure 2: Outer Loadings Results, all items load onto expected constructs at values above the recommended 0.7 Wong, (2013) or higher (therefore achieving convergent validity) except for AOM6, which is at 0.6415 but is still within limits (i.e. > 0.6) for a survey design. This indicates indicator reliability. Items load onto expected constructs at values above 0.7, except AOM6, (therefore convergent validity) and do not cross-load highly on other constructs (therefore discriminant validity is achieved).

5.2 Validity Results

	AVE
Awareness of Monitoring	0.6107
Awareness of Severity	0.7128
Celerity	0.7177
Certainty	0.6949
Compliance to the Information Security Policy	0.7658
Realism	1
Severity	1

Figure 3: Average Variance Extracted (AVE)

As per Siponen & Vance, (2010) an additional test of convergent validity used by Fornell & Larcker, (1981) is that the “average variance extracted (AVE), which is a measure of variance explained by a latent construct for the variance observed in its measurement items, should be at least .50 or higher”. This test will assist with establishing convergent validity. All constructs from the model (See figure 3: AVE) are greater than .50. Therefore all constructs establish convergent validity.

	Awareness of Monitoring	Awareness of Severity	Celerity	Certainty	Compliance to the Information Security Policy	Realism	Severity
Awareness of Monitoring	**0.7815**						
Awareness of Severity	0.5147	**0.8443**					
Celerity	0.4693	0.3895	**0.8472**				
Certainty	0.6733	0.7438	0.4024	**0.8336**			
Compliance to the Information Security Policy	-0.1909	-0.1729	0.0618	-0.29	**0.8751**		
Realism	0.2067	0.0352	0.2329	0.1351	0.1029	**Single item construct**	
Severity	-0.3565	-0.6695	-0.3211	-0.657	0.1844	-0.096	**Single item construct**

Figure 4: Discriminant Validity

Fornell & Larker, (1981) suggest that the “square root” of AVE of each latent variable should be greater than the correlations among the latent variables Fornell & Larker, (1981). For all items in bold in Figure 4: Discriminant Validity, this number is larger than the correlation values in the column of “Awareness of monitoring” (0.7815) and also larger than those in the row of “Awareness of Monitoring”. A similar observation is also made for the remaining latent variables. The result therefore indicates that discriminant validity is well established.

	Cronbachs Alpha
Awareness of Monitoring	0.8979
Awareness of Severity	0.7948
Celerity	0.8088
Certainty	0.8179
Compliance to the Information Security Policy	0.8473
Realism	1
Severity	1

Figure 5: Cronbach alpha figures

Scale reliability for each constructs measurement would be assessed using Cronbach's α (ensuring internal consistency). All constructs from the model (see figure 5 – Cronbach alpha figures) are above the recommended 0.7 as stated by Nunnally, (1978). This indicates internal consistency reliability. Celerity is a new variable and was tested for reliability using Cronbach's α and as per the above was 0.8088 which values exceed the recommended minimum value of 0.7 as stated by Nunnally, (1978).

Latent Variable	Indicator	Loadings	Indicator reliability (i.e loading squared)	Cronbach's Alpha	AVE
Awareness of Monitoring	AOM1	0.84661	0.7168	0.8979	0.6107
	AOM2	0.8569	0.7343		
	AOM3	0.80706	0.6513		
	AOM4	0.83999	0.7056		
	AOM5	0.71444	0.5104		
	AOM6	0.64154	0.4116		
	AOM7	0.738	0.5446		
Awareness of Severity	AOS1	0.87611	0.7676	0.7948	0.7128
	AOS2	0.92641	0.8582		
	AOS3	0.71603	0.5127		
Celerity	C1	0.68075	0.4634	0.8088	0.7177
	C2	0.9147	0.8367		
	C3	0.92361	0.8531		
Certainty	CE1	0.79687	0.6350	0.8179	0.6949
	CE2	0.81186	0.6591		
	CE3	0.88917	0.7906		
Compliance to the Information Security Policy	CISP1	0.89833	0.8070	0.8473	0.7658
	CISP2	0.89739	0.8053		
	CISP3	0.82776	0.6852		
Realism	R1	1	1.0000	1	1
Severity	SE1	1	1.0000	1	1

Table 1: Results summary for reflective outer models

As per table 1, this is a summary outline of the external loadings, indicator reliability, cronbach's alpha and the AVE. As described previously all items are within their recommended or minimum levels. The results of the above tests demonstrate that our model meets or exceeds the rigorous standards expected for positivist IS research Straub et al. (2004).

5.3 Model Analysis

Barclay et al., (1995) indicates that a rule for determining minimum sample size would be 10 multiplied by X number. (X would be the number of indicators for the exogenous latent variable). This is known as the 'rule of 10'. Accordingly, 70 would be a minimum sample size for this study - being 10 x 7 items the highest number of indicators for the exogenous latent variable (See Figure 6: PLS-SEM Results Awareness of monitoring) being seven.

The survey was sent to over 448 individuals, of whom the response rate received was 121 responses, which is a response rate of 23%. This means that on average one in five respondents would reply and complete the survey and the survey results are above the minimum sample size of 70. 60% of the respondents were male (which is reflective of the population in the mining industry with traditionally more males than females), approximately 35% of the population was female and the rest preferred not to provide their gender. The majority of the respondents (84%) were below the age of 54 years old with 35% of respondents in the 35-44 category. There were less than 1% of the respondents in the 65-74 categories, which is to be expected due to the normal retirement age of 65. The response rate from the various countries, Canada, Europe and South Africa was 16%, 20% and 64% respectively. This is reflective of the fact that there is a larger base of individuals in the southern hemisphere and also during the survey a lot of individuals in the northern hemisphere were on summer holidays during this time period. From an education perspective, 60% of the respondents had a degree (associate to doctorate with the bulk, 66% having a bachelor degree.) This indicates that over half of the sample population who responded would have attended a tertiary university institute. Of the total sample size there was a representation of 18% from senior management, with

the majority, 46%, being lower level management or from supervisor level.

In the study performed by Siponen & Vance, (2010), using a hypothetical scenario they found that the password scenario had the highest realism within the respondents and as such a similar hypothetical scenario was used within this research study. The scenario provided to the respondents was rated as 8.09 (this was for the average score for realism on an 11-point scale of 0 to 10), which illustrated that the sample indicated that the scenario was realistic for participants. For the question “There is a high chance that you would do what the individual in the described scenario did” an average score of 2.44 (on a scale of 0 to 10) showing many individuals indicated they would not perform what the individual in the scenario did.

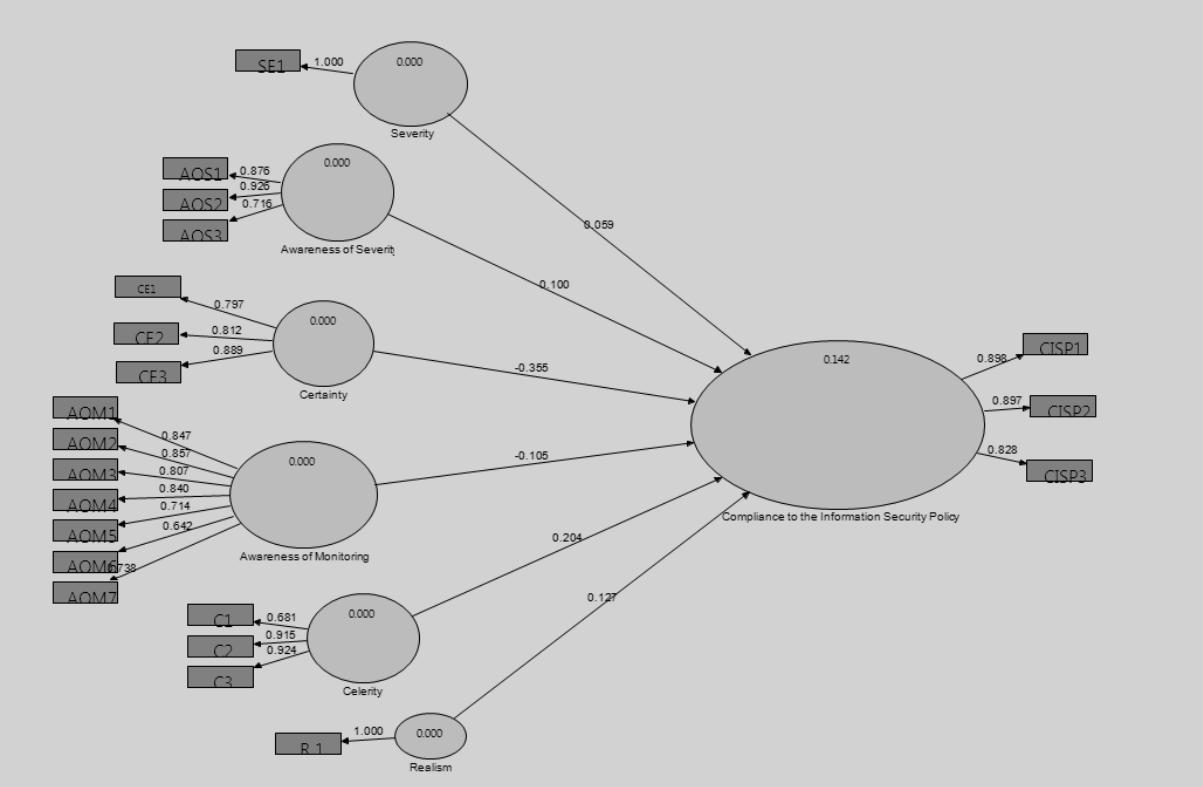


Figure 6: PLS-SEM Results

As per Figure 6, the coefficient of determination of, R2 is 0.142 for the compliance to the Information Security construct. The six latent variables therefore explain 14% (0.142028) of the variance.

The inner model suggests that Certainty (β=0.355, p ≤ 0.05) has the strongest effect on compliance to the Information Security and is statistically significant (i.e. the null hypotheses for H3 is rejected) followed by Celerity (β=0.204, p< 0.13).

H3 and H5 hypotheses path relationships are all statistically significant as the "standardized" path coefficient should be larger than 0.20, Wong, (2013), however H1, H2 & H4 are not statistically significant. The standardised path coefficient for Awareness of severity, Severity and Awareness of monitoring are 0.100, 0.059 & 0.105 respectively. It can therefore be concluded that Certainty (H3) and Celerity (H5) are strong predictors of compliance to the Information Security Policy but Severity, Awareness of severity and awareness of monitoring do not predict compliance to the Information Security Policy directly.

Analysis of the stop criterion changes shows that the algorithm converged after 7 iterations, which mean the data are normal, and did not require further investigation.

5.4 Test of Research Method

	T Statistics
Awareness of Monitoring -> Compliance to the Information Security Policy	0.7339
Awareness of Severity -> Compliance to the Information Security Policy	0.6308
Celerity -> Compliance to the Information Security Policy	1.4971
Certainty -> Compliance to the Information Security Policy	1.9147
Realism -> Compliance to the Information Security Policy	1.4352
Severity -> Compliance to the Information Security Policy	0.3911

Table 2: T-Statistics of Path Coefficients (Inner Model)

The path coefficient is not significant for any of the constructs in Table 2 as they are all below 1.96. The closest item to the 1.96 is the construct "certainty" which is at 1.9147 followed by Certainty at 1.49.

	T Statistics
AOM1 <- Awareness of Monitoring	4.3116
AOM2 <- Awareness of Monitoring	4.005
AOM3 <- Awareness of Monitoring	3.602
AOM4 <- Awareness of Monitoring	3.5384
AOM5 <- Awareness of Monitoring	3.4642
AOM6 <- Awareness of Monitoring	2.8139
AOM7 <- Awareness of Monitoring	3.9299
AOS1 <- Awareness of Severity	3.9218
AOS2 <- Awareness of Severity	4.7404
AOS3 <- Awareness of Severity	2.9425
C1 <- Celerity	1.8402
C2 <- Celerity	2.3083
C3 <- Celerity	2.4413
CE1 <- Certainty	4.106
CE2 <- Certainty	4.2856
CE3 <- Certainty	8.8149
CISP1 <- Compliance to the Information Security Policy	10.3851
CISP2 <- Compliance to the Information Security Policy	9.642
CISP3 <- Compliance to the Information Security Policy	11.484
R 1 <- Realism	0
SE1 <- Severity	0

Table 3: T-Statistics of outer loadings

The path coefficient is highly significant for all of the constructs in Table 3 (except for C1, R1 and SE1) as they are all above the recommended 1.96 for t-values to be of significance.

Chapter 6: Interpretation of findings

6.1 Discussion of findings

Bosworth, (2005) describes general deterrence theory as designed to prevent crime in the general population. Bosworth, (2005) mentions that “people choose to obey or violate the law after calculating the gains and consequences of their actions”. In the case of the Information Security policy, which is the law that governs Information Security within an organisation, it defines the lines of what an individual would have to debate if the gains of breaking the “law” would outweigh the proposed disciplinary actions (i.e. consequences). This section will interpret the findings and discuss implications for practice and the research limitations.

The two hypotheses shown to be strong predictors are the following:

H3: *The certainty of an end-user breaching the Information Security Policy would be positively associated with an end-user complying with the Information Security Policy.*

H5: *The quicker the end-user is informed of the offence committed against the Information Security policy the more the positive association with an end user complying with the Information Security policy will be.*

The research study has concluded based on the results above that for deterrence theory that Certainty (H3) and Celerity (H5) are strong predictors of compliance to the Information Security Policy. This means that the research objective to determine if certainty of being caught ensures compliance to the Information Security Policy and the other research objective, to analyse if the celerity (swiftness) of sanctions determines compliance to the Information Security Policy were both proven to be strong predictors. This is interesting, as it would imply that individuals are more concerned when it comes to compliance to the Information Security policy of the certainty of being caught or how quick they will be caught rather than the severity of what will happen if they are caught.

The following research objectives did not predict compliance to the Information Security Policy directly:

- To determine if the extent of the severity ensures compliance to the Information Security Policy and the related hypotheses was.
- To determine if awareness of severity ensures compliance to the Information Security Policy
- To determine if awareness about monitoring occurring of the Information Security Policy ensures compliance

The following hypothesis did not predict compliance to the Information Security Policy directly:

H1: *The severity of the disciplinary action would be positively associated with an end-user complying with the Information Security policy.*

H2: *The awareness of the severity would be positively associated with an end-user complying with the Information Security policy.*

H4: *The awareness of the certainty of an end-user breaching the Information Security policy would be positively associated with an end-user complying with the Information Security policy.*

In general the severity component at an organisation would mean you could be dismissed which would imply you would have trouble being able to meet your monetary obligations and yet based on the data this is not really a concern.

The data reflect that severity does not predict compliance to the Information Security Policy directly. The highest predictor above all else is that the certainty of being caught for breaching the Information Security Policy ensures compliance to the Information Security Policy followed by the quicker one is caught from a breach of the Information Security Policy will ensure compliance to the Information Security Policy.

The awareness of the fact that one could be dismissed if they do not follow the Information Security Policy is also not a predictor of compliance to the Information Security policy as well as the awareness that monitoring about the Information Security Policy is occurring does not predict compliance to the Information Security Policy. This is also interesting as if the data subjects mention that being caught is their main reason for complying with the policy it also infers that they might believe that even though they are being monitored, they have no reason to believe they are actually being monitored besides being told that they are being monitored.

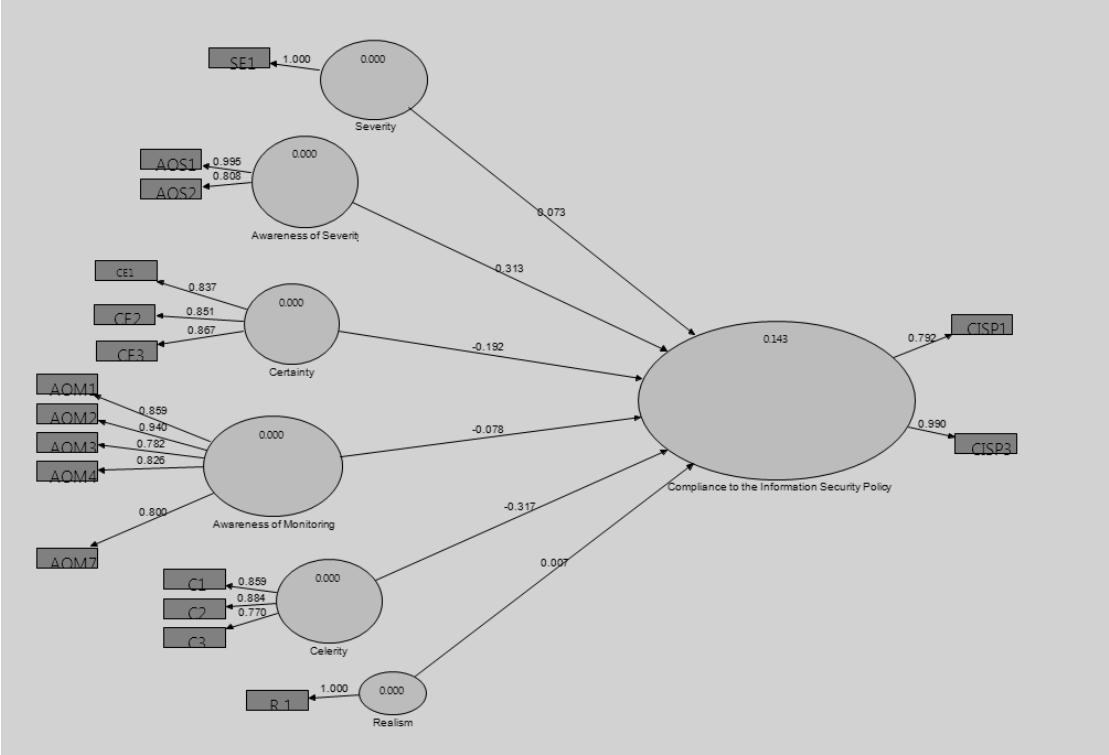


Figure 7: Female PLS-SEM Results

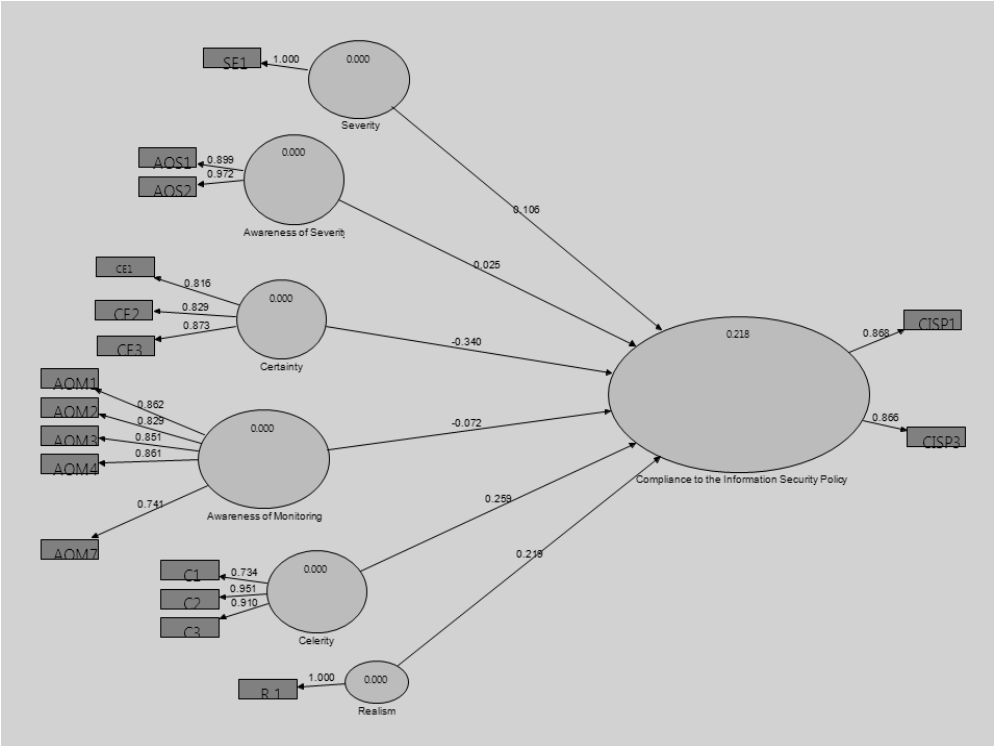


Figure 8: Male PLS-SEM Results

Further to the original analysis performed above, the PLS-SEM results were also completed for the gender of males and females to ascertain if there were any major changes from the original base analysis of information. For males (See Figure 8 – note items which were below the 0.7 were removed for this analysis) it was concluded that Certainty (H3), (β=0.340, $p \leq 0.04$) and Celerity (H5), (β=0.259, $p \leq 0.07$), both items larger than 0.20, Wong, (2013), are strong predictors of compliance to the Information Security Policy but Severity, Awareness of severity and awareness of monitoring do not predict compliance to the Information Security Policy directly. This analysis was directly correlated in line with the original analysis. The same analysis was performed for females (See Figure 7 – note items which were below the 0.7 were removed for this test) and it was concluded that awareness of severity (H2), (β= 0.313, $p \leq 0.94$), larger than 0.20, Wong, (2013) was the highest predictor of compliance to the Information Security Policy. Sample sizes were considerable lower than males and therefore the data for the females would not be as representative as the males. The p values for females for awareness of severity were also not in statistically significant range.

The research however illustrated that for males certainty was the highest predictor and for females awareness of severity was the highest predictor to compliance to the Information Security Policy. Regardless of the p values for females being statistically significant, the data illustrates that different approaches to ensuring compliance to the Information Security Policy might need to be two fold to address both males and females. Males needing the certainty and celerity components being fulfilled and females needing the awareness of the severity component. An effective approach would then be to address both male and female areas to ensure maximum compliance to the Information Security Policy.

The research showed that between genders there are different preferences to ensure compliance the Information Security policy and could be a further study as to why this is occurring.

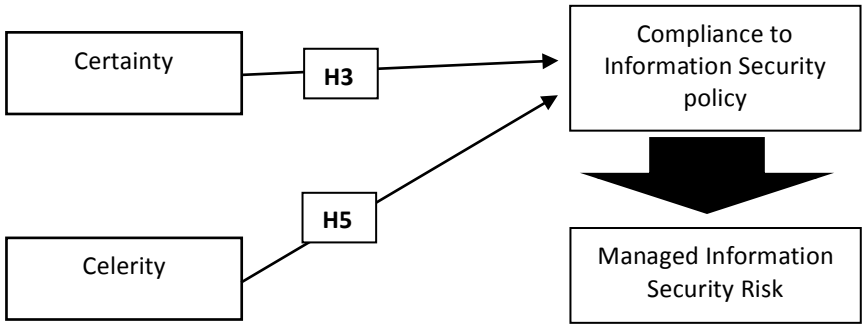


Figure 9: Conceptual model

Figure 9 shows the conceptual model that is informed by the empirical evidence. The model shows that some factors, e.g. the hypotheses H1, H2 and H4 are not significant in ensuring compliance to the Information Security Policy. The research data has shown a strong predicator to both certainty and celerity to ensure compliance to the Information Security policy (as illustrated above in the analysis) while the other hypotheses were not shown to be strong predictors. The updated model in Figure 6 displays from the research study of which hypotheses were strong predictors of constructs to the compliance of the Information Security Policy. For practitioners it has shown that respondents are more likely to ensure compliance to the Information Security policy if they know they will be caught and that they will be caught quickly. This will be challenging for those that create policy as with every policy control requirement, one would have to think carefully how one

could easily make respondents feel certain if they did not adhere to that policy control requirement they would be caught and they would be caught almost immediately. If for every policy control requirement this could be achieved the Information Security policy would not just be a piece of paper but would indeed be brought to life as individuals would be complying.

6.2 Implications for practice

From a practical point of view, it is clear to practitioners that based on the two hypotheses being strong predictors of compliance to the Information Security Policy; the following would need to be addressed if compliance is to be achieved:

- If an individual does not adhere to the Information Security Policy he/she will be caught
- If an individual does not adhere to the Information Security Policy he/she will be caught quickly (i.e. when the non-compliance occurs)

This ultimately means that Information Security practitioners should rather be focusing on what tools (e.g. monitoring) will actually ensure that people will be caught (certainty) should they not comply with the policy. This research also shows that practitioners should also try and find means that would catch individuals breaching the policy quickly if they wanted to ensure compliance to the Information Security policy.

Conversely for the other hypotheses, it means that the following does not help achieve compliance, as they were all weak predictors of compliance.

- Awareness of disciplinary actions would need to be given to end-users
- Awareness of the fact that end-users are being monitored to see if they are breaching the Information Security policy
- Disciplinary action to occur should there be a breach of the Information Security policy

Most companies would have a banner when you log into your machine stating that your communication could be monitored and this is usually also mentioned in your

employee contract. Based on the research though it shows this is not a strong indicator for compliance to the Information Security policy and thus trying to use awareness campaigns that state you could be dismissed are of little value. Disciplinary actions for individuals is also of little value as individuals are more concerned by the fact about themselves getting caught and not too concerned about the disciplinary actions. This means that an organisations current process for dismissal is probably already sufficient and should not be a key focus to achieve compliance to the information security policy.

This would give clear direction to practitioners that in order to have a workable Information Security policy, the statements in the Information Security Policy would need to be assured to end users that non-compliance would be certain and occur in a swift manner.

6.3 Limitations of the study

A limitation of this study as per Siponen & Vance, (2010) is if individuals who are participating in this survey have already committed an offence with regards to the Information Security policy, individuals might respond inaccurately in order to preserve their self-image. During the period of this research paper an awareness around the Information Security policy did occur (which is normal as awareness for Information Security is the norm within organisations on an annual basis) and as such this could be a threat to the internal validity as a history threat, where the observed effects are caused by historical events Bhattacherjee, (2012). This means for this study that by deploying the research instrument to the sample frame, the campaign could have been affected by individuals when answering questions to the scenario. History is a threat to the internal validity. Another limitation is that the data was collected in a cross-sectional manner and therefore common method bias could be a limitation Chen et al., (2012).

A threat to the external validity of this research paper could be the Hawthorne effect, in which subjects know they are participating in an experiment and therefore the results are biased. Potential apprehension bias to answering, based on the topic of transgressing the Information Security policy, is also a possibility and was

attempted to be reduced through the anonymity of participating in the research. As per Siponen & Vance, (2010) the dependent variable, compliance to the Information Security policy also raised the question if intention is indicative of actual behavior.

Chapter 7: Evaluation of the research and conclusion

7.1 Introduction

This chapter summarises the research report by reflecting on the research methodology and design to identify if the initial research objectives have been met. It will also establish the relevance of deterrence theory has been established through the research methodology and testing. The conclusion will provide an over-arching summary of this research paper.

7.2 Overview of the research

This study is divided into seven chapters. The first chapter discusses the introduction of compliance with an organisation's Information Security Policy around deterrence theory and discusses the background of the study. The second chapter discusses a review of the literature, including the limitations and findings of previous research studies. The third chapter discussed deterrence theory in more detail, including the context of the study, the problem statement, the goals and research objectives of the study. Chapter three also discussed the theoretical framework for this research study. The fourth chapter discusses in detail around the research methodology and design as well as the collection of data and sampling method used. Further to this the ethics of the research paper is mentioned in this chapter. Chapter 5 explains the data analysis and a discussion of the findings, showing the validity results (e.g. Cronbach alpha), the model analysis and the test of the research methods. Chapter 6 discusses the interpretation of the findings, the impacts for practitioners and the research limitations. The final chapter, chapter 7, discusses the evaluation of the research, relevance of the research methodology, recommendation for future studies and lastly a conclusion for this research thesis.

7.3 Research questions revisited

The study contribution aimed to identify if user compliance with an organisation could be achieved using the Information Security Policy based on deterrence theory using the above research questions. All research questions below followed the approach of obtaining the information through a sample frame completing a survey via an online assessment, upon which the information was analysed to provide inferences to support the research question findings below. The following below gives a brief summary of each research question.

Research Question 1: How does the severity of the disciplinary action affect compliance to the Information Security Policy? The following research question **did** not predict compliance to the Information Security Policy directly. The severity of the disciplinary action did not directly indicate compliance to the Information Security Policy based on the analysis of the data. This implies that individuals are actually not concerned about the disciplinary action should they not comply with the Information Security Policy. On a worst case scenario the disciplinary action for not complying with the Information Security Policy could be your employment contract is terminated which would mean you would no longer earn an income.

Research Question 2: Does the higher the certainty of being caught for breaching the Information Security Policy affect compliance to the Information Security Policy? The following research question did predict compliance to the Information Security Policy directly. The certainty of being caught directly ensured compliance to the Information Security Policy. This means that individuals felt that the more certain they would be of being caught, the more likely they would actually comply with the Information Security Policy.

Research Question 3: What is the effect of the quicker the disciplinary action occurring from a breach of the Information Security Policy effect compliance to the Information Security Policy? The following research question did predict compliance to the Information Security Policy directly. The quicker a person gets caught not complying with the Information Security policy the more likely the person would be to comply to the Information Security policy.

Research Question 4: How does the higher awareness about the severity of the Information Security Policy effect compliance to the Information Security Policy? The following research question did not predict compliance to the Information Security Policy directly. This means that the more people are aware of the disciplinary actions that could be taken against a person (e.g. an employee contract being terminated) does not ensure higher compliance to the Information Security Policy.

Research Question 5: How does the higher the awareness that monitoring about the Information Security Policy is occurring affect the compliance to the Information Security Policy. The following research question did not predict compliance to the Information Security Policy directly. This means that the more individuals are aware that they are being monitored does not ensure more compliance to the Information Security Policy.

7.4 Relevance of the research methodology

This section discusses the research methodology used and its relevance and appropriateness to reach the results of the research objectives. The research design followed a hypothetical scenario method (See Appendix A) using an online survey design based on deterrence theory by framing hypotheses following a similar approach to the research design to Siponen & Vance, (2010) while using a hypothetical model based on a scenario Siponen & Vance, (2010). As per Siponen & Vance, (2010), Myyry et al., (2009) and Chen et al., (2013) a hypothetical model based on a scenario was used to test the above hypotheses. Siponen & Vance, (2010) state that this is also known as a vignette or policy capturing method. The vignettes “present subjects with written descriptions of realistic situations and then

request responses on a number of rating scales that measure the dependent variables of interest" as cited by Trevino (1992), pp. 127-128 from Siponen & Vance, (2010). Following the completion of the survey the data was analysed and inferential analysis occurred. As per Bhattacherjee, (2012) inferential analysis is the statistical testing of hypotheses. Following the research methodology of previous research in this domain the research methodology, it was deemed to be fit for purpose for this research paper.

7.5 Relevance of deterrence theory to the study

Bosworth, (2005) described general deterrence theory as designed to prevent crime in the general population. Bosworth, (2005) identified there to be three key components for deterrence theory which are severity, certainty and celerity of punishment. The data being analysed showed a direct link to deterrence theory for certainty and for celerity but no direct link to severity.

7.6 Recommendations for further studies

This study focused on a global mining industry and it could be extended into other production environments using quantitative methods to see if the inferences made were similar or if there were significant changes. Another recommendation would be to extend the simulation scenario used to see if more scenarios reflected in any change in the analysis of the results to further prove deterrence theory within compliance to the Information Security Policy. The fact that severity is not a concern for most individuals is interesting and could be further explored as to the "why" people are not concerned about the severity. There could be many reasons for this, i.e. people could feel that even though monitoring is occurring they have no evidence that they are actually being "caught" or reprimanded by line management. It would also be interesting to see if people were aware of someone else being reprimanded for committing an Information Security offence if that would have any effect on their behavior.

7.7 Reflection on the research study

Siponen & Vance, (2010) has also indicated in the research findings presented above that they found formal sanctions do not predict IS security policy violations. This means that for deterrence theory, severity is not a strong predictor of compliance to the Information Security policy and supported in this research as well. This research has further shown the strong predictor of the certainty of an end-user breaching the Information Security Policy would be positively associated with an end-user complying with the Information Security Policy. The research has also shown the strong predictor of the quicker the end-user is informed of the offence committed against the Information Security policy the more the positive association with an end user complying with the Information Security policy will be. In contrast, this research paper has only found two of the three components of deterrence theory to be strong predictors of compliance to the Information Security Policy with severity indirectly showing compliance to the Information Security policy.

D'Arcy et al., (2009) found perception of sanctions to be more valid than the actual sanctions themselves. In this research it was found for the, awareness of severity, the compliance to the Information Security Policy was indirectly affected and there was no data that showed statistical significance. This is a contradiction to the finding by D'Arcy et al., (2009). It is quite possible as this is a mining environment the results would be different from D'Arcy et al., (2009). This being said though when the analysis for males and females was performed, for females there was a link between the perceptions of sanctions being more valid, even though the data was not statistical significant.

7.8 Conclusion

The research revealed deterrence theory can be used as a lens to study and determine compliance to the Information Security Policy. The study, however, shows that only two of the three constructs, namely certainty and celerity seem to be significant from deterrence theory with severity not showing any direct link to compliance. It was also shown that individuals being aware of the severity or even that they are being monitored for not complying with policy had no positive support for complying with the Information Security Policy.

The data shows that individuals are not concerned about the consequences of their actions, that there are consequences or that they are being monitored for non-compliance. What does concern individuals is that how certain it is that they will be caught and also how quick they will be caught. If individuals feel they will be caught and they will be caught quickly then they will actually comply with the Information Security Policy. There could be many factors for the belief in individuals around this but from an Information Security perspective, the fact that people are not concerned about the consequences or that they are being monitored almost implies that people seem to not believe that they are actually being monitored or that people actually will be disciplined and would be an area to further explore for statistical evidence. This is almost like an individual speeding on the highway, realising that he is breaking the law and being told that they do monitor speed traffic, but the individual still breaks the law because he knows of nobody who has been prosecuted and has never seen any evidence of being monitored. This being said people still break the law even after having received countless traffic fines.

For security practitioners this could be a game changer, as the data would suggest that more investment should be placed in actually informing end users soon after committing a policy violation that we are aware they have done so and that a further breach could mean the severity items will come into play (e.g. employment termination). An organisation that is assured that when they do not follow the rules, they will be caught and caught swiftly would establish a culture where the Information Security Policy is not just a piece of paper, but actually a management tool for ensuring a conscious Information Security culture.

Appendix A - Questionnaire

Demographic Questions

1. Please indicate your gender:

    - Male
    - Female
    - Prefer not to say

2. Please indicate your location:
    - Europe
    - Canada
    - South Africa
    - Prefer not to say

3. Please indicate your age range
    - 18-24 years old
    - 25-34 years old
    - 35-44 years old
    - 45-54 years old
    - 55-64 years old
    - 65-74 years old
    - 75 years or older
    - Prefer not to say

4. Please indicate your level of education
    - Some high school, no diploma
    - High school graduate, diploma or the equivalent
    - Some college credit, no degree
    - Trade/technical/vocational training
    - Associate degree
    - Bachelor’s degree
    - Master’s degree

- Doctorate degree
- Prefer not to say

5. Please indicate your current band* level
    - Band 1
    - Band 2
    - Band 3
    - Band 4
    - Band 5
    - Band 6
    - Band 7
    - Band 8
    - Band 9
    - Band 10
    - Prefer not to say

*Band is the local company's employee HR levels

Research Questions

For each of the following statements, please indicate how true it is for you, using the following scale:

1	2	3	4	5	6	7	8	9	10
not at all true				somewhat true					very true

All questions will be based on the following hypothetical scenario:

The employee is a junior manager in a small company where she was recently hired. Her company has a strong policy that each computer workstation must be password-protected and that passwords are not to be shared. However, the employee is on a business trip and one of her co-workers needs a file on his computer. The employee expects that sharing her password could save the company a lot of time. She is aware of the importance of not sharing passwords with coworkers due to mandatory

Information Security training. The employee shares her password with her co-worker. Given this hypothetical scenario and assuming you were the employee, please specify the extent to which you would agree or disagree with the following statements:

If you were caught violating the company Information Security policy you would receive disciplinary action.
If you were caught and received formal disciplinary action, this would cause a problem for you in your life.
If you were caught and received a verbal warning, this would cause a problem for you in your life.

Certainty

There is a high chance you would receive disciplinary action if you had violated the company information security policy.
There is a high chance you would receive disciplinary action if your manager found out you had violated the company information security policy.
There is a high chance you would receive a verbal warning if your manager found out you had violated the company information security policy.

Awareness of severity

If I violate organisational Information Security policies, I would probably be caught.
If I violate organisational Information Security policies, I will be caught.
My company would take disciplinary action against the employee sharing his/her password if he/she was caught.

Awareness of monitoring

Employee computer practices are properly monitored for policy violations.
I believe that computing activities are monitored by my organisation.
I believe that my organisation monitors computing activities to ensure that employees are performing only explicitly authorised tasks.
I believe that my organisation reviews logs of employee computing activities on a regular basis.
I believe that my organisation conducts periodic audits to detect the use of authorised software on its computers.
I believe that my organisation actively monitors the content of employees' e-mail messages.
I believe that my organisation would have been able to monitor what the scenario character did.

Celerity

If the employee was immediately informed of his/her transgression against the Information security policy and there was a first warning, this would stop the individual from transgressing the Information Security policy again.
If the employee was informed of his/her transgression against the Information security policy 1month later and there was a first warning, this would stop the individual from transgressing the Information Security policy.
If the employee was informed of his/her transgression against the Information security policy 3 months later and there was a first warning, this would stop the individual from transgressing the Information Security policy.

Compliance to the Information Security Policy

There is a high chance that you would do what the employee in the described scenario did.
There is a possibility that you would do what the employee in the described scenario did.
You would not do what the employee in the described scenario did.

Realism

This was a realistic scenario.

Appendix B: Literature Source Questions

Construct	Item	Source
Severity	“How much of a problem would it be if you received severe sanctions if you violated the company information security policy? “	Siponen & Vance, (2010)
Severity	“How much of a problem would it create in your life if you were formally sanctioned for doing what [the scenario character] did? “	Siponen & Vance, (2010)
Severity	“How much of a problem would it create in your life if you were formally reprimanded for doing what [the scenario character] did? “	Siponen & Vance, (2010)
Certainty	“What is the chance you would receive sanctions if you violated the company information security policy? “	Siponen & Vance, (2010)
Certainty	“What is the chance that you would be formally sanctioned if management learned that you had violated company information security policy? “	Siponen & Vance, (2010)
Certainty	“What is the chance that you would be formally reprimanded if management learned you had violated company information security policy? “	Siponen & Vance, (2010)
Awareness of severity	“If I violate organisation security policies, I would probably be caught. “	Herath & Rao, (2009)
Awareness of monitoring	“Employee computer practices are properly monitored for policy violations. “	Herath & Rao, (2009)
Awareness of monitoring	“I believe that employee computing activities are monitored by my organisation. “	Chen et al., (2012)
Awareness of	“I believe that my organisation monitors computing activities to ensure that employees	Chen et al., (2012)

monitoring	are performing only explicitly authorized tasks. “	
Awareness of monitoring	“I believe that my organisation reviews logs of employee computing activities on a regular basis. “	Chen et al., (2012)
Awareness of monitoring	“I believe that my organisation conducts periodic audits to detect the use of authorized software on its computers. “	Chen et al., (2012)
Awareness of monitoring	“I believe that my organisation actively monitors the content of employees’ e-mail messages. “	Chen et al., (2012)
Compliance to Information Security policy	“What is the chance that you would do what the individual in the described scenario did? “	Siponen & Vance, (2010)
Realism (not part of construct)	How realistic was the scenario for you?	Siponen & Vance, (2010)

References

Barclay, D., Higgins, C., & Thompson, R. (1995). The partial least squares (PLS) approach to causal modeling: Personal computer adoption and use as an illustration. *Technology studies*, 2(2), 285-309.

Bhattacherjee, A. (2012). *Social science research.* Tampa, Fla.: A. Bhattacherjee. 1-150.

Boss, S.R & Kirsh, L.J & Angermeier, I & Shingler, R.A & Boss, R.W (2009). If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security. *European Journal of Information Systems* 18, 151-164.

Bosworth, M. (Ed.). (2005). *Encyclopedia of prisons & correctional facilities*. (Vols. 1-2). Thousand Oaks, CA: SAGE Publications. 233-237.

Bulgurcu, B & Cavusoglu, H & Benbasat, I (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly* Vol. 34 No. 3. 523-548.

Chen, Y., Ramamurthy, K., & Wen, K. W. (2012). Organisations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information Systems*, 29(3), 157-188.

Cook, T. D., & Campbell, D. T. (1979). *Quasi Experimentation: Design and Analytical Issues for Field Settings*, Chicago: Rand McNally.

Dennis, A. and Valacich, J. (2001). Conducting experimental research in information systems. *Communications of the association for information systems*, 7(1), 1-41.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security*, 04(02), 92-100.

D'Arcy, J & Herath, T (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems* 20, 643-658.

D'Arcy, J & Hovav, A & Galletta, D (2009). User awareness of security countermeasures and its impact on Information Systems misuse: a deterrence approach: a deterrence approach. *Information Systems Research* Vol 20, No. 1, 79-98.

Fornell, C & Larcker, D (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, *Journal of Marketing Research* (18:1), 39-50.

Gefen, D & Straub, D. W. (2005). A Practical Guide to Factorial Validity Using PLS-Graph: Tutorial and Annotated Example, *Communications of the AIS* (16:5), 91-109.

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

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

Lee, A. S. (1989). A scientific methodology for MIS case studies. *MIS Quarterly*, 13(1): 33–50.

Lee, A. S. (1991). Integrating positivist and interpretive approaches to organisational research. *Organisation science,* 2(4), 342-365.

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

Nunnally, J. C. (1978). *Psychometric theory*. New York: McGraw-Hill.

Paternoster, R, & Simpson, S (1996). Sanction Threats and Appeals to Morality: Testing a Rational Choice Model of Corporate Crime, *Law & Society Review* (30:3), 549-584.

Ponemon Institute (2013). 2013 Cost of data Breach Study: United States. Ponemon Institute sponsored by Symantec Corporation, Cupertino, CA.

Siponen, M & Vance, A (2010). Neutralaization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* Vol 34 No 3, 487-502.

Straub, D. W., Boudreau, M., and Gefen, D. (2004). Validation Guidelines for IS Positivist Research, *Communications of the Association for Information Systems* (13:24), 380-427.

Ugrin, J. C., & Pearson, J. M. (2010). Understanding the Effect of Deterrence Mechanisms on cyberloafing: Exploring a General Deterrence Model with a Social Perspective. *In ICIS* (p. 98).

Weber, J. (1992). Scenarios in business ethics research: Review, critical assessment, and recommendations. *Business Ethics Quarterly*, 137-160.

Verizon (2014). Verizon 2014 Data breach investigations report, Verizon enterprise, 1-60

Wong, K. K. K. (2013). Partial least squares structural equation modeling (PLS-SEM) techniques using SmartPLS. *Marketing Bulletin*, 24(1), 1-32.