2016

A Theory on Information Security

Craig A. Horne
The University of Melbourne, chorne@student.unimelb.edu.au

Atif Ahmad
The University of Melbourne, atif@unimelb.edu.au

Sean B. Maynard
The University of Melbourne, seanbm@unimelb.edu.au

A Theory on Information Security

Craig A. Horne
Department of Computing and Information Systems
The University of Melbourne
Victoria, Australia
Email: chorne@student.unimelb.edu.au

Atif Ahmad
Department of Computing and Information Systems
The University of Melbourne
Victoria, Australia
Email: atif@unimelb.edu.au

Sean B. Maynard
Department of Computing and Information Systems
The University of Melbourne
Victoria, Australia
Email: sean.maynard@unimelb.edu.au

Abstract

This paper proposes a theory on information security. We argue that information security is imperfectly understood and aim to bring about an altered understanding of why efforts are made to engage in information security. The goal of information security is widely recognised as the confidentiality, integrity and availability of information however we argue that the goal is actually to simply create resources. This paper responds to calls for more theory in information systems, places the discussion in philosophical context and compares various definitions. It then identifies the key concepts of information security, describes the relationships between these concepts, as well as scope and causal explanations. The paper provides the theoretical base for understanding why information is protected, in addition to theoretical and practical implications and suggestions for future research.

Keywords

Information security, resources, controls, threats, theory development.

1 INTRODUCTION

Despite the concept of information security being very well established, the reasons and motivations behind it are imperfectly understood. This paper seeks to explain how and why the phenomena that comprise the concepts of information security occur. The emphasis for this paper is to explain the information security concepts and relationships between them in order to alter our understanding of why we protect information.

This proposed theory on information security simply states that the motivation behind all attempts by an organisation to secure information against threats is to create resources that can later improve organisational performance. Information will degrade over time without adequate controls implemented for its protection. In terms of the taxonomy of information systems theories presented by Gregor (2006), this manuscript provides a (Type 2) high-level theory for explanation, describing how and why the phenomenon of information security occurs.

The theory on information security originates from the area of information systems, built entirely from concepts that relate to information and the breadth of systems that it can reside on. It applies to different levels, including strategies to protect information used by individuals, groups, organisations and also protects information shared between organisations. The results are that, depending on the information affected, degradation over time may reduce the usefulness of the resource and thus lead to the potential erosion of competitive advantage or organisational success.

The paper proceeds in three major sections, with the major headings and sections structure adapted from Rivard (2014). In the next section, we introduce information security, discuss why a theory on information security is needed and carefully examine issues with existing theory. Secondly, we explain the theory on information security. Thirdly, we examine the implications for the development of this theory. Finally, we briefly draw conclusions, consider limitations and offer proposals for future research to improve our theoretical understanding of information security.

2 WHAT IS INFORMATION SECURITY?

The following section begins with a narrative describing why a new theory on information security is needed. This description of what motivates the study is based on an exploration of the theoretical issues in relevant literature. The result is a set of conditions that this new theoretical development then meets.

2.1 Motivating the Study

This paper is broadly motivated by calls for 'good theory' within the domain of information systems (Webster and Watson 2002; Zmud 1998; Zmud et al. 2001). The current paucity of good quality theories in the information systems domain leads to calls for development of our 'own' theory (Markus and Saunders 2007; Weber 2003; Weber 2012). Importantly, there have been calls for bolder and more original information systems explanatory theory (Grover et al. 2008). The development of new ideas and theories is scarce yet essential (Markus and Saunders 2007; Rivard 2014). Therefore, to begin with, as Weber (2003, pp. iii) states, "*choosing the phenomena we wish to explain or predict—is the most important decision we make as a researcher*".

More specifically, this paper is motivated by an apparent gap in the literature where a theory on information security is not apparent. A search of the academic literature, as described in the next section, does not reveal any literature that purports to offer a theory on information security. This search of overlooked areas is a form of neglect-spotting (Sandberg and Alvesson 2011).

Stronger theory can be produced from linking theories of diverse types and academics have been urged to consider combining other types of theory with their own (Gregor 2006). Towards that, using this theory on information security as one that underpins a theoretical perspective on information security strategy in organisations could prove useful (Horne et al. 2015).

There are theories that relate to information security. For example, the *Theory of Information Warfare* presents a model of information warfare in terms of four main elements: information resources, players, offensive operations, and defensive operations (Denning 1999). The *Theory of Protection Motivation* predicts users' intentions to protect themselves after receiving fear-arousing recommendations (Rogers 1975). There are no theories however where the locus of knowledge is in information security alone.

This gap however is not because information security is uninteresting. Almost every organisation requires information to function and disruption to information from a security breach can often lead to disruption of an organisation's operations (Cavusoglu et al. 2004). Therefore filling this gap will make a valuable contribution to the body of knowledge.

2.2 Relevant Literature

A thematic study of the information systems literature is presented, in order to develop a perspective on information security and its interactions. The contextual setting is described before information security itself is examined. With this understanding, a theory on information security can then be posited based on commonly-accepted philosophy.

2.2.1 Context

The theories or knowledge within any discipline are explained based on questions grouped within four classes which, in descending order, are 1. domain, 2. ontology, 3. epistemology and 4. socio-political (Gregor 2006). This section explores the information security concept within the context of these four classes of questions.

- Domain of Information Systems

Information systems has been defined as a collective term that refers to a number of areas of application, including enterprise integration, natural language translation, geographic information systems, legal information systems, and biological information systems (Guarino 1998). Separately, a core set of phenomena that defines the information systems field has been defined as including information technology (IT) capabilities, the IT artefact, IT practices, usage and impact (Benbasat and Zmud 2003). At the broadest level, the domain of information systems has been defined and explained as a system composed of people and computers that processes or interprets information, which is the view adopted throughout the rest of this paper (D'Atri et al. 2008).

- Ontological Approach

Theory is understood within information systems as being broad in nature, to encompass frameworks, models, or the body of knowledge (Gregor 2006). The ontological character of theory types has been articulated as having five categorisations: analysis, explanation, prediction, explanation and prediction, and design and action (Gregor 2006). These categorisations provide researchers with a language to describe the various components of theory.

- Epistemological Approach

To explore how theory can be constructed and what research methods can be used, we note that discussion in this area often contrasts the positivist and interpretivist views, or the quantitative and qualitative views (Gregor 2006). As explained later in Section 3.2 - Theory Type, the type of theory expounded in this paper is explanatory in nature, and theories of this nature are often associated with research in the interpretivist paradigm (Gregor 2006).

- Socio-political Approach

Exploring where theory has been developed to date, we find that there have been a surprisingly low number of theories, (i.e. fewer than half a dozen) that, when developed, originated solely from the area of information systems (Markus and Saunders 2007). Other theories have originating areas that include both information systems and a reference discipline, whilst the remainder originate solely from another discipline (Gregor 2006).

Information security is a phenomenon within the information systems domain because it involves people protecting information that resides on computers, which are all common elements consistent with information systems. From an information systems viewpoint, information security is concerned with protecting information (Siponen and Oinas-Kukkonen 2007).

2.2.2 Defining Information Security

This section documents the definition and goal for each of computer security, information security and cyber security. Computer security, also known as information and communication technology (ICT) security, is the security of the computers that process and store information (Von Solms and Van Niekerk 2013). The goal of computer security is the confidentiality, integrity, availability, non-repudiation, accountability, authenticity, and reliability of information resources (Von Solms and Van Niekerk 2013).

Information security used to be purely technical, however has evolved over time to keep pace with changes to computers and networks (Von Solms and Van Niekerk 2013). The goal of information security involves preserving the confidentiality, integrity and availability of business information (McCumber 1991; Posthumus and von Solms 2004). As well, the goal of information security is to safeguard business continuity and reduce business impairment by constraining the effect of security incidents (Von Solms 1998). In another contribution the goal of information security was stated to be confidentiality, integrity, availability and non-repudiation of information (Siponen and Oinas-Kukkonen 2007).

Cyber security is different to information security (Von Solms and Van Niekerk 2013). Although they are very different, the term cyber security seems to be used interchangeably with the term information security in academic literature (Von Solms and Van Niekerk 2013). Cyber security transcends the boundaries of information security to include the defence of information and also people (Von Solms and Van Niekerk 2013). The goal and general security objectives of cyber security are the availability, integrity and confidentiality of an organisation's assets including networks, infrastructure, information and personnel (Von Solms and Van Niekerk 2013).

Examining the above discourse, we can see that there are three different definitions for computer security, information security and cyber security but that their goals seem to be roughly similar, in that they are internally-focussed and revolve around confidentiality, integrity, and availability. This homogeneity of goals is incongruous given the disparity in definitions and the following section will provide an improved goal for information security.

3 A THEORY ON INFORMATION SECURITY

A theory can be defined as "*a statement of relations among concepts within a boundary set of assumptions and constraints*" (Bacharach 1989, pp. 496). We argue that information security needs its own distinct goal, not just to copy the goal of computer security, and then deconstruct the proposed theory on information security into its various elements. This section describes the conceptual elements of the proposed theory, the relationships between the concepts, and proposed use of the theory.

3.1 Theory Overview

Information security is a conscious or subconscious process in which people and organisations attempt to create sustainably-viable resources, from information. They do so by applying suitable controls to protect information from threats, according to the goals for the use of that information. This then results in sustainable resources. Information security focusses on what protection is afforded to information and what use that protected information can then offer organisations.

3.2 Theory Type

A taxonomy of theory types articulates five categorisations: analysis, explanation, prediction, explanation and prediction, and design and action (Gregor 2006). This theory embodies the second type: a theory which provides "*an explanation of how, why, and when things happened*" (Gregor 2006, pp. 619). To clarify, this paper does not describe and categorise themes within information security, as this alone is not theory (Bacharach 1989; Rivard 2014). Rather, this paper distils complex concepts in information security and then offers a new explanation of what the motivations behind it are, using clear language.

Theories for explanation are described as an ideal type of theoretical contribution (Rivard 2014). Pure theory papers with explanations of theoretical mechanisms are welcomed as essays with highly valued characteristics (Markus and Saunders 2007). Other researchers have posited theories which are explanatory in nature without testable propositions (Orlikowski and Robey 1991). The writing of a paper where the end product is purely the advancement of a new theory via a detailed explanation is perfectly acceptable (Walsham 1995).

Construct validity can be said to have been achieved when, amongst other principles, the interlocking system of laws which constitute a theory (called a nomological network) are made clear, the theoretical constructs are observable, and the constructs in the nomological net have been elaborated on (Cronbach and Meehl 1955). It is understood that in the early history of a nomological net, as described in this paper, the network will be limited and have few connections.

3.3 Assumptions

Clarifying the assumptions of information security is important otherwise there is a risk of inappropriate use of the construct. This would then adversely affect construct validity and potentially the cumulative research tradition (Roberts et al. 2012).

Firstly, information security *depends on a completed information classification assessment*. This identifies what information is owned by the organisation and therefore what information needs to be protected. It also identifies what bits of information are more important than others. Without this assessment of information that is required to be protected, there is no way of clearly identifying which controls are most appropriate to deploy.

Secondly, an organisation's information security *depends on the security budget*. If the security budget is not large enough to procure the minimum number of controls necessary to protect the information identified in the classification assessment, then the integrity of the information is threatened.

Finally, information security *depends on an organisation's ability to match controls with threats*. Inappropriate selection of controls can lead to either wasteful spending on unnecessary controls or conversely, inadequate protection of information which threatens its ability to be sustainably used.

3.4 Structural Components

There are various taxonomies of theory structure with one example describing the parts as being constructs, associations, states, events, and the whole theory as having importance, novelty, parsimony, level and falsifiability (Weber 2012). The structure used in this paper however is based on the "*structural components of theory*" (Gregor 2006, pp. 620). It includes means of representation, the constructs which together form the nomological net, the relationships between the constructs and the scope. Care is also taken to explain why some theory components were not applicable, such as causal explanations, testable propositions and prescriptive statements.

3.4.1 Means of Representation

This theory on information security must be represented physically (Gregor 2006). Figure 1 below shows the four constructs included in this theory on information security and the three relationships between the constructs.

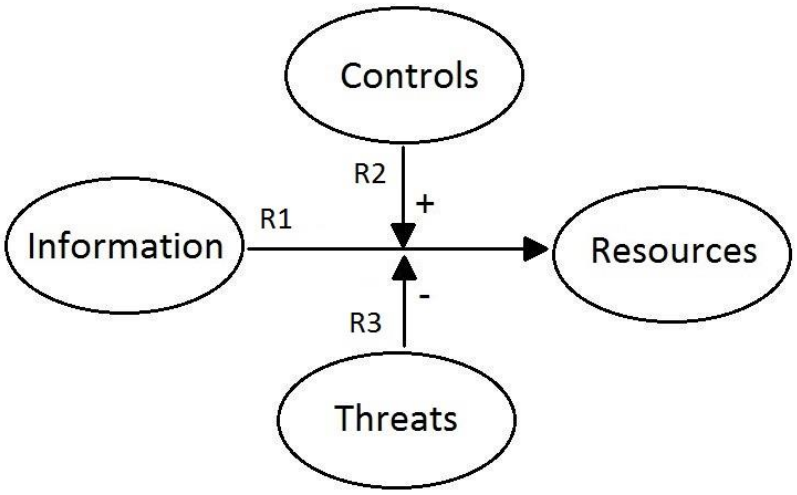

Figure 1: Schematic of Theory on Information Security

3.4.2 Constructs

The nomological network is comprised of four main constructs: information, controls, threats and resources. The following section describes each in turn and ascribes meaning to each. Care is also taken to identify whether the construct is observable, because a necessary condition for a construct to be scientifically admissible is that it be part of a nomological net of observables (Cronbach and Meehl 1955). The reason for this is so that we can then apply the famous *Verification Principle,* which argues that only statements which are provable by observation can convey factual information.

- Information

Information is seen as amorphous and can be printed on paper, stored on computers, sent by post or electronically, shown on videos and articulated in a discussion (Von Solms and Van Niekerk 2013). As well as being stored on physical media such as paper and digital media such as computers, information can also reside on cognitive media, i.e. people's minds (Ahmad et al. 2005). Information can also have various levels of sensitivity, is difficult to control which sometimes results in leakage, and is intangible in nature (Ahmad et al. 2005). Information however is not data, with the distinction being that data are raw facts and information is processed data that is meaningful (McKinney Jr and Yoos 2010). It is interesting to note that information hosted in the cloud brings its own set of challenges including (1) long-term viability, where information restoration becomes doubtful should the cloud vendor become bankrupt, and (2) information availability, where cloud vendors may not restore to a different environment should the information become unavailable (Catteddu 2010).

Information has some attributes including sensitivity and level of analysis. Non-sensitive information can be unclassified or if sensitive, classified as PROTECTED, CONFIDENTIAL, SECRET or TOP SECRET. This classification is then used as a basis for allocating access rights to organisational staff (Ahmad et al. 2014). Information is created and used at all levels of analysis within an organisation at varying sensitivities and Table 1 below provides examples of each:

Level of Analysis	Non-sensitive Information	Sensitive Information
Individual	Desk phone number	Passwords
Group	Department name	Customer sales list
Organisational	Website URL	Trade secrets
Inter-organisational	Purchase order number	Sales contract pricing

Table 1. Examples of Organisational Information and Level of Analysis

- Controls

Organisational security controls (or countermeasures) are defined as an appropriate mix of physical, technical or operational security controls. The goal of controls is to mitigate the risks to information (Posthumus and von Solms 2004). Controls are used to protect information by reducing the risk posed by exposures or vulnerabilities arising from threats (Von Solms and Van Niekerk 2013). A strong set of protective controls can provide an organisation with an effective defence capability and an organisation's capabilities provide the best defence against the existing array of competitive forces (Porter 1980).

Controls stipulated by standards are intended to prevent and detect attacks from threats, primarily through the use of technical, formal, and informal controls. Technical controls are the computer-based countermeasures. Formal controls are the policies, procedures, and rules that direct staff. Informal controls refer to the development of a security culture and the provisioning of education, training and awareness programs (Beebe and Rao 2010).

- Threats

There are many threats to the integrity, confidentiality, and availability of organisational information along with many countermeasures (Workman et al. 2008). Threats to information systems security include unauthorised access, changing of information, and the destruction of protective infrastructure that helps preserve the confidentiality, integrity, and availability of the information (Workman et al. 2008). Various threats persistently target exposures or vulnerabilities and ultimately have a adverse impact on information (Beebe and Rao 2010; Von Solms and Van Niekerk 2013).

- Resources

Resources have been defined as "*inputs into the production process- they are the basic unit of analysis. The individual resources of the firm include items of capital equipment, skills of employees, patents, brand names, finance*" (Grant 1991, pp. 118). Grant (1991) then continues that the organisation should then inventory the available resources and assess them for value generation, before developing a strategy to maximise the value from each one.

A competing view on business strategy defines resources as comprising all assets, capabilities, processes, information and knowledge (Barney 1991). Resources have also been defined as strengths that the organisation can use to formulate and implement their strategies (Porter 1981).

Information resources are crucial to supporting organisational performance by providing prospects for the establishment of competitive advantage and as such, preservation of information-based, intangible resources is a significant imperative for organisations (Porter and Millar 1985; Teece 2000). For the financial returns to an organisation to be sustainable, the resources that support them must also be sustainable (Grant 1991). The longevity of the of an organisation's competitive advantage also depends on the speed at which its supporting resources degrade (Grant 1991).

A key point is that information already exists so it is disingenuous to suggest that protecting it creates an entirely new entity. What does happen however is that by protecting information with controls, it becomes a robust, ruggedised resource, resilient to threats. This resource can then be relied upon and trusted by the organisation to not degrade over time and provide the same utility now as in 20 years.

To illustrate, imagine a pharmaceutical organisation that has, through a set of multi-year expensive trials, successfully developed a new chemical formula for a proposed drug it wishes to take to market. This chemical formula on its own is extremely vulnerable because if a competitor organisation can steal it through industrial espionage and quickly bring it to market, then the investment has been wasted. Once it has been protected with a patent however (which is a form of security control) then it will serve as a source of competitive advantage for the organisation for the next 20 years. In this example, the theory on information security in this paper would argue that the chemical formula is information, the patent application process is a control and the completed patent is a resource.

3.4.3 Statements of Relationship

This section describes the relationships between constructs which can be variously described as associative, compositional, directional or causal (Gregor 2006). The nature of the theory described in this paper means that the relationships are described succinctly but clearly and carefully.

- R1 – Relationship between Information and Resources

Information has been conceptualised as amorphous and intangible, with varying degrees of sensitivity, various storage platforms and varying levels of analysis. Resources have been conceptualised as information-based, sustainable, traceable, durable and able to be assessed for potential use in driving competitive advantage. When information is converted into a resource, there are many inferences for the final form that it takes and the following is a discussion of them.

The *cause* of information being converted into resources is the application of protective controls. When these controls are applied, the resulting resources cease to be amorphous and intangible because they can now be recorded in an asset tracking register. The storage platform may also change due to access restrictions placed on the new resource. Two attributes will remain consistent however, which are sensitivity and level of analysis. The only potential changes may be that sensitivity is upgraded once maximum value is assessed and level of analysis may change once the resource is made available for use throughout the organisation. The creation of a robust resource through the application of security controls to information is consistent with the definitions of a resource being sustainable and durable.

- R2 – Relationship between Controls and Information

Controls positively *cause* information to be protected. Controls have been defined as being formal, informal or technical and all three forms can be applied to information that resides on physical, digital and cognitive media. For example, with information that resides on physical media such as paper, a formal control might be take the form of message handling procedures that dictate how the page is to be marked with a classification indicating the sensitivity of the information and also dissemination limiting markers. An informal control might include training on how to mark the paper accordingly. A technical control might be a filing cabinet that the paper can be stored in.

- R3 – Relationship between Threats and Information

Threats negatively *cause* information to become degraded. Threats intend to degrade the integrity, confidentiality and availability of information, with some threats being known and some unknown. Threats are persistent (Baskerville 2005). The implication of this is that information will always be degraded over time if there are no controls. Even if there are protective security controls, if we accept that some threats are unknown (i.e. dynamic, unique, targeted, customised), then the controls won't defend effectively against some threats and information will be degraded.

3.4.4 Scope

Abstracting ideas to a higher level and generalising about a phenomenon, its interactions and the degree of causality are at the heart of theory development (Gregor 2006). The scope of a theory is described by the generalisability of the construct relationships using modal qualifiers (for example *some* or *all*) and explanations about boundaries (Gregor 2006).

In this theory on information security, a statement on the modal qualifiers used to describe the relationship between controls and threats is: *Some information is protected by some controls to produce all resources*. An implication of this statement is that if information has not been protected by a control, then it cannot be considered a resource. Another is that all information to be used for organisational purposes is to be protected. Also, this theory forbids the use of unprotected information in organisations. The reason that the qualifier *all* was not used with information or controls is that there is no way of determining whether this theory holds true for all information and controls since the authors do not have access to all information and controls to make an assessment.

The boundaries of this theory on information security include that it specifically applies to the protection of information and not to the protection of the infrastructure, networks or platforms that information resides on. Protection of infrastructure, networks and platforms is better known as computer security, communications security or cyber security (Siponen and Oinas-Kukkonen 2007). This theory is not bounded by levels of analysis as the use of this theory to explain why organisations protect information applies equally at the individual, group, organisational and inter-organisational levels, i.e. resources are created and used at all four levels.

3.4.5 Theory Components Not Present

There are three structural elements to this theory on information security that are not present, given this type of theory is explanatory not predictive. They are a definitive causal explanation, testable propositions and prescriptive statements, which are explained more fully in the following sections.

- Causal Explanations

This theory on information security states that the application of controls *cause*s the conversion of information into resources. However, can this be said to be always true? There are four different types of causal analysis (Gregor 2006):

i. Regularity (or nomological) analysis, i.e. ‘A causes B’;
ii. Counterfactual analysis, i.e. ‘If not A, then not B’;
iii. Probabilistic causal analysis, i.e. ‘A increases the likelihood of B’;
iv. Manipulation or teleological causal analysis, i.e. ‘If A, then B’;

In this paper, the terms *explanation* or *causal explanation* refer to the third type of causal analysis, being the probabilistic causal analysis type. In other words, the application of controls increases the likelihood of information being converted into resources. The reason is that this probabilistic type of causality is more suited to social sciences, and in this case, an infinite number of people are interacting with an infinite number of controls protecting an infinite amount of information, which means we lack a closed system where all the variables can be identified (Gregor 2006). If we lack the ability to identify all the variables, then we cannot claim to be partaking in regularity analysis.

Probabilistic reasoning alone however, is not enough to provide definitive statements of relationships amongst phenomena, which is why this theory component is said to be not present (Gregor 2006).

- Testable propositions or hypotheses

The hallmark of scientific theory is that universal statements can be made about constructs and their relationships that are falsifiable (i.e. testable) (Gregor 2006). Theories for prediction provide testable propositions that can be evaluated empirically (Gregor 2006). Explanatory theories however do not provide any testable propositions (Gregor 2006). This explanatory theory on information security should therefore not be applied deterministically.

- Prescriptive Statements

Prescriptive statements are the steps in a list that, when followed, lead to the creation of an artefact (Gregor 2006). This theory on information security does not provide any prescriptive statements about the manner in which controls should be applied to information in order to protect it and create

resources. Therefore, prescriptive statements are said to not be part of this explanatory theory on information security.

4 IMPLICATIONS OF THEORY ON INFORMATION SECURITY

This section advances the various implications of the research model and these are separated into both research and practice areas (Zmud 1998). Some of these implications inform the suggested future research directions in Section 5 Conclusion.

4.1 Theoretical

Implications for theoretical research include the possible linking of this theory on information security with the theory on internal analysis, which considers the use of resources to be fundamental to the creation and protection of competitive advantage. This highlights the potential for supporting the further developmental work being conducted on understanding information security strategy. For example, resources are combined to produce capabilities, which then form the main basis for an organisation's competitive advantage subject to certain criteria (Grant 1991; Porter 1980).

Alternatively, as described in Section 2.1 - Motivating the Study, this theory on information security could form the basis of a theoretical perspective on information security strategy in organisations. The theory could explain the motivation behind efforts to protect strategic information at the organisational and inter-organisational levels. Research into information security strategy forms an emerging field that requires a theoretical base.

4.2 Practical

Implications for practice include ideas for the situational contexts where information security would be most applicable (Zmud 1998). Practical ways that this theory on information security can make an impact include indicating the need for better identification and management of resource and controls.

5 CONCLUSION

The study advances knowledge in the information security field by creating a new understanding of what information security is and the motivations behind it. The following section recaps the contribution made in this paper, identifies the limitations constraining research into information security and offers suggestions for future research directions.

5.1 Contribution

This section provides a strong rationalisation for why the conceptualisations developed in this article have advanced our collective understanding of the information security phenomenon.

Based on our review, no theory on information security was apparent in the literature and this paper now offers one. This theory on information security states that the goal focussing all attempts by an organisation to secure information against threats is to create resources that can then later be used for organisational performance. The confidentiality, integrity and availability of information is the goal of controls not information security.

5.2 Limitations of Research into Information Security

The theory on information security is of help to academics looking to explain the theoretical base for conceptual models and frameworks that involve information security. We have described firstly, what type of theory it is and secondly, its structural components including individual construct elements and the relationships between them. However, we still have limitations on our perception of information security theory and this section describes them.

Firstly, information security has been conceptualised in various forms, including as a process (Von Solms and Van Niekerk 2013). It has also been variously been described as a capability and a framework (Siponen and Oinas-Kukkonen 2007). This raises concerns around construct validity issues as adhering to one conceptualisation risks marginalising another.

Secondly, this information security theory can be applied at various levels, as stated previously in Section 3.4.4 - Scope. However, this does not take into account communication required between the number of people who may have to cooperate at group level as opposed to individual level, for instance. At inter-organisational level, there are differences between the way that organisations

collaborate as opposed to the way that a staff group would collaborate. As a result, the nomological net for each of the levels will be different.

Thirdly, there does not seem to be a way to measure when information has been protected enough by controls and can therefore be deemed a resource. If this knowledge could be developed, 'minimum-viable resource' criteria could be developed.

5.3 Future Research Directions

Information security theory has fecundity and raises new opportunities for information systems scholars to develop the body of knowledge that currently exists on information security. The authors hope this paper raises more questions than can be answered and provides the impetus for further research to be conducted. The answers to some of these questions will also have contributions towards practice. The following are three suggested research directions for information security theory development, with these directions being adapted from Zmud (1998).

Firstly, the theory presented in this paper can be refuted by developing alternative new theories on information security. Hopefully different plausible theories supported by disparate groups of researchers will arise and stimulate intellectual debate on the nature of information security.

Secondly, existing theories from reference disciplines can be applied to information security. From sociology, how could *Conflict Theory,* which focuses on competition (threats?) to resources (information?) and the inherent iniquity afforded some units (organisations?) in society, be adapted to information security? From economics, how could the *Pareto Principle Theory* (the 80/20 rule) be adapted to the application of expensive controls in information security?

Thirdly, improvements to the theory described in this manuscript and its use can be further developed. For example, additional theorising of this theory could result in a deeper understanding of the relationship between threats and controls. Do they have a bi-directional relationship? Could the use of particular controls dictate the threats that present themselves, both internal and external? Could the relationship between the constructs within this theory be reduced to a scientific law through the development of a mathematical statement such as I x (C/T) = R? How could this paper provide the theoretical base for conceptual models or frameworks of information security-related topics?

6 REFERENCES

Ahmad, A., Bosua, R., and Scheepers, R. 2014. "Protecting Organizational Competitive Advantage: A Knowledge Leakage Perspective," *Computers & Security* (42), pp 27-39.

Ahmad, A., Ruighaver, A., and Teo, W. 2005. "An Information-Centric Approach to Data Security in Organizations," *TENCON 2005 2005 IEEE Region 10*: IEEE.

Bacharach, S.B. 1989. "Organizational Theories: Some Criteria for Evaluation," *Academy of Management Review* (14:4), pp 496-515.

Barney, J. 1991. "Firm Resources and Sustained Competitive Advantage," *Journal of Management* (17:1), pp 99-120.

Baskerville, R. 2005. "Information Warfare: A Comparative Framework for Business Information Security," *Journal of Information System Security* (1:1), pp 23-50.

Beebe, N.L., and Rao, V.S. 2010. "Improving Organizational Information Security Strategy Via Meso-Level Application of Situational Crime Prevention to the Risk Management Process," *Communications of the Association for Information Systems* (26:17), pp 329-358.

Benbasat, I., and Zmud, R.W. 2003. "The Identity Crisis within the Is Discipline: Defining and Communicating the Discipline's Core Properties," *MIS Quarterly* (27:2), pp 183-194.

Catteddu, D. 2010. "Cloud Computing: Benefits, Risks and Recommendations for Information Security," in: *Web Application Security*. Springer, pp. 17-17.

Cavusoglu, H., Cavusoglu, H., and Raghunathan, S. 2004. "Economics of It Security Management: Four Improvements to Current Security Practices," *The Communications of the Assoc for Information Systems* (14:1), p 37.

Cronbach, L.J., and Meehl, P.E. 1955. "Construct Validity in Psychological Tests," *Psychological Bulletin* (52:4), p 281.

D'Atri, A., De Marco, M., and Casalino, N. 2008. *Interdisciplinary Aspects of Information Systems Studies: The Italian Assoc for Information Systems*. Springer Science & Business Media.

Denning, D.E.R. 1999. *Information Warfare and Security*. Addison-Wesley Reading MA.

Grant, R.M. 1991. "The Resource-Based Theory of Competitive Advantage: Implications for Strategy Formulation," *California Management Review* (33:3), pp 114-135.

Gregor, S. 2006. "The Nature of Theory in Information Systems," *MIS Quarterly* (30:3), pp 611-642.

Grover, V., Lyytinen, K., Srinivasan, A., and Tan, B.C. 2008. "Contributing to Rigorous and Forward Thinking Explanatory Theory," *Journal of the Assoc for Information Systems* (9:2), p 40.
Guarino, N. 1998. "Formal Ontology and Information Systems," *Proceedings of FOIS*, pp. 81-97.
Horne, C.A., Ahmad, A., and Maynard, S.B. 2015. "Information Security Strategy in Organisations: Review, Discussion and Future Research Directions," *The 26th Australasian Conference on Information Systems*, Adelaide, Australia.
Markus, M.L., and Saunders, C. 2007. "Looking for a Few Good Concepts and Theories for the Information Systems Field," *MIS Quarterly* (31:1), pp iii-vi.
McCumber, J. 1991. "Information Systems Security: A Comprehensive Model," *Proceedings of the 14th National Computer Security Conference*, Washington: National Institute of Standards and Technology. National Computer Security Center.
McKinney Jr, E.H., and Yoos, C.J. 2010. "Information About Information: A Taxonomy of Views," *MIS Quarterly* (34:2), pp 329-344.
Orlikowski, W.J., and Robey, D. 1991. "Information Technology and the Structuring of Organizations," *Information Systems Research* (2:2), pp 143-169.
Porter, M.E. 1980. "Competitive Strategy: Techniques for Analyzing Industries and Competitors." New York: Free Press.
Porter, M.E. 1981. "The Contributions of Industrial Organization to Strategic Management," *Academy of Management Review* (6:4), pp 609-620.
Porter, M.E., and Millar, V.E. 1985. "How Information Gives You Competitive Advantage," *Harvard Business Review* (63:4), pp 149-152.
Posthumus, S., and von Solms, R. 2004. "A Framework for the Governance of Information Security," *Computers & Security* (23:8), pp 638-646.
Rivard, S. 2014. "Editor's Comments: The Ions of Theory Construction," *MIS Quarterly* (38:2), pp iii-xiv.
Roberts, N., Galluch, P.S., Dinger, M., and Grover, V. 2012. "Absorptive Capacity and Information Systems Research: Review, Synthesis, and Directions for Future Research," *MIS Quarterly* (36:2), pp 625-648.
Rogers, R.W. 1975. "A Protection Motivation Theory of Fear Appeals and Attitude Change1," *The Journal of Psychology* (91:1), pp 93-114.
Sandberg, J., and Alvesson, M. 2011. "Ways of Constructing Research Questions: Gap-Spotting or Problematization?," *Organization* (18:1), pp 23-44.
Siponen, M.T., and Oinas-Kukkonen, H. 2007. "A Review of Information Security Issues and Respective Research Contributions," *ACM Sigmis Database* (38:1), pp 60-80.
Teece, D.J. 2000. "Strategies for Managing Knowledge Assets: The Role of Firm Structure and Industrial Context," *Long Range Planning* (33:1), pp 35-54.
Von Solms, R. 1998. "Information Security Management (3): The Code of Practice for Information Security Management (Bs 7799)," *Information Management & Computer Security* (6:5), pp 224-225.
Von Solms, R., and Van Niekerk, J. 2013. "From Information Security to Cyber Security," *Computers & Security* (38), pp 97-102.
Walsham, G. 1995. "Interpretive Case Studies in Is Research: Nature and Method," *European Journal of Information Systems* (4:2), pp 74-81.
Weber, R. 2003. "Editor's Comments: The Problem of the Problem," *MIS Quarterly* (27:1), pp iii-xii.
Weber, R. 2012. "Evaluating and Developing Theories in the Information Systems Discipline," *Journal of the Association for Information Systems* (13:1), pp 1-30.
Webster, J., and Watson, R.T. 2002. "Analyzing the Past to Prepare for the Future: Writing a Literature Review," *Management Information Systems Quarterly* (26:2), pp xiii-xxiii.
Workman, M., Bommer, W.H., and Straub, D. 2008. "Security Lapses and the Omission of Information Security Measures: A Threat Control Model and Empirical Test," *Computers in Human Behavior* (24:6), pp 2799-2816.
Zmud, R. 1998. "" Pure" Theory Manuscripts," *MIS Quarterly* (22:2), pp xxix-xxxii.
Zmud, R., Robey, D., Watson, R., Zigurs, I., Wei, K., Myers, M., Sambamurthy, V., Webster, J., Agarwal, R., and Lee, A. 2001. "Research in Information Systems: What We Haven't Learned," *MIS Quarterly* (25:4), 2001, pp v-xv.

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for their valuable contributions to this paper. Also, this paper would not have been written without the outstanding efforts of pioneering scholars such as

Shirley Gregor and Ron Weber, who took the time to identify the path forward for other scholars wanting to develop a theory. To Suzanne Rivard, thank you for your patience and kind, gentle support.

COPYRIGHT