12-15-2019

A theory on information security: A pilot study

Craig A. Horne
The University of Melbourne, craig@informationalrisk.com

Sean B. Maynard
The University of Melbourne

Atif Ahmad
The University of Melbourne

A Theory on Information Security: A Pilot Study

Craig A. Horne[1]
School of Computing and Information Systems, The University of Melbourne,
Parkville, Victoria, Australia

Sean B. Maynard
School of Computing and Information Systems, The University of Melbourne,
Parkville, Victoria, Australia

Atif Ahmad
School of Computing and Information Systems, The University of Melbourne,
Parkville, Victoria, Australia

ABSTRACT

This paper[2] extends a proposed theory on information security using pilot data to further refine and elaborate. We argue that the goal of 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 recognized as the confidentiality, integrity and availability of information however we argue that the goal is actually to create business resources. This paper responds to calls for more theory in information systems and challenges our thinking. In a phenomenological grounded theory study, this paper identifies the core concepts of information security, and describes the relationships between these concepts. The paper provides the theoretical base for understanding why information is protected, in addition to theoretical and practical implications, and future research suggestions.

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

[1] Corresponding author. hornec@unimelb.edu.au +61 3 8344 1573

[2] An earlier version of this paper without data was published in proceedings at Australasian Conference on Information Systems 2016, see:
Horne, C.A., Ahmad, A., and Maynard, S.B. 2016. "A Theory on Information Security," *The 27th Australasian Conference on Information Systems*, Wollongong, Australia.

INTRODUCTION

Despite the practice of information security being very well established, the theoretical goals and motivations behind it are imperfectly understood. The emphasis for this paper is to explain the information security concepts and relationships between them in order to alter our understanding of why organisations protect information. 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).

More specifically, this paper is motivated by an apparent gap in the literature where a theory on information security is not apparent to explain why organisations secure their information. 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 gap however is not because information security is uninteresting. 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.

The aim of this research is to increase understanding about why organisations invest in information security. The scope of this paper includes analysing information security as defined in the information systems literature and experienced within Australian-headquartered organisations. We gain an understanding of the phenomena under investigation from 10 individuals who are accountable or responsible for securing information within their respective organisations, and who have personal experience with information security.

The paper proceeds in five major sections. After this introductory section, the next section reviews definitions of information security, examines gaps in existing theory, and

describes the research methodology. Third, we describe findings from the data. Fourth, we refine our proposed theory on information security. Finally, we draw conclusions, consider limitations and offer proposals for future research to improve our theoretical understanding of information security.

REVIEW – WHAT IS INFORMATION SECURITY?

This review section considers varying definitions of information security, and then reviews the theoretical literature for related theories. The result is a set of gaps and problem conditions that this research looks to fulfil.

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, we see that there are three different definitions for each of 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.

Theoretical Background

The role of prior theory and theoretical frameworks can be useful in qualitative studies and sensitivity to these can help identify key concepts that have been previously discovered or help inform the choice of methodology to be used in the study (Corbin and Strauss 2008; Wiesche et al. 2017). When examining a web-based resource that lists 104 theories which are commonly used in information systems, including theories originating from other disciplines, there are some extant theories related to information security (Larsen and Eargle 2018). 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 few theories that relate specifically to information security, leading to a narrow definition.

RESEARCH METHODOLOGY

This information security research falls within the domain of information systems, which has been defined and explained as a system composed of people and computers that processes or interprets information, and is the view adopted in this paper (D'Atri et al. 2008). 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). 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). In this research, a combination of methodologies is used, which include a phenomenological approach to the type of data collected and a grounded theory approach to data collection and analysis. Grounded theory is flexible and can be combined with other methodologies (Urquhart and Fernandez 2013). The phenomenology methodology puts the focus on understanding the lived experiences of the research participants and the grounded theory aspects guide the techniques for data collection, analysis, and presentation.

The primary method selected was interviews, long enough to investigate the topic in depth, lasting ~45 minutes, which were audio-recorded and transcribed (Polkinghorne 1989). An interview protocol was developed and can be viewed in Appendix 1: Interview Protocol. The interviews were semi-structured with a set of questions to guide the interview, however interesting answers were investigated further with unstructured follow-up questions. Data analysis began immediately after the first interview was completed, to identify related concepts and begin refining interview questions for the next interview (Corbin and Strauss 2008; Glaser and Strauss 1967). Open coding of the primary data to break them up into concepts according to

ideas or themes related to the subject matter was followed by axial coding to relate concepts with other concepts to create categories (Corbin and Strauss 2008; Glaser and Strauss 1967; Wiesche et al. 2017). During data analysis, questioning and constant comparison techniques were mainly used and supplemented by other techniques such as flip-flop, personal experiences, identifying red flags, emotions and time (Corbin and Strauss 2008).

FINDINGS

The aim of this section is to describe the findings after analysis of the data, providing a rich description of the concept of information security, analysed for its properties and dimensions, noting any variations throughout. After the data were analysed, the analyses were aggregated into categories, integrated, and interpreted in relation to the overall research (Corbin and Strauss 2008). Table 1 lists 10 research participants who were accountable for information security in their organisations.

Table 1. Data Collection Phase Sample – Organization Demographics

Participant	Industry	Size*	Job Title	Quals	Certificates	Experience
1 FedGov2	Government	Very Large	Dir ICT Sec	None	None	6 years
2 FinCo2	Finance	Very Large	Head InfoSec	BMath	CISSP	22 years
3 ITCo3	ICT	Medium	CEO	BCom	CISSP	18 years
4 ITCo4	ICT	Very Large	CSO	MCM	CISM	16 years
5 FedGov3	Government	Very Large	Cyber Policy	BA	None	4 years
6 TelCo1	Telecom	Very Large	CSO	MBA	None	5 years
7 EnerCo1	Energy	Very Large	CISO	MBA	None	20 years
8 AvCo1	Aviation	Very Large	CISO	None	CISSP	25 years
9 MgtCo2	Consulting	Very Large	Partner	MBA MIT	11+	18 years
10 FinCo3	Finance	Very Large	Head InfoSec	MBA	SABSA	15 years

*Small= 1-20 employees, Medium= 21-100, Large= 101-1,000, Very Large= 1,001+

Information

Information is a core category at the heart of information security, that has several properties and dimensions for each. MgtCo2 stated "*we are pushing toward a data-centric approach to security, because … we believe that [organisations] can then decide where they want to spend the money.*" The four main concepts related to information that emerged from the data were accessing the functionality provided by information, controlling and securing information, information as an asset, and information value.

Information has a value, which is one of its properties. In terms of dimensions, research participants did not universally agree on how to precisely measure the value of information other than to say it was generally high, even to the point of being irreplaceable such as proprietary intellectual property, or it was low. Information was then used as an asset to achieve business goals. As AvCo1 shared,

"We use something called most valuable information. You're probably familiar with the term crown jewels. With any company, there's always a set of what you call mission critical assets and that can be a set of IT applications or information database or whatever. You've got mission critical assets that without them, the company would either cease to function or even go out of business if they were compromised or unavailable in some way."

Information value can also change over time, typically decreasing. FedGov2 confirmed, "*90 percent of the data that sits within our data holdings is probably short-term or volatile data. It's good for a point in time, and then after that it becomes historical.*" Organisation may take an active approach to deciding whether to hold valuable information internally or not. FedGov2

offered "*it's around setting your information strategy about what's the important data, what are your high-value assets, and how much do you want to protect them?*"

Normally, most organisations identify their information, assess its value, and then assign a classification to it. FedGov2 stated, "*It's not just the classification that determines how we store and handle our information, it's the value.*"

Controls

Information is classified based on its value and then these classifications drive which controls are applied to the information to secure it. FinCo3 stated, "*those labels on those documents … drive a differential application of security controls. So, things that aren't very sensitive, we don't put as much energy into securing them as we do those things that are very sensitive*."

Identification of irreplaceable high value information has implications for the storage of that information, as organisations wanted to maintain complete control over it, reducing the risk of its loss as low as possible. ITCo4 confirmed "*The highly-sensitive trade secret type information is generally kept on isolated systems within our corporate environment.*"

Interestingly however, organisations sometimes mix high and low value information together when storing it, either through accident or convenience, which may waste money on unnecessarily expensive controls. ITCo4 commented,

"Traditionally, organisations, particularly the on-premise environments, don't make any distinction [between high and low value data] and that's a part of the problem. So, they use really expensive hardware and services, and they just store all their data together."

Getting it right however results in a business benefit, which is the conservation of security budget so that more financial resources are available to protect high-value information with better quality security controls. TelCo1 clarified, "*By categorising the information, you can actually get bang for your buck. You can put the right security controls around the [information] that matters. … Which one are you going to protect?*"

Goals

When questioned about what the goal of information security was, research participants sometimes stated the obvious, which was the goal is to keep information secure. AvCo1 for example, stated "*the goal of information security in an organisation is, obviously, the CIA, confidentiality, integrity, and availability of information assets. That's the key goal.*"

Goals often interrelated and supported each other however. Interestingly, the goal of information security was not always viewed however as simply keeping information secure. In a variation of this concept, the goal of information security was sometimes perceived as supporting the organisation in achieving its organisational goals. FinCo2 stated that the goal of information security was to "*protect the operation of the organisation. Make sure the organisation is able to operate safely*". ITCo4 commented "*The goal of information security is to enable the business to achieve its outcomes in a secure and managed way.*" MgtCo2 thought the goal of information security was "*to help the organisation accelerate its growth in a secure manner*."

Organisations instead sometimes viewed keeping information secure as the goal of implementing security controls. ITCo4 offered "*the goal of security controls is to be able to technically implement control over the information that you are going to produce, generate, disseminate, and store in various locations.*"

Threats

One key property of organisations is their ability to conduct effective information security, with dimensions ranging from ineffective to effective. Information can never be perfectly secure due to the existence of unknown threats. Zero-day exploits, which are newly-discovered vulnerabilities that could be used to conduct an attack, serve to highlight the existence of unknown persistent threats. An organisation's inability to perfectly convert unknown threats into known threats affects confidence levels in its security leaders, and TelCo1 believed organisations need to take a pragmatic approach to balancing security needs with business decisions, explaining "*Take a balanced approach on a commercial basis … you can't be a security purist because you might as well shut the shop and lock the doors and walk away.*"

Threats are mostly known so can be prevented, but there are some threats that are unknown. Information is generally stored in known repositories within the organisation however some valuable information is unknowingly stored together with non-valuable information, making it vulnerable. Also, security controls are generally selected and implemented according to sound heuristics and frameworks, however their effectiveness is unknown, given threat actors routinely impair their functionality. So, some threats are unknown, some valuable information is unknown, and the effectiveness of security controls is unknown. These three areas of uncertainty combined make it impossible for information security to be completely effective. ITCo3 continued with an example serving to highlight the problem with measuring information security, stating,

"As an example, people often bandy around spam numbers. We blocked 600 email-based attacks this month, and then next month you say we blocked 700 attacks this month. Great, is

that a good trend, or is that a bad trend? Then the next month you block 400 attacks. Does that mean you're blocking fewer attacks or there were fewer attacks and you blocked just as many of them? And is that something that you've actually affected, or is that just a random variation in attackers going after whoever they're going after?"

The volume of unknown threat vectors might be small but they're still there. Therefore, organisations cannot claim to have 100% protected their information. The clear majority of potential attacks can be identified so preventative security controls can be implemented to mitigate the risk of an attack. FedGov3 confirmed "*these days, you can never know whether something is completely safe or not, but you can have a clear indication.*"

Organisations did not raise or lower the value of the information dynamically in response to threats, but it's possible that they should be, according to MgtCo2 who stated, "*in my personal experience, they're not that mature*".

Resources

Organisational productivity can be negatively affected in the event of a security breach, as employee resources are often redeployed internally to remediate the situation. FinCo2 explained, stating,

"Productivity. If we had a serious incident, there's a serious breach, we would end up assigning a significant workforce to work out what happened, and respond and recover from that sort of activity, and that would require engagement of media outlets, our regulators, our technology teams, our business teams to go and talk to customers. It would be a massive hit on productivity. Instead of working on new things, we would basically go into holding pattern for a period of time while we suffer the storm."

EnerCo1 identified that various resources can have their productivity affected, not just employees, such as their manufacturing plants, stating,

"I'd say generation sites is probably the big thing. I suppose … if [Supervisory Control and Data Acquisition] SCADA systems got ransomwared … stopping our manufacturing plants, where we manufacture electricity, that's a big thing."

The loss of trade secrets or IP can lead to a loss of competitive advantage and market position, through leakage of trade secrets to competitors or a decrease in revenue. MgtCo2 gave an example, stating,

"For example, if there is a data breach … in the mining sector, information around their digging, their next geospatial data, where the next multiple years of millions of dollars of mining revenues are going to come from then, yes, it does have an impact."

FedGov2 experienced the effects of organisations losing trade secrets to well-prepared competitors, stating, "*We've certainly seen in the past, organisations who've suffered some sort of breach, lose a lot of business to a competitor who's got a rock-solid security model.*"

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 replicate the goal of computer security. We deconstruct the proposed theory on information security into its various concepts, and the relationships between the concepts.

Theory Overview

Information security is a process where people and organisations attempt to create sustainably-viable resources, from information. They apply suitable controls to protect information from threats, according to the goals of the organisation, which results in sustainable resources. Controls are applied to ensure the confidentiality, integrity, and availability of the information. Information security focusses on what protection is afforded to information of varying value and what use that protected information can then offer organisations.

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).

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).

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). First, information security *depends on a completed information classification assessment*. Second, an organisation's

information security *depends on the security budget.* Third, information security *depends on an organisation's ability to match controls with threats*.

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.

Means of representation

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

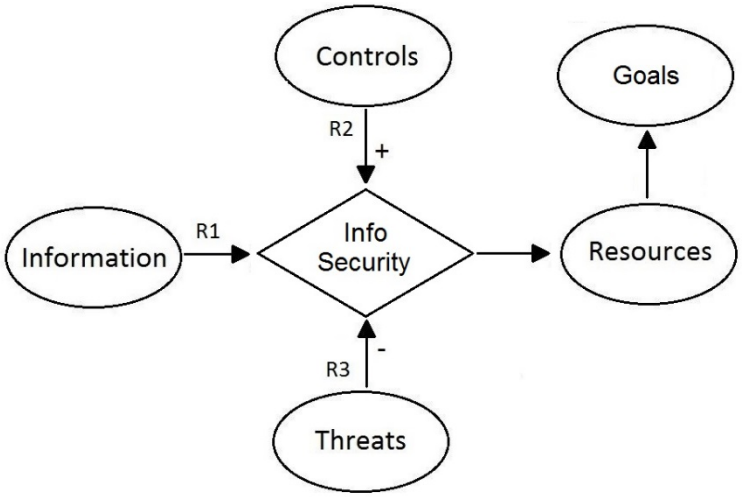

Figure 1. Layout of Figures and Captions for Figures

Constructs

The nomological network is comprised of key constructs: information, controls, threats and resources. The following section describes each in turn and ascribes meaning to each.

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 2 provides examples of each:

Table 2. Examples of Organisational Information and Level of Analysis

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

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 an 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.

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 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.

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.

CONCLUSION

This paper offers a strong rationalisation for why the conceptualisations developed in this research 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. Our proposed 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.

There are various implications of the research model and these can be separated into both research and practice areas (Zmud 1998). 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. 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.

Limitations of Research into Information Security

There are limitations on our perception of information security theory, some of which follow. First, information security has been conceptualised in various forms, including as a process (Von Solms and Van Niekerk 2013), and as a capability and a framework (Siponen and Oinas-Kukkonen 2007). These raise concerns around construct validity issues, as adhering to one conceptualisation risks marginalising another. Second, this information security theory can be applied at various levels. Third, 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.

Future Research Directions

The following are suggested research directions for information security theory development, with these directions being adapted from Zmud (1998). First, the theory presented in this paper can be refuted by developing alternative new theories on information security,

hopefully stimulating intellectual debate on the nature of information security. Second, existing theories from reference disciplines could 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? Third, improvements to the theory described in this manuscript and its use could be further developed.

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.

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," *Communications of the Association for Information Systems* (14:1), p 37.

Corbin, J.M., and Strauss, A. 2008. *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory*, (3rd ed.). Thousand Oaks, CA: Sage Publications Inc.

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. 1999. *Information Warfare and Security*, (8th ed.). MA, USA: ACM Press Books.

Glaser, B.G., and Strauss, A.L. 1967. *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago, IL, USA: Aldine Publishing Company.

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.

Larsen, K.R., and Eargle, D. 2018. "Theories Used in Is Research Wiki." Retrieved 27/07/2018, from http://IS.TheorizeIt.org

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.

Polkinghorne, D.E. 1989. "Phenomenological Research Methods," in: *Existential-Phenomenological Perspectives in Psychology,* R.S.V.a.S. Halling (ed.). New York, USA: Plenum Press, pp. 41-60.

Porter, M.E. 1980. *Competitive Strategy: Techniques for Analyzing Industries and Competitors*. NY, USA: The 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.

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.

Urquhart, C., and Fernandez, W. 2013. "Using Grounded Theory Method in Information Systems: The Researcher as Blank Slate and Other Myths," *Journal of Information Technology* (28:3), pp 224-236.

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.
Wiesche, M., Jurisch, M.C., Yetton, P., and Krcmar, H. 2017. "Grounded Theory Methodology in Information Systems Research," *MIS Quarterly* (41:3), pp 685-701.
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.

APPENDIX A – INTERVIEW PROTOCOL

This list of interview questions following the introductory demographic questions about the participant's background and organisational attributes:

a. What is the goal of information security?
b. How important is information to an organisation?
c. How can information become unusable over time?
d. How do threats affect an organisation's information?
e. How do security controls affect an organisation's information?
f. What is the goal of implementing security controls?
    f.a. If participant offers the same answer as (a) goal of information security, then why?

ACKNOWLEDGEMENTS

The authors would like to thank the reviewers for their valuable contributions to this paper. This research received funding support from Australian Government Research Training Program Scholarship.