Pattern, Practice, and Potency of Information Systems Security Research: A Methodological Perspective

RUILIN ZHU

A thesis submitted in fulfilment of the requirements for the degree
of Doctor of Philosophy in Information Systems
The University of Auckland
2017

This page intentionally left blank

TABLE OF CONTENTS

ABSTRACT

As the use of information systems (IS) has become more widespread, information systems security (ISsec) has grown in significance. Prompted by the need for safe, robust and reliable systems, much research has been conducted in this area. However, this research is generally viewed as esoteric and incomplete, doing little to allay people's security concerns; thereby hindering the further development of this discipline.

In order to gain a better understanding of ISsec and, more importantly, to lend impetus to the creation of a systematic research roadmap, this study undertakes a comprehensive survey of ISsec literature. It draws on the reticulated model of science and multilevel theory to compare the paradigms, methods, theories and analysis found in different research tracks.

Keyword selection was employed to identify 108 pieces of ISsec research published in 12 of the top IS journals. These were chosen as together they represent the highest and well-accepted standards of research quality and reflected the primary research focuses of the ISsec community. An examining framework was then developed that incorporated the most authoritative and popular typology for each of the four targeted components (paradigm, theory, method and analysis). The introduction of these research components makes this framework significantly different from its

predecessors in that it facilitates the systematic comparison and contrast of ISsec research. Following this systematic comparison, it was possible to categorise all of the articles into clusters or tracks.

The analysis identifies a pattern of four research tracks in ISsec research. Each track represents a particular combination of the four research components and is named according to its core theme: ISsec economic research, ISsec behavioural research, ISsec strategic research and ISsec design research. In the next stage of the analysis, each track is examined individually to identify the practices within that track, including any limitations regarding the methodological components. Where such limitations are identified, recommendations are made for improving future practice.

The analysis moves on to discuss the potency of ISsec research, considering the ramifications of the defined pattern and practices, and demonstrating how ISsec might progress to become more theoretically rigorous and empirically relevant. It highlights the close but long-overlooked connections within existing ISsec research, and builds a viable research matrix by delineating existing research patterns and analysing previous research practices. It goes on to describe the core differences between the four tracks, arguing that even if researchers adopt a wider range of methodological components, as recommended, the tracks are unlikely to be assimilated. Finally, it acknowledges the need for the ISsec community to engage with the concept of ISsec and further develop theory in the discipline by examining the nature of the four research tracks, and their

relationships. Consequently, it seeks to develop a conception of ISsec; thereby providing a foundation for better understanding this field.

It is hoped that this work has enriched the understanding of ISsec research by distinguishing the predominant pattern, extended ISsec research practices by bridging the current research gap, and confirmed the methodological and practical developments of ISsec research by identifying the latent potency that resides in the inter-relations among tracks. This enables it to further conceptualise ISsec to shed light on its nature and implications. The findings are potentially useful both to academics and practitioners.

Keywords: Information Systems, Information Systems security, research methodology, literature survey, reticulated model of science, multilevel theory

This page intentionally left blank

ACKNOWLEDGEMENTS

Undertaking the Ph.D. in New Zealand has been a truly life-changing and concept-shaping experience. It would not have been possible without the generous support and unreserved guidance I have been fortunate enough to receive from many people over the years. I wish to offer my most heartfelt thanks to the following.

First and foremost, I want to thank my adviser Dr. Lech J. Janczewski, for his advice and support, and his willingness to allow me to pursue research on topics about which I am passionate. It has been a great honour to be his first Chinese doctoral student. He has taught me, both consciously and unconsciously, how to conduct good information systems security research. I appreciate all his contributions of time, effort and funding to make my Ph.D. experience possible, productive and stimulating.

The members of the ISOM department in The University of Auckland Business School have contributed immensely to my personal and professional time in New Zealand. The department has been a source of good advice and collaboration. Moreover, I found its joy and enthusiasm for life and research have been contagious and motivational, especially during the more difficult times.

I am especially grateful for the support, encouragement and advice offered by the Head of Department, Professor Michael D. Myers. Despite having a full schedule, he has

always encouraged my research and allowed me to grow as an information systems scholar. His advice on both my research and my career has been invaluable.

Many thanks also to Professor Ananth A. Srinivasan for always keeping his office door open and being available whenever needed. His advice on matters of quantitative research methodology has done much to make the paper more informative and interesting.

I acknowledge with gratitude the funding received towards my Ph.D. from The University of Auckland Doctoral Scholarship Fund. I am also grateful for the funding I received through the ISOM department.

I greatly appreciate the support received during my academic visits to Imperial College London (UK) and Georgia State University (Atlanta, USA) during the first phase of my research. Thanks go to Dr. Emil C. Lupu and Professor Richard L. Baskerville for making the first few months of Ph.D. research all the more interesting, and for ensuring I stayed on the right path.

My thankfulness is also extended to the support I received during my collaboration with Monash University (Melbourne, Australia). I am especially grateful to Dr Aashish Srivastava for believing in my research and for the financial support received through the Australian Endeavour Fellowship to undertake the research analysis.

My time at The University of Auckland Business School has been made enjoyable in large part by my colleagues. I am grateful for the time spent with my office mates in Room 587, who have always been so helpful throughout my thesis. In particular, I would like to thank Smita Paul and Mr. Samuel Spink-McCarthy for their kind, caring and generous help during my time in Auckland. I am indebted to them for opening their homes to me and for being enormously helpful in numerous ways. My time in New Zealand has also been enriched by my friends Mr. Tobias Riasanow, Ms. Catharina M. Mail, Ms. Chrissy Bretherton, Ms. Josephine Yean Theen Lee, Ms. Sandra Yan, Dr. Giannoula Karamichailidou, and Professor Charlene Lee.

A very special thank you to Ms. Carolyn Marshall for checking my academic writing with patience and care.

Most of all, I would like to say a heartfelt thank you to my Mum and Dad for all their love and encouragement. They raised me with a love of knowledge, supported me in all my pursuits, always believed in me and encouraged me to follow my dreams. Loving and patient parents, their faithful support during all the stages of my Ph.D. has helped carry me through some difficult times. Thank you!

Finally, to anyone may I have forgotten, I apologise. Thank you as well.

This page intentionally left blank

LIST OF TABLES

LIST OF FIGURES

SECTION I INTRODUCTION

This section outlines the background to the research. It begins by explaining the necessity and importance of this research, highlighting the contrast between the high demand for secure information systems (IS) and the low output in terms of systematic information systems security (ISsec) research. This is followed by a chapter examining the strengths and weaknesses of the existing literature within this field. The section concludes with a statement of the two research questions that guided the investigation.

Chapter 1 BACKGROUND

As Information Systems (IS) have developed over the last few decades, their popularity has spread to the extent that they are now deployed in almost all organisations. Bodies of all types and sizes have adopted IS for administrative, managerial, marketing, communication and production purposes in their efforts to adapt to a fast-changing world and enhance competitiveness. The growing popularity of IS has sparked a series of research activities aimed at boosting efficiency and reliability, resulting in a continuously-evolving methodology. Subsequently, this has influenced IS development clearly and directly (Hirschheim, 1985).

Information Systems security (ISsec), however, has received little attention, compared with other IS issues (Brancheau et al., 1996; Siponen et al., 2008). According to a 2013 survey released by the UK's Department for Business, Innovation and Skills (the latest available), 42% of large organisations do not provide any ongoing security awareness training to their staff, despite 78% being attacked by an unauthorised outsider in the preceding year (BIS, 2013). But safe, robust and reliable IS are crucial if an organisation is to achieve its business goals (Yeh & Chang, 2007).

The need to develop effective ISsec should be driving academic activity, but published anecdotal evidence and existing ISsec survey research suggest that research in ISsec lags the general advances in IS (Siponen et al., 2008); moreover, it is often perceived

as esoteric and inconclusive. The few existing studies are isolated rather than systematic, and ISsec research generally has been disjointed. Those studies that do contain in-depth analysis focus only on a small number of ISsec research outputs, while those that examine a large number of articles merely list their conclusions rather than presenting an adequate analysis. Thus, a comprehensive study of ISsec research is overdue.

The main purpose of this research is to provide practical suggestions for the improvement of ISsec research methodology that draw on a large quantity of research articles. The literature survey was conducted from a methodological perspective in anticipation of establishing the methodological pattern of ISsec research, identifying the most popular practices, proposing more comprehensive ones, and identifying their underlying potency. The researcher aims to provide detailed descriptions of current ISsec research and analyse the methodologies employed to offer suggestions for future research. It is noteworthy that the literature survey was undertaken at the time of this research's commencement (2014-2015). Consequently, the contemporary reader may find the research articles in the survey slighted outdated. However, they reflected the state-of-art status of ISsec domain at the time of their publication.

The next chapter begins this process by examining the literature pertaining to ISsec to identify current research activities. This is followed by a review of the literature on ISsec research. The research questions and research aims were generated based on these reviews. Chapter 3 begins the discussion of the research methodology by explaining how the scope of the literature survey was determined and how the retrieval process

was conducted, while Chapter 4 discusses the theoretical underpinnings of the study and the development of the examining framework. Chapter 5 presents the preliminary research results, indicating the overall pattern of ISsec research, while Chapters 6 to 9 discuss current research practices in each of the four identified tracks, making recommendations where appropriate for their development and extension. Chapter 10 draws these findings together to trace the influence and development of current ISsec research, highlighting its potency. This chapter attempts to theorise ISsec further by analysing all the research tracks and dimensions. Chapter 11 concludes the research by highlighting the implications of the findings and suggesting potential areas for future investigation.

Chapter 2 LITERATURE REVIEW

Mounting threats to IS security and the growing attention paid to this issue have prompted a range of studies on ISsec. Several important threads have been developed in ISsec research, but have not been woven together into a cohesive fabric. To achieve a better understanding of current ISsec research activities and establish a clear research pattern, this chapter reviews the literature pertaining to ISsec and ISsec research. It summarises briefly the current activities in ISsec research before identifying research gaps.

2.1 INFORMATION SYSTEMS SECURITY

As modern business environments have become more dynamic and competitive, many organisations have chosen to equip themselves with a more agile and flexible IS to respond to internal and external changes. However, as organisational dependence on IS has grown, so too has the number of security incidents (Ahmad et al., 2014). Thus, it has become increasingly vital to protect these systems. Researchers responding to these security concerns have focused on a range of topics, including the use of software to detect IS security abuses (Nance & Straub, 1988), measures for preventing IS security abuses (Straub, 1990) and perceptions of the adequacy of IS security (Goodhue & Straub, 1991).

While seeking ways to organise the literature in the review, the researcher recognised the difficulty of crafting a fully comprehensive list that avoids bias towards some sub-area of ISsec or certain disciplines. To avoid this problem, the researcher decided to adopt the three ISsec categories proposed by Siponen (2005): access to IS, the management of ISsec, and the development of secure IS.

2.1.1 Access to IS

Access to IS relates to the various means used to control subjects' access to objects requiring information security; for example, files, directories, tuples or relations (Sandhu, 1993). Authentication is a key stream within this research track. Authentication is the process of verifying the identity of a user, device or other entity in an information system, often as a prerequisite to allowing access to resources in the system (Kissel, 2013). The authenticating entity accomplishes verification by matching some short-form indicator of identity, such as a shared secret that has been pre-arranged during enrolment or registration. Methods of authentication are usually grouped into three categories: knowledge-based (what you know, e.g., password), which is characterised by secrecy or obscurity; object-based (what you have, e.g., token), which is characterised by physical possession; and ID-based (who you are, e.g., biometric), which is characterised by uniqueness to one person (O'Gorman, 2003).

Knowledge-based authentication is most likely to rely on a password comprising a single word, phrase and/or personal identification number (PIN) that must be kept secret

by the user. Passwords continue to be used in various contexts, from logging-in to online services to depositing and withdrawing cash, despite numerous studies highlighting the central vulnerability of this method; in other words, a memorable password is easier for an attacker to guess, while a long, random, regularly changed password is difficult for the user to remember (Furnell et al., 2006; Pond et al., 2000).

Object-based authentication was developed to address this problem. In this method, a physical device or token is required to perform authentication. This will either be a secure storage device containing passwords, or an active device that generates one-time, time-synchronous or challenge-response passphrases (Baumgart et al., 2007).

Biometric identification involves measuring some feature or characteristic of the user that is sufficiently distinct for use in identity authentication (Rowe, 2009). Such ID-based authentication is the subject of increased attention but also some controversy; although convenient and safe, there are concerns over privacy. Notwithstanding these reservations, its use is spreading and becoming more standardised (Ellerbrok, 2011). There are three main domains of biometric identification (Bhattacharyya et al., 2009):

(1) Physiological biometrics rely on the uniqueness of an individual's physical characteristics. Typical examples in this class are fingerprint, facial recognition, hand geometry and iris recognition;

(2) Behavioural biometrics are related to behavioural characteristics, such as signature, keystroke dynamics and voice; and

(3) Cognitive biometrics is a newly-developed domain that measures human perceptions in a brain-machine interface. The brain's response to certain stimuli may be used to trigger a search of the IS database.

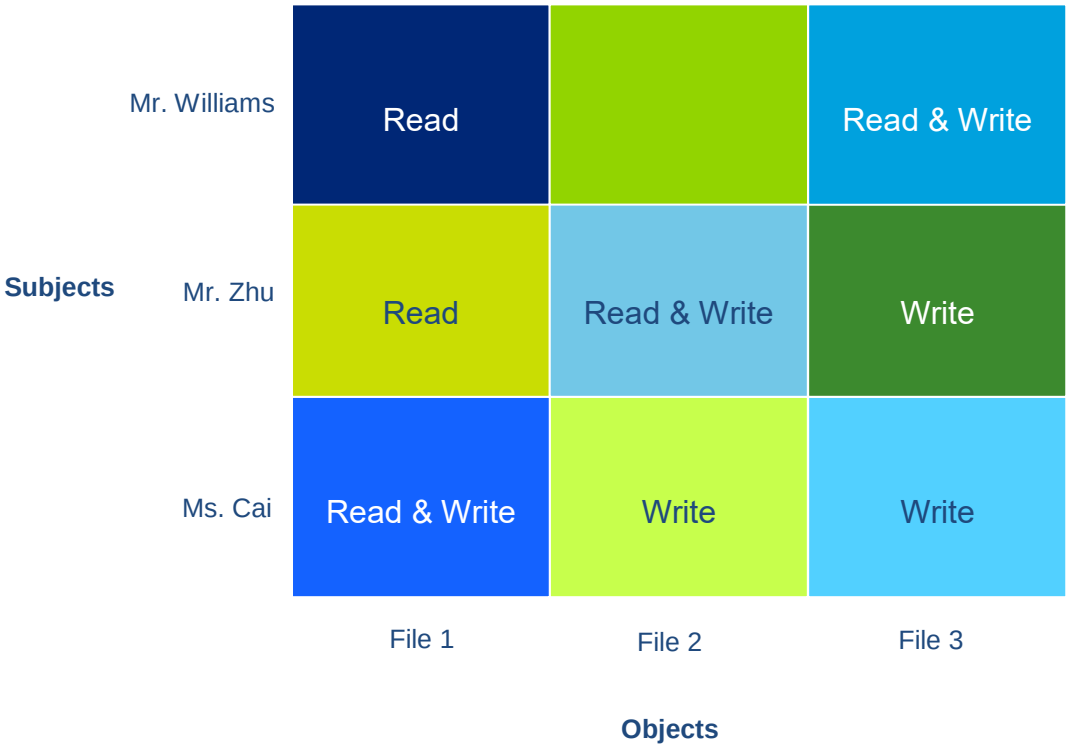
The inextricable link between authenticator and owner means that biometrics are regarded generally as safer and more robust than passwords and tokens (which can be lent or stolen). Nevertheless, even biometric features can be copied or counterfeited to gain unauthorised access to a security system (Uludag et al., 2004). In other words, none of these methods (passwords, tokens or biometrics) is unassailable.

Consequently, another research stream has emerged that focuses on non-technological issues around IS access. It concentrates not on developing more effective methods of identity authentication, but on controlling access and limiting the activity of legitimate users (Damianou et al., 2001). This control is exercised through a set of rules that mediates every access attempt by a self-claimed user. Researchers in this area have developed several abstractions, including the access matrix, mandatory access control (MAC), discretionary access control (DAC), role-based access control (RBAC) and attribute-based access control (ABAC).

The access matrix is the most widely-accepted conceptual model specifying the rights subjects have over objects (Sandhu, 1992). Specifically, there is a row in the matrix for each subject and a column for each object. Each matrix cell stipulates whether the subject in a given row has access to the object in a given column. Controlling access

means ensuring only authorised operations are executed. Figure 2.1 provides a simple example of an access matrix.

Figure 2-1: Example of an Access Matrix



MAC policies, usually associated with the Bell-LaPadula Confidentiality Model (Lindqvist, 2006), govern access based on security classification. Subjects and objects are assigned a security level; in the case of the former, the security level indicates their perceived trustworthiness, while the latter reflects the sensitivity of the information contained therein. A subject can be granted access to an object only if some relationship is satisfied between the security levels associated with the two. While the introduction of security levels supports security by placing restrictions on user actions, it prevents dynamic alteration of the underlying policies.

Conversely, DAC policies govern access to information on the basis of the user's identity and authorisation to access any given object (Osborn et al., 2000). Each request to access information is checked against the specified authorisations. The problem with DAC is that maintaining the system and verifying security principles is extremely difficult because it is the users who control access rights to owned objects.

Despite the similarities of MAC and DAC in delegating the access permission, their differences are summarised here in brief. In general, within DAC environment, individuals can secure or open up access to controlled objects entirely at their discretion. These permissions are active when the users are the owners of objects, and they can further grant permissions to other users and groups in the same system. In this regard, DAC is based on resource ownership. Within MAC, however, the individuals have no such discretion; the users that can access only protected objects are established by the root user, thus, they cannot alter access. This is to suggest MAC is an administrator-centred model.

RBAC is a much more generalised model than either MAC or DAC, providing a policy-neutral framework that allows access control to be customised on a per-application basis (Ferraiolo et al., 2001). It combines the MAC and DAC models, regulating users' access to information based on the activities they execute in the IS. RBAC requires identification of the user's role; in other words, the actions and responsibilities associated with their specific activities. Rather than specifying all the accesses to which each user is entitled, access is attached to specific roles, with the user playing that role

being allowed access to all areas/information for which the role is authorised. The consolidation of access control for multiple users into a single role allows for much easier management of the overall system and much more effective verification of security policies (Oh & Park, 2003).

ABAC is a similarly flexible approach to access control; limited only by the computational language and the richness of the available attributes, it is ideally suited to today's diverse and rapidly changing environments (V. Hu et al., 2015). ABAC allows for a higher number of discrete inputs into an access decision, consequently generating a larger set of possible combinations of variables to inform a larger and more definitive set of possible rules. This flexibility enables access rules to be created without the need to specify individual relationships between each subject and object.

In summary, while technically-based research aims for safer, more user-friendly and convenient ways to authenticate user identity, the primary focus of non-technical research is to draft smarter policies that offer greater flexibility while maintaining strict control over authorisation.

2.1.2 ISsec Management

ISsec management refers to the measures organisations take to keep their IS secure. A key stream within this research area is ISsec policy, which has been the focus of interest of numerous researchers. Sanderson and Forcht (1996), for example, highlight the importance of security policies, Pounder (1997) examines European Union information

security proposals, Dhillon (2007) presents a meta-analysis of the meaning of security policies and related concepts, and Doherty and Fulford (2005) and Siponen and Iivari (2006) analyse the design, development and alignment of security policy. As information technology has advanced, research in this track has also begun to discuss security policies in more specific contexts, such as mobile-phone communications (Chan et al., 1993), the outsourcing of security (Sherwood, 1997) and the cloud-computing environment (Jaeger et al., 2008).

The literature suggests that where security policies are in place to help safeguard against the misuse, abuse and destruction of IS assets, users, especially employees, are often slow to comply with these documents (Ifinedo, 2012). Several studies have been undertaken to investigate the factors that may serve to inhibit or encourage security policy compliance in organisations (e.g. Herath & Rao, 2009b), resulting in the emergence of a new research stream focusing on the human perspective of ISsec management. This investigates end-user behaviours to identify the factors that yield compliance with information security policy. The literature recognises that insiders (i.e. employees who are authorised to use a particular system or facility) (Colwill, 2009) may jeopardise information security through ignorance, mistakes or even deliberate acts, and that this can pose a major challenge for organisations (Johnston & Warkentin, 2010; Sarkar, 2010).

Most empirical studies that have investigated end-user behaviours assume that employees simply choose to engage in inappropriate behaviours (Workman et al., 2008).

Those studies (D'Arcy & Herath, 2011; Rhee et al., 2009) that have focused on preventative strategies (e.g., sanctions) to reduce IS misuse and computer abuse have therefore been conducted either from a criminological perspective (e.g., general deterrence theory, rational choice theory, situational crime prevention theory) or that of the health belief model (i.e. protection motivation theory). The former tends to accept sanctions and penalties as the sole means of deterring IS misuse and abuse (Herath & Rao, 2009b); thereby implying that if violations are severely punished, employees will cease to engage in unacceptable behaviour. However, while these studies have advanced knowledge in this area, new insights are emerging to challenge this view. Vance et al. (2012), for example, reveal that security policy compliance research that draws on criminology and fear appeal theories does not always explicate noncompliance behaviours. They argue that erring employees may use neutralisation techniques to circumvent or minimise the effects of reprisals from their organisation.

Since behavioural intentions are rooted in socialisation and social influence, in addition to personal beliefs and cognition, many other factors may also impact on compliance behaviour vis-a-vis security policy (Doherty & Fulford, 2006). Identifying these factors is central to expanding the literature on ISsec and defining where organisations should focus when devising mechanisms to improve employee compliance. Researchers have approached this task from both the micro and macro-level perspectives. Those investigating micro-level factors include Tyler and Blader (2005), who argue that the motivation to follow (or not to follow) rules and regulations is internal and depends on the employee's intrinsic desires. Conversely, Kirsch and Boss (2007) highlight the role

played by external motivators. They conclude that rewards are ineffective in convincing individuals to comply with security policies, but that specifying policies, evaluating behaviours and computer self-efficacy are effective. Meanwhile, Pahnila et al. (2007) offer a theoretical model proposing that information quality impacts significantly on actual compliance; that threat appraisal and facilitating conditions have a significant effect on attitude towards compliance; but that neither sanctions nor rewards influence users' intention to comply or actual compliance. Researchers investigating macro-level factors that affect compliance include Hu et al. (2012), who posit that cultural differences moderate the execution of security policies. This view is echoed by Myyry et al. (2009), who suggest that moral reasoning and personal values influenced by social factors can explain a user's adherence to information security policies.

Furthermore, scholars have highlighted the role of security awareness in making users behave more responsibly. With the introduction of the personal computer and the increasing complexity and reliability of information technology, IS have become an indispensable part of daily operations for a wide range of end-users. It is vital that these users are security-aware, although as the NIST (National Institute of Standards and Technology) states in its Special Publication 800-16: "Awareness is not training. The purpose of an awareness presentation is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognise IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information" (NIST, 1998).

Since NIST issued its Special Publication, a series of conceptual studies (Furnell et al., 2002; Hentea et al., 2006) have reiterated the importance of information security awareness. Examples include Puhakainen and Ahonen (2006), who propose measures for improving information security awareness campaigns, and D'Arcy et al. (2009), who suggest that organisations should promote user awareness of security policies as one of three key countermeasures to reduce IS misuse. Others have explored the relationship between awareness and behaviour; Albrechtsen and Hovden (2010) investigated the positive effect of awareness on behaviour, while Bulgurcu et al. (2010) conducted an empirical exploration of the role information security awareness plays in determining compliance behaviour. Researchers interested in security awareness have focused primarily on the organisational level and company environments; however, Siponen's (2001) five-dimension information security awareness framework encompasses both organisational and societal levels. The user dimension, nevertheless, has been largely neglected (Furnell et al., 2006; Herath & Rao, 2009b), leading Tariq et al. (2014) to call for studies that examine the issue from an individual perspective. When Zhu (2015a, 2015b) responded by investigating customers' security awareness in the context of Internet banking, which he found lacking.

However, some scholars question whether security awareness alone is sufficient to prevent information misuse. Like the NIST publication quoted above, Katsikas (2000) and Wilson and Hash (2003) argue that security awareness merely means being alert to the concept of information security; the purpose of security awareness presentations is to ensure only that individuals know their roles and responsibilities in protecting the

information they possess (Amankwa et al., 2014). Therefore, they caution against relying solely on awareness, and recommend education as a practical measure to protect information security.

According to Amankwa et al. (2014), information security education seeks to provide the recipient an understanding of information security documents; thereby equipping them with the skills and competencies required to ensure the confidentiality, integrity and availability of information. This education generally takes the form of in-depth theoretical instruction over a long period (Garrido & Bandyopadhyay, 2009); thus, rendering it more systematic and comprehensive than security awareness presentations and more likely to support security effectively. The significance of such instruction is emphasised by Mabece et al. (2016), who argue that organisations should educate all new employees about information security and its practices to ensure the protection of their information assets. Similarly, several researchers (Aboutabl, 2006; Lo et al., 2015; Pastor et al., 2010) have addressed the question of how best to establish an informative, effective and practical curriculum for information security education.

In summary, beyond demonstrating the direct influence of security policies on ISsec management, academics have attempted to understand the antecedents of user compliance and security awareness by disentangling the relationships between micro and macro-factors and security-related outcomes. Moreover, this research stream seeks to deliver better information security by developing security education.

2.1.3 Development of Secure IS

Secure IS development refers to the process of embedding security elements in all phases of a system's development lifecycle (safety requirements analysis, safety design, safety code, safety testing and a series of safety processes) and ensuring the security of software products throughout (Kocher et al., 2004). It is viewed generally as a very effective way of reducing security flaws; in particular, logic errors in system security requirements analysis and system design.

Developing secure IS involves collecting a set of security requirements, expressing and modelling these security requirements, and ensuring the IS meets the stated requirements. It is vital that the IS are properly protected from the very beginning (Mellado et al., 2007), as the organisation may face huge losses if it fails at a later stage. A critical part of the security development process is security requirements engineering. This involves the use of techniques, methods and standards for tackling this task in the IS development cycle (Haley et al., 2006). It adopts repeatable and systematic procedures to ensure the set of requirements gathered is complete, consistent, analysable and easy to understand by the various actors entwined in the development of the system (Fabian et al., 2010). However, the increasing complexity of applications and services has made this task more difficult, and there is now a wide range of standards addressing requirement collection, including ISO/IEC 27000, ISO/IEC 13335, ISO/IEC 15408, NIST/FIPS 199, NIST/FIPS 200, and NIST/SP-800. Further IS security requirements have been proposed by Toval et al. (2002), Popp et al. (2003) and

Breu et al. (2004). Collectively, these address security requirements at all stages of the IS development cycle.

Another stream in this research field focuses on methods for developing secure IS. This encompasses structural and object-oriented notations for modelling security aspects (Baskerville, 1989), and measures for analysing the security of business processes (Herrmann & Pernul, 1999). The earliest IS development method employed checklists and simple risk analysis to support decision-making. Its simple approach to the specification of system design evolved from the experience of early practitioners in the computer industry. Later methods emphasised the mechanistic partitioning of complexity in a desired system and entailed a search for the critical controls that would provide satisfactory protection for an entire IS. Another suggested method focused on abstract models to understand the diverse and dynamic security needs in IS. More recently, Fernández-Medina et al. (2004) introduced an extension of the Unified Modelling Language (UML) that allows scholars to represent the main security information of data and its constraints of datasets in multidimensional (MD) modelling at the conceptual level. This method allows both information and user to be grouped into security classes, making it possible to implement secure MD models that can implement multilevel IS at any stage.

Another research stream addresses technology-related issues, such as the security of GCI/API programming and ActiveX security (Garfinkel & Spafford, 1997), security aspects of code distribution (Zhang, 1997) and the difficulties of developing

architecture for mobile software agents (Vogler et al., 1997). This stream is discussed more in the realm of computer science and software engineering. Of greater relevance within the context of this research are the studies exploring key, backup, recovery and contingency management, and those on cryptographic techniques (including the keys used for encryption and decryption) and security checklists (Smith & Sherwood, 1995). Finally, management standards, such as BS ISO/IEC 27000 (Humphreys, 2006) and ITSEC (Straw, 1995), outline the actions organisations should take to understanding the fundamentals, principles and concepts, to improve protection of their information assets.

2.1.4 Summary

Unlike more mature disciplines, such as computer science and computer engineering, there is neither a universally-accepted common body of ISsec knowledge nor a model structure for ISsec (Crowley, 2003). Therefore, it is perhaps unsurprising that the researchers mentioned above have very different views on the key information security problems and how they might be resolved. Furthermore, it is apparent that scholars working within one research track frequently appear unaware of the contributions made by researchers in other tracks. Consequently, there is a general lack of understanding of the connection between discoveries and developments. This has two major implications. First, scholars in different tracks may end up trying to reinvent the wheel. Second, it underlines the point that addressing security problems holistically requires interdisciplinary efforts (Willison & Siponen, 2007).

2.2 INFORMATION SYSTEMS SECURITY RESEARCH

A number of useful contributions have been made by authors examining ISsec research. Generally, they have concentrated on two dimensions: secure IS development research and overall ISsec research. These contributions are summarised below.

2.2.1 Secure IS Development Literature Research

Baskerville (1993) pioneered the exploration of ISsec research, detailing the lack of consistency between system development methods in general and security development methods in particular by comparing the two. He examined all the main secure IS development methods across three generations to illustrate their strengths and weaknesses. Baskerville argues that security development methodology should be merged with mainstream systems development methodologies, as they share many common objectives, methods, challenges and primary concepts. He cautions that security methods will not progress unless they are integrated into general IS development methods.

Siponen (2005) goes a step further by examining the orientation of five secure IS development paradigms. Concluding that the prevailing methodology is technical in orientation, he argues for greater emphasis to be placed on socio-technical and social methods. Moreover, he calls for the conceptual development approach to be supplemented with rigorous empirical investigation. More importantly, based on prior

work, he classifies the methods into five generations, and further recommends the method moving towards social and adaptive approach.

Fernández-Medina et al. (2006) approach their critical review of 11 secure system design methodologies from the position that it is better to anticipate potential security problems than merely to provide security defences. Arguing that every methodology has limitations while comprising vital aspects concerning security that must be considered, they propose a standardised methodological approach that would allow engineers to account for security aspects when constructing an IS. Their results support Baskerville's notion of a rapprochement between ISsec methodology and IS methodology, and confirm Siponen's view that a socio-technical perspective is required.

2.2.2 IS Security Research Literature Research

The study of ISsec research as a discipline did not emerge until the 2000s. Dhillon and Backhouse (2001) were among the pioneers, analysing 11 ISsec studies and adopting sociological paradigms developed by Burrell and Morgan (1979) to illustrate the need for understanding the social, as well as the technical, aspects of ISsec. They concluded that while IS research in general has moved away from a narrow technical viewpoint, ISsec research continues to be dominated by technical and functionalist preconceptions; moreover, the use of socio-organisational perspectives to understand ISsec remains at the theory-building stage. Accordingly, they called for further exploration.

Those responding to their call (Siponen, 2005; Siponen et al., 2008) found that ISsec research is dominated by a symbolic system of practical logic – a finding that appears to corroborate the notion that ISsec research is inclined generally towards non-empirical and atheoretical research activities. These authors argue that ISsec research is tied too closely to information technology; thereby resulting in its habitus countering that of overall IS research. They too have called for further investigation of ISsec research methodology in the hope of highlighting ways to improve the discipline.

2.2.3 Summary

Although these studies provide some insight into ISsec research, they are not without their limitations. For example, Fernández-medina and his colleagues concentrate only on the development of secure IS and system design methods and methodologies, which is only one of the three research tracks within the ISsec field. Dhillon and Backhouse may have tried to broaden the discussion, but their arguments are not based on widely-accepted theoretical paradigms; furthermore, their applicability is undermined by the fact that the authors are discussing only the development of secure IS. They adopt sociological theory but ignore the key influence of IS theoretical paradigms on ISsec research. Finally, they review a limited number of articles, which raises questions about the generalisability of their conclusions.

Siponen's researches are comparatively systematic; he examines many articles and arrives at some momentous conclusions. However, he presents only a general picture

of the patterns within ISsec research; he does not explain why this picture is the way it is or anticipate its possible consequences, nor does he make any recommendations for how it might be improved. His most recent research was conducted in 2008, but during the past few years, tremendous changes have occurred in ISsec and numerous advances have been made. This research aims to reflect these changes and incorporate the new contributions.

In summary, previous ISsec studies have shortcomings that seriously impair their validity. In theoretical terms, they document phenomena rather than offering methodological improvements, and make no practical recommendations for future research activities.

2.3 Research Questions

The findings from the literature review generated two key research questions. There are three main tracks within ISsec research, but while advances have been made within each track, their lack of integration means that overall progress has been patchy. The first question pertains to the overall pattern of the tracks.

> ***Research Question 1***: whether there are latent connections between the tracks. If there are, what is the nature of these connections; if not, how does the relationship differ from connection?

Previous studies of ISsec have made limited contributions, but it is hoped to go further and provide feasible recommendations for future research by specifying the methodological concerns.

> ***Research Question 2***: is it possible to build up coherent and systematic methodological practices that might be used to direct future research activities within the ISsec field?

This is the first time both research questions have been asked; arising from ISsec. These two research questions are crucial: the researcher is endeavouring to change the current disconnected, fragmented research picture into something connected, coherent and systematic, and to help future researchers select the most appropriate methodology for their ISsec research. By addressing these questions, it is hoped that this research will make two key contributions. In theoretical terms, identifying the pattern of ISsec research will enable the researcher to achieve a holistic and unified view of this research field, while the development of a connected and systematic research methodology and identification of a research potency should be of value to future researchers. It is even possible that delineating the full picture of ISsec may reveal undiscovered research tracks. Secondly, in practical terms, the identification of pattern and practice may establish a research blueprint, offer guidance to researchers looking to choose the most suitable research methodology, and serve as a benchmark for the evaluation of research activities.

SECTION II METHODOLOGY

This section introduces the methodology employed to direct the research. The methodology of an instance of research may be defined as the structured set of activities that are implemented to pursue the research objectives. Since the research in this case involved the collection and systematic review of a large quantity of research articles, it was especially important that these activities be carefully structured. Having selected the reticulated model of science and multilevel theory as the theoretical framework, the scope of the literature review was determined and the process for retrieving, selecting and screening articles designed. An original examining framework was then developed to analyse the retrieved literature. This differs from previous frameworks in that it incorporates four research components that represent collectively the research process, reflecting the focus on methodology.

Chapter 3 RESEARCH DESIGN

The design of a research is determined primarily by the nature of the research questions raised and their context in the literature. In terms of this research, the exploratory nature of the research questions (whether and how questions) and the limited number of literatures (only five pieces of extant articles) clearly indicated the necessity of an in-depth examination of the relevant area. The focus on latent connections among various ISsec research called for an interpretive approach to understand this field. The interpretive paradigm was chosen as the overarching philosophic stance was because the main purpose of this research was not to test theory or verify the hypothesises, but rather to understand the research context of ISsec scholars for each piece of work on which they previously worked. Specifically, it is hoped to access the meanings assigned to these researches, and to restore the scenarios where the social interpretation with scholarly meaning were produced and reinforced by the authors. More importantly, this research attempted to identify the understudied fact that how ISsec research practices and implications were formed and informed by shared research methodology and social norms within the scholarly setting.

Klein and Myers (1999) proposed several principles for the appropriateness of interpretive research in IS. They posited that the most fundamental principle is the hermeneutic circle, which entails a process of understanding a complex whole from preconceptions regarding each component's meaning and the interrelationship among

them. In other words, it illustrates the importance of apprehending both "parts" and "whole" of the focal phenomenon through several iterations of the hermeneutic circle. To this end, it fits well with this research's process, which is specified in subsequent sections. In addition, Klein and Myers (1999) recommended the principle of contextualisation, whereby a critical reflection of the social background of the research setting is required to inform the intended readers of how the current situation under investigation emerged. This research, which aims to identify the research setting for each journal article, was context-based, and thus suitable for interpretive research. Moreover, they favoured the principle of interaction between the researcher and the "subject" (ISsec research in this case), where the "data" (articles in this case) was socially constructed from a historical perspective. To identify and establish the possible connections between each ISsec research track, the researcher must recognise a broader socio-historical process (Kahn, 1989) in which the data can be better understood. In conclusion, from both ontological and epistemological perspectives, the choice of interpretive stance was sound, proper, and necessary.

In terms of the research method, quantitative and qualitative researches are the most popular and are widely adopted. In fact, several quantitative studies have been conducted to date on the usages of different research components in ISsec research. Most literatures specify the frequencies of the most widely-utilised paradigm, method, theory, and analysis in their research without examining anything further. The efficacy of research methodology in ISsec seems to affect the actual research activities and its ramifications in a very complicated manner. ISsec research has been studied by

quantitative research outside its own unique context, which consequently steers the attention away from the situation where ISsec research can be properly undertaken and understood. According to Kaplan and Maxwell (1994), the goal of understanding a particular social and institutional context is largely lost in the process when textual data are quantified. In this regard, quantitative research does not present the whole picture of ISsec research, given that it necessarily overlooked the external ambience – the social context – where IS phenomena and ISsec research are enforced. Furthermore, quantitative research cannot account for contingency, which is crucial for ISsec research due to the complexity of the inherent nature of each research question.

In contrast, qualitative research is designed to help scholars understand people and social and cultural contexts within which they live (Myers, 1997). It, thus, enables scholars to study in-depth the focal topic through consideration of its social implications. Different from quantitative research, seldom leading to a clear policy advice (Graaf and Huberts, 2008), which is important in directing scholars to better utilise methodology, qualitative research frequently culminates in the provision of constructive and workable suggestions that can be practically implemented. Consequently, the qualitative method was selected as it was believed mostly likely to render an insight into the current ISsec research and its imminent context.

To uncover the potential challenges and opportunities in relation to ISsec research, it was first necessary to capture the current state of research in this discipline. The literature review needed to be sufficiently large to be comprehensive but remain

practically workable. Therefore, it was necessary to define the scope of the survey and develop criteria regarding the types of studies to include in the work. The decision was made to focus on journal, rather than conference, articles as they are generally longer and more detailed, and therefore, both more systematic and more conclusive. The fact that journals are published at regular intervals also means they provide a better indication of the pace of change. It was then necessary to develop an efficient search and screening strategy, and finally, an analytical scheme outlining how the studies would be analysed and coded.

The first phase of the literature survey was conducted between June 2014 and August 2014. In this pilot study, data was collected from articles in *Management Information Systems Quarterly* (MISQ) and the *European Journal of Information Systems* (EJIS) to capture and compare overall trends. These two journals are the most prestigious publications in the IS field, representing the highest research quality of IS research. Based on the results of this initial analysis, changes were made to the method by which articles were retrieved, and the categorisation of data. In the second phase of the survey, from October 2014 to March 2015, the search was widened to cover the major IS journals. The process of selecting these journals is discussed in the following section.

3.1 Publication Outlet Selection

The decision was made to focus on mainstream and well-known IS journals as it was felt that these were most likely to thoroughly document the progress being made in

ISsec and reflect significant developments. However, the criteria for judging the "top" journals vary from region to region, and from school to school. For example, while the widely-accepted ranking produced by the Australian Council of Professors and Heads of Information Systems (ACPHIS, 2013) lists 13 A* journals and 39 A journals, the ranking produced by the Association for Information Systems (AIS, 2011) forsakes tiers and lists 108 journals, the first 20 of which differ from those selected by ACPHIS. There is an overall understanding that the scholarship differs between US and European schools (Galliers & Whitley, 2007), and this is reflected in their respective criteria pertaining to directing, selecting and publishing journal articles (Chen & Hirschheim, 2004). In fact, some of the articles that feature in these journals are not IS papers (Chua et al., 2002), much less ISsec papers. Consequently, they may not be reliable indicators of their quality and relevance in terms of ISsec.

To address this concern, the following criteria were applied when selecting journals for review:

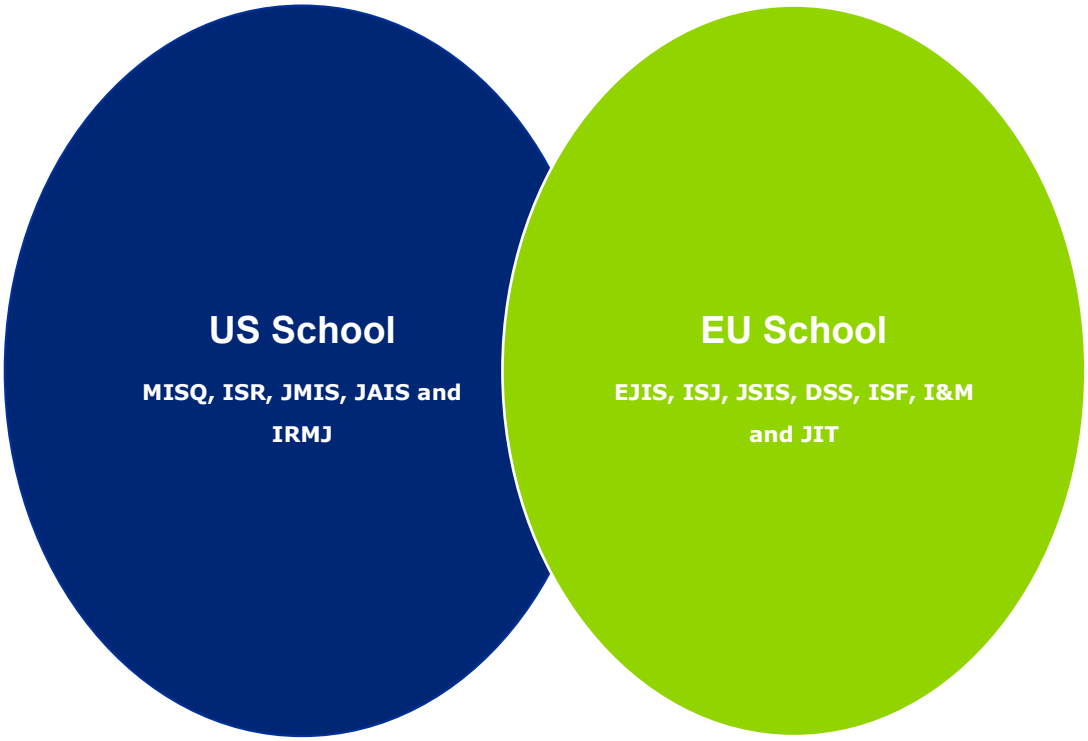
(1) they had to be among the top-listed publications on lists that restrict themselves to IS journals;

(2) they had to reflect the research status quo in both the US and European schools; and

(3) they had to contain at least a few articles related to ISsec research.

If only one or two relevant articles appeared in one issue, previous issues were examined to check that these were not one-offs and that the journal had an established tradition of publishing ISsec research. Application of these criteria to the lists and journals produced the following list of research journals: US – *MISQ*, *Information Systems Research* (ISR), *Journal of Management Information Systems* (JMIS), *Journal of the Association for Information Systems* (JAIS) and *Information Resources Management Journal* (IRMJ); EU – *EJIS*, *Information Systems Journal* (ISJ), *Journal of Strategic Information Systems* (JSIS), *Decision Support Systems* (DSS), *Information Systems Frontiers* (ISF), *Information and Management* (I&M) and *Journal of Information Technology* (JIT). In total, five journals from the US and seven from the EU were chosen (Figure 3-1), avoiding over-emphasis on, or bias towards, either school.

Figure 3-1 Journals Selected from the US and EU Schools



3.2 Research Article Retrieval

After identifying the target journals, the next step was to select the ISsec research articles for analysis. It was important to obtain a high-quality sample of the right size; too broad a sample might produce an overwhelming number of articles, including many that might not be relevant but, conversely, too narrow a selection might render generalisation difficult. The decision to focus on articles published between 2008 and 2015 was made for two main reasons: first, because there have been no surveys of ISsec research since 2008 (Siponen & Oinas-Kukkonen, 2007; Siponen et al., 2008; Villarroel et al., 2005; Willison & Siponen, 2007) and second, because the aim is to reflect the latest developments in ISsec research.

The process of filtration started with a keyword search using "security" as the search term, but when it became apparent that other articles concerned broadly with the concept of security had different keywords, such as password, trust, compliance, fraud and attack, these words were also used as keywords. The final list of keywords used to find articles was: security, risk, threat, trust, fraud, attack, password, compliance, phishing and vulnerability. To increase the reliability of the article retrieval process, inter-rater reliability criteria were applied, with filtration and retrieval being conducted in different venues at different workstations over several rounds (taking several weeks). When the results were pooled and analysed, some articles were dropped as irrelevant. For instance, some articles containing "security" as a keyword were indeed discussing job security, while others were exploring security issues from a very technical perspective (e.g., how to parse passwords or defend a technology framework from

possible attacks). A few articles which did discuss ISsec from a purely information systems perspective were editorial reviews or guidelines rather than research articles. These were also excluded. In total, 108 articles were retrieved from the 12 journals listed above.

It should be noted that security is not synonymous with privacy. This research primarily focuses on research in ISsec – privacy is relevant only since it is affected by the implementation of security measures or lack thereof. There is a plethora of social and political considerations that determine privacy rights and obligations, but these are outside the scope of this research.

3.3 Research Article Analysis

In order to systematically assess the selected articles and highlight methodological issues, it was necessary to develop an examining framework. This focused on the philosophical assumption, cognitive aim, operational dimension and interpretive level of the articles, with studies classified and coded according to:

(1) how the research topics were conceptualised;

(2) how the research data was collected and measured;

(3) how the research activities were operationalised; and

(4) how the research findings and results were analysed.

This allowed the researcher to identify the pattern of current ISsec research, discover its common practices and underlying relationships and, thereby, assess its latent potency.

The examining framework was applied to all retrieved articles to obtain information pertaining to each component. This set of information can be found at certain part of a research paper; specifically, the research paradigm was described primarily in the introduction and/or methodology section(s), while the research method was presented in the methodology section. The research theory was initially introduced in the section of theoretical framework, while the research analysis was discussed in the results and/or discussion section(s).

The inter-rater reliability criterion was again utilised during this stage based on the full-text analysis. Four rounds analysis for each component with different orders was undertaken at different venues. The first round was paradigm, theory, method, and analysis; the second was theory, method, analysis, and paradigm; the third was method, analysis, paradigm, and theory; and the fourth was analysis, paradigm, theory, and method. Then, all the results were pooled together to decide the type for each component in every article. If the discrepancy occurred during these rounds for certain articles, the analysis phase was repeated until a consensus was reached.

In short, the retrieved articles were examined in multiple rounds. In each case, the full text was analysed, as this was considered the most reliable way to develop relevant research outputs (Willison & Siponen, 2007). To safeguard reliability, the inter-rater

reliability criteria were applied again at this stage. The analysis phase, including the development of the examining framework, are discussed in detail in the next chapter.

Chapter 4 Analysis Method

Chapter 3 discusses the steps that were employed to select and retrieve 108 research articles; this chapter describes the development of the theoretical and examining frameworks that were employed for their analysis. A research methodology is a clearly defined sequence of operations (House et al., 1995; Iivari et al., 1998) that are designed to assist the researcher in generating valid and reliable research results. These activities may include administering and analysing a survey, conducting controlled experiments, engaging in ethnography or participant observation and developing root definitions and conceptual models. This study focuses specifically on ISsec research methodology, or those principles, practices and procedures that help ISsec researchers to produce and present research that will be accepted as valuable, rigorous and publishable (Peffers et al., 2007). The methodology will inevitably make implicit or explicit assumptions about the nature of the world and of knowledge (Mingers, 2001), and these will determine the methods and techniques employed (Katz & Kahn, 1978). These components all had to be reflected in the examining framework.

4.1 Theoretical Framework

To make a comparison of existing ISsec studies from a methodological perspective, it was necessary to develop a general conceptual framework. Previous studies have utilised a variety of frameworks, but considering Burrell and Morgan's (1979) argument

that research within different paradigms is not comparable and that some paradigms are in fact irreconcilable, it was decided that these frameworks would be unsuitable for this study. Instead, the reticulated model of science and multilevel theory were adopted as the theoretical lens through which to examine the research questions. These are introduced in the following sections.

4.1.1 Reticulated Model of Science

Laudan's (1984) reticulated model of science posits that methods, theories and themes change incrementally and one at a time, and that these methods, theories and themes are rationally negotiable. Scientific progress is measured in terms of one's gradual movement towards a goal; if the goal changes, then the standard(s) regarding what constitutes progress change correspondingly. Therefore, scientific progress can be rationally evaluated, despite its relativity to fixed goals. As Laudan's model operates across paradigms, it was a suitable framework for comparing the features of ISsec research literature; methodologies were examined in terms of the three elements of the model – methods, theories and themes – plus paradigm and analytical approach.

To facilitate the discussion of the research questions, a taxonomy was required to relate the discrete ISsec research works to the perspective of the broader ISsec research community. Research paradigms are variously classed as positivist, interpretive and critical (Orlikowski & Baroudi, 1991), while research methods are either quantitative (laboratory experiments, field experiments and surveys) (Galliers, 1992) or qualitative (case studies, action research, ethnography and grounded theory) (Myers, 2008).

Analysis and discussion take place at the individual, organisational or societal level (Smith et al., 2011). A flexible approach was adopted in the grouping of the articles, which expressed a variety of theories and were drawn from a range of disciplines.

4.1.2 Multilevel Theory

Multilevel theory (MT) is first and foremost underpinned by general systems theory (GST), which was the dominant perspective in the twentieth century. However, while GST is essentially holistic in outlook and seeks to establish general understanding across phenomena to generalise key principles (Klein & Kozlowski, 2000), MT adopts a micro-macro perspective (MiMaP). It recognises that while micro phenomena are embedded within a macro context, macro phenomena often emerge from micro elements (Hitt et al., 2007); the micro perspective emphasises the variation among individuals, while the macro perspective focuses on the collective response from a group of individuals, regardless of individual variation. MT spans the levels of organisational behaviours and performance and bridges the micro-macro divide. By acknowledging the influence of the organisation on individuals' actions and the influence of the individual's action on the organisation, a richer and deeper understanding of organisational phenomena is facilitated (Klein et al., 1999).

The central concept of MT is that organisational phenomena reside within nested arrangements; thus, an individual is nested in groups or other subunits, which are subsequently nested within the organisational hierarchy and the industrial environment. Hitt et al. (2007) observe that this arrangement has certain implications for

organisational research; however, others (House et al., 1995; Klein et al., 1994) highlight MT's ability to connect previously unlinked constructs within organisational literature. A second advantage of MT is that it illustrates the contexts surrounding individual variation and organisational aggregation, giving it the potential to yield important practical insights.

Rousseau (1985) provides useful guidance for those undertaking MT-oriented research, advising that scholars should simultaneously consider the levels of theory, measurement and analysis that are most appropriate to the constructs under investigation. Level of theory refers to the focal unit to which the investigation is intended to apply, while "Level of measurement refers to the unit to which the data are directly attached, and the level of analysis is the unit to which data are assigned for hypothesis testing and statistical analysis" (Rousseau, 1985).

4.2 Examining Framework

The examining framework encompasses four components that together represent the complete research activity-chain. These four components are (in order of completion):

(1) Research paradigm: describes the scholars' philosophical assumptions;

(2) Research theory: sets out their cognitive aims;

(3) Research method: boundaries the operational dimension; and

(4) Research analysis: decides the interpretive level of the research context.

These are discussed in more detail in the following sections.

4.2.1 Research Paradigm

All IS scholars undertake their research holding a number of explicit and implicit philosophical assumptions about the nature of human organisations, the nature of their particular search/review and the expected results. These assumptions play a crucial role in guiding the IS research procedure, directly affecting not just the likelihood they will get a result but the very nature of these results; in other words, the assumptions that are adopted will determine both the research approach and the potential research outcomes.

Consequently, recent decades have seen IS researchers pay increased attention to their choice of paradigm. New paradigms have been developed (e.g., Burrell & Morgan, 1979; Orlikowski & Baroudi, 1991) and alternatives have become more widely accepted; for example, interpretivism. Researchers have become more willing to employ a combination of paradigms in the belief that this will allow them to investigate multiple research dimensions in a manner that is not possible with a mono-paradigmatic approach. However, the advance of paradigmatic pluralism has not been universally accepted. Landry and Banville (1992), for example, suggest that it is fragmenting IS research rather than uniting it – but supporters such as Robey (2003) advocate the necessity of research diversity. He is echoed by Klein (2003), who explains why the fragmented adhocracy has occurred and how the IS community can address this issue.

Several theoretical perspectives have been employed in the IS domain. Burrell and Morgan's (1979) sociological paradigm features a 2*2 matrix to help classify and understand sociological theories based on four major paradigms, which coalesced into two fundamental issues: whether social theories were emphasising regulation and stability or emphasising radical change, and whether theories were subjective or objective. In this sense, four paradigms were generated, and they were functionalist paradigm (objective-regulation), interpretive paradigm (subjective-regulation), radical humanist paradigm (subjective-radical change), and radical structuralist paradigm (objective-radical change).

Orlikowski and Baroudi (1991) were the first to identify the various paradigms employed in IS literature, which they achieved by surveying 155 research articles published between 1983 and 1988. Following the classification of research epistemologies proposed by Chua (1986), they identified the positivist, interpretive and critical paradigms as the most widely used. According to the authors, these three paradigms differ in three main respects: their assumptions about reality, knowledge, and the relationship between the two. The nature of physical and social reality is a matter of ontology; that is, the debate over whether physical and social reality is objective and exists independently of humans, or subjective and exists only through humans' intervention. A paradigm's assumptions of knowledge, and the criteria for constructing and evaluating this knowledge, reflect its epistemological and/or methodological stance, while assumptions about the relationship between reality and knowledge reflect its stance on the purpose of knowledge in practice.

(1) The positivist paradigm

The positivist paradigm aims to test theory to arrive at a better predictive understanding of a phenomenon. Ontologically, it assumes that the phenomenon can be understood by objectively measuring a set of known, fixed variables. In other words,, an objective physical and social world exists independently of humans, the nature of which can be apprehended, characterised and measured with relative ease. The role of the researcher is to uncover, rather than intervene in, this objective reality. Epistemologically, the positivist perspective is concerned with the empirical testability of theory. The positivist researcher pursues this aim using sanctioned research methodologies, such as sample surveys and controlled experiments (indeed, Kraemer et al. (1987) assert that this is the only way to obtain valid knowledge). Finally, the paradigm assumes that the relationship between knowledge and reality is generally technical, and that the researcher can produce a desired state of affairs, natural or social, if the appropriate general laws are known and the relevant initial conditions are capable of manipulation (McCarthy, 1981).

(2) The interpretive paradigm

Conversely, the interpretive paradigm assumes that scholars can create subjective understanding by interacting with the surrounding world, and that phenomena are understood by accessing the meanings assigned to them. Ontologically, interpretivism stresses the importance of subjective meanings and social-political and symbolic action in the processes through which humans construct and re-construct their reality (Burrell

& Morgan, 1979). IS scholars adopting the interpretive perspective assume the social world is produced and reinforced by humans through their actions and interactions; since there can be no focal objects without humans, these objects can only be understood or measured subjectively, and reality can only be interpreted rather than discovered.

Epistemologically speaking, Rosen (1991) suggests that: "social process is not captured in hypothetical deductions, co-variances, and degrees of freedom. Instead, understanding social process involves getting inside the world of those generating it". Unlike the positivist perspective, interpretivism claims that the researcher must apprehend how practices and meanings are formed and informed by shared social norms in order to understand social reality. Consequently, the method most likely to generate valid knowledge is the field study, as this allows examination of the phenomenon within its social setting. In terms of the relationship between knowledge and reality, interpretivism posits that the researcher can never be value-neutral and that they will always be implicated in the phenomenon being studied. In other words, the researcher's own experiences, beliefs and values will always direct their interest and inform their assumptions; thereby helping shape their research activities.

(3) The critical paradigm

Finally, the critical paradigm critiques deep-rooted contradictions within social systems with the aim of emancipating individuals from restrictive social conditions. Ontologically, the most important attribute of the critical perspective is its introduction

of the historical view; it asserts that social reality is historically constituted, and that focal objects are not confined to existing in a particular state (Chua, 1986). Rather, they are capable of improvement by anyone who recognises their potential. Simultaneously, it recognises that humans generally lack the capacity to bring about this improvement because their own potential is constrained by the prevailing economic, political and cultural systems. The critical perspective enables the researcher to gain insight into these systems as the first step to eliminating their domination.

The epistemological stance of the critical perspective is that knowledge is grounded in both social and historical practices. This commitment to the processual view of phenomena means that critical studies tend to be longitudinal (Benson, 1973); examples include long-term historical studies and ethnographic studies of organisational processes and structures. The reliance on historical analysis is compatible with the belief that a phenomenon can only be understood by examining "what it has been, what it is becoming, and what it is not" (Chua, 1986). Finally, as far as the relationship between knowledge and reality is concerned, the critical paradigm sees it as the researcher's responsibility to create knowledge (of the restrictive conditions of the status quo) to initiate change within this reality.

Since these three paradigms are the most widely used and guide nearly all research in IS, they were adopted as the criteria for the philosophic assumption component of the examining framework (Table 4-1).

Table 4-1 Three Types of Research Paradigm

Research Paradigm	
1	Positivist
2	Interpretive
3	Critical

4.2.2 Research Theory

In general, theory is developed to describe, explain and enhance the understanding of the world and predict future events. Consequently, examination of the nature of theory occurs in almost all disciplines, and more established disciplines have considerable histories of enquiry into this issue. IS scholars have drawn on and adapted theoretical bases from a number of other disciplines, including psychology, sociology, economy, finance and management (Siponen et al. (2008) identify 38 theories that have been imported into ISsec research from other disciplines). However, as it is increasingly recognised as a discipline in its own right, it is beginning to make its own theoretical contributions.

Despite the general recognition of its importance, however, IS theory development remains in its early stages. Many IS researchers use the word theory to describe their theoretical considerations without defining explicity their views of theory. For instance, although Mingers (2001) assesses the influence of different research paradigms on the IS discipline, he fails to provide concrete discussion of the nature or type of theory.

This led Gregor (2002) to emphasise the need for theory building in IS. Concluding that theory is invented rather than discovered, she explains that: "theory answers a human need to make sense of the world and to accumulate a body of knowledge that will aid in understanding, explaining, and predicting the things we see around us, as well as providing a basis for action in the real world" (Gregor, 2002).

Numerous attempts have been made to develop a taxonomy of theory. Markus and Robey (1988); for example, characterise theory in terms of its causal structure. Meanwhile, Neuman (2000) advocates a five-dimension framework to categorise theory according to direction, level, attribute, forms of explanations, and assumptions and concepts. Little has been done in terms of investigating underlying causal relationships between research endeavours and results (Lee et al., 1997); nevertheless, Gregor (2006) has categorised theory according to its primary purpose, arguing that as an applied discipline, IS adopts theory to build knowledge which is then expected to be put to practical use. She discerns five distinct theoretical approaches: theory for analysing, theory for explaining, theory for predicting, theory for explaining and predicting, and theory for design and action.

(1) Theory for analysing

Theory for analysing examines the question of "what is"; that is, it describes or classifies specific dimensions of the focal object. Studies employing analysis theory, the most basic type, describe previous research findings regarding one or more specific characteristics of an individual, team or phenomenon. This type of theory contributes

to knowledge building by providing a clear delineation of the uniformities of the phenomenon under investigation.

(2) Theory for explaining

Theory for explaining seeks primarily to explain "how" and "why" phenomena occur. According to Gregor (2006), there are two subtypes of this kind of theory: high-level and low-level. While the former aims in general to replace conventional notions with more insightful global thinking, the latter focuses on phenomena within a specified real-life situation (in particular, it is useful for identifying causality).

(3) Theory for predicting

Theory for predicting consider these explanatory factors in order to make logical and testable predictions about the future to answer the "what will be" question. It does not, however, explain the underlying causal relationships between dependent and independent variables. It has proved useful in identifying the relationships and degree of generality of the unknown focal object, which is of considerable practical importance.

(4) Theory for explaining and predicting

Theory for explaining and predicting seeks to demonstrate the existence of a phenomenon, answer the questions of "how", "why" and "when" it occurs, and discover "what will" happen in the future. It concentrates on understanding underlying causes,

prediction, and the description of theoretical constructs. It has been adopted largely for theory building and/or theory testing.

(5) Theory for design and action

Finally, theory for design and action aims to explain the principles by which systems are created and, thus, guide the development of IS as it relates to the question of "how to do". This type of theory plays an important role in ISsec research as it helps shape IS development processes and IS development concepts.

The examining frameworks offered in previous studies tend to list only a limited range of theories. However, it would be inefficient, if not impossible, to develop a framework that statistically examines the theoretical perspective of every piece of ISsec research; in any case, such attention to detail may blur the overall picture. Therefore, it was necessary to choose an alternative theory-related criterion that would be easy to manipulate while accurately reflecting the range of theoretical perspectives employed in the sample articles. Gregor's five-type typology of theory was selected because it effectively indicates the cognitive aim of a piece of research and represents the theoretical foundation of IS in a concise and informative way (Table 4-2).

Table 4-2 Five Types of Research Theory

Research Theory	
1	Analysis
2	Explanation
3	Prediction
4	Explanation and prediction
5	Design and action

4.2.3 Research Method

Significant attention has been paid to the research methods applied to IS research, as they reflect the researcher's implicit or explicit assumptions regarding the nature of the world and knowledge. The research method can be viewed as the operational dimension for provoking a response from the world; the nature of this response will depend on both the world and the research's underlying assumptions. Different methods generate information about different aspects of the world. This information is used to construct theories about the world, which in turn condition the experience of the world. It is commonly held that research methods are bound to particular paradigms and that, as these paradigms are incommensurable, it is illogical to mix methods from different paradigms. However, Mingers (2001) asserts that it is both desirable and feasible to combine different research methods to gain richer and more reliable results.

Several authors have sought to classify existing studies by research method in the hope of encouraging the adoption of a wider range of methodological approaches. Benbasat et al. (1989), for example, compared studies employing qualitative research methods with those using experimental and survey-based research methods. Meanwhile, Alavi et al. (1989) divided the empirical studies they examined into eight categories according to whether they were based on laboratory experiments, field experiments, field studies, case studies, surveys, MIS instruments, ex-post descriptions, or other methods. Similarly, Orlikowski and Baroudi (1991) surveyed 155 articles, classifying studies according to whether they were based on surveys, laboratory experiments, case studies, mixed methods, instrument development, protocol analysis or action research.

Among these different taxonomies, the most consistent comparisons are between empirical and non-empirical (Alavi et al., 1989) and quantitative and qualitative (Benbasat et al., 1989) methods. However, both classifications have limitations; such stark dichotomies are too simplistic, especially when one considers that there are more than 10 frequently-used methods in current IS and most can be employed across the paradigms. For example, Klein and Myers (1999) indicate that quantitative/qualitative research can be positivist, interpretive or critical. Moreover, some research methods can be used in the context of both quantitative and qualitative research. In other words, general classifications may be useful in understanding a researcher's approach, but they give no insight into the appropriateness of the paradigm and theory or the overall consistency of the researcher's activities. A method taxonomy should, therefore, be concerned not only with the method itself, but also with theoretical considerations. It

needs to be sufficiently abstract to categorise a range of research, but concrete enough to provide rich insights into the research activities.

This study employs the taxonomy of method proposed by Hevner et al. (2004). These authors group methods under the explanation (behavioural) paradigm and the improvement paradigm:

(1) The explanation (behavioural) paradigm: seeks to develop and verify theories that explain or predict human or organisational behaviour influenced by technology; and

(2) The design paradigm seeks to extend the boundaries of human and organisational capabilities by creating new and innovative artefacts with technology.

Both paradigms are fundamental to the IS discipline, positioned as it is at the confluence of people, organisations and technology (Table 4-3).

Table 4-3 Two Main Types of Research Method

Research Method		
1	Explanation paradigm (Behavioural paradigm)	Quantitative method
		Qualitative method
2	Improvement paradigm	Design-science method

4.2.4 Research Analysis

Analysis is an indispensable part of most IS research articles, as this is where the preliminary research results are positioned within a broader context. The analysis presents the research outcomes, summarising the outputs from theoretical exploration and connecting theory with practice by explaining how the research applies to a real social setting. The fact that this essential stage has been overlooked frequently in previous reviews of ISsec research reduces the value of these reviews. Moreover, it enhanced the significance of incorporating it into the examining framework for this study.

Like IS research, ISsec research addresses fundamentally the relationship between information technology and organisations. By their very nature, organisations are multilevel: individuals work in groups, teams work within the organisation, and the organisation interacts with other organisations (Klein et al., 1994). Since no construct is level-free, examining organisational phenomena will lead to level issues. But while scholars have long recognised that organisational phenomena unfold within complex and dynamic systems (Katz & Kahn, 1978), they often neglect to address the multilevel dynamics of these social systems (Kozlowski & Klein, 2000). Instead, they adopt either a micro or a macro stance, resulting in the proliferation of research paradigms (Hitt et al., 2007) but yielding only a partial understanding of behaviours occurring at either level (Porter, 1996). MT-enabled analysis is one way to stimulate the development of a more expansive paradigm, which will permit a more in-depth understanding of organisational phenomena.

Multilevel thinking has emerged from empirical attempts to understand ISsec by examining organisational-level factors and individual behaviours. As the field has advanced, research has shifted from exploring security-related phenomena at a single level (e.g., Puhakainen (2006), whose proposed design for improving information security awareness campaigns was targeted at the group level, and D'Arcy et al. (2009), whose recommendations to reduce information systems misuse (see section 2.1.2) were aimed at the organisational level), to developing a more complex understanding of these phenomena from different levels. In the security awareness research stream, for example, researchers exploring the relationship between awareness and behaviour (e.g., Albrechtsen & Hovden, 2010; Bulgurcu et al., 2010) have examined the phenomenon from different perspectives and integrated focal levels to show that organisational policy and individual behaviours both play an important role in security awareness. Thus, security awareness inherently is a multilevel problem. Similar conclusions might be drawn within other ISsec research streams, such as privacy and BYOD (bring your own device).

Overall, management research has adopted three levels of analysis, which have been adapted for ISsec research (Gupta et al., 2007).

(1) Individual level

At the individual level, ISsec has been studied in terms of the factors that foster or curb an individual's security awareness or perceived security. The main aim here is to discern which unknown security-related variables or factors influence known outcomes

or phenomena, in order to establish causal relationships. However, recent studies, particularly those addressing security within organisations, have been more concerned with employing a psychological, economic or societal lens to investigate how individuals impact security. The purpose of these studies is to understand how individuals react under specific circumstances, and to predict the likely consequences of these actions.

(2) Organisational level

Organisational-level research has focused on the impacts of technology and new products/business/structures on various types of organisation. This research investigates how organisations respond to newly-adopted security products and/or services with the aim of improving outcomes. Moreover, it is interested in understanding how established organisations develop new rules and strategies to improve security and governance, and how these rules and security-related decisions affect the organisation upon their implementation.

(3) Societal level

Finally, research at the societal level has focused on ISsec management; in other words, the interplay between the structure and dynamics of society on the one hand, and the emergence of new threats on the other. Researchers focusing on this level believe that certain security concerns originate not with the individuals or organisations who use products and services, but with the society in which these individuals and organisations

are embedded. They seek to understand how the culture, beliefs and norms of certain types of society affect security in general, and the impacts inter-organisational linkages have on security issues. These three levels are listed in Table 4-4.

Table 4-4 Three Levels of Research Analysis

Research Analysis	
1	Individual level
2	Organisational level
3	Societal level

4.2.5 Summary of Examining Framework

In summary, the examining framework comprises four components: research paradigm, research theory, research method and research analysis. Together, the entire research procedure is covered, and the theoretical, methodological and practical perspectives addressed (Table 4-5).

Table 4-5 Framework for Examining Information Systems Security Research

Objective	Philosophical Assumption	Cognitive Aim	Operational Dimension	Interpretive Level
Procedure	Research Paradigm	Research Theory	Research Method	Research Analysis
Criteria	Positivist	Analysis	Explanation/Behavioural	Individual level
	Interpretive	Explanation	Improvement	Organisational level
	Critical	Prediction		Societal level
		Explanation and prediction		
		Design and action		

The advantages of this comprehensive framework for examining ISsec research are threefold. Firstly, unlike previous frameworks, which have either focused on certain component(s) of ISsec research or been based on less widely-accepted paradigms, this framework is adapted from widely-recognised and well-established research and considers all key components of the ISsec research process. Consequently, it allows for a more thorough understanding of the ISsec research in the sample.

Secondly, previous studies that have examined theory and/or method have focused primarily on the specific type of theory or method employed. This makes it difficult, if not impossible, to identify the latent connections between the dozens of different

theories and methods. To the best of the researcher's knowledge, this is the first attempt to map out an examining framework that combines components by integrating their underlying assumptions; thereby enabling the identification of possible relationships from a coherent and interconnected perspective.

Thirdly, this expanded examining framework can examine ISsec research activities from a holistic and integrated perspective as it evaluates the work from multiple levels on which the concepts or constructs are nested. This yields clear benefits: on the one hand, it fosters synergy within ISsec by rendering a rich portrait of organisational phenomena; and on the other, it illuminates the steps that ISsec researchers have taken or should take, separately, collectively or progressively, to address the security issues at the intersection of information technology and organisations.

SECTION III FINDINGS

This section presents the research outcomes from the literature survey. The examining framework was applied to the 108 articles retrieved from the 12 journals to arrive at a series of initial results for each of the four research components. These results were then combined to establish the overall trends in ISsec research. Based on the trend, an additional step was taken to cluster them into four main tracks as the main pattern of ISsec research. These tracks, which differ significantly in terms of how they combine the research components, collectively represent the current pattern of ISsec research.

Chapter 5 PATTERN OF ISSEC RESEARCH

As described previously, 108 articles were retrieved from 12 leading journals. The number of ISsec articles obtained from each journal varied significantly; for example, there was only one relevant paper regarding security published in *JIT* during the given time frame, while *MISQ* accepted 20 in the same period (Figure 5-1). The uneven distribution is evidence that some journals are more interested in ISsec research than others, which is one reason why it was necessary to draw on a large journal pool to obtain a fair picture of current activities in ISsec research.

The number of retrieved articles was almost the same across the two schools, with 55 being identified from the US school and 53 from the EU school (Figure 5-2). This suggests an unbiased journal selection process.

The distribution in terms of year of publication was much more even, with a similar number of articles being published annually between 2009 and 2012. However, 2014 saw the number of published articles rise to 20. Since data for the study was collected only up to March 2015, just 13 were retrieved from that year. Had data been collected for the whole year, it is likely that the number would have been close to that seen in 2014 (Figure 5-3). This trend is indicative of the growing attention being paid to ISsec research. Moreover, there is every reason to believe that the number of articles being accepted by leading publications will continue to climb.

Figure 5-1 Articles Retrieved from Each Journal

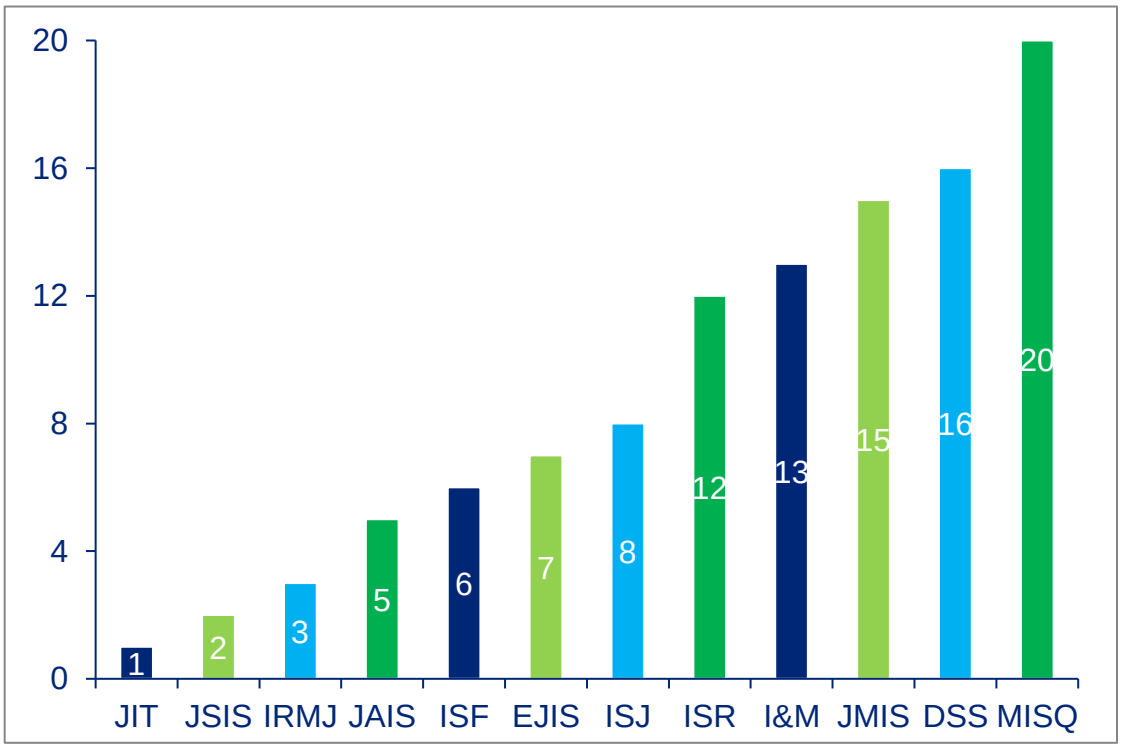


Figure 5-2 Articles Retrieved from Each School

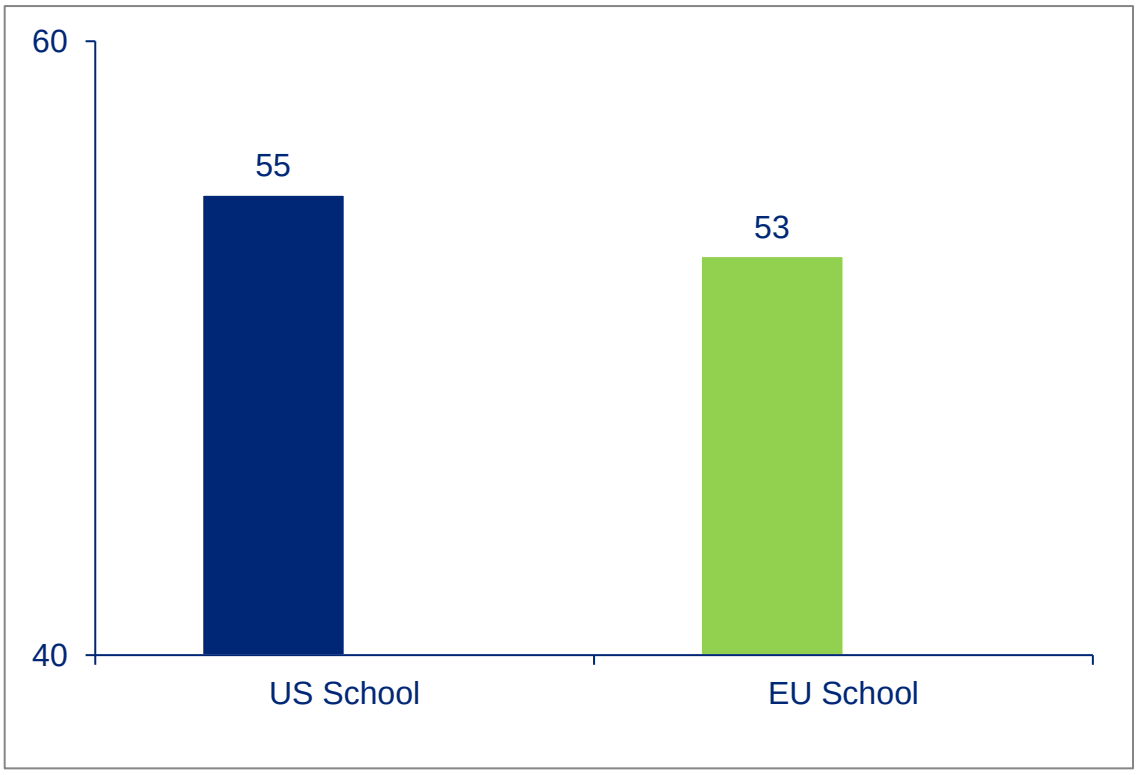
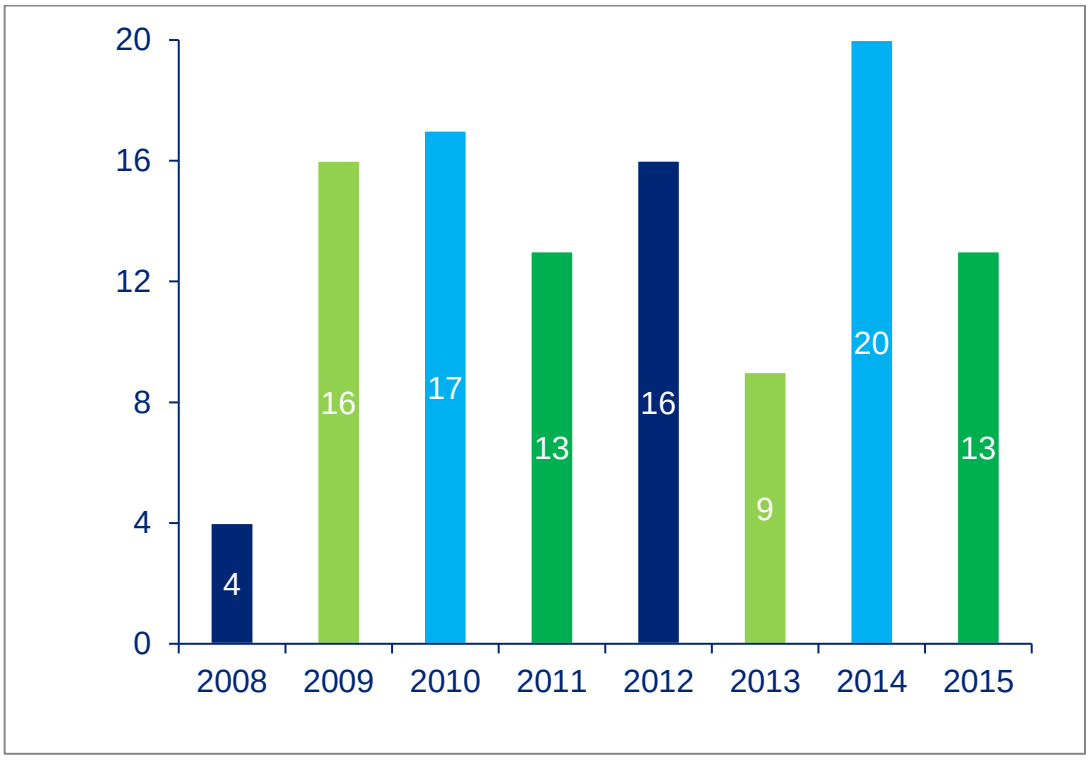


Figure 5-3 Articles Retrieved from Each Year



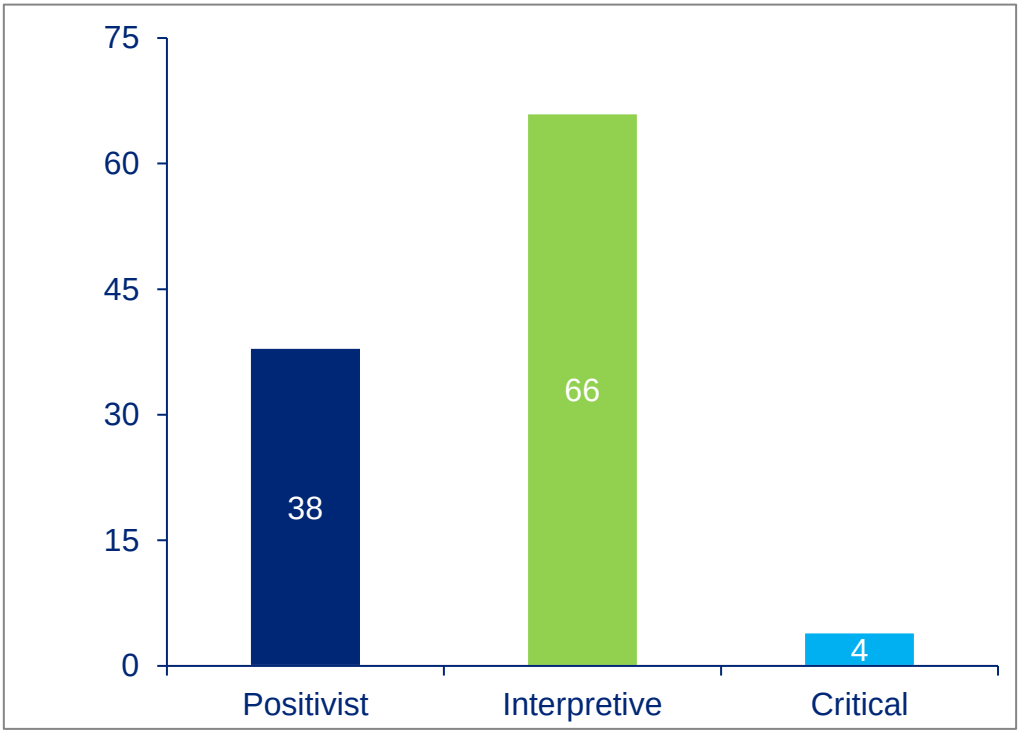
5.1 Initial Results

Following four rounds of full-text analysis, as specified in Chapters 3 and 4, four sets of initial results were obtained from the data analysis.

The analysis began with the application of Orlikowski and Baroudi's (1991) three-type typology (see section 4.2.1) to identify the research paradigm underlying each article. As discussed previously, the positivist, interpretive and critical paradigms differ in terms of their assumptions about reality, knowledge and the relationship between the two. Most scholars specify their philosophic assumptions either explicitly or implicitly in the introduction and/or methodology (research design) sections; therefore, relevant information was gathered from these areas. Of the 108 articles, 38 were positivist in

orientation, while just four followed the critical paradigm. The interpretive category was by far the largest with 66 papers (Figure 5-4).

Figure 5-4 Statistics on Research Paradigms

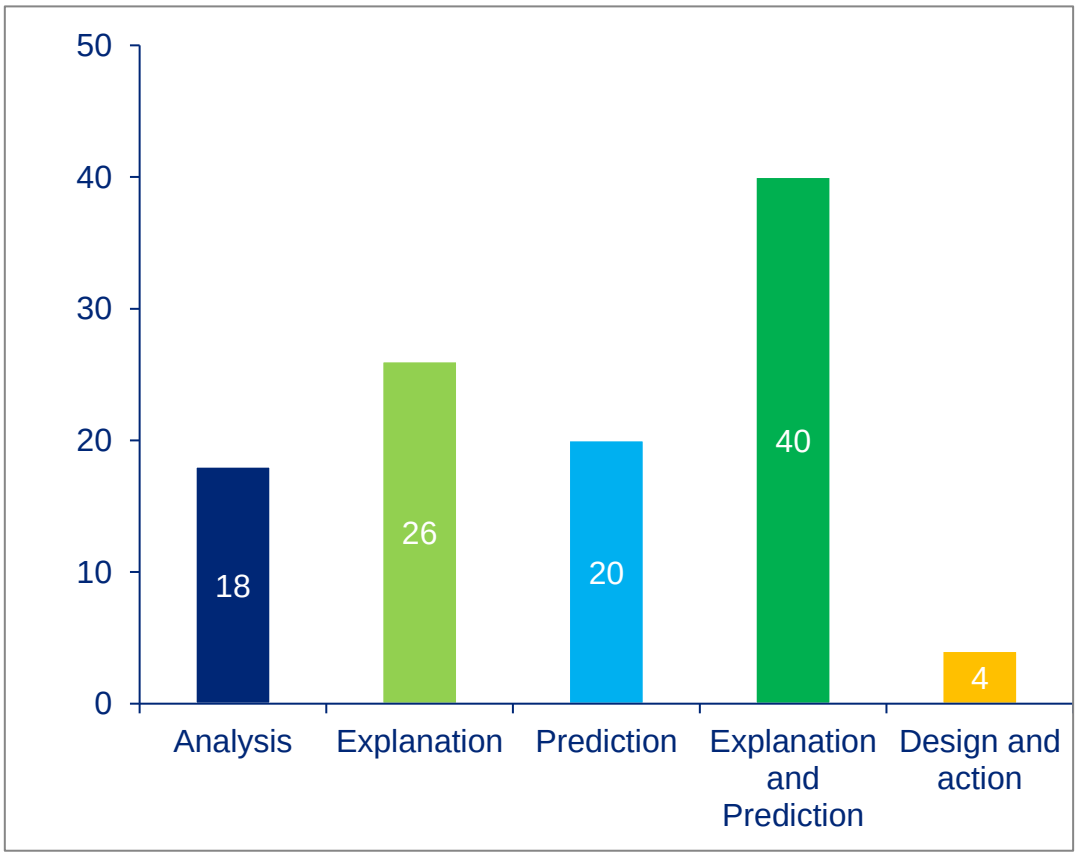


The authors of the articles in general explain their theoretical concerns and choices in the theoretical framework section. Accordingly, these sections were examined closely as the first step to categorising the articles according to Gregor's (2006) five-type typology (see section 4.2.2).

Eighteen articles were based on analysis theory, employing a range of theories including institutional theory, compliance theory, security policy dimension and grounded theory. Twenty-six employed theory for explaining (drawing on structuration theory, rational choice, protection motivation theory, social control theory and actor-

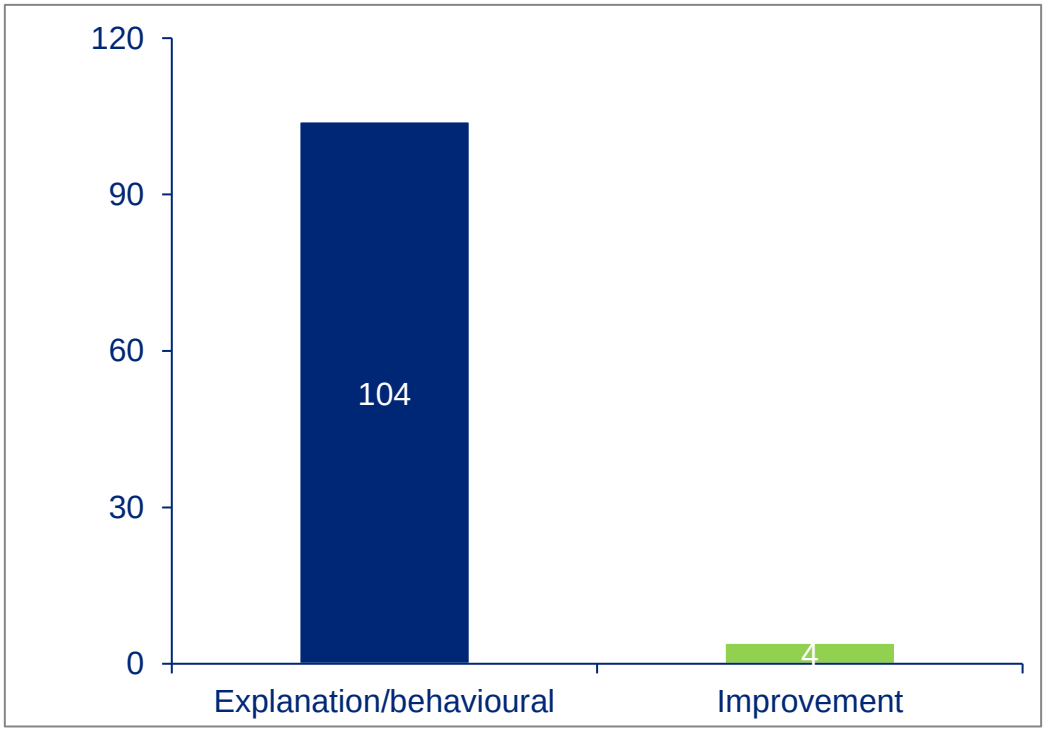
network theory) and 20 employed theories for predicting (including game theory, theory of planned behaviour, neutralisation theory and statistical learning theory). The largest group was that employing theory for explaining and predicting; the 40 articles in this category drew on a range of theories including the technology acceptance model, cognitive evaluation theory and technology threat avoidance theory. Finally, just four articles employed theory for design and action. Typically these referred to biological immune systems, system dynamics and secure systems design. The summary of the adopted theory is illustrated in Figure 5-5.

Figure 5-5 Statistics on Research Theory



As discussed in section 4.2.3, Hevner et al. (2004) classify research methods as either explanation/behavioural-oriented or improvement-oriented. Overall, researchers elaborate their choice of research method in the methodology and/or research design sections; examination of these sections revealed that 104 of the selected articles were explanation/behavioural-oriented, with the remaining four being improvement-oriented (Figure 5-6).

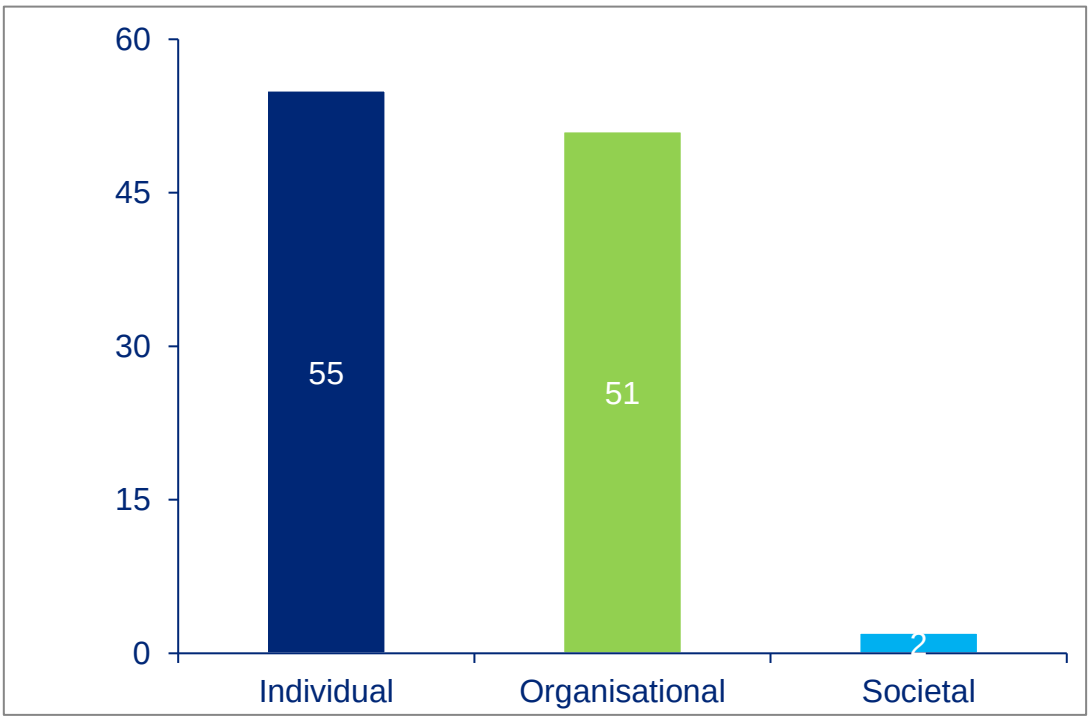
Figure 5-6 Statistics on Research Method



Gupta et al. (2007) suggest there are three main levels of research analysis (see section 4.2.4). Typically, IS research papers contain a discussion section whereby the researcher analyses the research outcomes and attempts to apply them theoretically and practically to a specific context. Examination of these sections revealed that 55 papers

were conducted at the individual level, while 51 were conducted at the organisational level. Only two papers were undertaken at the societal level (Figure 5-7).

Figure 5-7 Statistics on Research Analysis



5.2 Preliminary Results

Since the aim was to delineate the overall pattern of current ISsec research, the four sets of results were combined to generate a comprehensive picture (see Table 5-1).

Since too much detail might make broader patterns harder to discern, the preliminary results were consolidated where possible. Thus, in the theory dimension, theories for explanation, prediction and explanation and prediction were combined into a broader explanation and/or prediction category. Secondly, the dimension "research analysis" was viewed as the aftermath of each research activities as it deals primarily with a

specific discussion based on its result(s), which are concluded through the previous process of research paradigm, research theory, and research method. From this process, it was found that the articles were clustered largely into four types (Table 5-2) with different combinations in their philosophical assumption, cognitive aim, operational dimension and interpretive level.

Table 5-1 Breakdown of Preliminary Literature Examination Results

Paradigm	Theory	Method	Analysis	Number
Philosophical Assumption	Cognitive Aim	Operational Dimension	Interpretive Level	
Positivist	Explanation	Explanation (Behavioural)	Societal	1
	Analysis		Organisational	1
	Explanation and Prediction		Individual	24
			Organisational	6
	Prediction		Individual	1
		Improvement	Organisational	1
	Design	Improvement	Organisational	4
Interpretive	Explanation	Explanation (Behavioural)	Individual	19
			Organisational	6
	Prediction		Individual	13
			Organisational	4
	Explanation and Prediction		Individual	6
			Organisational	4
	Analysis		Individual	7
			Organisational	7
Critical	Prediction	Explanation (Behavioural)	Individual	1
	Analysis		Organisational	2
			Societal	1

Table 5-2 Preliminary Pattern of ISsec Research

Track	Paradigm Philosophical Assumption	Theory Cognitive Aim	Method Operational Dimension	Analysis Interpretive Level	Number
1	Positivist	Explanation and/or Prediction	Explanation (Behavioural)	Individual	9
				Organisational	22
				Societal	1
2	Interpretive	Explanation and/or Prediction	Explanation (Behavioural)	Individual	38
				Organisational	14
	Critical			Individual	1
3	Positivist	Analysis	Explanation (Behavioural)	Organisational	1
	Interpretive			Individual	7
				Organisational	7
	Critical			Societal	3
4	Positivist	Design	Improvement	Organisational	4
		Prediction		Organisational	1

Table 5-2 summarises the various combinations of methodological types identified within each of the four clusters or tracks, highlighting the largest subgroups. These include articles in Track 1 aimed at the organisational level, and articles in Track 2 employing the interpretive paradigm and aimed at the individual level.

Most of the articles in Track 1 addressed the issue of security from the economic perspective, either by mathematical modelling or employing economic/financial theory. These articles include one by Cavusoglu et al. (2008), published in *JMIS*, which examines one organisation's security investment decisions by modelling its decision-making process. Adopting a positivist position, the study draws on both design and

game theories. Another article in Track 1 was by Fang et al. (2014), who investigate the interdependent security issue at one firm by modelling the problem as a signalling-screening game. In view of this economic perspective, this track was named ISsec economic research.

Track 2, which comprised articles with a behavioural focus, accounted for almost 50% of the sample. One example was the research conducted by Tu et al. (2015), who draw on social learning theory to examine how key information sources influence users' motivation to protect their mobile devices against loss and theft. Chatterjee et al. (2015) were also in this track with a study aimed at unravelling the factors underlying unethical IT use. This track was labelled ISsec behavioural research.

Track 3 was concerned largely with the adoption and outcome of strategy; therefore, it was labelled ISsec strategic research. The research of Chang and Wang (2011) belongs in this category. These authors investigate how the distribution of information systems resources by top management affects, and is affected by, IS management architecture. Herath and Rao (2009a), meanwhile, investigated protection motivation and deterrence with the aim of building a framework for security policy compliance in the organisational context.

Track 4 was small, comprising a mere four papers. The main aim of these articles (e.g., El-Gayar and Fritz, 2010) was to identify ways of making systems more adaptable and better able to protect organisations from potential attacks. This track was labelled ISsec design research.

Table 5-3 summarises the four tracks that make up the pattern of ISsec research, alongside their dominant methodological characteristics.

Table 5-3 Pattern of ISsec Research and its Main Tracks

Main Tracks	Paradigm	Theory	Method	Analysis
	Philosophical Assumption	Cognitive Aim	Operational Dimension	Interpretive Level
ISsec Economic Research	Positivist	Explanation and Prediction	Explanation (Behavioural)	Organisational
ISsec Strategic Research	Interpretive	Analysis	Explanation (Behavioural)	Organisational
ISsec Behavioural Research	Interpretive	Explanation	Explanation (Behavioural)	Individual
ISsec Design Research	Positivist	Design	Improvement	Organisational

Previous classification systems, such as the three-track typology proposed by Siponen (2005), are rooted fundamentally in the research topic, but this has obvious drawbacks. To start, it is impossible to anticipate and enumerate all potential topics for ISsec, but more importantly, topic-based classification systems must be updated frequently if they are to respond to advances in information technology and shifting public concerns. Conversely, this pattern-based classification system provides a consistent and coherent reference for assessing the nature of any ISsec research.

The framework highlights that the various research dimensions have a synergistic influence rather than an accruing effect (Doty & Glick, 1994), and that the quality of a piece of research must be judged holistically. In addition, it allows scholars to envisage

a more systematic approach to ISsec research in the four tracks; for example, fidning new ways to combine components.

SECTION IV DISCUSSION

This section offers an in-depth analysis of the four main tracks identified in the literature survey. The section aims to stimulate reflection on the practices in each track, in anticipation of encouraging a more reasoned and mindful approach to methodology.

One of the most pronounced features of contemporary ISsec research is the broad range of research perspectives employed. These researches are marked by a plethora of methodological combinations, each containing bespoke philosophical paradigms, theories, methods and analysis. Given the complexities of security issues, the existence of plurality of perspectives facilitates the exploration of phenomena from diverse frames of references. In this regard, the research practices must effectively render this implication from the ways in which the research activities are undertaken.

Chapter 6 ISSEC ECONOMIC RESEARCH

Since the end of the 1990s, IS has been an indispensable part of everyday life. Unfortunately, advances in computer security technology and management have often been unable to keep up with those in computing in general (Whitman, 2004). Consequently, IS security breaches are daily occurrences, causing tremendous financial and reputational losses (He et al., 2014). Therefore, it is unsurprising that ISsec has become an increasingly important issue within IS research in recent years. The result has been a large stream of research focusing on the technical defences (e.g., encryption, access control and firewalls) associated with protecting information and detecting intrusions. However, as Zhao et al. (2008) demonstrate, the Internet can also be viewed as an economic system. This means that attention also needs to be paid to the economic incentives driving its users. This is the view of Anderson and Moore (2006), who observe that security failures are caused at least as often by bad incentives as by bad design, and that systems are particularly prone to failure when the person guarding them does not incur the full cost of this failure. Concluding that effective information security requires not just technical solutions but also economic incentives, some researchers have applied economic modelling and managerial accounting techniques (e.g., capital budgeting and incentive compensation) to explore information security.

Research focusing on the economic aspects of ISsec is still rather sparse, but it is developing quickly. Overall, researchers in this track use economic modelling to assess

the relation between the level of investment in information security and the vulnerability of an information set under different returns scenarios. The work conducted to date provides generic guidance in two related areas:

(1) the optimal level of investment in ISsec, and where this should be targeted; and

(2) the economic aftermath of information security breaches, such as the effect on stock value.

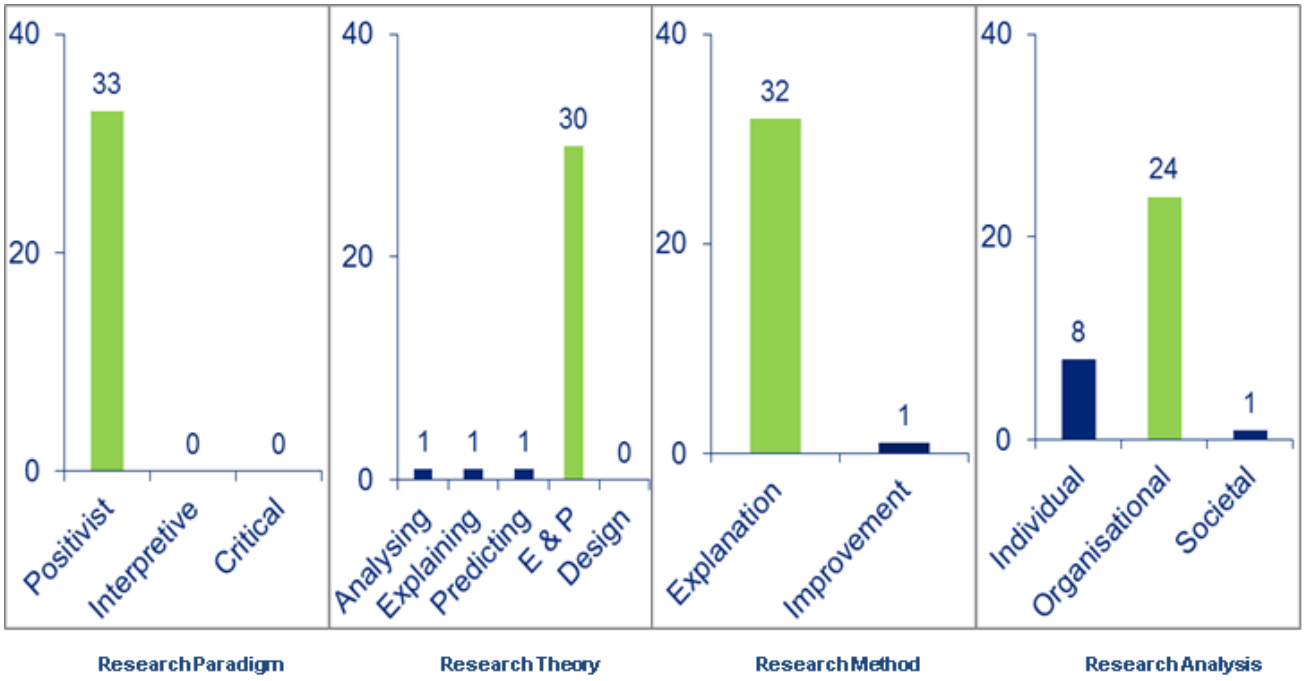
The first stream has been addressed in general terms (Gao et al., 2015; Gordon & Loeb, 2002; Hausken, 2006) and in the context of a specific class of security solutions, Intrusion Detection Systems (Cavusoglu et al., 2005). In both cases, research has focused on the organisational level. The central theme in this stream has changed from what is technically possible to what is economically efficient (Anderson & Moore, 2006), while the common approach has been to treat security risks as exogenous, even when both external attacks and internal threats are being investigated. Since determining the appropriate level of ISsec investment has become one of the critical decisions faced by chief security officers (Cavusoglu et al., 2004), this is an area of particular interest for researchers. Karofsky's (2001) examination of current practices in ISsec, for example, reveals that managers generally view security investment in the same way as any other IS investment, using decision-theoretic risk management or (more commonly) other less-sophisticated techniques to determine the level of investment.

As far as the economic consequences of security breaches are concerned, it is widely accepted that security attacks have resulted in financial losses to businesses amounting to billions of dollars worldwide (Anderson et al., 2013). One of the important tasks of research in this stream is to assess this impact. Numerous approaches have been taken, including attempts to quantify the financial impact of virus attacks and security breaches by measuring stock market reactions (Hausken, 2014). Such studies have produced contradictory empirical results, however, regardless of the strong theoretical basis for hypothesising a negative market reaction to security breaches. Scholars attempting to understand the reason for the mixed results have already investigated that short-term and long-term effects should be differentiated, and that there should be further investigation of whether the nature of the security breach affects the severity of its impact on market values (Cavusoglu et al., 2004; Kannan et al, 2007).

6.1 Dominant Type

ISsec economic research is dominated by the positivist paradigm and explanation and prediction theory; it generally chooses an explanation/behavioural research method and undertakes analysis at the organisational level (Figure 6-1).

Figure 6-1 Dominant Components in ISsec Economic Research



6.1.1Research Paradigm

As indicated above, the positivist research perspective dominates ISsec economic research, as it dominates research in the areas of finance and economics. Ontologically, positivist ISsec economic researchers assume that the physical and social world exists independently of humans and that it can be objectively characterised and measured. Typically, organisations are understood to have a structure and reality beyond the actions of their staff (Fang et al., 2014). Moreover, understanding phenomena is a matter of modelling and measurement, of constructing an appropriate set of variables and an accurate set of instruments to capture the essence of the phenomenon. Furthermore, a clear and fixed relationship is assumed between the variables in the researcher's model, and real-world events and objects. The researcher plays a neutral role in the investigation; uncovering, rather than intervening, in the phenomenon. When

investigating the use of investment to protect the confidentiality, availability, authenticity, non-repudiation and integrity of information, they assume structure to be objective and hence capable of being interpreted via numerous variables or parameters, such as the loss conditioned on a breach occurring, the probability of a threat occurring, and vulnerability (Bandyopadhyay et al., 2014; Huang et al., 2014).

Epistemologically, the positivist perspective adopts a hypothetic-deductive approach to scientific explanation; that is, it is primarily concerned with the empirical testability of theories. Gibbons (1987) argues that the concept of positivist science "must be redefined in order to eliminate the evaluative dimension and to ensure uniformity of measurement among researchers". Accordingly, researchers are expected to be impartial observers and to evaluate or predict actions or processes objectively. They should not allow personal opinion or subjective judgement to impact the research process. In the case of the sample articles, the researchers all seek to build up a model by drawing on financial or economic theories, and then to verify this with empirical data. The main aim is to have a practical impact on ISsec practice; that is, to enable organisations to make more effective security investment. This is reflective of the relationship between theory and practice, as assumed by the positivist paradigm. This relationship is seen as primarily technical, suggesting that a desired state of affairs can be achieved if the appropriate general laws are known.

6.1.2 Research Theory

The theories adopted in ISsec research are for explaining and predicting. As discussed previously, this set of theories, which is employed in both the natural and social sciences, explain how and why phenomena occur and predict outcomes from a set of explanatory variables or parameters. They emphasise frequently that the world may be viewed in a certain way, with the aim of instigating an altered understanding of how and why things are. They seek to understand underlying causes, make predictions and describe theoretical constructs. In ISsec economic research, the task of explaining and predicting is generally completed by combining two discrete theories, one for explaining and one for predicting, rather than by employing a single composite theory. This may be because the available composite theories for explaining and predicting, such as the technology acceptance model and cognitive evaluation theory, are mainly focused on individual behaviour. They do not fit in this context, where organisational operations are invariably discussed.

For example, Cavusoglu et al. (2008) choose decision theory and game theory as their overarching theoretical framework. Decision theory, the theory for explaining, assumes that the decisions of the focal firm have no impact on the attacker. The firm estimates how much effort a hacker would have to expend in an attack and the probability of this happening and uses the data as parameters in its payoff maximisation model to determine the optimal investment level. Although the firm assumes that its actions do not have any impact on the hacker, the hacker, being strategic, maximises his or her expected utility by first assessing the firm's vulnerability. The predictive nature of game

theory helps the focal firm to anticipate the behaviour of the strategic hacker in response to its actions and to make its decisions accordingly. The nature of the game that will be played depends on the timing of the hacker's and the firm's actions. In the simultaneous scenario, the hacker and the firm make their effort and investment decisions simultaneously. In the sequential scenario, however, the firm makes its investment decision first and then the hacker makes his or her effort decision after contemplating the firm's investment decision. Both scenarios are plausible in security contexts, and game theory makes them researchable by facilitating the prediction of both actors' behaviours and decisions. By adopting both theories, Cavusoglu et al. can provide a complete picture of how a firm makes its security-related decisions.

6.1.3 Research Method

Information systems are implemented within an organisation for improving effectiveness and efficiency. The capabilities of the IS and the characteristics of the organisation, its work systems, its people and its development and implementation methodologies together determine the extent to which this purpose is achieved (Silver et al., 1995). However, IS researchers can also contribute by developing and communicating knowledge to better facilitate the management of information technology and its use for managerial and organisational purposes.

Hevner et al. (2004) highlight that this knowledge is developed within two complementary but distinct paradigms, behavioural science and design-science (March & Smith, 1995). The behavioural science paradigm is rooted in natural science research

methods. It seeks to develop and justify theories that explain or predict organisational and human phenomena surrounding the analysis, design, implementation, management and use of IS. Ultimately, these theories inform researchers and practitioners of the interactions among people, technology and organisations that must be managed if an IS is to achieve its stated purpose; namely, improving the effectiveness and efficiency of an organisation. These theories impact, and are impacted by, design decisions made with respect to system development methodology, and functional capabilities, information content and human interface of the IS. The majority of ISsec economic research in the sample deploys methods from the behavioural science paradigm, such as quantitative surveys for data collection and hypothesis verification and mathematical modelling.

6.1.4 Research Analysis

The clear majority of ISsec economic research in the sample was conducted at the organisational level. It covers two domains: optimising information systems security investment; and the financial impacts of an IS security breach. Articles in the first domain focus on two main topics of analysis: the practical ramifications of the results derived from mathematical modelling; and how to make reasonable decisions based on the derived theoretical models. These questions are addressed primarily at the organisational level (there were a few cases at the individual level and very few at the societal level) in the context of a firm's business practices or its struggles against attackers.

In the second domain – the financial impacts of breaches in security – the main goal of the analysis is to estimate the impact on organisational costs, particularly the market value of publicly traded firms. Most of the sample articles conclude that security breaches that result in the revealing of company secrets or confidential client information can have particularly serious consequences, including litigation, government sanctions and loss of competitive edge. Organisations are often reluctant to reveal information about security breaches for fear of passing intelligence to hackers, but an even greater concern is the potential drop in market value (Goel & Shawky, 2009).

6.2 EXAMPLE

This section reviews one study that employs the dominant research approaches to explore firm investment in customer information security. This should help illustrate the typical characteristics of ISsec economic research.

The study of Lee et al. (2011) is among the 33 papers in this track, which was coherently structured, well written, and explicitly discussed; and was thus chosen as an example. It investigates how companies can balance the need for security investment against the drive to maximise profit. They are interested specifically in understanding how companies can balance the need to protect customers' personal information against the cost of this protection, and how they can identify the optimum level of security investment for this purpose. They handle these questions by introducing a mathematical

model to value ISsec investment decisions. They posit that companies faced with a range of ISsec investment options will take into account several factors when making their choice, including customer preferences (customers are more likely to be attracted by higher levels of protection) and the level of risk they are willing to tolerate to maintain acceptable profitability. The authors borrow the theory of value-at-risk from financial economics to model the operational risk (that is, the risk of monetary loss due to inadequate or failed internal processes, people and systems, or from external events). This allows them to consider risks from all sources and arrive at a comprehensive risk measurement. Next, they define a set of model parameters to deduce the mathematical relationships between revenue, the probability of a security attack and ISsec implementation costs, and to estimate the potential losses under two scenarios – inefficient and efficient information security.

The research contributes to the IS field by quantifying the trade-off between security investment (cost) and information security. The authors find that some investment is necessary to achieve a minimum level of protection, but beyond this, organisations can decide for themselves what their optimal level of security investment is by factoring in the cost of implementing ISsec measures and the concomitant risk mitigation.

6.3 Assessment

ISsec economic research has contributed to the field of information systems security primarily by explaining and predicting companies' security-related investment

decisions and behaviours. It has applied widely-accepted methodological components and standards, such as mathematical modelling, and has sought to expand knowledge by elaborating the causal relationships between investment, cost and profit. Research models and a handful of useful and practical results have appeared in various journals, and much has been learned about security-related investment. However, in general, it has not incorporated alternative philosophical stances; thereby precluding the potential for diverse forms of knowledge, different assumptions about reality and a variety of methodological approaches. In this regard, current ISsec economic research is inherently restrictive.

Several other limitations are evident. Firstly, ISsec economic research ignores the fact that human action is impacted by the historical and contextual conditions. This is no less true of ISsec, whose adoption within organisations is affected inevitably by the social context and issues of motivation, politics and culture. Neglecting these influences may lead to an incomplete picture of the issues, given the fact that positivist research studies are rooted in the status quo. Similarly, in choosing to utilise the theory of explaining and predicting, positivist researchers are adopting a predefined and circumscribed stance towards investigation of the phenomenon. The theoretic focus on what will be, rather than what is, or on questions of how and why, is not conducive to the discovery and understanding of non-deterministic relationships. Thus, the use of additional type of theory, such as analysis theory, is strongly recommended.

Furthermore, current ISsec economic research relies heavily on quantitative-based explanatory research methods; typically, mathematical modelling. Even in studies that aim to understand firms' decision processes, ISsec economic researchers have failed to obtain first-hand data from the focal firm; instead, they have relied exclusively on theory to indirectly apprehend the process. This method alone is insufficient and needs to be strengthened.

Finally, this research focuses overall on the organisational level. While studies have found theoretical evidence (from mathematical modelling) to suggest a relationship between security investment and operational targets, they have not explored the impact of individual practices or societal expectations on security investment decision-making. Consequently, analysis is required urgently at both individual and societal levels.

6.4 VARIANCE

As illustrated previously, the mainstream of ISsec economic research employs the positivist paradigm, explanation and/or prediction theory, explanation/prediction-oriented methods and organisation-level analysis. It is argued the necessity of expanding the current research approach by adopting alternative methodological components should be heightened.

6.4.1 Research Paradigm

Although widely accepted throughout the social sciences, the interpretive paradigm is seldom employed in ISsec economic research, despite the significant benefits of its usage. This perspective, which asserts that reality is socially constructed, is extremely useful in understanding the intersubjective meanings embedded in social life and the behaviours of social actors. Current ISsec economic research is somewhat lacking in this regard, with most studies assuming a linear and direct relationship between a company's security-related investment and its security outcome; thereby ignoring the context in which the company operates. Researchers in this track have not examined the reasons why companies make certain security-related investments, but focused instead on the amount invested. Neither have they investigated the influence of social context on investment decisions. Every company operates under a unique set of conditions (both in terms of internal governance and external social setting) as it pursues its designated managerial and financial targets. Researchers who neglect these conditions may end up misunderstanding the company's decisions. Therefore, a research from interpretive perspective is desired and needed (as highlighted in Table 6-1).

6.4.2 Research Theory

All available research in this track has been guided by explanation and/or prediction theory. Prediction theories, in particular (e.g., game theory and value-at-risk), have dominated researchers' attempts to identify how companies might reconcile their

security-related investment with their overall operational targets and how security breaches might potentially affect company profits and other financial targets. In other words, instead of examining the impact of security investments that have already been made, scholars have chosen to concentrate on the future.

Consequently, the theory of analysis has been devalued and downplayed, leaving unanswered research questions; for instance, why a company might choose to make a particular security-related investment, what their ongoing security targets are, and how these targets connect with their investment (highlighted in Table 6-1). Given the usefulness of analysis theory in understanding specific dimensions or characteristics of individuals, groups, situations and events, it is the contention that the time has come to adopt this type of theory to address these questions. Such a change is not without precedent; researchers have already shown they are willing to embrace new theoretical perspectives, moving from annual loss expectation in the early days of the discipline to value-at-risk, and then to game theory. Along the way, they have moved from focusing on a single company to investigating interdependent security investments made by two or more companies.

6.4.3 Research Method

Almost all extant research in this field has been undertaken using the quantitative-based method of mathematical modelling. While this undeniably has helped scholars understand the institutionalised processes within which security investment decisions are made and implemented, it has not facilitated the collection of data on how

individuals understand or act within these processes. Therefore, the employment of qualitative methods is (highlighted in Table 6-1), such as interviews, case studies and action research. Such methods make it easier to understand people and the contexts within which they live.

6.4.4 Research Analysis

Most of the analysis in ISsec economic research has been conducted at the organisational level, as this research has focused generally on organisations' decision-making in regard to ISsec investment. The research subjects have mostly been IT companies and financial institutions, and data collected at company level (e.g., investment decisions, size of investments, number of security incidents experienced by the company). Data has not been gathered at the individual or societal level, which means that researchers have failed to consider the impact of these security investments on employees and attackers, and on society as a whole.

However, researchers could make an invaluable contribution to the field by addressing the individual and societal levels. At the individual level, for example, ISsec economic research could focus on the factors that determine investment. There is scope for two streams of research here: one might look at individual subjects, investigating how top managers/CTOs make security-related decisions, while the other might employ a social psychology lens to examine the effect of the social and professional contexts on the investment behaviours and/or decisions of an individual or group of senior staff. At the societal level, ISsec economic research might focus on the interplay between the

structure and dynamics of society on the one hand, and the emergence and diffusion of security investment services on the other. Moreover, it should examine the impact of security investment on society at large; for example, on external costs and the potential for adverse selection.

In summary, it is recommended that ISsec economic research should also be conducted from the interpretive perspectives, and employ analysis theory at the individual and societal levels (highlighted in Table 6-1).

Table 6-1 Recommended Practices for Research Components in ISsec Economic Research

Research Component	Current Practice	Recommended Practice
Research Paradigm	Positivist	Positivist
		Interpretive
Research Theory	Theory for explaining and predicting	Theory for explaining and/or predicting
		Theory for analysing
Research Method	Quantitative-based explanation method	Quantitative-based explanation method
		Qualitative-based explanation method
Research Analysis	Organisational level	Organisational level
		Individual level
		Societal level

Chapter 7 ISSEC BEHAVIOURAL RESEARCH

ISsec behavioural research encompasses all the complexities of human activity that influence the confidentiality, integrity and availability of information and IS (Zhang & Galletta, 2006). Coverage of ISsec in the popular media and trade journals over the past 10 years has focused primarily on finding technical solutions to the problem of security breaches, but it is not enough to rely solely on technical solutions and authoritarian mandates, as these fail to address the underlying behavioural causes of the problem. Worse yet, recent evidence suggests that if authoritarian approaches go too far, they can backfire, causing insider-related problems to increase rather than decrease (D'Arcy et al., 2014).

Technology and behaviour are inseparable in IS (Hevner et al., 2004); thus, ISsec is as much a behavioural issue as a technical one. Users adapt their behaviours to the requirements of the system, but they may also attempt to modify aspects of the system to make it easier to use (DeSanctis & Poole, 1994). The resulting "technology in practice" (Orlikowski, 2000) may differ significantly from the system designer's intention and may yield counterintuitive results (Gray & Durcikova, 2005). To understand the effects of user behaviour on information security, researchers and practitioners must incorporate frameworks from disciplines outside of computer science and electrical engineering that examine human perceptions, beliefs, motivations and behaviours.

One emerging research stream on the human perspective of ISsec focuses on end-user behaviours; specifically, the factors that produce compliance. End-users operating in decentralised environments, whether they share or have sole responsibility for their computing resources, commonly receive input from others regarding the most effective information assurance practices (Warkentin & Johnston, 2006). Paradoxically, this input from others may have the opposite of its intended effect by causing users to change their behaviour in ways that might compromise security (Guo et al., 2011). Therefore, scholars believe that user behaviours can cause the actual level of security provided by a specific authentication credential to be much lower than the analysis of its technical specifications would predict. Furthermore, they underscore the need to consider user experience and perceptions of authentication mechanisms. If users perceive a system in a negative light, they are less likely to use it voluntarily; if its use is mandatory, they are likely to circumvent or modify features they regard as overly burdensome (Herley, 2009). Research in this stream concentrates primarily on two groups of individual actors:

(1) employees in the organisational environment (Puhakainen & Siponen, 2010); and

(2) the consumers of Internet services (Yang & Padmanabhan, 2010).

It treats these individuals in two main ways: as the weakest link in the security chain (Im & Baskerville, 2005; Ng et al., 2009; Vroom & Von Solms, 2004) or as the protective stewards of sensitive information (Dinev et al., 2009; Stanton & Stam, 2006).

Employees are generally viewed as the key link in ISsec, and frequently the weakest link in the corporate defences (Bulgurcu et al., 2010). However, many organisations recognise that their employees can also be great assets in the effort to reduce information security risk. Since employee compliance with ISsec rules and regulations is key to strengthening information security, understanding compliance behaviour is crucial for organisations that want to leverage their human capital. When individuals choose to disregard security policies and procedures, they put the organisation at risk. Consequently, the main question in this research stream is how organisations motivate their employees to behave responsibly.

Employees' abuse and misuse of IS resources is identified in the literature as the major insider-related information security issue. Most of the early empirical studies investigating end-user behaviours assumed that employees simply choose to engage in inappropriate behaviours, and they therefore focused on deterrent and preventative strategies (e.g., sanctions) for reducing IS misuse and computer abuse (Mirchandani & Motwani, 2003). Willison (2006) went further, arguing that organisations (and scholars) need to understand the actual behaviours of offenders at various stages of their misuse so that they can implement controls or safeguards that will reduce employees' ability to misuse the IS at each stage and, ultimately, influence their decision-making processes. Other researchers in this stream have investigated the antecedents of employee security behaviour, revealing the relationships between end-user security behaviour (such as password management and obtaining security training) and a combination of situational

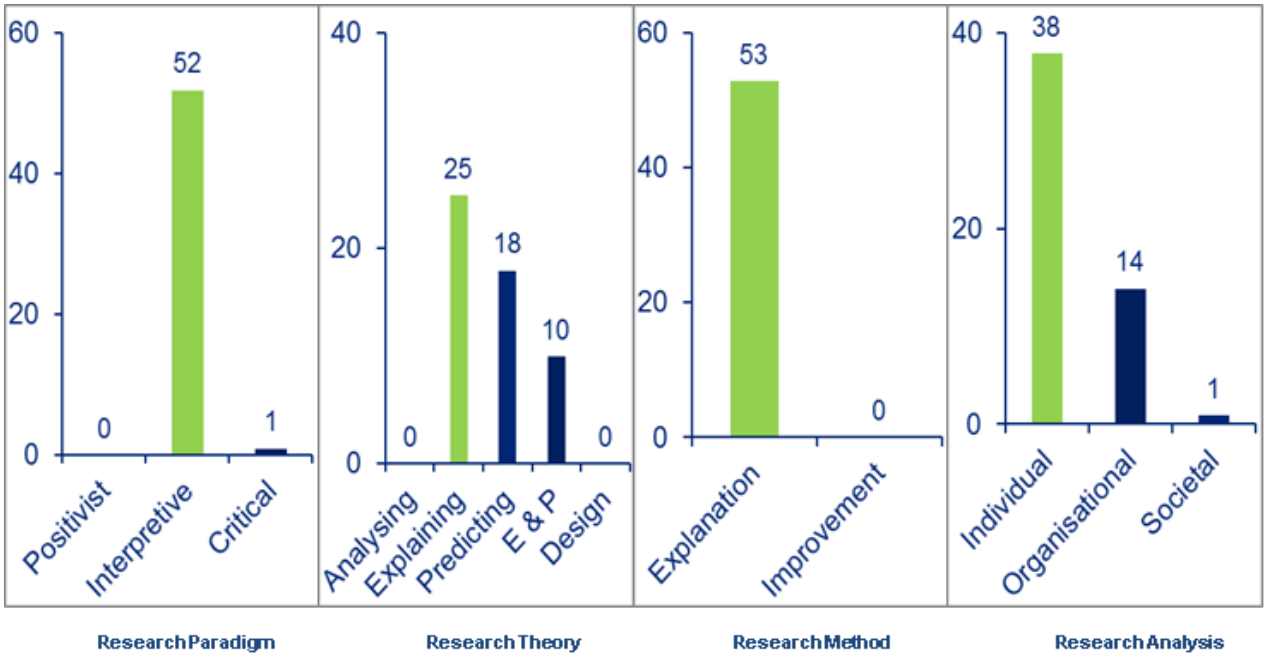
factors (such as organisational type) and personal factors (such as income level and job role) (Boss et al., 2009; Lee & Lee, 2012; Posey et al., 2014).

The second stream pertains to computer users in non-work environments (i.e. general customers). These environments differ from organisational settings in the absence of managerial interventions and controls. Examples of studies in this stream include: Chang and Chen (2009), who apply the decomposed theory of planned behaviour to identify the factors that influence home users' intention to practise computer security (family, peer and mass media influence, perceived usefulness and self-efficacy are identified as important); and Chatterjee et al. (2015), who investigate the determinants of safe online behaviour (they find online safety involvement, self-efficacy and personal responsibility to have a significant influence).

7.1 Dominant Type

ISsec behavioural research is dominated overwhelmingly by the interpretive paradigm. It tends to employ theories of explaining and (mainly quantitative) explanation/ behavioural research methods, and discuss its outcomes at the individual level (Figure 7-1).

Figure 7-1 Dominant Components in ISsec Behavioural Research



7.1.1 Research Paradigm

The interpretive perspective is becoming increasingly popular in the information systems field, including in ISsec behavioural research. This paradigm asserts that reality, and the knowledge obtained from reality, are socially constructed; the world is not a fixed constitution of objects, but "an emergent social process – as an extension of human consciousness and subjective experience" (Burrell & Morgan, 1979). The target of interpretive research, therefore, is to understand how individuals enact reality through their involvement in this social process, and how these outcomes in turn affect their social reactions and build social structures. Since the world is not objective and given, but produced and reinforced by individuals' actions and interactions, the researcher can only understand it, and other socially constructed communities such as organisations and groups, through their own social participation. This has several

implications: firstly, that their interpretation of reality will be shaped by social systems, which may shift over time as social circumstances, objectives and constructions change; and secondly, they cannot avoid being implicated in the phenomenon being studied. Their own values, experiences and beliefs, themselves shaped by their social context, will inevitably influence their investigation.

Puhakainen and Siponen's (2010) study is one example of the interpretive paradigm being employed to explore employee compliance. Their action research examines the impact of ISsec training programmes on employee compliance, concluding that employees actively process the information they receive and then decide for themselves whether to comply with the company's security policy. Their decisions are also likely to be affected by social and personal circumstances. It was not expected that the policy would be obeyed without its reasonableness being questioned. Hence, the authors assume this study holds a relativist ontology, meaning multiple realities are socially constructed by the employees (Guba & Lincoln, 1989).

7.1.2 Research Theory

Twenty-five of the 53 articles in this research stream employ theory for explaining. This type of theory addresses how and why phenomena occur; its main concern is not to arrive at testable predictions about the future, but to demonstrate how the world may be viewed in a certain way, with the aim of cultivating an altered understanding of how and why things are.

The theories adopted in ISsec behavioural research include the theory of planned behaviour (TPB), protection motivation theory and social learning theory. These all fall into the subtype of theories that give explanations for how and why things happen in some particular real-world situation. TPB has proved highly successful in explaining behaviours. It examines an individual's intention to perform a certain behaviour by considering three determinants: attitude (towards the behaviour), subject norm and perceived behavioural control. Attitude refers to the overall evaluation of the behaviour, while subjective norm is what the individual believes others think about their ability to perform the behaviour. Perceived behavioural control is the extent to which performance of the behaviour is perceived as easy or difficult (Ajzen, 1991). TPB assumes a direct link between perceived behavioural control and the actual behaviour.

7.1.3 Research Method

Like ISsec economic research, ISsec behavioural research has mainly adopted the behavioural science paradigm, developing and justifying theories to explain organisational and human phenomena related to the implementation and utilisation of information systems. Similarly, it also relies heavily on quantitative methods; all but one (which uses qualitative approach) of the ISsec behaviour articles in the sample draw on the literature to propose hypotheses which are then justified using quantitative data. Only one article in this research track utilises a qualitative research method; in this case, action research.

Most of the research articles develop their theoretical framework by expanding and developing extant theories, and they are focused on verifying the existence of causal relationships between variables. For example, Chang and Chen (2009) draw on the cognition-affect-behaviour model to examine the influence of customer interface quality, perceived security and customer loyalty on customer security behaviour on an e-commerce website. Having added their own variables to the model, they conducted a questionnaire survey to verify their inter-connections. The article is an example of how ISsec behavioural research generally expands upon and verifies already theorised relationships, adapting its research questions to these settled contexts. In other words, it normally borrows its concepts and theoretical and conceptual variables from other disciplines.

7.1.4 Research Analysis

In both employee- and customer-oriented studies, analysis is usually conducted at the individual level. At this level, research falls into two different but connected streams. One stream of research studies the factors that affect user security behaviours in theoretical terms. Myyry et al. (2009), for example, report that employees' intention to comply with ISsec policies is affected significantly and positively by their perceptions regarding the organisation's vulnerability to potential security threats, the perceived severity of these threats, whether they believe they can apply and adhere to the policies, their attitude towards compliance, and the social norms around compliance. More recently, a second stream has examined user security behaviours with a view to

instigating practical improvement. Thus, Puhakainen and Siponen's (2010) examination of employees' security behaviour leads them to recommend that compliance can be improved by implementing a systematic information systems security training programme.

7.2 EXAMPLE

This section reviews one of the articles examining user security behaviour to demonstrate how the dominant methodological components are employed typically in this research track. This article, chosen for its coherence and cohesion in structure and writing by Dinev et al. (2009), investigates the impact of national culture on user behaviour towards protective information technologies. The study is one of the few cross-cultural comparative studies to have been conducted in ISsec behavioural research; thereby enhancing its significance, given that organisations are increasingly operating internationally and employing multinational staff.

The authors focus on the United States and South Korea. They argue that as two well-established democracies with highly advanced Internet infrastructure and services but radically different cultures, philosophies and values, these nations provide a thought-provoking window into the influence of national culture on user security behaviour. They utilise the TPB (Ajzen, 1991) as the theoretical lens to examine user behaviour, combining it with Hofstede's (1993). cultural framework to investigate the cultural dimension. The cultures of the United States and South Korea are classified according

to the five dimensions of Hofstede's framework and these five cultural effects incorporated into the TPB as moderating factors. Empirical data for the study was collected from tertiary school students in both countries over a period of four weeks, with 227 usable survey responses (out of the 339 returned responses) being subjected to quantitative analysis. Structural equation modelling was employed to test the relationships among the constructs where the moderator was a discrete variable in multi-groups. The results support the authors' hypothesis that cultural difference is an important factor affecting user security behaviour and security outcomes.

The study contributes theoretically by identifying the factors that influence computer users' decision to use protective information technologies against harmful technologies such as spyware. More importantly, it is the first study to offer empirical confirmation that culture impacts positively on the relationship between attitudes and behavioural intention, and actual behaviour. Practically, the research highlights to companies, especially multinational corporations, the need to adopt different approaches for different countries in relation to raising user security awareness and improving behaviour.

7.3 Assessment

ISsec behavioural research has expanded the understanding of information systems security by incorporating behavioural analysis and focusing specifically on the individual using the products and services. One of the most important contributions of

ISsec behavioural research has been to introduce human influence into the discussion of seemingly technological problems. Consideration of the human factor has played a pivotal role in enabling researchers to dissect and analyse security puzzles, as it allows a range of factors (e.g., organisational sanctions, individual dispositions, security-related attitudes and beliefs and workplace context) to be linked to employees' security compliance decisions using theories borrowed from other disciplines. Consequently, ISsec behavioural research has demonstrated both academics and practitioners the importance of taking human factors, as well as technical issues, into consideration.

However, from a methodological perspective, this research track is deficient in a variety of ways. First and foremost, it is overwhelmingly inclined towards the interpretive paradigm, with almost all researchers favouring this over the positivist and critical alternatives. It is understandable that the research pattern has progressively shifted from a positivist stance to an interpretive one, but the track would also benefit from more contributions from within the critical paradigm.

Regarding the research theory, a wide range of explanation theory has been used. As discussed above, this type of theory is content to explain how and why phenomena occur; with its help, research questions such as how user security-related behaviours are affected by various factors, and why employees and/or customers fail to comply with security guidance, have been asked, examined and relatively satisfyingly answered. Beyond this, however, a larger area remains unexplored. It is still unknown, for example, how user security behaviour might be improved, what the current situation is for user

security behaviour, and how much difference it makes when internal and external factors are properly addressed. ISsec behavioural research cannot be regarded as conclusive until it answers these questions, but its current choice of theory cannot fulfil this requirement.

The choice of research methods in the sample articles is consistent with the explanation/behavioural paradigm, with most relying on quantitative methods to approach their research questions. These quantitative methods are useful for examining and verifying known relationships, but much less so for developing latent relationships or discovering unknown relationships.

Finally, 38 out of the 53 articles observe behaviours at the individual level. This level of analysis is straightforward to follow and relatively easy to understand; therefore, it is easy to observe why it has been the preferred starting point for researchers in this track. As ISsec research progresses, however, researchers need to follow-up by addressing the organisational and societal levels.

7.4 VARIANCE

This section introduces measures designed to address the deficiencies mentioned previously and expand research practices in paradigm, theory, method, and analysis respectively within this track.

7.4.1 Research Paradigm

The widespread adoption of the interpretive perspective has extended the scope and depth of research beyond what was possible under the positivist perspective, but there is a strong argument for introducing the critical perspective into ISsec behavioural research (highlighted in Table 7-1). More than either the positivist or the interpretive researcher, the critical researcher attempts to evaluate and transform the social reality under scrutiny; in other words, they aim to initiate social change by actively affecting the phenomena they are investigating. Unlike positivism and interpretivism, which are concerned solely with predicting or explaining the status quo, the critical stance aims to critique existing social systems and reveal any conflicting and contradictory phenomena that inhere within their structure but hinder their further development. Therefore, research that adopts a critical stance may help overcome oppressive social systems by fostering individual and collective self-consciousness and understanding of existing social conditions.

The critical paradigm asserts that social reality is historically constituted, and that individuals and social communities are not confined to existing in a particular state (Chua, 1986). Similarly, knowledge is also grounded in social and historical practices; hence, there is no theory-independent collection and interpretation of evidence to prove a theory. Its historical dimension means that the critical paradigm could be employed to examine security behavioural issues from a longitudinal perspective. Overall, it is believed that the behaviours and decisions of an individual are influenced to some degree by his or her past experience; under this paradigm, it would be possible to

identify how behaviour is cumulatively shaped and affected by a series of sequentially connected events. Moreover, the theoretical flexibility of the paradigm means that the research focus could be shifted to the social practices organisations employ to control employees. This would benefit those scholars who recognise an underlying conflict between what employees want and how firms are governed, and who are interested in understanding how struggles between the two sides influence the eventual deployment of security systems and policies and their results.

7.4.2 Research Theory

Despite evidence of a shift (18 of the sample articles employ theory for predicting and ten employ theory for explaining and predicting), almost half of the articles are limited to theory for explaining. However, explanation theory deals mainly with "how" and "what" questions to identify the possible causes of a phenomenon; it does little to help ISsec behavioural research achieve its aim of enhancing users' security awareness and introducing safe and responsible behaviours. Therefore, there is an argument for the adoption of other types of theories, such as analysis theory, prediction theory and theory for explaining and predicting in future research in this track. Together, these might provide answers not just to the "what" and "how" questions but also the "why" and "what will be" questions. Specifically, scholars might investigate the nature of employees' or users' behaviour. Is it a response to external stimuli (security policies and regulation, for instance), or an extension of internal cognition (security awareness,

for instance)? They might also ask how users' security-related behaviours can be improved, and what effect specific corrective measures might have.

In short, extending the range of theories utilised in ISsec behavioural research (highlighted in Table 7-1) will greatly diversify the range of potential research topics, in addition to expanding the research realm from events of the past and present to possible future developments.

7.4.3 Research Method

As suggested in the previous sections, noticeable gaps exist in terms of research methods, with much emphasis placed on quantitative examination. This could be due to many reasons, including sampling, statistical analyses, errors of exclusion of important factors, and divergent conceptualisations of security-related behaviours. Clearly, there is a need to reconcile such method that has been used much. Quantitative methods are useful for investigating known relationships, but less so for identifying unknown relationships. Most of the researchers in this track construct their theoretical framework by adding new variables to known theoretical models. However, while this introduces new factors into the debate, studies based largely on already-identified connections can make only a limited contribution. It is important for IS scholars to focus on less known, and to discover unknown, factors, variables and relationships. The researcher would also contend that the understanding of ISsec behavioural issues is constrained by the fact that prior studies have focused primarily on linear relationships

and/or analyses. The possibilities remain open that key relationships between the variables are nonlinear.

The researcher would echo others in calling for qualitative research to be conducted in this track (highlighted in Table 7-1). Qualitative research is designed to help researchers better understand people and the social and cultural contexts within which they live (Myers & Avison, 1997). Qualitative methods would allow researchers to develop a theoretical account of the general features of a topic while simultaneously grounding the account in empirical observations or data. They have already been proven extremely useful in identifying new variables and developing context-based, process-oriented descriptions and explanations of phenomena.

7.4.4 Research Analysis

Building on the analysis conducted at individual level, more work can be done at both organisational and societal levels. Employee security behavioural issues happen in the organisational context, so it is surprising that most research so far has not situated its discussion at this level. Research streams at this level might include investigation of the factors that affect an organisation's ability to improve/monitor employee security behaviour, and the factors that affect whether an organisation is able to appropriate the value from employee security behaviour.

Since both employees' and customers' security behaviour can lead to significant societal benefits or costs, some research should also be undertaken at societal level.

Studies might investigate what societal factors affect user security behaviour (for instance, national culture), and how users' behaviour may affect society's external costs (highlighted in Table 7-1).

Table 7-1 Recommended Practices for Research Components in ISsec Behavioural Research

Research Component	Current Practice	Recommended Practice
Research Paradigm	Interpretive	Interpretive
		Critical
Research Theory	Theory for explaining	Theory for analysing
		Theory for predicting
		Theory for explaining and predicting
Research Method	Quantitative-based explanation method	Quantitative-based explanation method
		Qualitative-based explanation method
Research Analysis	Individual level	Organisational level
		Societal level

In conclusion, it is suggested that ISsec behavioural research would benefit if researchers were to look beyond the current dominant components and expand their practice to include the critical paradigm; theory for analysing, theory for predicting and theory for explaining and predicting; qualitative methods; and organisational and societal-level analysis (Table 7-1).

Chapter 8 ISSEC STRATEGIC RESEARCH

Organisations rely increasingly on information and related systems for the strategic advantages they provide, but these systems are a growing source of organisational risk (Bulgurcu et al., 2010; Lee et al., 2013). Correspondingly, it has the effective management of information security has increased in importance (Ransbotham & Mitra, 2009). Traditionally, ISsec management has relied on technological solutions to improve information security (Cavusoglu et al., 2005; Siponen, 2005), but it is becoming increasingly apparent that consideration of socio-organisational elements is essential. Consequently, a new perspective of ISsec has emerged in the literature. This perspective focuses on the managerial processes that facilitate the effective deployment of technical solutions, tools, policies, resources and personnel to create a secure computing environment. It considers the issues from the viewpoint of the managers who are charged with securing their enterprise's information technology assets; technical solutions are regarded as important, but the main focus is on the managerial actions that promote a secure information environment.

Early work in this track identified the managerial challenges in implementing security measures (Boockholdt, 1989), the effectiveness of security countermeasures (Straub, 1990), discovering and disciplining IS abuses (Kankanhalli et al., 2003), the unique threats that exist in a networked environment (Portnoy et al., 2001), and security methods in systems development (Baskerville, 1993). More recent research has focused

on how power, politics, resistance, norms and culture affect the implementation of information systems security strategies.

Two main research streams have emerged in ISsec strategic research, the first of which relates to information security policy and employee compliance therewith. The ISsec policy is viewed as an increasingly important business document (Doherty & Fulford, 2005). It covers a broad set of security concerns (Rees et al., 2003), establishing "the organisation's approach to managing information security" (Höne & Eloff, 2002), and providing practical guidance on the "means" of information security management, as well as the desired "ends" (Stahl et al., 2012). It plays an important role in emphasising management's commitment to, and support for, information security (Doherty & Fulford, 2006). Consequently, there is a growing consensus within the literature that the security policy is uniquely well placed to proactively safeguard the availability and integrity of corporate information resources (Doherty et al., 2009; Herath & Rao, 2009b). Key areas of focus for researchers within this stream have included the effectiveness and cost of security policy enforcement measures, and finding the balance between productivity and strict security compliance, and between budgetary control and security compliance.

This stream focuses on how to design an effective security policy and increase the overall level of employee compliance. But while recent research has laid down frameworks for developing systematic security policy and applied several theories to explain compliance behaviours and related phenomena, to date, the findings have been

mixed. In practical terms, the compliance issue is complicated, with many employees being apathetic towards ISPs and ignoring them (Boss et al., 2009) or trying to circumvent them (D'Arcy et al., 2014); or even worse, doing the opposite of the desired behaviour and thus undermining the security of the organisation (Posey et al., 2011). (Recent extreme-case examples include Private Manning leaking US military documents to Wikileaks and Eric Snowden leaking NSA documents to the worldwide press.) (Thorsen et al., 2013; Greenwald, 2014) Conversely, other studies (Siponen & Iivari, 2006) have demonstrated the critical role played by information security policies and standards in managing security risks.

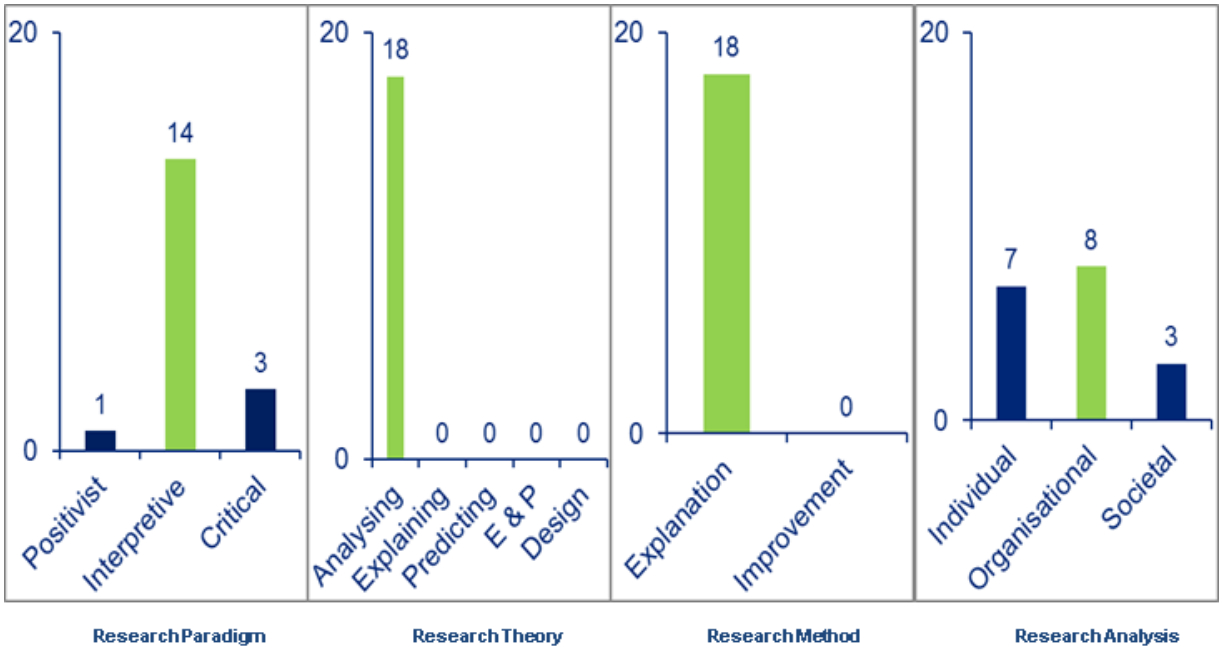
The other research stream within the ISsec strategic track puts emphasises security resources and their governance. Previous research has identified a variety of information systems security resources. These can be organised into three subsets: information technology resources, relationship resources and IS infrastructure resources (Chang & Wang, 2011). The first of these refers to the ISsec expertise and skills that a company possesses, while the second refers to the extent to which the information department collaborates with other functional units internally (i.e. finance or production) and external business partners (i.e. suppliers or customers) to achieve its security aims. The third subset – IS infrastructure resources – refers to the technical and management architectures that provide the functions and services that support system security (Srinidhi et al., 2015). Research in this stream remains nascent, but has so far tackled questions such as how resources should be allocated and responsibilities delegated, and how security decisions should be made so as to reduce the likelihood or

impact of a breach. In other words, this research stream aims to produce a system of governance that will collectively preserve IS confidentiality, integrity and availability.

8.1 Dominant Type

ISsec strategic research is dominated by research that adopts the interpretive perspective and employs analysis theory and explanation/behavioural methods. Analysis is conducted most frequently at the organisational level (Figure 8-1).

Figure 8-1 Dominant Components in ISsec Strategic Research



8.1.1 Research Paradigm

Like ISsec behaviour research, ISsec strategic research is conducted largely within the interpretive paradigm. Research in this paradigm aims to investigate the interactions between individuals and social reality, and monitor the mutual effects. Thus, ISsec

strategic researchers generally believe that an organisation's ability to meet security targets depends less on technology, compiling lengthy policies or the random use of security resources than it does on the surrounding power, politics, resistance, norms and culture. They attach importance to the security policies that are implemented in almost every company, but they argue that these policies must be examined in conjunction with users' behaviours; in other words, ISsec policies should never be drafted and executed – nor can they be understood – without consideration of the socially-bounded internal and/or external factors that surround the policy, management board and employees. Similarly, any investigation of security resource decision-making and allocation should take account of the context in which the focal company is embedded.

Ransbotham and Mitra (2009) approached the issue of ISsec management by developing a conceptual model of the information security compromise process in one organisation using one year's worth of alert data from its intrusion detection devices. They adopted an interpretive paradigm, focusing on the relevant managerial processes within their focal company (that is, the processes controlling the distribution and deployment of technical solutions, tools, resources and personnel to protect ISsec) and analysed the findings to offer possible countermeasures.

8.1.2 Research Theory

In contrast to the previous two types of research, ISsec strategic research generally employs analysis theory. Analytic theories, which analyse "what is" as opposed to explaining causes or predicting outcomes, address primarily the description of the

dimensions or characteristics of phenomena and the elaboration of how these dimensions or characteristics are interrelated. Such theories are especially useful when the phenomenon is recently emerged or is little known.

A variety of theories have been adopted in ISsec strategic research, including institutional theory (IT) and compliance theory (CT). IT posits that an organisation exists not only in a physical and tangible environment, but also in an institutional environment comprising ideas, cultures, customs and beliefs. It further asserts that the institutional environment (e.g., via market pressures) can strongly influence the development of formal structures in an organisation, often more profoundly than other factors. It recognises three dimensions of institutionalism: cultural-cognitive, normative and regulative, each of which may influence the organisation. Similarly, CT posits that in the drive for compliance – that is, to ensure their members act as per their organisational directives – organisations tend to exercise three types of control: coercive, remunerative and normative. Most organisations employ all three types of control, but to different degrees.

8.1.3 Research Method

Like ISsec economic and behavioural research, ISsec strategic research tends to employ the behavioural science paradigm. However, a more diverse range of research methods was evident in this track, with some researchers adopting qualitative tools.

Quantitative methods were used mainly to test empirically the relationships between various factors affecting policy and compliance, alongside the relationship between policy and compliance. Moreover, they were used to compare organisations' allocation of security resources with their identified security concerns and requirements, and to develop guidelines for the governance of these resources.

Fewer articles in the sample employed qualitative methods such as the case study, but those that did are worthy of attention. On the one hand, these articles give further insight into the relationships and resource allocation decisions identified in the quantitative research, and on the other, they introduce new factors for consideration by later studies. These articles illustrate the growing trend within this track for using qualitative methods to conduct empirical examinations and develop concepts.

8.1.4 Research Analysis

Eight of the 18 articles in the ISsec strategic research track are aimed at the organisational level because the original intention was to provide suggestions to these organisations under investigation. Overall, the analysis centres on the nature of security policies and the factors that should be incorporated into these policies. For instance, Hedström et al. (2011) argue that security policies should express organisational values and be designed both to improve security awareness and enhance individuals' motivation to act responsibly and in accordance with firm policies. Noting the heterogeneity of security practices and organisational values in this highly-regulated space, they suggest that organisations need to be more strategic in their approach to

security and compliance. Likewise, the research on resources and governance encountered a similar question in differentiating between the security resources and establishing their connections to governance. For example, Chang and Wang (2011) employ the resource-based view as a theoretical lens through which to examine the role played by IS resources in determining the level of information security an organisation can achieve. Their findings reveal that IS infrastructure resources impact significantly on information security and its governance.

However, unlike the other three ISsec research tracks, which tend to be monolithic, the ISsec strategic research track is characterised by a range of analytical approaches. Seven of the sample articles were analysed at the individual level, and three at the societal level. This reflects both the importance and the complexity of security strategy. Since Dhillon (2007) first pointed out that companies have made little effort to address strategic concerns about ISsec in their corporate governance arrangements, the IS community has emphasised the strategic value of ISsec. Empirical data identifying internal staff as the most significant threat to information security has highlighted the importance of its behavioural and social dimensions and confirmed the significance of all three analysis levels in strategic research. Therefore, it is unsurprising to see a relatively well-distributed pattern of analysis adoption.

8.2 Example

The research paper examined here serves as a typical example of how the ISsec strategic research in the sample employs the methodological components discussed earlier. The paper, clearly organised and discussed in-depth, by Hsu et al. (2012), is a systematic exploration into the institutional influences on information security management as an administrative innovation. Since most institution-centred frameworks overlook the effect pressures of institutional conformity have on external economic efficiency and internal organisational capability, they fail to depict how organisations adopt and assimilate administrative innovations in response to institutional pressures. Accordingly, the authors incorporate these missing elements into their study with the aim of arriving at a new, rationalised security management process to manage risk, preserve the confidentiality, integrity and availability of information and ensure business continuity.

Initially, they introduce the notion that information security management is an administrative, rather than a technological, innovation. They highlight that security problems arise not from a lack of technology – organisations have a range of technologies at their disposal to protect information security – but from the fact that the management of information security is still at a primitive stage. They adopt IT, with its concepts of coercive, mimetic and normative isomorphism, to show that various internal and external factors affect the extent to which organisations attribute importance to information security management as an administrative innovation. They

then develop an integrative model to identify the relevance of three institutional forces to information security management in South Korea.

Their data was collected using a two-phase, questionnaire-based survey distributed to 500 large firms listed in Maeil Business Newspaper's Annual Corporation Reports in Korea. Partial least squares analysis was employed to evaluate the proposed model and its hypotheses. Their findings provide strong evidence that management perceptions influence an organisation's decisions about which best practices to adopt for information security management. Furthermore, from an institutional viewpoint, the study demonstrates that institutional rules and norms place strong pressure on firms to adopt and assimilate information security management innovations.

The implications of this research are multi-fold. Theoretically, they developed and tested empirically an integrative and explanatory framework of information security diffusion processes, while highlighting the importance of the external environment on the adoption and assimilation of information systems security management practice. Methodologically, departing from both security effectiveness/misuse and risk management research, they utilised the social-organisational perspective to investigate information systems security management. Practically, their results indicate that in the early stages of information security management innovation, supervisory authorities can play a significant role in stimulating and enforcing the adoption and assimilation of new management practice.

8.3 Assessment

As a clear and strong response to the call for information security issues to be examined from a social-organisational perspective, the ISsec strategic research track has done much to expand current research. It has brought the strategic perspective into the foreground by focusing on the managerial processes that are integral to creating a secure computing environment, while its use of the interpretive perspective has allowed examination of those involved in devising and implementing ISsec strategy. Although it takes technical tools into consideration, its focus is on managerial behaviour and its influence as the antecedent of and response to this strategy. Moreover, it has helped identify the most critical security resources and established comparatively systematic governance guidelines to help organisations achieve their security targets. In general, it has highlighted the importance of taking managerial factors into account in any ISsec system.

Nonetheless, there remains room for development. For example, the interpretive perspective continues to dominate this track; there was only one positivist article and just three in the critical paradigm (Figure 8-1). While the degree of paradigmatic diversity is encouraging, further progress is required. In terms of research theory, the dominance of one approach is even more pronounced, with all 18 articles in this track employing analysis theory. This seeks typically to describe "what is" – in this case, the dimensions and nature of security policies and employees' compliance with these policies, and the kind of security resources organisations have and how these are deployed. It does not address the questions of "how" and "why", but these are the

questions that must be asked if research is to go beyond examining the status quo and identify ways of making improvements.

In terms of research method, researchers in this track have focused much attention on the explanation/behavioural paradigm and quantitative methods. Scholars have identified possible relationships between known variables drawn from existing theories and frameworks, and have successfully used quantitative methods to verify them, but there now needs to be more qualitative exploration of these relationships. With the research scope being broadened to incorporate numerous other spheres, more theoretical and practical contributions can be expected.

Finally, there is a danger that the dominance of organisational-level analysis in this track may prevent the ramifications of the research from being appreciated more broadly. However, there is evidence that researchers are waking up to the importance of individual-level analysis, with seven articles in the sample attempting to connect security policy with employee behaviours, and to societal-level analysis, with three articles observing the influence of social factors such as cultural and social norms.

8.4 VARIANCE

Several improvements can be made within this track in terms of its philosophic paradigm, theory, method and analytical approach.

8.4.1 Research Paradigm

Supplementing the interpretive paradigm with the critical perspective would enrich the philosophic stance and allow an alternative view of ISsec strategic issues. As discussed earlier, apart from the subjective understanding of and involvement into the socially constructed phenomena, the critical stance also enables the examination from a historical view that aims at moving off the conflicting and contradictory issues. In other words, the critical perspective can emancipate humans from low efficient disorder by critiquing the status quo. This adheres to the aim of ISsec strategic research to investigate how power, politics, resistance, norms and culture affect security issues.

One example of researchers adopting the critical paradigm in this track is Stahl et al.'s (2012) study of information security policy in the UK's National Health Service. These authors identify ideology and hegemony as having a greater effect on information security policy than any other factor. More elements may be discovered from such research. Tthus, additional critical studies are highly recommended (highlighted in Table 8-1).

8.4.2 Research Theory

It is understandable that due to the complicated nature of the issues involved, most ISsec strategic research generally focuses on the elucidation of security policies and security resources – the "what is" question. Consequently, a compatible type of theory – analysis theory – is widely adopted. However, as the understanding of these issues grows, the scope of this research track is expanding to address "how" and "why" questions. In

order to address these questions, other types of theories are needed. It is therefore argued that the theory of explaining, theory of predicting, and theory of explaining and predicting should be used as these tackle the "how", "why" and "what will be" questions (highlighted in Table 8-1).

For instance, Hedström et al. (2011) found that multiple forms of rationality are employed in organisational actions at any one time for information security management and compliance, acknowledging the inherent nature of value conflicts in complex organisational work environment by using the theory for analysing. While contributing to practice and research by treating ISsec as contextual and seeing users as resources, they leave open questions such as how organisational and/or employees' values might be manipulated to influence the practice of information security, and how value-based compliance affects ISsec in the focal company.

8.4.3 Research Method

Similar to the previous two types of research, ISsec strategic research generally favours the explanation/behavioural paradigm and quantitative methods to disentangle problems. However, while quantitative methods are widely used to verify relationships derived from theories, these are not suitable for mapping out new variables or constructing new connections. As research in this track becomes more holistic and in-depth in approach, qualitative methods will become increasingly indispensable (highlighted in Table 8-1).

Among those researchers who have employed qualitative methods, most use the case study as their main approach to explain and further develop the relationships between security policy and compliance, and security resources and governance. However, a wide range of qualitative tools is available, such as action research, ethnography and grounded theory. Each of these is particularly useful for addressing certain types of question, but all have the potential to provide specific and coherent insights.

8.4.3 Research Analysis

Further work should be undertaken at both individual level and societal level (highlighted in Table 8-1) in this track. Questions surrounding security policies and compliance, for example, inevitably require examination of employee behaviour; indeed, tentative efforts have already been made to examine employee behaviours in respect to enforced policies and compliance. Such topics are likely to become more popular and important as research in this track advances, rendering individual-level analysis increasingly relevant. Simultaneously, societal-level analysis is essential; not only are an organisation's decisions and strategies likely to have a discernible social impact, but societal factors such as the prevailing culture, norms and beliefs will also affect its security policy and security resources.

Table 8-1 Recommended Practices for Research Components in ISsec Strategic Research

Research Component	Current Practice	Recommended Practice
Research Paradigm	Interpretive	Interpretive
		Critical
Research Theory	Theory for analysing	Theory for explaining
		Theory for predicting
		Theory for explaining and predicting
Research Method	Quantitative-based explanation method	Quantitative-based explanation method
		Qualitative-based explanation method
Research Analysis	Organisational level	Individual level
		Societal level

If ISsec strategic research is to continue making valuable contributions to academia and industry, it must expand its research methodology. Researchers in this track are therefore recommended to consider employing the critical perspective; theory for explaining, theory for predicting, and theory for explaining and predicting; a broader

range of qualitative tools; and both individual- and societal-level analysis (highlighted in Table 8-1).

Chapter 9 ISSEC DESIGN RESEARCH

The importance of design is well recognised in IS literature. Benbasat and Zmud (1999) argue that the relevance of IS research is related directly to its applicability in design, asserting that the implications of empirical IS research should be implementable, synthesise an existing body of research, or stimulate critical thinking among IS practitioners. IS artefacts can be categorised broadly as constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices) and instantiations (implemented and prototype systems) (Hevner et al., 2004).

These are concrete prescriptions that enable IS researchers and practitioners to understand and address the problems associated with the development and implementation of information systems within organisations. Design-science, as the other side of the IS research cycle, is responsible for creating (and subsequently evaluating) IS artefacts to solve identified organisational problems. Such artefacts may take the form of software, formal logic and mathematics or informal natural language descriptions.

ISsec design research is an important part of IS design. A lack of appropriate access control on information exchange among business activities can leave organisations vulnerable to information assurance threats. Meanwhile, a gap between systems development and systems security may leave software developers with an inadequate

understanding of security risks. Typically, there are two stages in security design: conceptual design and design development (Adams & Sasse, 1999). The goals of the conceptual design phase are to understand relevant security systems, policies, procedures and responses, to identify what is required of the proposed system and to develop a preliminary design that meets end-user expectations as well as operational, financial and regulatory requirements. Understanding and clearly defining the user's needs and expectations is critical. This is best achieved by completing a "basis of design" document. It is also important to conduct a system needs analysis, for which it will be necessary to research any codes, regulations, standards and statutes that may affect the design and implementation of the security system.

Once the conceptual design phase is done, the design development phase begins. The goals of this second phase are to ensure that the system meets the organisation's current and future needs, and that it is specified in a manner that will allow the ultimate operator submitting a proposal to completely understand the requirements of the system, including components, integration, migration, installation, support and maintenance. Current research in the ISsec design research track tends to follow these two phases; in the conceptual design phase, the main emphasis is on the security requirements associated with constructs and models (El-Gayar & Fritz, 2010), while in the design development phase, efforts have focused on improving methods and instantiations (Nazareth & Choi, 2015).

In general, system development methodologies incorporate security requirements as an afterthought in the non-functional requirements of systems, but it is worth incorporating security as a functional requirement in the early stages of requirement specification and analysis. Summarising existing ISsec development approaches, Siponen (2005) identifies the need to develop theoretically and empirically grounded ISsec methods, while Siponen et al. (2006) argue that existing secure IS design fails to satisfy secure systems design requirements. Together, these comments suggest that security is not fully integrated into all phases of system development (Apvrille & Pourzandi, 2005).

Thus, an IS methodology is required that includes security as a functional requirement in all stages of system development (Baskerville, 1988). Although Siponen et al. (2006) develop enriched-use case descriptions that incorporate security policies and restrictions, enriched-use case descriptions do not capture the security requirements for information exchange from a business-process perspective.

Other researchers have attempted to provide more detailed and specific descriptions of the requirements by drawing on theories from other disciplines to understand what users want and the factors that affect their needs. Similarly, researchers in the design development phase have imported theories and approaches from other areas to address unsolved problems or find more efficient solutions (Hevner et al., 2004).

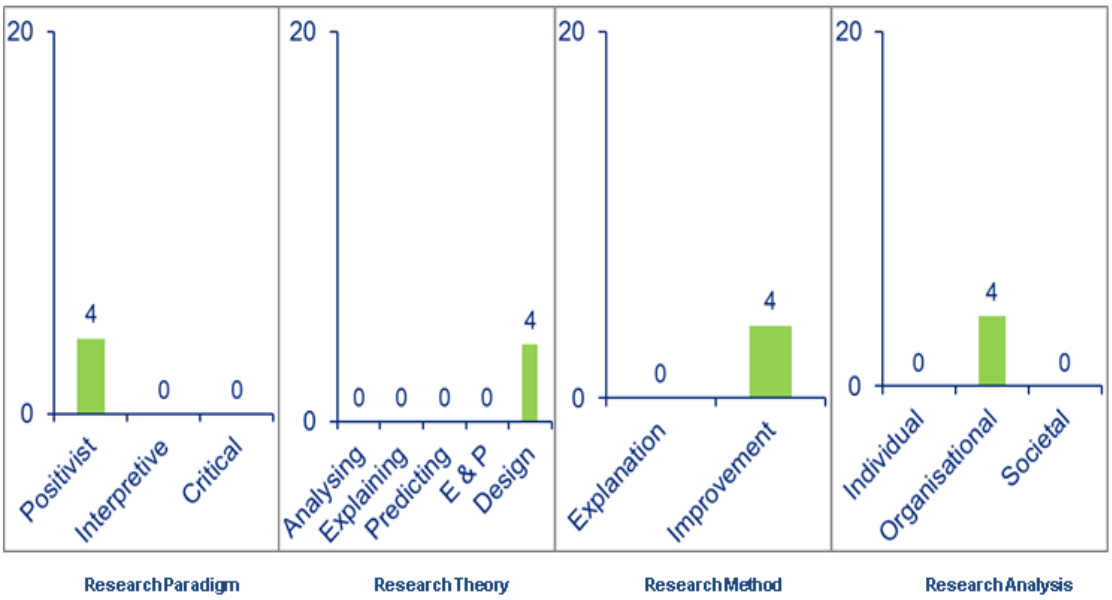
Wong et al. (2012), for example, borrowed concepts from several other areas to find better ways of detecting credit card fraud. The requirements of their system were simply that it should identify fraud accurately, quickly, and that it should not classify a genuine

transaction as fraud. To date, numerous efforts have been made with an obvious pattern of the systems progressive evolvements by absorbing new algorithms and generating refined prototypes. They began with neutral and Bayesian networks, the two most traditional methods, before borrowing the concept of the support vector machine (considered one of the best classifier algorithms) from statistical learning theory to improve efficiency and accuracy. Inspired by the emergence of data mining technology, they then incorporated new algorithms, including decision trees, fuzzy logic networks and hidden Markov models, before finally drawing on biological systems and incorporating artificial immune systems and genetic algorithms. The development of their fraud detection system is just one example of how ISsec design research at the design development phase has evolved steadily.

9.1 DOMINANT TYPE

ISsec design research is dominated by the positivist stance, theories of design and action, the design-science (improvement) paradigm and analysis at the organisational level (Figure 9-1).

Figure 9-1 Dominant Components in ISsec Design Research



9.1.1 Research Paradigm

IS design research and, thus, ISsec design research inherit their essential characteristics from the disciplines of computer science and engineering science from which it emerged. Design is conceptualised as both a process and a product; accordingly, ISsec design research shifts perspective continuously between design processes and designed artefacts for the same complex problem. The relationship between the two is clear: artefacts are built to resolve problems and satisfy identified requirements. The practical outcomes of these artefacts are then used to assess and refine the design process. Thus, ontologically and epistemologically, it falls within the positivist paradigm.

9.1.2 Research Theory

The theories adopted in ISsec design research primarily are those for design and action. This type of theory tackles the issue of how to do something. It is concerned with the principles of form and function, method and justificatory theoretical knowledge that are used in the development of secure information systems. Theories identified within the timeframe of this thesis include information security management models, multiple criteria decision-making models, statistical learning theory and artificial immune systems. Nazareth and Choi (2015), for example, evaluate one information security management model in an attempt to provide guidance to the relevant parties. They drew on multiple areas to adapt the model, which encompassed software vulnerability, risk assessment, attack motivation, threat detection, deterrence and security costing. The model was enhanced with the inclusion of additional constructs and refined through the recalibration of equations to ensure that potentially anomalous situations were prevented. They emphasised creating a quantifiable, more easily verifiable model, and one that was pitched more at the organisational level than at the individual or societal levels.

9.1.3 Research Method

ISsec design research is dominated by the design-science (improvement) paradigm. Rooted in engineering and the science of the artificial, this is fundamentally a problem-solving paradigm that seeks to define the ideas, practices, technical capabilities and products through which the analysis, design, implementation, management and use of

information systems can be accomplished most effectively. This method enables scholars to apply, test, modify and extend existing theories and/or artefacts by drawing on their own experience, creativity, intuition and problem-solving capabilities.

Thus, Nazareth and Choi (2015) used structural validation to assess whether their prototype information security management model reflected accurately the real world. They achieved this using structural verification and extreme condition analysis. Structural verification tested whether the constructs in the model (i.e. attacks, damages, risk, vulnerability and costs) were consistent with the descriptive knowledge of the real-world phenomena being modelled, while extreme condition analysis assessed whether the parameters in the model behaved appropriately under extreme conditions. The behaviour of the model during execution was then assessed, along with the degree of confidence that could be placed in the results.

9.1.4 Research Analysis

Typically, analysis in this track is conducted at the organisational level. Those articles that aimed to identify more accurately security requirements concentrated largely on identifying the security-related requirements associated with specific functions; for example, access control and data filtration. Those focusing on design development, meanwhile, were concerned with how certain types of security systems could be improved and refined. In both cases, the researchers were striving to provide practical suggestions for organisations; the only difference was that the research for the conceptual design phase involved investigation of the organisation, while that

conducted for the design development phase involved investigation on behalf of the organisation.

9.2 EXAMPLE

This section examines one of the articles in the ISsec design research track whose methodological choices are consistent with the dominant type. Consequently, it will provide some insight into how these components are utilised to construct design research.

As highlighted at the beginning of this chapter, Wong et al. (2012) drew on the concept of the artificial immune system for their research into credit card fraud detection with clear structure and in-depth analysis. Despite ongoing efforts to refine fraud detection systems, credit card fraud remains one of the biggest concerns in the development of its service and networks. The detection of online credit card fraud is essentially a classification problem – transactions need to be classified as either legitimate or anomalous. Nevertheless, as scammers employ increasingly sophisticated methods, it is becoming more and more necessary to employ non-traditional mechanisms as a defence. Wong et al.'s adoption of the artificial immune system concept is one such non-traditional tactic.

The artificial immune system has several fundamental characteristics that can be adapted and used as design principles in the ISsec design domain. The authors drew on these characteristics to develop a credit card fraud detection system containing a

transaction processor and a detector generator. A set of real credit card transaction data was then used to test and evaluate the system in numerous computer lab simulations. To facilitate the smooth running of these tests, a test platform was developed that provided automated executions of tests without the need for manual input. The test results strongly supported the effectiveness of the vaccination algorithm augmentation in improving detection performance, with all the test runs that utilised the vaccination algorithm augmentation demonstrating a higher detection rate than those that did not.

In practical terms, the upgraded prototype offered by these authors represents one innovative solution to the security problems faced by financial institutions. In terms of their contribution to the existing research, they introduce a different approach to system development, which they prove empirically to be useful and effective.

9.3 Assessment

ISsec design research has helped improve security systems so that they can better meet organisational requirements in terms of detecting, preventing and mitigating potential risks. It has achieved this goal in two main ways: by obtaining more detailed, specific and accurate user requirements from focal organisations, and by developing more robust, efficient and effective systems. In this way, it has successfully refined outdated and low-efficiency systems through the discrete but integrated processes of conceptual design and design development. One of the most important contributions is to transform scientific and theoretic outcomes into artefacts with practical value.

However, there are ways in which the ISsec design research track itself might be further refined. As far as the philosophical paradigm is concerned; for example, while the positivist stance is clearly the best suited to the process of system development, it might be argued that user requirements would be better understood if other perspectives were enabled. User requirements are influenced by a wide range of human, cultural and societal factors, and there is a danger that not acknowledging the subjective nature of these requirements may jeopardise their completeness and accuracy.

In terms of the theory adopted, most research has limited itself to employing theory for design and action. In its concentration on system development, it has ignored the fact that user requirements need to be identified systematically and accurately, instead identifying them in a very atheoretical manner. Thus, doubts arise regarding the rigorousness of these requirements.

Although the choice of the design-science paradigm is highly consistent with the other dominant methodological components in this track, the lack of reliable methods in the conceptual design and verification stage means ISsec design research is not as informative as it should be. Similarly, its concentration on organisational-level analysis means that the findings are too narrow to provide real support to focal organisations. They ignore end-users, who, as the presumed weakest link in the IS, are more likely to be vulnerable to attack, and fail to examine the motivations of the attackers themselves. In any case, the adoption of concepts from other disciplines necessitates the expansion of the research analysis in this track to multiple levels. For example, the introduction of

biological mechanisms means that studies must address issues (e.g., human behaviours, especially attackers' intentions) at the individual level.

9.4 VARIANCE

The following sections suggest measures that might be employed to address the limitations discussed above.

9.4.1 Research Paradigm

The interpretive or critical perspective could be incorporated into research at the conceptual design phase. The major task in this phase is comprehensively to identify and understand users' needs and requirements. This involves the researcher applying their own subjective understanding (and by extension their own experience and beliefs) to the socially constructed situation in the focal corporation. The application of the interpretive paradigm may help them gain a more in-depth understanding of this situation (highlighted in Table 9-1).

9.4.2 Research Theory

It is recommended that the atheoretical nature of the conceptual design phase be changed and that researchers employ theory for analysing, theory for explaining, theory for predicting or theory for explaining and predicting to determine and understand users' requirements (highlighted in Table 9-1). Analysis theory addresses "what is" questions, while theory for explaining addresses "how" and "why", theory for predicting deals

with "what will be" and theory for explaining and predicting addresses "how", "why" and "what will be." Each provides a window for understanding a specific aspect of users' requirements. For instance, scholars are interested in how best to obtain useful and accurate requirements and why certain requirements are crucial for users. By drawing on the relevant theories, these questions can be answered more accurately; thereby assisting the next stage of the design process.

9.4.3 Research Method

As with the research paradigm and theory, expanding the range of methods employed will increase the likelihood that users' requirements will be correctly identified and verified. The explanation/behavioural paradigm could be incorporated into the research design for both phases; at the conceptual design phase, a survey or questionnaire could be distributed to users for them to indicate their requests and requirements, while a case study or a piece of action research could be conducted as part of the system verification process. The design-science method will undoubtedly continue to play the pivotal role in ISsec design research, but it would benefit further from drawing on other methods (highlighted in Table 9-1).

9.4.4 Research Analysis

I would recommend that the current organisational-level analysis be supplemented with analysis conducted at the individual level. As discussed above, obtaining users' requirements involves the researcher negotiating human issues and behaviours; these

requirements are affected by several internal and external factors that can make them difficult to identify. Individual-level analysis may help researchers better understand and summarise users' key needs. Moreover, the increasingly advanced nature of security fraud necessitates the incorporation of new algorithms, some of which focus on biological and neuroscience issues such as attackers' motivation and behaviours. Analysis at the individual level is also needed to justify the choice of these newly-introduced theories/methods (highlighted in Table 9-1). Similarly, a societal-level analysis is also recommended. The analysis at this level will enable researchers to better collect the requirements that the entire society has laid on secure IS, such as the newly-draft regulations, refined compliance standards (highlighted in Table 9-1).

In conclusion, it is suggested that ISsec design research would benefit and be able to make a greater contribution if the methodological components that currently dominate this track were supplemented with new methodological components list in Table 9-1 at specific points during the research process.

Table 9-1 Recommended Practices for Research Components in ISsec Design Research

Research Component	Current Practice	Recommended Practice
Research Paradigm	Positivist	Positivist
		Interpretive and critical at specific points
Research Theory	Theory for design and action	Theory for design and action,
		Theory for analysing, theory for explaining, theory for predicting, and theory for explaining and predicting can be used at specific points
Research Method	Design method	Design method
		Explanation method can be used at specific points
Research Analysis	Organisational level	Organisational level
		Individual level
		Societal level

Chapter 10 POTENCY OF ISSEC RESEARCH

Traditionally, technical methods have received the most attention from information security professionals as the primary means of preventing breaches. However, over-reliance on technical solutions and authoritarian mandates leads to security practices that users find ultimately ineffectual because they are unable to solve the underlying causes of the problems. Worse yet, authoritarian approaches, if too strict, can be counterproductive and increase, rather than reduce, insider-related problems (D'Arcy et al., 2014). Finding alternative solutions means developing a thorough understanding of information security issues. This requires researchers and practitioners to take a holistic view, drawing on non-technological perspectives where necessary. Against this backdrop, ISsec research has emerged as a key track within the IS discipline.

10.1 INFLUENCES OF ISSEC RESEARCH

Much research has been conducted already into security issues in IS, but this research is viewed typically as piecemeal, fragmented and unsystematic, as discussed previously (Siponen et al., 2008). This can be attributed to several factors. First, ISsec is relatively new compared with other tracks in IS, having only emerged when academics realised that security technology will work only if users deploy its features correctly (Anderson, 2001). Security issues were thus first investigated within the realm of Management Science, with concepts and theories being borrowed from other disciplines to examine

these issues from non-technical perspectives. The field has also been relatively slow to develop; it has been observed that research in ISsec lags the general advances in IS (Siponen et al., 2008) and that it has not reached the same level of maturity as research in IS and other scientific disciplines (Chen & Hirschheim, 2004). However, this is understandable, given the underdevelopment of security methodologies (Siponen, 2005). More importantly, there has been no empirical exploration of research patterns and practice within the discipline, until now. Without such a survey, it is impossible to understand, much less evaluate, current developments and trends within ISsec research.

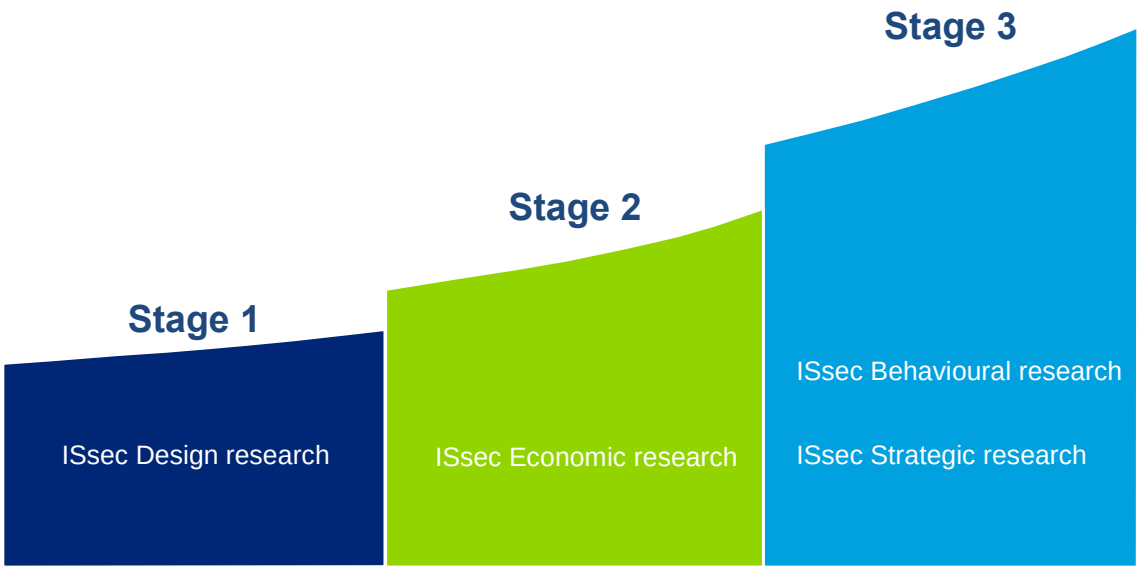
The review conducted here shows that the development of ISsec research has been more resilient and rational than previously thought, despite its methodological deficiencies. The overarching pattern of research within the discipline is best characterised as a knowledge chain, along which researchers inch progressively towards their target – developing safe and convenient IS. The chain begins with ISsec design and the question of how to fashion reliable and robust systems (either by obtaining more specific users' requirements or building up more effective systems). This track lies conceptually at the bottom of the entire ISsec structure and serves as the bedrock on which further ISsec research becomes possible.

On the platform of tangible systems, another type of mechanism (economic motivation) comes into the research spotlight in ISsec economic research (the technical mechanism is covered in ISsec design research). This track explores the motivations behind and effects of ISsec technology and investment in tandem, linking the domains of

technology and management and shifting the emphasis from the security weaknesses within techniques and systems to the incentives that motivate users to select, implement and utilise security protocols.

In the third stage, having examined systems and motivations, the research focus moves to the actors who play the game of security – the end-users and firms. These are the concerns of ISsec behavioural research and ISsec strategic research respectively. ISsec behavioural research explores how end-users receive, understand and respond to security-related incentives, while ISsec strategic research focuses on how firms initiate, devise and transmit these incentives. Together, the two tracks seek to uncover the nature and appeals of the actors involved in this process. Simultaneously, they are passing back the key attributes of the actors to ISsec economic researchers and ISsec design researchers so that they might refine incentives and systems, and testing and evaluating the improvement measures that aggregate from the two prior phases (Figure 10-1).

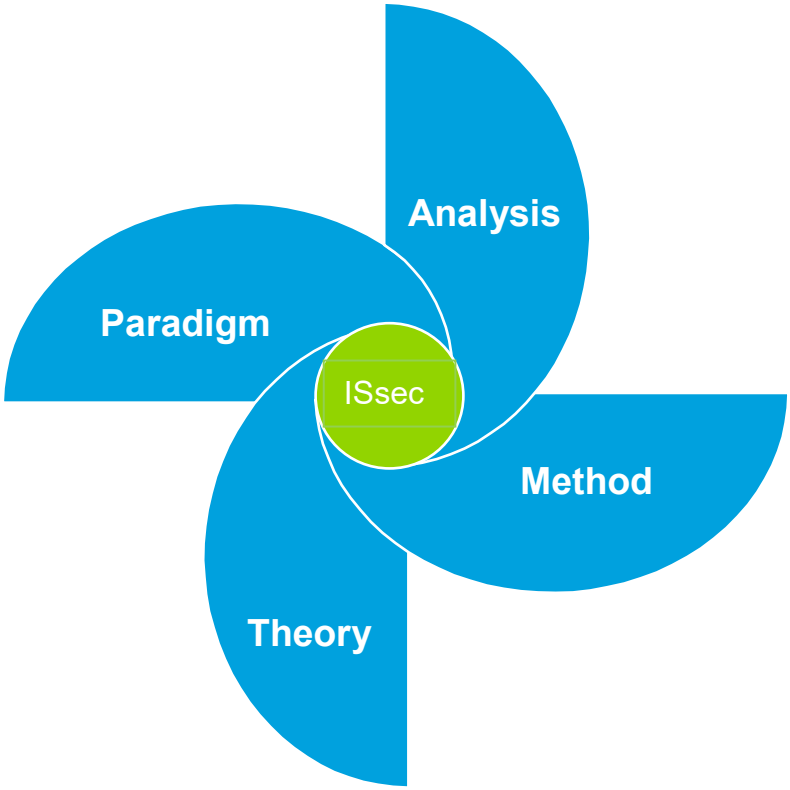
Figure 10-1 Development of Research Tracks in ISsec Research Pattern



With regard to research practice, the literature survey confirms that ISsec research has been conducted in a methodologically-consistent manner, widely adopting the same four research components as general IS research.

Paradigmatically, ISsec research has either adopted a positivist perspective (to investigate the objective, fixed, causal relationships between focal phenomena and their antecedents), or an interpretive or critical perspective (to investigate the subjective, flexible, affecting relationship). This diversity of approach has both been fuelled by and encouraged the introduction of a similarly diverse theoretical range. Researchers employ analysis theory to describe the nature of focal objects, explanation theory to elucidate causal relationships, prediction theory to understand the consequences of actions, and design and action theory to improve systems. Moreover, paradigmatic diversity has been facilitated by and contributed to the development of a range of research methods, whether explanation/behavioural or design-oriented, quantitative or qualitative. Furthermore, it has enabled analysis to be conducted across three levels – individual, organisational and societal. In short, ISsec research has been institutionalised through the four research components, which ensure its continuity (Figure 10-2).

Figure 10-2 Connections of ISsec Research Practices



10.2 Relationships Among Tracks in ISsec Research

Apart from the logic connections between these tracks, how are they related in terms of content and structure? The pattern identified above indicates that the emphasis in current ISsec research is mainly on economic drivers, human behaviours, managerial strategies and system design. Thus, ISsec economic research seeks to identify the optimum level of security investment and the economic factors that drive security concerns, while ISsec behavioural research deals with the human perceptions, beliefs, motivations and behaviours that affect and/or are affected by security issues. ISsec strategic research investigates the managerial dimension of information security, and ISsec design research addresses the question of how best to design more secure systems. Collectively, these four research tracks expand current understanding of information

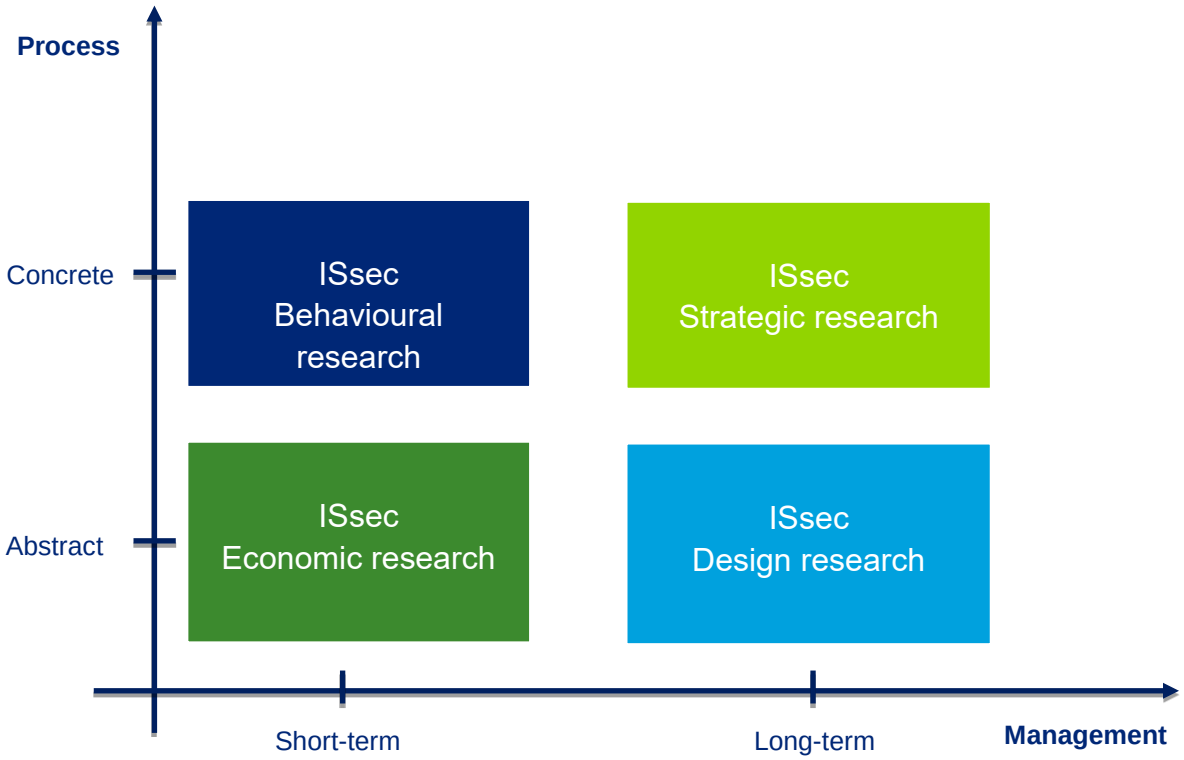
systems security phenomena beyond the technical bedrock by illustrating the importance of economic considerations, behavioural influences, strategic outcomes and design targets.

From a process perspective, ISsec design research and ISsec economic research are related to abstract processes, while ISsec behavioural research and ISsec strategic research address more concrete processes. The first two are essentially abstract in nature as they mainly discuss security phenomena and solutions in an ideal rather than real-life context; ISsec design research aims at laying down a rigid and reliable prototype for building robust security systems, while ISsec economic research seeks to provide a process for calculating the optimum investment needed to realise security goals.ISsec behavioural research and ISsec strategic research, on the other hand, focus on the security issues that arise in real-life settings; ISsec behavioural research demonstrates the concrete process through which security goals are affected by a wide range of behavioural attributes, while ISsec strategic research institutionalises the process through which organisational security goals are achieved.

With regard to their managerial perspective, ISsec economic research and ISsec behavioural research focus on relatively short-term management issues, while ISsec design research and ISsec strategic research are concerned with the longer-term. Specifically, the purpose of ISsec economic research is generally to guide an imminent security-related investment or decision; likewise, ISsec behavioural research examines behavioural attributes with a view to understanding what immediate impact they have

(in terms of benefit or cost) on security. ISsec design research and ISsec strategic research, in contrast, focus on longer-term security measures. ISsec design research aims to build reliable and robust systems that can withstand repeated security attacks and tolerate multiple breaches over a given time frame. Similarly, ISsec strategic research aims to produce a set of policies and regulations that will help companies manage their security performance over a prolonged period. In brief, short-term managerial-oriented research (ISsec economic and ISsec behavioural research) strives to mitigate the most pressing security threats and problems. Conversely, long-term research (ISsec design and ISsec strategic research) aims to improve current and future security systems and policies, either via a top-to-bottom or bottom-to-top managerial route (Figure 10-3).

Figure 10-3 Positioning of Four ISsec Research Tracks



Collectively, by approaching information systems security issues from different perspectives and with diverse focuses, these four research tracks can examine security phenomena in a coherent and holistic manner. Beginning with abstract theoretical and practical research architectures, attention is drawn to the concrete factors and processes influencing security before proceeding to examine the short-term impact of economic and behavioural factors. Finally, they consider structural and strategic factors to suggest long-term security-improvement targets. Therefore, the four tracks are closely interconnected and mutually informative. Jointly, they describe the entire security research process, from abstract level to concrete level, clearly and specifically. Moreover, they offer a coherent picture of the overall security management process from immediate concerns to future challenges. Consequently, they weave a complete research roadmap that offers numerous promising research areas.

However, research in this area has been limited in terms of its methodological choices. Typically, it follows IS research in adopting the four components of research paradigm, research theory, research method and research analysis. While there is no single overarching methodological underpinning, it exhibits a largely uniform approach to these four components. This study draws on the reticulated model of science and MT to offer numerous suggestions for improvement. All four research tracks are advised to become more diverse and inclusive by expanding current practice to include the three main research paradigms, four research theories, a wider range of research methods and three levels of research analysis (Table 10-1).

It might be argued that expanding the range of research components in each track may invalidate the research pattern identified here; in other words, the current differentiation of ISsec research into four clusters may no longer work if all four tracks adopt a similar combination of research components (especially in the case of ISsec economic research, ISsec behavioural research and ISsec strategic research). However, the researcher would counter this by arguing that in each track, the pattern of methodological components has its origins in the ultimate purpose of the track; it is determined by the nature of the track rather than the researcher's preferences. Since there are fundamental differences between the tracks, these methodological patterns will never disappear (though they are likely to be less obvious than they are now) even if researchers employ a wider range of research tools.

Table 10-1 Summary of Recommended Practices for Research Components in ISsec Research

Research Component	Recommended Practice	Research Track(s) Applied
Research Paradigm	Positivist	ISsec Design
	Interpretive	ISsec Economic, ISsec Behavioural, and ISsec Stragetic
	Critical	
Research Theory	Theory for analysing	ISsec Economic, ISsec Behavioural, and ISsec Stragetic
	Theory for explaining	
	Theory for predicting	
	Theory for explaining and predicting	
	Theory for design and action	ISsec Design
Research Method	Explanation/Behavioural method (Both qualitative and quantitative approaches)	ISsec Economic, ISsec Behavioural, and ISsec Stragetic
	Improvement method	ISsec Design
Research Analysis	Individual level	ISsec economic, ISsec behavioural, ISsec stragetic, and ISsec Design
	Organisational level	
	Societal level	

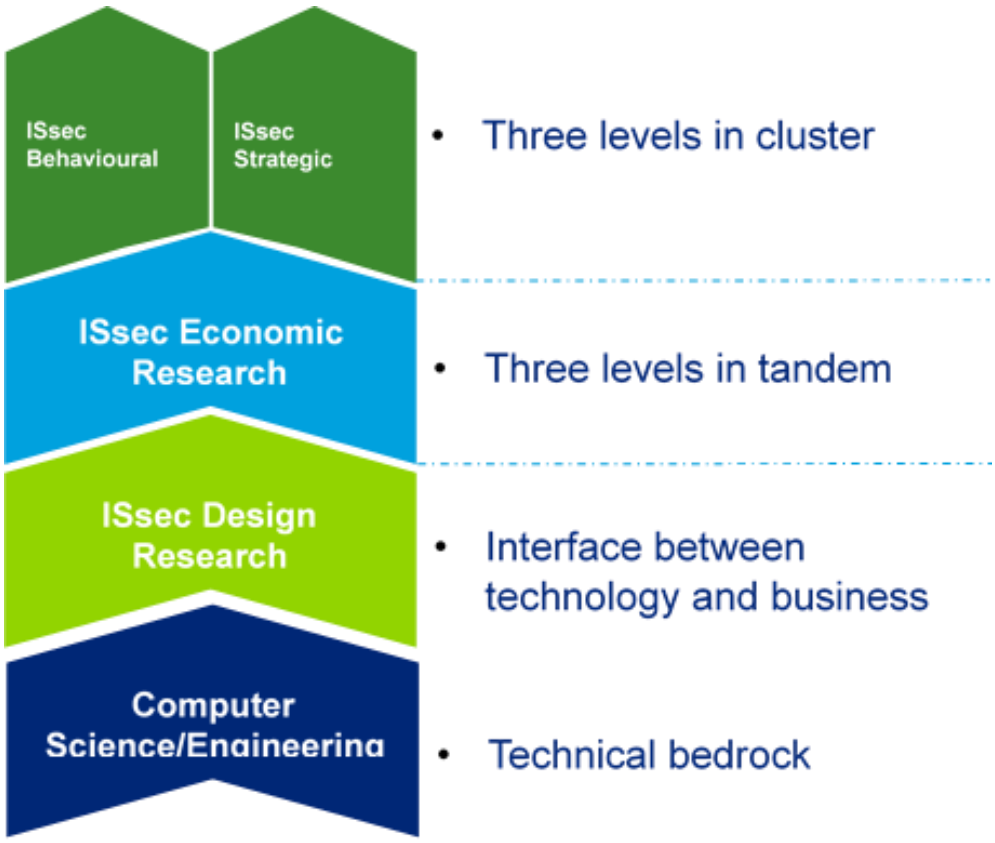
ISsec design research, for example, is fundamentally socio-technical in nature. It paraphrases the technical and abstract descriptions and requirements that come from computer science and engineering into an understandable deliverable that can be

executed within a business setting. Typically regarded as the interface between technology and business, it extends the technical into the business domain with the ultimate target of building a robust, reliable and safe system.

ISsec economic research is concerned essentially with the issue of motivation, whether this is individual motivation, organisational motivation or societal motivation. It draws on economic and/or financial methods to investigate how actors at these three levels respond to security issues, with the ultimate aim of arriving at an optimum situation where individuals, organisation or society reap the maximum possible benefits from security investment. To achieve this, it may investigate the three levels simultaneously. In contrast, ISsec behavioural research takes a sequential approach, establishing the process through which a series of security-related behaviours affect individuals, organisations and society, and vice versa. Its multilevel roadmap starts with individual-level analysis before extending to the organisational and societal levels.

Similarly, ISsec strategic research aims to examine the outcomes of an organisation's response to security phenomena at various focal levels. Its core mission is to discover how sets of security-oriented policies and regulations influence individuals, organisations and society, and vice versa. In this track, the multilevel route generally starts with organisational-level analysis (or very rarely, societal-level) before expanding outwards to the individual and societal levels (Figure 10-4).

Figure 10-4 Progression of Layers for Four ISsec Research Tracks



Far from rendering the four research tracks indistinguishable, diversifying ISsec research methods would encourage more in-depth research in each track; thereby permitting them to be differentiated more clearly. In summary, while the four ISsec research tracks are connected by a common purpose – that is, to illustrate the process by which security concerns arise and are addressed – they are different in terms of their methodological components. These differences would not be obscured by adopting additional components; rather, they would become more obvious.

10.3 THEORISING ISSEC

That ISsec as a field is interested in IS as a subject should be clear. This is recognised widely in the IS community, but even here, the term "information systems security" is sometimes used interchangeably with "information security" and even "computer security". The concept of information security refers to the use of physical and logical data access controls to ensure the proper use of data and to prohibit unauthorised operations on records and files, in addition to loss, damage or misuse of information assets (Peltier, 2005). Conversely, computer security, which is based on mathematical constructions, analyses and proofs, relates to the use of inductive and deductive reasoning to examine the security of devices constructed following the engineering rules from key axioms and to discover underlying principles (Bishop, 2002). Indeed, the concept of ISsec typically is taken for granted and seldom defined or examined explicitly. This is perhaps symptomatic of a general need for the ISsec community to further its engagement with the core concepts that are crucial to itself and its research. Truex et al. (2006) suggest that a primary research goal in any field is theory development, either by building new theory or challenging and refining existing constructs. Meanwhile, Yin (2013) advises that such development can be achieved through analytical generalisation. It is argued that by building up a picture of the ISsec research pattern and practices and acknowledging their strengths and weaknesses, this study consolidates, enriches and furthers the understanding in this field. Furthermore, it offers a opportunity to develop theory by re-examining what ISsec is and what it entails.

The identified pattern of ISsec research comprises four tracks, each of which emphasises a different aspect of ISsec. These conceptualisations overlap or clash depending on the assumptions they make about the nature of ISsec. For example, while ISsec behavioural research and ISsec strategic research both focus on the end-user, ISsec design research places emphasis on the artefacts and structures of ISsec, leaving little room for economic concerns, a central topic in ISsec economic research. The breadth and diversity of current research activities make it especially necessary to scrutinise and critically reflect upon these various conceptualisations of ISsec. Therefore, this is the aim of the following parts.

(1) Design view

The design-oriented view conceptualises ISsec as the outcome of reliable and robust IS, as achieved by understanding, explaining and improving the usage and performance of designed artefacts. These artefacts may include algorithms, human/computer interfaces and system design methodologies or languages (Vaishnavi & Kuechler, 2004).

(2) Economic view

The economic-oriented view conceptualises ISsec as the evaluation of security incentives and investment with a view to minimising both cost and the risk of an attack or breach. This evaluation must be dynamic and encompass all phases of a company's operations (Tsiakis & Stephanides, 2005).

(3) Behavioural view

The behavioural-oriented view conceptualises ISsec as the aftermaths of individual behaviours in a specific context, such as a firm or a service, relating to protecting the assets of the IS. These assets may include computer hardware, networking infrastructure and relevant information (Crossler et al., 2013).

(4) Strategic view

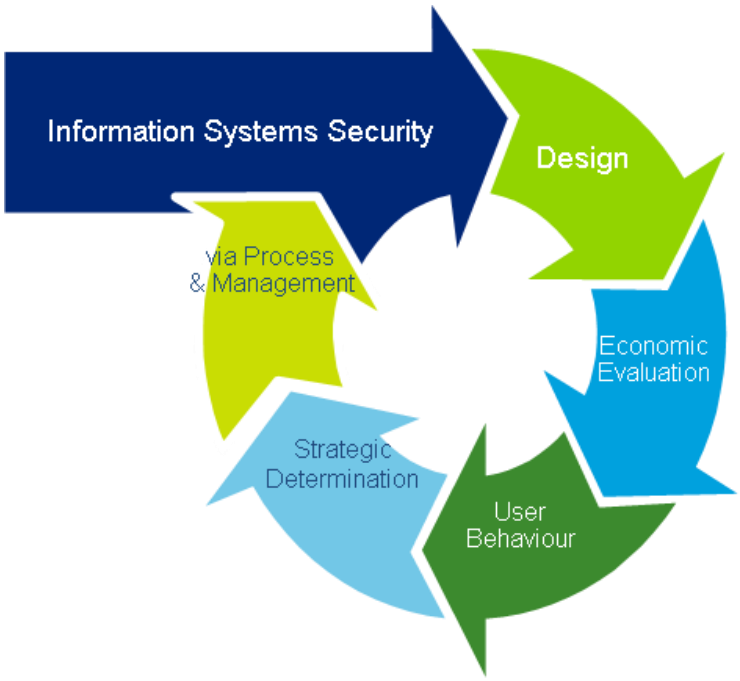
Finally, the strategy-oriented view conceptualises ISsec as the determination of plans and policies to protect IS assets (specifically, what assets must be protected and the degree of protection to be provided for them). These plans and policies must address the different aspects of IS in a balanced and integrated manner (Dutta & McCrohan, 2002).

These views variously provide deeper insight into the role of design, user, evaluation and determination supported and enabled while complicated and diversified by IS regarding security phenomenon. It has been argued that these four views are related in two dimensions – process and management. Looking at these dimensions enables IS community to understand how different conceptualisations of ISsec are interconnected. The process dimension emphasises the activities performed within and supported by research tracks (Alter, 2008); specifically, the processing of data into information and the disseminating and delivering of information (Turban & Volonino, 2010). The management dimension, meanwhile, is continuously changing and adapting, with

systems, staff, regulations and goals in a constant state of flux (Pettigrew, 1999). This emphasises the ongoing change from short-term to long-term, and highlights the relevance of the context in which the focal subjects operate.

The above discussion further confirms the interrelationships between the four research tracks. Similarly, the two dimensions of ISsec are mutually dependent. The rationality of these views and dimensions indicates that these conceptualisations do not exist in isolation, but rather through their mutual interaction. This perspective allows academia to treat ISsec as a polymorphic because all its aspects are so intertwined that they have to be understood as a whole. To this end, ISsec is viewed as a desired and stable status of IS that is an entanglement of design, economic evaluation, user behaviour and strategic determination, whereby all tracks are in a continuous process and through a constant management of interdependency (Figure 10-5).

Figure 10-5 Conceptualisation of ISsec



In summary, based on the pattern and practices identified from the literature survey, and drawing on the potency of ISsec that was figured out, it is understandable that the concept of ISsec has been defined by disentangling the research activities, and entangling the research aspects and dimensions.

SECTION V CONCLUSION

This section begins by reviewing briefly the research process and discussing the contributions made by the study. It then considers the theoretical, methodological and practical implications of the findings and the limitations of the study before offering some suggestions for future research.

The object of this section is to provide a concise concluding discussion of and reflection upon the whole research to better understand its nature and provide the foundation for future endeavours in this area.

Chapter 11 SUMMARY

Information systems (IS) are implemented within an organisation for the purpose of improving its effectiveness and efficiency. As modern business environments have become more dynamic and competitive, these systems have become increasingly important, but their security is under mounting attack. In the battle to ensure systems remain safe and reliable, researchers and practitioners have proposed a range of technical solutions and security initiatives, but it is the search for technical solutions that has dominated the thinking of many in the ISsec field. Dhillon and Backhouse (2001) criticised this trend, stressing instead the importance of the socio-organisational perspective in ISsec research. Indeed, since then, more researchers have sought to examine security issues from non-engineering/technical perspectives. This has helped develop the discipline to some degree, but it remains generally regarded as lagging the general advances in IS, and its findings are regarded as patchy and inconclusive.

In response to these concerns, several scholars have attempted to map current ISsec research in the hope of making it easier to undertake, understand and evaluate research endeavours in this field. These efforts have some significant shortcomings. Some of this research was conducted when the IS discipline was still in its early stages and did not follow the widely-accepted research rules, while later research was rooted either in less well-known paradigms or ignored crucial methodological concerns. Considering these obvious deficiencies, the researcher felt it was time to launch a more inclusive

and comprehensive study into ISsec research; one that would encompass recent research practices, reflect current research trends and promote future research efforts.

Initially, an eight-year time frame was employed, from 2008, when the last similar research was undertaken, to 2015. This yielded a comparatively large sample pool. The research was built on two main theories: the reticulated model of science and MT. The former facilitated the literature survey through which the preliminary data was collected, and the latter facilitated the discussion and analysis of this data. Drawing on both theories, a framework was constructed for examining the retrieved articles. The framework encompassed the four key research components – research paradigm, research theory, research method and research analysis. The last component has always been neglected in this type of research; as far as it is concerned, this is the first time that research analysis has been incorporated into such a review. In total, 108 pieces of research were selected from 12 of the most authoritative and popular journals in the IS community. These research articles were analysed using the examining framework and the results used to identify the current pattern of ISsec research. Four research tracks were identified within the discipline based on how they used the research components. These tracks were labelled ISsec economic research, ISsec behavioural research, ISsec strategic research and ISsec design research.

The findings reveal that ISsec economic research is rooted typically in the positivist paradigm, explaining and predicting theory, explanation/behavioural methods and organisational-level analysis; ISsec behavioural research tends to employ the

interpretive paradigm, explanation theory, explanation/behavioural methods and individual-level analysis; ISsec strategic research mostly employs the interpretive paradigm, analysis theory, explanation/behavioural methods and organisational-level analysis; and ISsec design research adopts the positivist paradigm, design theory, design methods and organisational-level analysis. The analysis process involved exploring each track in detail to identify ways in which the research methodology might be improved. Where there was a possibility of expanding current practice to include a more diverse range of components, this was discussed and recommended.

11.1 CONTRIBUTIONS

The research has generated several contributions; however, listing them does not account sufficiently for their individual and joint strengths. The primary goal for this section is not only to enumerate, but also to position them in the places where the gaps existed to ensure a clearer thread can be followed. In view of this, a reflective and critical narratives are utilised to summarise the contributions that are achieved through this research. The overall contributions can be understood approximately from two dimensions: the tangible dimension, which illustrates externally the direct results coming out from the article, and the intangible dimension, which distinguishes itself internally from other researches.

11.1.1 Tangible Contribution

Content contributions are made to ISsec research by critically engaging with the pattern, practices and potency of ISsec, as evidenced in a wide range of articles drawn from leading IS research publications. These are direct outcomes from the research, which are summarised briefly below.

(1) Pattern

It identifies the pattern of ISsec research as consisting of four research tracks and demonstrates the important contribution made by each track to ISsec research by emphasising specific aspects of the discipline. Research patterns identified by this research relate to the four ISsec research tracks; namely, ISsec economic research, ISsec behavioural research, ISsec strategic research, and ISsec design research. For a long time, ISsec was deemed as the lack of typology in differentiating various research activities within the field given that there is no well-grounded and IS-focused classification system can be applied to a vast number of ISsec literatures. Admittedly, the deficiency in categorisation is understandable considering the nascent nature of ISsec research and its relatively short history in IS domain that becomes an independent subject. However, this situation has significantly prevented the understanding towards and explorations of ISsec research from being elevated to a higher level because the community does not know whether certain work has ever been conducted before, and in what aspect it can be viewed as original and significant. García and Calantone (2001) suggested that it is only possible to advance the knowledge of certain field by

understanding the difference between its numerous research attempts – the typology. To this end, the pattern is overdue and crucial.

Thus, this research has had the embracement of a consistent pattern in ISsec by identifying four distinctive research tracks based on the different combinations of research components. Different from the existing typologies that were either borrowed from the domain of computer science security or generated without giving any specific classifying criteria, this pattern focuses only on the ISsec research articles from leading journal publications with systematic and well-accepted standards (the four research components in ISsec research). Consequently, with the pattern being identified and handy, the scholarly community is able to situate each ISsec research article to the most appropriate research group where its strength(s) and shortcoming(s) can be better recognised and evaluated by the fellow scholars who share the expertise in similar track.

(2) Practice

By examining the research practices within each track, it is able to reveal their merits and weaknesses and to recommend ways of making their methodologies more inclusive. The research practices are clustered surrounding the combinations of research components and their additions to the current routines where necessary. ISsec research has been viewed as fragmented, piecemeal, and unsystematic (Siponen et al., 2008), but the reasons were not stated explicitly by Siponen. The researcher posits that it was largely because the unguided conduct in ISsec research activities, apart from the overlapping or lacking classification system (which has been explained and remedied

in the previous part). Extant researches only revealed some popular or "mainstream" research efforts in carrying out ISsec research without any critiques on the contemplations regarding their underlying assumptions. Hence, the community did not receive any specific reasonable and workable advice on furthering the breadth and/or depth of current research. It led to the situation where a similar set of methodologies has been repeatedly utilised against different phenomena; thus, the results were indeed available but mirroring. For example, an interpretive research by adopting Planned Behaviour Theory and quantitative method has been witnessed in a wide range of subjects when topic of the user acceptance towards a new service or product is concerned; this set of practices can be found in from Internet banking research to mobile banking exploration, from Chinese instance to other countries' cases.

The simple reiteration of well-established research practices on different research themes provided limited competence in driving ISsec further and better. However, the scholars have no better options as the practices were either passed on from other domain in IS instead of within ISsec or not adequately supplemented with reasonably justified conducts that are pertinent to ISsec research. The critical examination of the four research tracks reveals that certain practices dominate within each track, often to the detriment of the width and depth of the research in that track. Current research practice within the tracks cannot therefore be regarded as methodologically sound or comprehensive. This leads the research to recommend that the range of practices employed in each track should be expanded; thus, the introduction of practices in this research is particularly important.

Examining the research practices within each track reveals their strengths and weaknesses, and recommends ways of making their methodologies more inclusive. The research contributed to the existing research routines by commending the new sets of research conducts that can be used in four ISsec tracks. Departing from the heated debate on the socially-constructed understanding (interpretive stance) about Internet banking, mobile banking, or even webchat banking adoption, a socially and historically-enabled explorations (critical stance) regarding these topics can be anticipated at the next stage. This will lead to steady progress towards coherent, systematic, and elevating scholarly activities.

(3) Potency

ISsec has encountered an embarrassing situation as what the researcher has recently: a research manuscript in ISsec can be submitted to IS conference or journal, computer science one, or information technology one; the researcher has been labelled as the technical person in a business school or the business person in an engineering school. The question has been raised frequently by security specialists in both industry and academia: what is the difference between ISsec, information security, and computer science security?

Previous endeavours were in vain, given that the community has not yet possessed the knowledge of ISsec boundary or its veins, and the concept of ISsec cannot be deduced without any feasible grounds. Nevertheless, the absence of its concept has impaired the credibility of ISsec and, thus, prohibited it from being further evolved into a more

mature area. The detrimental aftermaths start to surface: the progress in ISsec has generally lagged overall advance in IS (Siponen et al., 2008), and ISsec has been eliminated from some leading IS conferences, such as ECIS 2016[1] and ECIS 2017[2]. This is both disappointing and frustrating. Baskerville and Myers (2002) suggested that if the discipline becomes mature, it is not only the referring one, but also the reference one, which is able to lend conceptual and theoretical support to other disciplines. However, without even conceptualising its core definition (information systems security), ISsec cannot easily and reasonably becomes academically mature. To this end, it is time to conceptualise ISsec within IS domain.

As the pattern (typology of ISsec) is identified, which is able to boundary the scope of ISsec research, and the practices being proposed, which illustrates the veins that are currently engaged, all required information is sufficiently collected. Therefore, this research contributed to academia by identifying the potency of ISsec research by specifying its relations and conceptions evoked by the pattern and practices. The research also engages with the practical and conceptual foundation for understanding ISsec. Rather than seeing each track of ISsec research as a discrete stream existing in isolation, it suggests that they build on each other as they move from technology to socio-technology, and that they are further interconnected by the two dimensions of process and management. The potency of the discipline resides in its steady

[1] Please see the track information at http://www.ecis2016.com/RESEARCH-PAPERS.html
[2] Please see the track information at http://www.ecis2017.eu/tracks/

development and the close connections that consolidate and augment its pattern and practices.

The research presents conceptualisations of the four dimensions of ISsec (design, behaviour, economy and strategy), demonstrating that these are all related in nature. Moreover, they are connected on the course of entanglement where they are engaged in a constant process of adapting to the changing management. Thus, it can contribute to the theorisation of ISsec by proposing that ISsec can be conceived as a desired and stable IS status, which is polymorphic in nature.

It is believed that the conceptualisation of ISsec not only reveals the inherent connection between IS and ISsec, but also distinguishes ISsec from other long-time interchangeably used concepts; for example, information security and computer science security. More importantly, with its four underpinnings being identified (economic view, behavioural view, strategic view, and design view), the community has been provided with the expertise as well as toolkits to examine ISsec phenomena adequately.

11.1.2 Intangible Contribution

The intangible contributions of this research are threefold, as the findings may be of use to both academic scholars and industrial practitioners. Specifically, the contributions are mainly surrounding theoretical, practical, and methodological aspects, which will be discussed in detail below.

(1) Theoretical Contribution

Theoretically, to the best of the researcher's knowledge, the study is the first to map out the pattern of ISsec research from the methodological perspective; thereby helping scholars to better understand and evaluate ISsec research. The discipline has long lacked a well-grounded classification system, partly because IS scholars typically regard ISsec as a technical endeavour that belongs in the disciplines of computer science and engineering; and partly because, being newer and less popular than other areas of IS research, it has lagged behind in terms of overall progress. Most importantly, most previous studies have employed too small a sample pool and generated too little data for the researcher concerned to develop such a classification system.

The need for a classification system in ISsec has been increasing. Scholars are looking for such a system as without it, they cannot define the current scope of ISsec research and establish a consensus on what has been done and what has not. This is the reason current ISsec research is viewed generally as piecemeal and fragmented. Furthermore, without a classification system, it is very difficult, if not impossible, to evaluate the research that has been done. Scholars have no systematic framework for comparing studies, even those studies that discuss the same topic, because they have no criteria for judging their points of difference or similarity. By setting out the pattern of ISsec research, this study goes some way towards elucidating the connections and differences between studies and addressing these concerns. The nature of each track is delineated by referring to the combination of methodological components that dominate within

that track (the premise being that a certain combination of components generates a certain type of research). The resulting pattern will help scholars assess the scope and depth of current studies, and see how methodology might be improved. Meanwhile, the theorisation of ISsec will help scholars apprehend its concentrations and define its scope, which is different from that of information security and/or computer security.

Previous attempts to classify ISsec research have taken the research topic as the main or sole indicator. This approach has obvious shortcomings, however; namely, it is extremely difficult to list all available topics. Moreover, a long list is likely to contain overlapping or conflicting topics, making it unreliable. Where researchers have focused on research components, they have considered only selected components, resulting in datasets that are incomplete and, therefore, incapable of producing accurate classification systems. Conversely, this research has not only approached the literature review from the methodological perspective, but also considered all the key methodological components. Research paradigm, research theory, research method and research analysis are all considered on the assumption that, as ISsec research follows IS research practices, the choice of components can bespeak the underlying relations and rations. The follow-up empirical efforts confirmed that this approach is not only workable and useful, but also that consideration of all four methodological components is indispensable if the aim is to classify or uncover the connections between research streams.

(2) Practical Contribution

Practically, the study has ramifications for both academic and industrial practitioners. Academic practitioners may find it a useful guide because it enables them to locate their own work within the identified research pattern and offers recommendations for how they might expand their choice of methodological components. It makes it relatively easy for them to see which areas have not been covered properly, or which research paradigm or research theory has been under-utilised; thus helping them judge how they can best contribute to the discipline. Moreover, it makes it easier for scholars to evaluate existing ISsec research as it gives them a systematic framework that facilitates reliable comparison and assessment.

This research may also benefit industrial practitioners. The identification of four ISsec research tracks allows practitioners to situate themselves in different scenarios and understand how to respond to their own security needs in the context of level analysis. The introduction of MT suggests to which level (individual, organisational or societal) the research (in other words, security issues/questions) is applied. Thus, if their concerns are mainly around firms, they may need to seek help from ISsec economic or strategic research, as these two explore security issues at the organisational level. Alternatively, if their focus is on employees or customers, they will find it most useful to refer to ISsec behavioural research.

(3) Methodological Contribution

Speaking from a methodological perspective, the research has also made concrete contributions to the academia. The research stresses implicitly the importance of the alignment of four research components as a whole to ensure the ISsec research being undertaken methodologically consistent and sound. Furthermore, it eliminates the invisible bond on the set of methodologies that can be applied to ISsec research activities by expanding the ranges of practices.

More importantly, the research borrowed a concept from the discipline of Management Science, where MT emerged and has been continuously developed. The introduction of MT can clear up the cross-level error (Rousseau and Thomashunt, 1995), referring to a type of ungrounded research where the data was collected at one level while the analysis was conducted at different level. Once MT has been specified, the scholars in ISsec may use the concept to re-frame their methods by maintaining the coherent and consistent level throughout the entire research. In addition, some underexplored level in ISsec, such as societal level, has been identified and further facilitated with recommended practices in certain track. Consequently, the ISsec community can push ahead with new methods to conduct research in some less-examined areas.

In conclusion, this research has contributed to the scholarly community in several perspectives from dual dimensions. Motivated by the complicated but confusing status of current ISsec research, the researcher intended to create a set of organised, structured, and explicit descriptions. The identification of pattern, practice, and potency serves the

goal sufficiently. Moreover, it sheds light on the theoretical, practical, and methodological aspects by initiating a broader discussion where the three tangible contributions are closely connected with their intangible counterparts.

11.2 LIMITATIONS

The research is not without limitations. These lie primarily in the classification of methodological components and the data sample. Specifically, the sources from which the data was collected and the process by which it was obtained –. The data was drawn from 12 of the top journals in the field of IS. However, while these journals are widely accepted and utilised by scholars in the discipline, they are not necessarily the most popular outlets for publishing ISsec research. It became apparent during the review process that several of the selected journals published very few ISsec-related articles during the eight-year time frame of the study; indeed, one had published only a single manuscript. This is due in part to the preference of some journals for research topics in other more popular and prolific fields; ISsec is only one small faction within numerous mature and well-developed IS sub-fields. The possibility also exists that some ISsec articles may go to other journals which are not on this list but which are influential within the ISsec community. These articles may also appear in some niche journals in other fields, such as cyber-security or Internet security. Furthermore, all journals are in English, suggesting that only English-written research in ISsec were obtained for the literature survey in the thesis. More research regarding ISsec should be conducted in other languages, such as Chinese, German.

The process of screening for relevant articles relied mainly on keyword selection, applied to titles, keywords and abstracts. This was then supplemented with cross-check and inter-criteria with the full texts to ensure accuracy. This process minimised the number of false positive errors as the irrelevant articles were all excluded, but may have increased the number of false negative errors during the keyword selection stage (there is a small chance that an article may have escaped detection because the keyword "security" appears only in its full text). Due to these two issues, just 108 articles were selected. Although this is sufficient to allow a rigorous literature survey, a larger sample would have been preferable.

The second limitation relates to the classification of methodological components. The development of the examining framework meant that a typology had to be established for each of the four components. This was relatively straightforward in the case of the research paradigm component, but the classification of the other three components; namely, research theory, research method and research analysis, is a more contentious issue. Care was taken to choose the most widely-accepted typologies after rounds of comparison and discussion, but it is admitted that the most widely-accepted options were not necessarily the most suitable for this research. Moreover, it is possible that some other classification system might have served it better. For example, the typology of research theory that was adopted is based on functionality (e.g., analysing, explaining predicting), but it could also have been based on focal level or origin. The findings might have differed significantly if other classification systems had been used. Although attempting to ensure the consistency and appropriateness of all classifications

employed across the research, and that they accorded with the methodological perspective, the researcher must accept the possibility that the classification could have been better.

11.3 Future Studies

The limitations discussed above, and the potential offered by the findings, suggest several possibilities in terms of future research. Firstly, the data sample could be enlarged by either extending the literature survey time window or expanding the sample pool; to start, simply extending the time window to cover the latest available year (2016) should increase the data entry. Alternatively, the sample could be supplemented by including more journals (especially those reflecting local ISsec efforts in areas such as the Great China Region, eastern Asia and Oceania) and high-quality papers delivered at prestigious academic conferences such as the International Conference on Information Systems (ICIS). Additionally, if the situation permits, other leading journals or conferences in other languages will also be considered and included to enlarge the database.

There is also scope for choosing other classification systems for some of the methodological components, possibly with the help of MT. To recapitulate, the overall logic is that individuals are nested in work groups, which in turn are nested in larger organisational units, such as sections, departments or divisions, which are nested in national or multinational organisations. These organisations are themselves nested in

overall performance environments, which in turn are nested in the societal setting. The precise number and nature of layers are likely to vary from one investigation to another (for the sake of simplicity, three typical layers are chosen in this research). The nesting arrangement has certain implications for ISsec researchers, whereby they are obliged to give careful thought to the levels of theory, measurement and analysis they will employ for the constructs included in their investigation. The level of theory refers to the focal level to which generalisations are meant to apply, the level of measurement refers to the unit to which data is directly collected, and the level of analysis is the unit where the data is assigned for discussion. Critically, these three facets must be aligned to minimise level-related confounds, or what are often referred to as "fallacies of the wrong level". It may be possible to apply MT to the theory, method and analysis components, though the relevance of the theory to IS (where it remains nascent) requires further verification. Nevertheless, it provides an alternative angle from which research questions can be examined.

Currently, it is rare for research to be multilevel; almost all research in ISsec is mono-level-based, with data collection and analysis being conducted at the same level. While it is recommended that ISsec research be conducted at more levels (e.g., more research is advocated at the organisational and societal levels in the ISsec behavioural track, and at the individual and societal levels in the ISsec strategic track), there lies another possibility that a single research can be and is favoured to be multilevel based. To this end, the recommendations for future research should be discussed further to incorporate this trend in multilevel research.

To conclude, despite its limitations, this study has ramifications for ISsec research in terms of its practice, method and usefulness. To ease the concerns over some main limitations, further tasks are expected in the following-up explorations, which may contribute more to the ISsec community.

APPENDIX: RETRIEVED ARTICLES FROM JOURNALS

#	Title	Author(s)	Journal	Year
1	Conceptualising improvisation in information systems security	Kennedy Njenga and Irwin Brown	EJIS	2012
2	Frame misalignment: interpreting the implementation of information systems security certification in an organisation	Carol W. Hsu	EJIS	2009
3	If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security	Scott R. Boss, Laurie J. Kirsch, Ingo Angermeier, Raymond A. Shingler and R. Wayne Boss	EJIS	2009
4	Managing the introduction of information security awareness programmes in organisations	Aggeliki Tsohou, Maria Karyda, Spyros Kokolakis and Evangelos Kiountouzis	EJIS	2013
5	Protection motivation and deterrence: a framework for security policy compliance in organisations	Tejaswini Herath and H. Raghav Rao	EJIS	2009

6	Secure activity resource coordination: empirical evidence of enhanced security awareness in designing secure business processes	Fergle D'Aubeterre, Rahul Singh and Lakshmi Iyer	EJIS	2008
7	What levels of moral reasoning and values explain adherence to information security rules? An empirical study	Liisa Myyry, Mikko Siponen, Seppo Pahnila, Tero Vartiainen and Anthony Vance	EJIS	2009
8	User behaviour towards protective information technologies: the role of national cultural differences	Tamara Dinev, Jahyun Goo, Qing Hu amd Kichan Nam	ISJ	2009
9	Security services as coping mechanisms: an investigation into user intention to adopt an email authentication service	Tejaswini Herath, Rui Chen, Jingguo Wang, Ketan Banjara, Jeff Wilbur and H. Raghav Rao	ISJ	2014
10	Blissfully ignorant: the effects of general privacy concerns, general institutional trust, and affect in the privacy calculus	Flavius Kehr, Tobias Kowatsch, Daniel Wentzel and Elgar Fleisch	ISJ	2015
11	Exploring the effects of organisational justice, personal ethics and sanction on Internet use policy compliance	Han Li, Rathindra Sarathy, Jie Zhang and Xin Luo	ISJ	2014
12	Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies	Paul Benjamin Lowry and Gregory D. Moody	ISJ	2014

13	Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust	Paul Benjamin Lowry, Clay Posey, Rebecca (Becky) J. Bennett and Tom L. Roberts	ISJ	2015
14	Information security policies in the UK healthcare sector: a critical evaluation	Bernd Carsten Stahl, Neil F. Doherty and Mark Shaw	ISJ	2012
15	Artificial immune systems for the detection of credit card fraud: an architecture, prototype and preliminary result	Nicholas Wong, Pradeep Ray, Greg Stephens and Lundy Lewis	ISJ	2012
16	An empirical analysis of software vendors' patch release behaviour: impact of vulnerability disclosure	Ashish Arora, Ramayya Krishnan, Rahul Telang and Yubao Yang	ISR	2010
17	Choice and chance: a conceptual model of paths to information security compromise	Sam Ransbotham and Sabyasachi Mitra	ISR	2009
18	Cloud implications on software network structure and security risks	Terrence August, Marius Florin Niculescu and Hyoduk Shin	ISR	2014
19	Configuration of and interaction between information security technologies: the case of firewalls and intrusion detection systems	Huseyin Cavusoglu, Srinivasan Raghunathan and Hasan Cavusoglu	ISR	2009

20	Contracting information security in the presence of double moral hazard	Chul Ho Lee, Xianjun Geng and Srinivasan Raghunathan	ISR	2013
21	Influence techniques in phishing attacks: an examination of vulnerability and resistance	Ryan T. Wright, Matthew L. Jensen, Jason Bennett Thatcher, Michael Dinger and Kent Marett	ISR	2014
22	Institutional influences on information systems security innovations	Carol Hsu, Jae-Nam Lee and Detmar W. Straub	ISR	2012
23	A value-at-risk approach to information security investment	Jingguo Wang, Aby Chaudhury and H. Raghav Rao	ISR	2008
24	The association between the disclosure and the realisation of information security risk factors	Tawei Wang, Karthik N. Kannan and Jackie Rees Ulmer	ISR	2013
25	The role of extra-role behaviors and social controls in information security policy effectiveness	Jack Shih-Chieh Hsu, Sheng-Pao Shih, Yu Wen Hung and Paul Benjamin Lowry	ISR	2015
26	User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach	John D'Arcy, Anat Hovav and Dennis Galletta	ISR	2009
27	When hackers talk: managing information security under variable attack rates and knowledge dissemination	Vijay Mookerjee, Radha Mookerjee, Alain Bensoussan and Wei T. Yue	ISR	2011

28	The impact of information security events on the stock value of firms: the effect of contingency factors	Ali Alper Yayla and Qing Hu	JIT	2011
29	Decision-theoretic and game-theoretic approaches to IT security investment	Huseyin Cavusoglu, Srinivasan Raghunathan and Wei T. Yue	JMIS	2008
30	Hacker behaviour, network effects, and the security software market	Debabrata Dey, Atanu Lahiri, and Guoying Zhang	JMIS	2012
31	Healthcare security strategies for data protection and regulatory compliance	Juhee Kwon and M. Eric Johnson	JMIS	2013
32	Information security: facilitating user precautions vis-à-vis enforcement against attackers	Ivan P. L. Png and Qiu-Hong Wang	JMIS	2009
33	Information security outsourcing with system interdependency and mandatory security requirement	Kai-Lung Hui, Wendy Hui and Wei T. Yue	JMIS	2012
34	Managing interdependent information security risks: cyberinsurance, managed security services, and risk pooling arrangements	Xia Zhao, Ling Xue and Andrew B. Whinston	JMIS	2013
35	Organisations' information security policy compliance: stick or carrot approach?	Yan Chen, K. Ramamurthy and Kuang-Wei Wen	JMIS	2012

36	Risks and benefits of signaling information system characteristics to strategic attackers	Marco Cremonini and Dmitri Nizovtsev	JMIS	2009
37	The behavioral roots of information systems security: exploring key factors related to unethical IT use	Sutirtha Chatterjee, Suprateek Sarker and Joseph S. Valacich	JMIS	2015
38	The deterrent and displacement effects of information security enforcement: international evidence	Ivan P. L. Png, Chen-Yu Wang and Qiu-Hong Wang	JMIS	2008
39	The influence of experiential and dispositional factors in phishing: an empirical investigation of the deceived	Ryan T. Wright and Kent Marett	JMIS	2010
40	The role of self-control in information security violations: insights from a cognitive neuroscience perspective	Qing Hu, Robert West and Laura Smarandescu	JMIS	2015
41	Understanding employee responses to stressful information security requirements: a coping perspective	John D'Arcy, Tejaswini Herath and Mindy K. Shoss	JMIS	2014
42	Understanding nonmalicious security violations in the workplace: a composite behavior model	Ken H. Guo, Yufei Yuan, Norman P. Archer and Catherine E. Connelly	JMIS	2011
43	Using accountability to reduce access policy violations in information systems	Anthony Vance, Paul Benjamin Lowry and Dennis Eggett	JMIS	2013

44	An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric	Allen C. Johnston, Merrill Warkentin and Mikko Siponen	MISQ	2015
45	Are markets for vulnerabilities effective?	Sam Ransbotham, Sabyaschi Mitra and Jon Ramsey	MISQ	2011
46	Avoidance of information technology threats: a theoretical perspective	Huigang Liang and Yajiong Xue	MISQ	2009
47	Circuits of power: a study of mandated compliance to an information systems security de jure standard in a government organisation	Stephen Smith, Donald Winchester, Deborah Bunker and Rodger Jamieson	MISQ	2010
48	Correlated failures, diversification, and information security risk management	Pei-yu Chen, Gaurav Kataria and Ramayya Krishnan	MISQ	2011
49	Detecting fake websites: the contribution of statistical learning theory	Ahmed Abbasi, Zhu Zhang, David Zimbra, Hsinchun Chen and Jay F. Nunamaker, Jr.	MISQ	2010
50	Differential effects of prior experience on the malware resolution process	Seung Hyun Kim and Byung Cho Kim	MISQ	2014
51	Fear appeals and information security behaviors: an empirical study	Allen C. Johnston and Merrill Warkentin	MISQ	2010

52	Growth and sustainability of managed security services networks: an economic perspective	Alok Gupta and Dmitry Zhdanov	MISQ	2012
53	Improving employees' compliance through information systems security training: an action research study	Petri Puhakainen and Mikko Siponen	MISQ	2010
54	Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness	Burcu Bulgurcu, Hasan Cavusoglu and Izak Benbasat	MISQ	2010
55	Insider threats in a financial institution: analysis of attack-proneness of information systems applications	Jingguo Wang, Manish Gupta and H. Raghav Rao	MISQ	2015
56	Insiders' protection of organisational information assets: development of a systematics-based taxonomy and theory of diversity for protection-motivated behaviors	Clay Posey, Tom L. Roberts, Paul Benjamin Lowry, Rebecca J. Bennett and James F. Courtney	MISQ	2013
57	Market value of voluntary disclosures concerning information security	Lawrence A. Gordon, Martin P. Loeb and Tashfeen Sohail	MISQ	2010
58	Neutralisation: new insights into the problem of employee information systems security policy violations	Mikko Siponen and Anthony Vance	MISQ	2010
59	Practising safe computing: a multimethod empirical examination of home computer user security behavioral intentions	Catherine L. Anderson and Ritu Agarwal	MISQ	2010

60	Proactive versus reactive security investments in the healthcare sector	Juhee Kwon and M. Eric Johnson	MISQ	2014
61	Quality competition and market segmentation in the security software market	Debabrata Dey, Atanu Lahiri and Guoying Zhang	MISQ	2014
62	The impact of malicious agents on the enterprise software industry	Michael R. Galbreth and Mikhael Shor	MISQ	2010
63	User participation in information systems security risk management	Janine L. Spears and Henri Barki	MISQ	2010
64	Financial impact of information security breaches on breached firms and their non-breached competitors	Humayun Zafar, Myung S. Ko and Kweku-Muata Osei-Bryson	IRMJ	2012
65	Governing information security: governance domains and decision rights allocation patterns	Yu (Andy) Wu and Carol Saunders	IRMJ	2011
66	Investigating the impact of publicly announced information security breaches on three performance indicators of the breached firms	Myung Ko, Kweku-Muata Osei-Bryson and Carlos Dorantes	IRMJ	2009
67	A behavioral analysis of passphrase design and effectiveness	Mark Keith, Benjamin Shao and Paul Steinbart	JAIS	2009

68	The order machine – the ontology of information security	Jukka Vuorinen and Pekka Tetri	JAIS	2012
69	Towards a new meta-theory for designing information systems (IS) security training approaches	Mari Karjalainen and Mikko Siponen	JAIS	2011
70	Understanding security behaviors in personal computer usage: a threat avoidance perspective	Huigang Liang and Yajiong Xue	JAIS	2010
71	Using measures of risk perception to predict information security behavior: insights from electroencephalography	Anthony Vance, Bonnie Brinton Anderson, C. Brock Kirwan and David Eargle	JAIS	2014
72	Metrics for characterizing the form of security policies	Sanjay Goel and InduShobha N. Chengalur-Smith	JSIS	2010
73	Value conflicts for information security management	Karin Hedström, Ella Kolkowska, Fredrik Karlsson and J.P. Allen	JSIS	2011
74	An economic mechanism to manage operational security risks for inter-organisational information systems	Fang Fang, Manoj Parameswaran, Xia Zhao and Andrew B. Whinston	ISF	2014
75	Dynamic competition in IT security: a differential games approach	Tridib Bandyopadhyay, Dengpan Liu, Vijay S. Mookerjee and Allen W. Wilhite	ISF	2012

76	Information systems resources and information security	Kuo-chung Chang and Chih-ping Wang	ISF	2011
77	Returns to information security investment: endogenizing the expected loss	Kjell Hausken	ISF	2014
78	Security investment and information sharing under an alternative security breach probability function	Xing Gao, Weijun Zhong and Shue Mei	ISF	2015
79	The impact of information security failure on customer behaviors: a study on a large-scale hacking incident on the Internet	MinJae Lee and JinKyu Lee	ISF	2012
80	A system dynamics model for information security management	Derek L. Nazareth and Jae Choi	I&M	2015
81	Bridging the divide: a qualitative comparison of information security	Clay Posey, Tom L. Roberts, Paul Benjamin Lowry and Ross T. Hightower	I&M	2014
82	Consumer perception of interface quality, security, and loyalty in electronic commerce	Hsin Hsin Chang and Su Wen Chen	I&M	2009
83	Employees' adherence to information security policies: an exploratory field study	Mikko Siponen, M. Adam Mahmoodb and Seppo Pahnila	I&M	2014
84	Estimating the market impact of security breach announcements on firm values	Sanjay Goel and Hany A. Shawky	I&M	2009

85	Incident-centered information security: managing a strategic balance between prevention and response	Richard Baskerville, Paolo Spagnoletti and Jongwoo Kim	I&M	2014
86	Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition	Princely Ifinedo	I&M	2014
87	Institutional pressures in security management: direct and indirect	Huseyin Cavusoglu, Hasan Cavusoglu, Jai-Yeol Son and Izak Benbasat	I&M	2015
88	Learning to cope with information security risks regarding mobile device loss or theft: an empirical examination	Zhiling Tu, Ofir Turel, Yufei Yuan and Norm Archer	I&M	2015
89	Motivating IS security compliance: insights from habit and protection motivation theory	Anthony Vance, Mikko Siponen and Seppo Pahnila	I&M	2012
90	Out of fear or desire? Towards a better understanding of employees' motivation to follow IS security policies	Jai-Yeol Son	I&M	2011
91	The effects of multilevel sanctions on information security violations: a mediating model	Ken H. Guo and Yufei Yuan	I&M	2012
92	Theorizing the concept and role of assurance in information systems security	Janine L. Spears, Henri Barki and Russell R. Barton	I&M	2013
93	A web-based multi-perspective decision support system for information security planning	Omar F. El-Gayar and Brian D. Fritz	DSS	2010

94	Allocation of resources to cyber-security: the effect of misalignment of interest between managers and investors	Bin Srinidhi, Jia Yan and Giri Kumar Tayi	DSS	2015
95	An exploration of risk information search via a search engine: queries and clicks in healthcare and information security	Jingguo Wang, Nan Xiao and H. Raghav Rao	DSS	2012
96	Development and validation of instruments of information security deviant behavior	Amanda M.Y. Chu and Patrick Y.K. Chau	DSS	2014
97	Firms' information security investment decisions: stock market evidence of investors' behavior	Sangmi Chai, Minkyun Kim and H. Raghav Rao	DSS	2011
98	IT security auditing: a performance evaluation decision model	Hemantha S.B. Herath and Tejaswini C. Herath	DSS	2014
99	Knowledge sharing and investment decisions in information security	Dengpan Liu, Yonghua Ji and Vijay Mookerjee	DSS	2011
100	Measuring perceived security in B2C electronic commerce website usage: a respecification and validation	Edward Hartono, Clyde W. Holsapple, Ki-Yoon Kim, Kwan-Sik Na and James T. Simpson	DSS	2014
101	Optimal information security investment in a healthcare information exchange: an economic analysis	C. Derrick Huang, Ravi S. Behara and Jahyun Goo	DSS	2014
102	Profit-maximizing firm investments in customer information security	Yong Jick Lee, Robert J. Kauffman and Ryan Sougstad	DSS	2011

103	Rethinking the role of security in client satisfaction with software-as-a-service (SaaS) providers	Sigi Goode, Chinho Lin, Jacob C. Tsai and James J. Jiang	DSS	2015
104	Security and performance in service-oriented applications: trading off competing objectives	Hangjung Zo, Derek L. Nazareth and Hemant K. Jain	DSS	2010
105	Security versus convenience? An experimental study of user misperceptions of wireless Internet service quality	Byung Cho Kim and Yong Wan Park	DSS	2012
106	Selection of optimal countermeasure portfolio in IT security planning	Tadeusz Sawik	DSS	2013
107	Studying users' computer security behavior: a health belief perspective	Boon-Yuen Ng, Atreyi Kankanhalli and Yunjie (Calvin) Xu	DSS	2009
108	Towards user patterns for online security: observation time and online user identification	Yinghui (Catherine) Yang and Balaji Padmanabhan	DSS	2010

References

Aboutabl, M. S. (2006). *The CyberDefense laboratory: a framework for information security education.* Paper presented at the 2006 IEEE Information Assurance Workshop, West Point, NY, USA.

ACPHIS. (2013). *IS Journal Ranking*. Retrieved March 21, 2015, from http://www.acphis.org.au/index.php/is-journal-ranking/rank-order

Adams, A., & Sasse, M. A. (1999). Users are not the enemy. *Communications of the ACM, 42*(12), 40-46.

Ahmad, A., Maynard, S. B., & Park, S. (2014). Information security strategies: towards an organisational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 357-370.

AIS. (2011). *MIS Journal Rankings*. Retrieved March 21, 2015, from http://aisnet.org/general/custom.asp?page=JournalRankings

Ajzen, I. (1991). The theory of planned behaviour. *Organisational Behaviour and Human Decision Processes, 50*(2), 179-211.

Alavi, M., Carlson, P., & Brooke, G. (1989). *The ecology of MIS research: a 20 year status review.* Paper presented at the Proceedings of the 10th International Conference on Information Systems.

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection: an intervention study. *Computers & Security, 29*(4), 432-445.

Alter, S. (2008). Defining information systems as work systems: implications for the IS field. *European Journal of Information Systems, 17*(5), 448-469.

Amankwa, E., Loock, M., & Kritzinger, E. (2014). *A conceptual analysis of information security education, information security training and information security awareness definitions.* Paper presented at the 9th International Conference for Internet Technology and Secured Transactions (ICITST), 2014. London, UK.

Anderson, R. (2001). *Why information security is hard - an economic perspective.* Paper presented at the 2001 Computer Security Applications Conference, New Orleans, Louisiana, USA.

Anderson, R., & Moore, T. (2006). The economics of information security. *Science, 314*(5799), 610-613.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., & Savage, S. (2013). Measuring the cost of cybercrime. *The Economics of Information Security and Privacy* (pp. 265-300). Springer Berlin Heidelberg.

Apvrille, A., & Pourzandi, M. (2005). Secure software development by example. *IEEE Security and Privacy, 3*(4), 10-17.

Bandyopadhyay, T., Liu, D., Mookerjee, V. S., & Wilhite, A. W. (2014). Dynamic competition in IT security: a differential games approach. *Information Systems Frontiers, 16*(4), 643-661.

Baskerville, R. (1988). *Designing information systems security*. John Wiley & Sons, Inc. New York, NY, USA.

Baskerville, R. (1989). Logical controls specification: an approach to information systems security. *Systems Development for Human Progress, 25*(4), 241-255.

Baskerville, R. (1993). Information systems security design methods: implications for information systems development. *ACM Computing Surveys (CSUR), 25*(4), 375-414.

Baskerville, R. L., & Myers, M. D. (2002). Information systems as a reference discipline. *MIS Quarterly*, 1-14.

Baumgart, R. H., Demsky, U., Martius, K., & Besch, M. (2007). *Method of using a security token.* U.S. Patent Application No. 11/703,603. Google Patents.

Benbasat, I., Cash, J. I., & Nunamaker, J. (1989). *The information systems research challenge*. Harvard Business School, Boston, MA, USA.

Benbasat, I., & Zmud, R. W. (1999). Empirical research in information systems: the practice of relevance. *MIS Quarterly*, Vol. 23 No 1, pp. 3-16.

Benson, J. K. (1973). The analysis of bureaucratic‐professional conflict: functional versus dialectical approaches. *The Sociological Quarterly, 14*(3), 376-394.

Bhattacharyya, D., Ranjan, R., Alisherov, F., & Choi, M. (2009). Biometric authentication: a review. *International Journal of u-and e-Service, Science and Technology, 2*(3), 13-28.

BIS. (2013). *2013 Information security breaches survey.* Retrieved March 21, 2015, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/200455/bis-13-p184-2013-information-security-breaches-survey-technical-report.pdf

Bishop, M. A. (2002). The art and science of computer security. Boston, MA, USA: Addison-Wesley Longman Publishing Co., Inc.

Boockholdt, J. (1989). Implementing security and integrity in micro-mainframe networks. *MIS Quarterly*, Vol. 13, No. 2, pp. 135-144.

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., & Boss, R. W. (2009). If someone is watching, I will do what I am asked: mandatoriness, control, and information security. *European Journal of Information Systems, 18*(2), 151-164.

Brancheau, J. C., Janz, B. D., & Wetherbe, J. C. (1996). Key issues in information systems management: 1994-95 SIM Delphi results. *MIS Quarterly*, Vol. 20, No. 2, pp. 225-242.

Breu, R., Burger, K., Hafner, M., & Popp, G. (2004). Towards a systematic development of secure systems. *Information Systems Security, 13*(3), 5-13.

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, pp. 523-548.

Burrell, G., & Morgan, G. (1979). *Social paradigms and organisational analysis: elements of the sociology of corporate life.* London: Heinemann Educational.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). A model for evaluating IT security investments. *Communications of the ACM, 47*(7), 87-92.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2004). The effect of Internet security breach announcements on market value: Capital market reactions for breached firms and Internet security developers. International Journal of Electronic Commerce, 9(1), 70-104.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16*(1), 28-46.

Cavusoglu, H., Raghunathan, S., & Yue, W. T. (2008). Decision-theoretic and game-theoretic approaches to IT security investment. *Journal of Management Information Systems, 25*(2), 281-304.

Chang, H. H., & Chen, S. W. (2009). Consumer perception of interface quality, security, and loyalty in electronic commerce. *Information & Management, 46*(7), 411-417.

Chan, K., Kwong, S., & Longginnou, L. (1993). *Security management on mobile-phone communication.* Paper presented at the TENCON'93. Proceedings. IEEE Region 10 Conference on Computer, Communication, Control and Power Engineering, 1993.

Chang, K.-c., & Wang, C.-p. (2011). Information systems resources and information security. *Information Systems Frontiers, 13*(4), 579-593.

Chatterjee, S., Sarker, S., & Valacich, J. S. (2015). The behavioural roots of information systems security: exploring key factors related to unethical IT use. *Journal of Management Information Systems, 31*(4), 49-87.

Chen, W., & Hirschheim, R. (2004). A paradigmatic and methodological examination of information systems research from 1991 to 2001. *Information Systems Journal, 14*(3), 197-235.

Chua, C., Cao, L., Cousins, K., & Straub, D. W. (2002). Measuring researcher-production in information systems. *Journal of the Association for Information Systems, 3*(1), 6.

Chua, W. F. (1986). Radical developments in accounting thought. *Accounting Review*, Vol. LXI, No. 4, pp. 601-632.

Colwill, C. (2009). Human factors in information security: the insider threat – who can you trust these days? *Information Security Technical Report, 14*(4), 186-196.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., & Baskerville, R. (2013). Future directions for behavioural information security research. *Computers & Security, 32*, 90-101.

Crowley, E. (2003). *Information system security curricula development.* Paper presented at the Proceedings of the 4th Conference on Information Technology Curriculum. (pp. 249-255). ACM. Lafayette, IN, USA.

Damianou, N., Dulay, N., Lupu, E., & Sloman, M. (2001). The ponder policy specification language. *Policies for Distributed Systems and Networks* (pp. 18-38). Springer Berlin Heidelberg.

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*(6), 643-658.

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

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

De Graaf, G., & Huberts, L. W. (2008). Portraying the nature of corruption using an explorative case study design. *Public Administration Review*, *68*(4), 640-653.

DeSanctis, G., & Poole, M. S. (1994). Capturing the complexity in advanced technology use: adaptive structuration theory. *Organisation Science, 5*(2), 121-147.

Dhillon, G. (2007). *Principles of information systems security: text and cases.* New York: John Wiley, Inc.

Dhillon, G., & Backhouse, J. (2001). Current directions in IS security research: towards socio‐organisational perspectives. *Information Systems Journal,*

11(2), 127-153.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: the role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: a critical study of the content of university policies. *International Journal of Information Management, 29*(6), 449-457.

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: an exploratory analysis. *Social and Human Elements of Information Security: Emerging Trends and Countermeasures*. pp. 326-342, IGI Global, Hershey, New York.

Doherty, N. F., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security, 25*(1), 55-63.

Doty, D. H., & Glick, W. H. (1994). Typologies as a unique form of theory building: towards improved understanding and modeling. *Academy of Management Review, 19*(2), 230-251.

Dutta, A., & McCrohan, K. (2002). Management's role in information security in a cyber economy. *California Management Review, 45*(1), 67-87.

El-Gayar, O. F., & Fritz, B. D. (2010). A web-based multi-perspective decision support system for information security planning. *Decision Support Systems, 50*(1), 43-54.

Ellerbrok, A. (2011). Playful biometrics: controversial technology through the lens of play. *The Sociological Quarterly, 52*(4), 528-547.

Fabian, B., Gürses, S., Heisel, M., Santen, T., & Schmidt, H. (2010). A comparison of security requirements engineering methods. *Requirements Engineering, 15*(1), 7-40.

Fang, F., Parameswaran, M., Zhao, X., & Whinston, A. B. (2014). An economic mechanism to manage operational security risks for inter-organisational information systems. *Information Systems Frontiers, 16*(3), 399-416.

Fernández-Medina, E., Trujillo, J., Villarroel, R., & Piattini, M. (2004). *Extending UML for designing secure data warehouses.* Paper presented at the International Conference on Conceptual Modeling. Shanghai, China.

Fernández-Medina, E., Trujillo, J., Villarroel, R., & Piattini, M. (2006). Access control and audit model for the multidimensional modeling of data warehouses. *Decision Support Systems, 42*(3), 1270-1289.

Ferraiolo, D. F., Sandhu, R., Gavrila, S., Kuhn, D. R., & Chandramouli, R. (2001). Proposed NIST standard for role-based access control. *ACM Transactions on Information and System Security (TISSEC), 4*(3), 224-274.

Furnell, S. M., Gennatou, M., & Dowland, P. (2002). A prototype tool for information security awareness and training. *Logistics Information Management, 15*(5/6), 352-357.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: a survey of end-users. *Computers & Security, 25*(1), 27-35.

Galliers, R. (1992). *Information systems research: issues, methods and practical guidelines*, ed. R.D. Galliers. Blackwell Scientific Publications: Oxford, pp. 144-162

Galliers, R. D., & Whitley, E. A. (2007). Vive les differences? Developing a profile of European information systems research as a basis for international comparisons. *European Journal of Information Systems, 16*(1), 20-35.

Gao, X., Zhong, W., & Mei, S. (2015). Security investment and information sharing under an alternative security breach probability function. *Information Systems Frontiers, 17*(2), 423-438.

García, R., & Calantone, R. (2002). A critical look at technological innovation typology and innovativeness terminology: a literature review. *Journal of Product Innovation Management*, *19*(2), 110-132.

Garfinkel, S., & Spafford, G. (1997). *Web security & commerce*. O'Reilly & Associates, Inc., Gravenstein Highway North, Sebastopol, USA.

Garrido, J. M., & Bandyopadhyay, T. (2009). *Simulation model development in information security education.* Paper presented at the 2009 Information Security Curriculum Development Conference.

Gibbons, M. T. (1987). *Introduction: the politics of interpretation*. New York: New York University Press.

Goel, S., & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information & Management, 46*(7), 404-410.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users: a study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13-27.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security (TISSEC), 5*(4), 438-457.

Gray, P. H., & Durcikova, A. (2005). The role of knowledge repositories in technical support environments: speed versus learning in user performance. *Journal of Management Information Systems, 22*(3), 159-190.

Greenwald, G. (2014). No place to hide: Edward Snowden, the NSA, and the US surveillance state. Penguin Books Limited.

Gregor, S. (2002). A theory of theories in information systems. *Information Systems Foundations: Building the Theoretical Base*, S. Gregor and D. Hart (eds.), Australian National University, Canberra, 2002b, pp. 1-20.

Gregor, S. (2006). The nature of theory in information systems. *MIS Quarterly*, Vol. 30 No. 3, pp. 611-642.

Guba, E. G., & Lincoln, Y. S. (1989). *Fourth generation evaluation.* Newbury Park, CA: Sage.

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

Gupta, A. K., Tesluk, P. E., & Taylor, M. S. (2007). Innovation at and across multiple levels of analysis. *Organisation Science, 18*(6), 885-897.

Haley, C. B., Moffett, J. D., Laney, R., & Nuseibeh, B. (2006). *A framework for security requirements engineering.* Paper presented at the Proceedings of the 2006 International Workshop on Software Engineering for Secure Systems. Shanghai, China

Hausken, K. (2006). Returns to information security investment: the effect of alternative information security breach functions on optimal investment and sensitivity to vulnerability. *Information Systems Frontiers, 8*(5), 338-349.

Hausken, K. (2014). Returns to information security investment: endogenising the expected loss. *Information Systems Frontiers, 16*(2), 329-336.

He, Y., Johnson, C., Renaud, K., Lu, Y., & Jebriel, S. (2014). *An empirical study on the use of the generic security template for structuring the lessons from information security incidents.* Paper presented at the 6th International Conference on Computer Science and Information Technology (CSIT), 2014. Amman, Jordan.

Hedström, K., Kolkowska, E., Karlsson, F., & Allen, J. (2011). Value conflicts for information security management. *The Journal of Strategic Information Systems, 20*(4), 373-384.

Hentea, M., Dhillon, H., & Dhillon, M. (2006). Towards changes in information security education. *Journal of Information Technology Education: Research, 5*(1), 221-233.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviours in organisations: role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154-165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: a framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

Herley, C. (2009). *So long, and no thanks for the externalities: the rational rejection of security advice by users.* Paper presented at the Proceedings of the 2009 Workshop on New Security Paradigms. Oxford, UK

Herrmann, G., & Pernul, G. (1999). Viewing business-process security from different perspectives. *International Journal of Electronic Commerce*, VOL.3, No. 3. pp. 89-103.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design-science in information systems research. *MIS Quarterly, 28*(1), 75-105.

Hirschheim, R. (1985). Information systems epistemology: an historical perspective. *Research methods in information systems*, 13-35.

Hitt, M. A., Beamish, P. W., Jackson, S. E., & Mathieu, J. E. (2007). Building theoretical and empirical bridges across levels: multilevel research in management. *Academy of Management Journal, 50*(6), 1385-1399.

Hofstede, G. (1993). Cultural constraints in management theories. *The Academy of Management Executive, 7*(1), 81-94.

Höne, K., & Eloff, J. H. P. (2002). Information security policy — what do international information security standards say? *Computers & Security, 21*(5), 402-409.

House, R., Rousseau, D. M., & Thomashunt, M. (1995). The Meso paradigm - a framework for the integration of micro and macro organisational-behaviour. *Research in Organisational Behaviour: an Annual Series of Analytical Essays and Critical Reviews, 17*, 71-114.

Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research, 23*(3-part-2), 918-939.

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

Hu, V., Ferraiolo, D. F., Kuhn, D. R., Kacker, R. N., & Lei, Y. (2015). *Implementing and managing policy rules in attribute-based access control.* Paper presented at the 2015 IEEE International Conference on Information Reuse and Integration (IRI).

Huang, C. D., Behara, R. S., & Goo, J. (2014). Optimal information security investment in a Healthcare Information Exchange: an economic analysis. *Decision Support Systems, 61*, 1-11.

Humphreys, T. (2006). State-of-the-art information security management systems with ISO/IEC 27001: 2005. ISO Management Systems, 6(1).

Ifinedo, P. (2012). Understanding information systems security policy compliance: an

integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security, 31*(1), 83-95.

Iivari, J., Hirschheim, R., & Klein, H. K. (1998). A paradigmatic analysis contrasting information systems development approaches and methodologies. *Information Systems Research, 9*(2), 164-193.

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: the enduring problem of human error. *ACM Sigmis Database, 36*(4), 68-79.

Jaeger, P. T., Lin, J., & Grimes, J. M. (2008). Cloud computing and information policy: computing in a policy cloud? *Journal of Information Technology & Politics, 5*(3), 269-283.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviours: an empirical study. *MIS Quarterly*, VOL. 34 No. 3, pp 549-566.

Kankanhalli, A., Teo, H.-H., Tan, B. C., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *International Journal of Information Management, 23*(2), 139-154.

Kannan, K., Rees, J., & Sridhar, S. (2007). Market reactions to information security breach announcements: An empirical analysis. International Journal of Electronic Commerce, 12(1), 69-91.

Kaplan, B., & Maxwell, J. A. (1994). Evaluating healthcare information systems: methods and applications. *Qualitative Research Methods for Evaluating Computer Information Systems. JG Anderson, CE Ayden and SJ Jay. Thousand Oaks, Sage*.

Karofsky, E. (2001). Return on security investment: calculating the security investment equation. *Secure Business Quarterly, 1*(2)

Katsikas, S. K. (2000). Healthcare management and information systems security: awareness, training or education? *International Journal of Medical Informatics, 60*(2), 129-135.

Katz, D., & Kahn, R. L. (1978). *The social psychology of organisations*. New York: Wiley.

Kirsch, L., & Boss, S. (2007). The last line of defense: motivating employees to follow corporate security guidelines. *ICIS 2007 Proceedings*, 103. Melbourne, Australia.

Kissel, R. (2013). *Glossary of key information security terms*. NIST IR 7298

Klein, H. K. (2003). Crisis in the IS field? A critical reflection on the state of the discipline. *Journal of the Association for Information Systems, 4*(1), 10.

Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and

evaluating interpretive field studies in information systems. *MIS Quarterly*, Vol. 23, No. 1, pp. 67-93.

Klein, K. J., Dansereau, F., & Hall, R. J. (1994). Levels issues in theory development, data collection, and analysis. *Academy of Management Review, 19*(2), 195-229.

Klein, K. J., & Kozlowski, S. W. (2000). *MT, research, and methods in organisations: foundations, extensions, and new directions.* San Francisco: Jossey-Bass.

Klein, K. J., Tosi, H., & Cannella, A. A. (1999). MT building: benefits, barriers, and new developments. *Academy of Management Review, 24*(2), 248-253.

Kocher, P., Lee, R., McGraw, G., Raghunathan, A., & Moderator-Ravi, S. (2004). *Security as a new dimension in embedded system design.* Paper presented at the Proceedings of the 41st Annual Design Automation Conference.

Kozlowski, S. W., & Klein, K. J. (2000). A multilevel approach to theory and research in organisations: contextual, temporal, and emergent processes. K. J. Klein & S. W. J. Koslowski (Eds.), MT, research, and methods in organizations: 3–90. San Francisco: JosseyBass.

Kraemer, H. C., Pruyn, J. P., Gibbons, R. D., Greenhouse, J. B., Grochocinski, V. J., Waternaux, C., & Kupfer, D. J. (1987). Methodology in psychiatric research: report on the 1986 MacArthur Foundation Network I Methodology Institute. *Archives of General Psychiatry, 44*(12), 1100-1106.

Landry, M., & Banville, C. (1992). A disciplined methodological pluralism for MIS research. *Accounting, Management and Information Technologies, 2*(2), 77-97.

Laudan, L. (1984). *Science and values* (Vol. 66). Berkeley: University of California Press.

Lee, B., Barua, A., & Whinston, A. B. (1997). Discovery and representation of causal relationships in MIS research: a methodological framework. *MIS Quarterly*, Vol. 21, No. 1, pp. 109-136.

Lee, J., Crossler, R., & Warkentin, M. (2013). Implications of monitoring mechanisms on bring your own device (BYOD) adoption. Paper presented at the 34th International Conference on Information Systems, Milan, Italy

Lee, M., & Lee, J. (2012). The impact of information security failure on customer behaviours: a study on a large-scale hacking incident on the Internet. *Information Systems Frontiers, 14*(2), 375-393.

Lee, Y. J., Kauffman, R. J., & Sougstad, R. (2011). Profit-maximising firm investments in customer information security. *Decision Support Systems, 51*(4), 904-920.

Lindqvist, H. (2006). *Mandatory access control.* Master's Thesis in Computing Science, Umea University, Department of Computing Science, SE-901, 87

Lo, D. C.-T., Qian, K., Chen, W., & Rogers, T. (2015). *A low cost, portable platform for information assurance and security education.* Paper presented at the 15th IEEE International Conference on Advanced Learning Technologies, 2015.

Mabece, T., Futcher, L., & Thomson, K.-L. (2016). *Towards using pervasive information security education to influence information security behaviour in undergraduate computing graduates*. Paper presented at the International Conference on Information Resources Management, 2016. Cape Town, South Africa.

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. *Decision Support Systems, 15*(4), 251-266.

Markus, M. L., & Robey, D. (1988). Information technology and organisational change: causal structure in theory and research. *Management Science, 34*(5), 583-598.

McCarthy, T. (1981). *The critical theory of Jurgen Habermas*. Cambridge, MA: The MIT Press.

Mellado, D., Fernández-Medina, E., & Piattini, M. (2007). A common criteria-based security requirements engineering process for the development of secure information systems. *Computer Standards & Interfaces, 29*(2), 244-253.

Mingers, J. (2001). Combining IS research methods: towards a pluralist methodology. *Information Systems Research, 12*(3), 240-259.

Mirchandani, D., & Motwani, J. (2003). Reducing Internet abuse in the workplace. *SAM Advanced Management Journal, 68*(1), 22.

Myers, M. D. (2008). *Qualitative research in business & management*. London: Sage Publications Limited.

Myers, M. D., & Avison, D. (1997). Qualitative research in information systems. *Management Information Systems Quarterly,* Vol. 21, No. 2, pp. 241-242.

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

Nance, W. D., & Straub, D. W. (1988). *An investigation into the use and usefulness of security software in detecting computer abuse.* Management Information Systems Research Center, Curtis L. Carlson School of Management, University of Minnesota.

Nazareth, D. L., & Choi, J. (2015). A system dynamics model for information security management. *Information & Management, 52*(1), 123-134.

Neuman, W. L. (2000). *Social research methods: qualitative and quantitative approaches*. 4th edition. Boston: Allyn and Bacon.

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

NIST (1998). *National Institute of Standards and Technology (NIST) information technology training requirements: a role-and performance-based model (NIST Special Publication 800-16).* Washington, DC: US Department of Commerce.

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE, 91*(12), 2021-2040.

Oh, S., & Park, S. (2003). Task–role-based access control model. *Information Systems, 28*(6), 533-562.

Orlikowski, W. J. (2000). Using technology and constituting structures: a practice lens for studying technology in organisations. *Organisation Science, 11*(4), 404-428.

Orlikowski, W. J., & Baroudi, J. J. (1991). Studying information technology in organisations: research approaches and assumptions. *Information Systems Research, 2*(1), 1-28.

Osborn, S., Sandhu, R., & Munawer, Q. (2000). Configuring role-based access control to enforce mandatory and discretionary access control policies. *ACM Transactions on Information and System Security (TISSEC), 3*(2), 85-106.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behaviour towards IS security policy compliance.* Paper presented at the 40th Annual Hawaii International Conference on System Sciences (HICSS), 2007.

Pastor, V., Díaz, G., & Castro, M. (2010). *State-of-the-art simulation systems for information security education, training and awareness.* Paper presented at the IEEE EDUCON Conference, 2010.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design-science research methodology for information systems research. *Journal of Management Information Systems, 24*(3), 45-77.

Peltier, T. R. (2005). Information Security Risk Analysis (2nd edition), Boca Raton, FL: CRC press

Pettigrew, A. (1999). *Organising to improve company performance*. Hot Topics, Vol. 1, No. 5, Warwick Business School, University of Warwick, Coventry, UK.

Pond, R., Podd, J., Bunnell, J., & Henderson, R. (2000). Word association computer passwords: the effect of formulation techniques on recall and guessing rates. *Computers & Security, 19*(7), 645-656.

Popp, G., Jurjens, J., Wimmel, G., & Breu, R. (2003). *Security-critical system development with extended use cases.* Paper presented at the 10th Asia-Pacific Software Engineering Conference, 2003.

Porter, L. W. (1996). Forty years of organisation studies: reflections from a micro perspective. *Administrative Science Quarterly*, 41: 262-269.

Portnoy, L., Eskin, E., & Stolfo, S. (2001). *Intrusion detection with unlabeled data using clustering.* Paper presented at the Proceedings of ACM CSS Workshop on Data Mining Applied to Security (DMSA-2001). Philadelphia, PA, USA

Posey, C., Bennett, R. J., & Roberts, T. L. (2011). Understanding the mindset of the abusive insider: an examination of insiders' causal reasoning following internal security changes. *Computers & Security, 30*(6), 486-497.

Posey, C., Roberts, T. L., Lowry, P. B., & Hightower, R. T. (2014). Bridging the divide: a qualitative comparison of information security thought patterns between information security professionals and ordinary organisational insiders. *Information & Management, 51*(5), 551-567.

Pounder, C. (1997). First steps towards a European Union policy on the securing of electronic communications. *COMPUT. SECUR., 16*(7), 590-594.

Puhakainen, P. (2006). A design theory for information security awareness. *working paper, Faculty of Science, University of Oulu, Finland.*

Puhakainen, P., & Ahonen, R. (2006). Design theory for information security awareness. Oulu, Finland: University of Oulu.

Puhakainen, P., & Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, Vol. 34, No. 4, pp 757-778.

Ransbotham, S., & Mitra, S. (2009). Choice and chance: a conceptual model of paths to information security compromise. *Information Systems Research, 20*(1), 121-139.

Rees, J., Bandyopadhyay, S., & Spafford, E. H. (2003). PFIRES: a policy framework for information security. *Communications of the ACM, 46*(7), 101-106.

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

Robey, D. (2003). *Identity, legitimacy and the dominant research paradigm: an alternative prescription for the IS discipline*: A response to Benbasat and Zmud's call for returning to the IT artifact. Journal of the Association for Information Systems, 4(1), 15.

Rosen, M. (1991). Coming to terms with the field: understanding and doing organisational ethnography. *Journal of Management Studies, 28*(1), 1-24.

Rousseau, D. M. (1985). Issues of level in organisational research: multi-level and cross-level perspectives. *Research in Organisational Behaviour, 7*(1), 1-37.

Rowe, R. K. (2009). *Systems and methods for improved biometric feature definition.* U.S. Patent No. 7,627,151. Washington, DC: U.S. Patent and Trademark Office. Google Patents.

Sanderson, E., & Forcht, K. A. (1996). Information security in business environments. *Information Management & Computer Security, 4*(1), 32-37.

Sandhu, R. S. (1992). *The typed access matrix model.* Paper presented at the 1992 IEEE Computer Society Symposium on Research in Security and Privacy.

Sandhu, R. S. (1993). Lattice-based access control models. *Computer, 26*(11), 9-19.

Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, 15*(3), 112-133.

Sherwood, J. (1997). Managing security for outsourcing contracts. *Computers & Security, 16*(7), 603-609.

Silver, M. S., Markus, M. L., & Beath, C. M. (1995). The information technology interaction model: a foundation for the MBA core course. *MIS Quarterly*, Vol. 19, No. 3, pp. 361-390.

Siponen, M. (2001). Five dimensions of information security awareness. *Computers and Society, 31*(2), 24-29.

Siponen, M. (2005). Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods. *Information and Organisation, 15*(4), 339-375.

Siponen, M., Baskerville, R., & Heikka, J. (2006). A design theory for secure information systems design methods. *Journal of the Association for Information Systems, 7*(1), 31.

Siponen, M., & Iivari, J. (2006). Six design theories for IS security policies and guidelines. *Journal of the Association for Information Systems, 7*(7), 445-472.

Siponen, M., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM Sigmis Database, 38*(1), 60-80.

Siponen, M., Willison, R., & Baskerville, R. (2008). Power and practice in information systems security research. *ICIS 2008 Proceedings*, 26.

Smith, H. J., Dinev, T., & Xu, H. (2011). Information privacy research: an interdisciplinary review. *MIS Quarterly, 35*(4), 989-1016.

Smith, M., & Sherwood, J. (1995). Business continuity planning. *Computers & Security, 14*(1), 14-23.

Srinidhi, B., Yan, J., & Tayi, G. K. (2015). Allocation of resources to cyber-security: the effect of misalignment of interest between managers and investors. *Decision Support Systems, 75*, 49-62.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: a critical evaluation. *Information Systems Journal, 22*(1), 77-94.

Stanton, J. M., & Stam, K. R. (2006). *The visible employee: using workplace monitoring and surveillance to protect information assets--without compromising employee privacy or trust.* Medford, NJ: Information Today, Inc.

Straub, D. W. (1990). Effective IS security: an empirical study. *Information Systems Research, 1*(3), 255-276.

Straw, J. (1995). *The Draft Federal Criteria and the ITSEC: progress towards alignment.* National Computer Security Conference, 1993 (16th) Proceedings: Information Systems Security: User Choices (p. 311). DIANE Publishing.

Tariq, M. A., Brynielsson, J., & Artman, H. (2014). *The security awareness paradox: a case study.* Paper presented at the 2014 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM).

Thomson, M. E., & Von Solms, R. (1998). Information security awareness: educating your users effectively. *Information Management & Computer Security, 6*(4), 167-173.

Thorsen, E., Sreedharan, C., & Allan, S. (2013). Wikileaks and whistle-blowing: The framing of Bradley Manning. In Beyond WikiLeaks (pp. 101-122). Palgrave Macmillan UK.

Toval, A., Nicolás, J., Moros, B., & García, F. (2002). Requirements reuse for improving information systems security: a practitioner's approach. *Requirements Engineering, 6*(4), 205-219.

Truex, D., Holmström, J., & Keil, M. (2006). Theorizing in information systems research: a reflexive analysis of the adaptation of theory in information systems research. *Journal of the Association for Information Systems, 7*(12), 797-821.

Tsiakis, T., & Stephanides, G. (2005). The economic approach of information security. *Computers & Security, 24*(2), 105-108.

Tu, Z., Turel, O., Yuan, Y., & Archer, N. (2015). Learning to cope with information security risks regarding mobile device loss or theft: an empirical examination. *Information & Management, 52*(4), 506-517.

Turban, E., & Volonino, L. (2010). *Information technology for management: improving performance in the digital economy*. Hoboken, NJ: Wiley.

Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal, 48*(6), 1143-1158.

Uludag, U., Pankanti, S., Prabhakar, S., & Jain, A. K. (2004). Biometric cryptosystems: issues and challenges. *Proceedings of the IEEE, 92*(6), 948-960.

Vaishnavi, V., & Kuechler, W. (2004). Design research in information systems. Retrieved March 21, 2015, from http://www.isworld.org/Researchdesign/drisISworld.htm

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

Villarroel, R., Fernández-Medina, E., & Piattini, M. (2005). Secure information systems development – a survey and comparison. *Computers & Security, 24*(4), 308-321.

Vogler, H., Kunkelmann, T., & Moschgath, M.-L. (1997). *An approach for mobile agent security and fault tolerance using distributed transactions.* Paper presented at the 1997 International Conference on Parallel and Distributed Systems.

Von Solms, R. (1998). Information security management (3): the code of practice for information security management (BS 7799). *Information Management & Computer Security, 6*(5), 224-225.

Vroom, C., & Von Solms, R. (2004). Towards information security behavioural compliance. *Computers & Security, 23*(3), 191-198.

Warkentin, M., & Johnston, A. C. (2006). IT security governance and centralized security controls. *Enterprise Information Assurance and System Security: Managerial and Technical Issues*, M. Warkentin, and R. Vaughn (eds.), Hershey, PA: Idea Group Publishing, pp. 16-24

Whitman, M. E. (2004). In defense of the realm: understanding the threats to information security. *International Journal of Information Management, 24*(1), 43-57.

Willison, R. (2006). Understanding the perpetration of employee computer crime in the organisational context. *Information and Organisation, 16*(4), 304-324.

Willison, R., & Siponen, M. (2007). *A critical assessment of IS security research between 1990-2004.* Paper presented at the 15th European Conference on Information Systems, St. Gallen, Switzerland.

Wilson, M., & Hash, J. (2003). Building an information technology security awareness and training program. *NIST Special Publication, 800*, 50.

Wong, N., Ray, P., Stephens, G., & Lewis, L. (2012). Artificial immune systems for the detection of credit card fraud: an architecture, prototype and preliminary results. *Information Systems Journal, 22*(1), 53-76.

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

Yang, Y. C., & Padmanabhan, B. (2010). Towards user patterns for online security: observation time and online user identification. *Decision Support Systems, 48*(4), 548-558.

Yeh, Q.-J., & Chang, A. J.-T. (2007). Threats and countermeasures for information system security: a cross-industry study. *Information & Management, 44*(5), 480-491.

Yin, R. K. (2013). *Case study research: design and methods.* (5th edition). Thousand Oaks, CA: Sage Publications.

Zhang, P., & Galletta, D. F. (2006). *Human-computer interaction and management information systems: foundations.* Armonk, NY: ME Sharpe.

Zhang, X. N. (1997). Secure code distribution. *Computer, 30*(6), 76-79.

Zhao, X., Fang, F., & Whinston, A. B. (2008). An economic mechanism for better Internet security. *Decision Support Systems, 45*(4), 811-821.

Zhu, R. (2015a). *Customer awareness of Internet banking security in China*. Paper presented at the WHICEB 2015, Wuhan, China.

Zhu, R. (2015b). *An initial study of customer Internet banking security awareness and behaviour in China*. Paper presented at the PACIS 2015, Singapore.