emerald PUBLISHING

ISSN 2056-4961
Volume **26** Number **2 2018**

Information and Computer Security

Value conflicts and information security management

Guest Editors: Fredrik Karlsson,
Ella Kolkowska and Marianne Törner

Editorial advisory board

Information and Computer Security
Vol. 26 No. 2, 2018
p. 145

2056-4961

Guest editorial

Value conflicts and information security management

This special issue focuses on a crucial but under-developed area in information security management research, namely, the complexity of information security when different practices, requirements and management systems meet and create tensions. In particular, this means highlighting value pluralism, value conflicts and dilemmas anchored in these practices, requirements and management systems. Such value conflicts could appear within or between organisations, as well as between different societal interests. Value conflicts involving information security, and the way these are dealt with, may not only influence information security *per se* but also organisational performance, working conditions and quality of life.

In recent years, the need to shift the focus of organisational research, from an either/or perspective where one value is prioritised before others, to one that engages with several values simultaneously has been increasingly acknowledged (Lewis and Smith, 2014; MacCormick and Parker, 2010; Törner *et al.*, 2017). Such a change in perspective is needed also in regard to information security management. Some scholarly work has been done, acknowledging that information security values may be in conflict with other organisational and professional values (Dhillon and Torkzadeh, 2006; Albrechtsen and Hovden, 2009; Myyry *et al.*, 2009; Hedström *et al.*, 2011). The area where value conflicts seems to have attracted the most attention is related to employees' non-compliance with information security policies and procedures; several scholars (Hedström *et al.*, 2013; Albrechtsen, 2007; Son, 2011; Vaast, 2007; Besnard and Arief, 2004) have shown that differences in goals and values are important to consider when analysing the reasons for employees' non-compliance. However, information security management systems themselves might not even be value-congruent; Karlsson *et al.* (2016) have, for example, found value conflicts in information security policies.

That said, most current information security research does not address value pluralism. Instead, information security is generally addressed from a value monistic perspective (Kolkowska *et al.*, 2017; Karlsson *et al.*, 2017). If acknowledged, value conflicts are often addressed through an either/or perspective, prioritising one value before others. Moreover, in practice, this prioritisation is often left to the employees (Kirlappos *et al.*, 2013). Johnson (2014) has claimed that organisational paradoxes – or rather dilemmas – cannot be handled in an either/or manner; instead, they are interdependent value couples. He acknowledged that these dilemmas create pressure, but although prioritising one value before the other may temporarily relieve the discomfort, it will not relieve the pressure. It will rather increase the demand for the other value, as the two poles of the dilemma are interdependent. It is therefore imperative to approach value conflicts in organisations through a more inclusive perspective.

To meet this need and to inspire more research from such a perspective, this special issue opens up for discussions on value pluralism, competing requirements and dilemmas in relation to information security management. Viewing competing requirements as often interrelated and even interdependent may provide better grounds for organisational and management system development, also regarding information security management.

Some of the studies in this special issue take an intra-organisational perspective on information security-related value conflicts; others take a broader societal one. Tu *et al.* emphasise the importance of strategic value alignment for successful information security

Information & Computer Security
Vol. 26 No. 2, 2018
pp. 146-149

2056-4961
DOI 10.1108/ICS-02-2018-0019

management. The authors argue that information security goals are not always linked to an organisation's main objectives, and this often results in value conflicts. The key to improve information security is to recognise such value conflicts and find a way to deal with them effectively. Based on findings from previous literature, the authors argue that the most proactive way to deal with value conflicts is to work towards value alignment. Thus, they suggest a model and verify key factors that impact the success of information security management at an organisational level from a strategic value alignment perspective. The model can be used to formulate practical guidelines for organisations to improve information security management and align information security management values with business strategies. The results from this study can also encourage information security managers' collaboration with top business managers.

Katajzi *et al.* address value conflicts related to employees' non-compliance with information security policies and procedures. More specifically, the authors use the escalation of commitment theories to explain the effect of lost assets on non-compliance with information security policies in terms of value conflicts. The study focuses on situations where investments in time, effort and resources are devoted to a task that meets with difficulties, leading to a possible failure in course of action. When confronted with such situations, one of the most challenging decisions that an employee has to make is whether to abandon a task that is difficult to complete without violating the information security policy or persist on it. The study shows that when employees are caught in tasks undergoing difficulties, they are more likely to increase non-compliance behaviour. By understanding how project obstacles result in such tasks, security managers can define new mechanisms to counter employees' shift from compliance to non-compliance.

Hedström *et al.* argue that a high-integrity electronic identity management system needs to be put in place to ensure patients' security and privacy. However, various stakeholders involved in the implementation of such systems may prioritise different values, jeopardising the integrity of the system and, consequently, privacy and security of the patients. The paper highlights value conflicts amongst stakeholders involved in the implementation of an electronic identity management system in a health organisation. Based on the values of individuals in this organisation, the authors define electronic identity management objectives. These objectives are then structured in objective hierarchies for each stakeholder group, allowing comparison across multiple stakeholder groups. Besides presentation and comparison of objective hierarchies in a health organisation, the paper also provides a foundation to evaluate and weigh different objectives for strategic decision management.

Karlsson *et al.* investigate information security value conflicts from an organisational culture perspective, based on the competing values framework (Quinn and Rohrbaugh, 1983). In a survey study, they approach two broad samples of white-collar workers and find that about one-third of the respondents experience conflicts between information security values and other organisational or individual values. The study shows that such conflicts are equally common in six different occupational branches in private and public sectors. Conflicts between information security values and work efficiency are the most common. An interesting finding in this study is that information security-related value conflicts are less common in organisations where employees experience a psychosocially supportive work situation. As one may expect, the authors also find that value conflicts are somewhat more common among respondents who handle highly sensitive information. In contrast, information security value conflicts are less common in organisational cultures characterised as bureaucratic.

Yayla *et al.* take a multinational perspective on information security management. They approach the challenges that multinational companies face when they attempt to implement

information security policies in their subsidiaries. Policies that do not take into account cultural differences may induce value conflicts in the subsidiaries and thus obstruct information security policy implementation. The authors develop a framework that can be applied in developing and implementing information security policy through multinational organisations. The framework presents not only challenges that may emerge in terms of cultural distance, institutional distance and stickiness but also three strategies that can effectively take on these challenges. The framework can thus guide information security policy implementation and help to reduce the related value conflicts.

Johansson *et al.* point to a need for a broader societal perspective on information security management and value conflicts. They argue that existing information security research has largely focussed on value conflicts between internal organisational values. Therefore, they turn their attention to values that originate from society and that may compete with information security values. In particular, they explore employees' attitudes to whistle-blowing and how such attitudes relate to information security. Hence, they address conflicts between information security and transparency and accountability. They draw on the results of a large-scale survey of white-collar workers. Their study shows that a majority of the respondents do not perceive whistle-blowing as conflicting with information security. Having said that, they show that the attitudes are highly dependent on the receiver of the information, i.e. whether whistle-blowing occurs inside or outside the organisation.

The papers collectively illustrate a range of different topics about value conflicts and information security management. They capture some of the breadth and complexities of this topic and, at the same time, contribute to the (incomplete) jigsaw puzzle of understanding value conflicts.

Fredrik Karlsson and Ella Kolkowska
School of Business, Örebro University, Örebro, Sweden, and
Marianne Törner
Department of Public Health and Community Medicine at Institute of Medicine, University of Gothenburg, Sweden

References

Albrechtsen, E. (2007), "A qualitative study of user's view on information security", *Computers & Security*, Vol. 26 No. 4, pp. 276-289.

Albrechtsen, E. and Hovden, J. (2009), "The information security digital divide between information security managers and users", *Computers & Security*, Vol. 28 No. 6, pp. 476-490.

Besnard, D. and Arief, B. (2004), "Computer security impaired by legitimate users", *Computer & Security*, Vol. 23 No. 3, pp. 253-264.

Dhillon, G. and Torkzadeh, G. (2006), "Value-focused assessment of information security in organizations", *Information Systems Journal*, Vol. 16 No. 3, pp. 293-314.

Hedström, K., Karlsson, F. and Kolkowska, E. (2013), "Social action theory for understanding information security non-compliance in hospitals: the importance of user rationale", *Information Management & Computer Security*, Vol. 21 No. 4, pp. 266-287.

Hedström, K., Kolkowska, E., Karlsson, F. and Allen, J.P. (2011), "Value conflicts for information security management", *Journal of Strategic Information Systems*, Vol. 20 No. 4, pp. 373-384.

Johnson, B. (2014), "Reflections: a perspective on paradox and its application to modern management", *Journal of Applied Behavioral Science*, Vol. 50 No. 2, pp. 206-212.

Karlsson, F., Hedström, K. and Goldkuhl, G. (2016), "Practice-based discourse analysis of information security policies", *Computer & Security*, Vol. 67, pp. 267-279.

Karlsson, F., Karlsson, M. and Åström, J. (2017), "Measuring employees' compliance – the importance of value pluralism", *Information and Computer Security*, Vol. 25 No. 3, pp. 279-299.

Kirlappos, I., Beautement, A. and Sasse, M.A. (2013), "'Comply or die' is dead: long live security-aware principal agents", in Adam, A.A., Brenner, M. and Smith, M. (Eds), *Financial Cryptography and Data Security – FC 2013 Workshops, USEC and WAHC 2013, Okinawa, Japan, April 1, 2013, Revised Selected Papers*, Springer-Verlag Berlin Heidelberg, pp. 70-82.

Kolkowska, E., Karlsson, F. and Hedström, K. (2017), "Towards analysing the rationale of information security noncompliance: devising a value-based compliance analysis method", *Journal of Strategic Information Systems*, Vol. 26 No. 1, pp. 39-57.

Lewis, M. and Smith, W. (2014), "Paradox as a metatheoretical perspective: sharpening the focus and widening the scope", *Journal of Applied Behavioral Science*, Vol. 50 No. 2, pp. 127-149.

Maccormick, J.S. and Parker, S.K. (2010), "A multiple climates approach to understanding business unit effectiveness", *Human Relations*, Vol. 63 No. 11, pp. 1771-1806.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T. and Vance, A. (2009), "What levels of moral reasoning and values explain adherence to information security rules? An empirical study", *European Journal of Information Systems*, Vol. 18 No. 2, pp. 126-139.

Quinn, R.E. and Rohrbaugh, J. (1983), "A spatial model of effectiveness criteria: towards a competing values approach to organizational analysis", *Management Science*, Vol. 29 No. 3, pp. 363-377.

Son, J.Y. (2011), "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies", *Information and Management*, Vol. 48 No. 7, pp. 296-302.

Törner, M., Pousette, A., Larsman, P. and Hemlin, S. (2017), "Coping with paradoxical demands through an organizational climate of perceived organizational support. An empirical study among workers in construction and mining industry", *Journal of Applied Behavioral Science*, Vol. 53 No. 1, pp. 117-141.

Vaast, E. (2007), "Danger is in the eye of the beholders: social representations of information systems security in healthcare", *Journal of Strategic Information Systems*, Vol. 16 No. 2, pp. 130-152.

Received 4 April 2017
Revised 31 January 2018
Accepted 7 February 2018

Strategic value alignment for information security management: a critical success factor analysis

Cindy Zhiling Tu
School of Computer Science and Information Systems, Northwest Missouri State University, Maryville, Missouri, USA, and
Yufei Yuan, Norm Archer and Catherine E. Connelly
DeGroote School of Business, McMaster University, Hamilton, Ontario, Canada

Abstract

Purpose – Effective information security management is a strategic issue for organizations to safeguard their information resources. Strategic value alignment is a proactive approach to manage value conflict in information security management. Applying a critical success factor (CSF) analysis approach, this paper aims to propose a CSF model based on a strategic alignment approach and test a model of the main factors that contributes to the success of information security management.

Design/methodology/approach – A theoretical model was proposed and empirically tested with data collected from a survey of managers who were involved in decision-making regarding their companies' information security (N = 219). The research model was validated using partial least squares structural equation modeling approach.

Findings – Overall, the model was successful in capturing the main antecedents of information security management performance. The results suggest that with business alignment, top management support and organizational awareness of security risks and controls, effective information security controls can be developed, resulting in successful information security management.

Originality/value – Findings from this study provide several important contributions to both theory and practice. The theoretical model identifies and verifies key factors that impact the success of information security management at the organizational level from a strategic management perspective. It provides practical guidelines for organizations to make more effective information security management.

Keywords Information security management, Top management support, Business alignment, Critical success factor, Organizational awareness, Value alignment

Paper type Research paper

1. Introduction

Information is a valuable resource that is critical for an organization's success, but it is also vulnerable to a variety of attacks from both inside and outside of the organization (Lowry and Moody, 2015). With the growing threat and severity of security attacks, information security has become increasingly important to the survival of organizations. An organization's main objective is to provide valuable services to society. By doing so, it also generates profits or other benefits to the organization, as well as benefits to its employees and customers. Information is useful to help organizations to make better decisions and provide better services. Information security, however, is not directly linked to this mission. Rather, it deals with the negative aspects of security threats, which is something to avoid if at all possible (Liang and Xue, 2009). This often creates value conflict. For instance, managers who focus on using a company's resources for business competition may ignore

Information & Computer Security
Vol. 26 No. 2, 2018
pp. 150-170

2056-4961
DOI 10.1108/ICS-06-2017-0042

security risks and optimistically think that these attacks will not happen (Rhee *et al.*, 2012). This results from viewing information security as a burden and not wanting to spend money on it. In general, employees are expected to do good jobs to be rewarded. They may have value conflicts toward security and view security policy as unnecessary or interfering with productivity (Guo *et al.*, 2011). From a customer perspective, the focus is to get good service conveniently. Therefore, customers may also view security measures such as complex password setting as headaches or the use of biometric identity authentication with privacy concerns (Breward *et al.*, 2017). To improve information security, the key is to recognize such value conflicts and find a way to deal with them effectively. Literature has shown that the most proactive way to deal with value conflicts is to work toward value alignment (Lynn Fitzpatrick, 2007). Specifically, for security-related value conflicts, it is important to create value alignment for all the parties involved in information security management (ISM).

ISM has been recognized widely as strategically important to organizations (Ma *et al.*, 2009; Nazareth and Choi, 2015). The goal of ISM is to protect the confidentiality, integrity and availability of information and to mitigate the various risks and threats to such information (Chang *et al.*, 2011; Posthumus and von Solms, 2004). Even though information security has been consistently identified at the top of the information systems (IS) agenda (Dutta and McCrohan, 2002), research on organizational perspectives of security management is limited as yet, but it is beginning to emerge as a field of study (Ransbotham and Mitra, 2009; Soomro *et al.*, 2016).

In practice, ISM standards are among the most widely used methods of security management. These standards aim to provide an international, authoritative and comprehensive benchmark for IS security and have been considered as being the keystone in any successful ISM activities (Von Solms, 1999). However, most ISM standards and guidelines are fostered by an appeal to common practice, offering little evidence of their usefulness and relevance in practice (Siponen, 2005). Practitioners have no way of evaluating the reliability (or objectivity) of the claimed best practices (Siponen and Willison, 2009). Hence, there is a need for rigorous qualitative and quantitative empirical studies to test and refine ISM methods in practical settings.

Effective ISM must implement organizational-level solutions to security problems in the organization's socio-organizational context (Kayworth and Whitten, 2010). Consequently, practitioners and scholars have recognized that the emphasis of information security should go beyond technical controls and incorporate business process and organizational issues (Choobineh *et al.*, 2007; Culnan *et al.*, 2008; Kayworth and Whitten, 2010; Ma *et al.*, 2009; Parakkattu and Kunnathur, 2010; Siponen, 2005; Siponen *et al.*, 2009; Van Niekerk and Von Solms, 2010). To achieve an acceptable level of information security, an appropriate set of security controls must be identified, implemented and maintained within the organization. However, even with well-developed security controls, organizations may not achieve ISM success if there is no organizational support and organizational awareness of security within the organization. Because of the complexity of security management issues and value conflicts, professional guidelines are very much needed. To address this research gap, this study focuses on ISM at the organizational level. Using strategic value alignment approach, we study the organizational factors that determine the success of ISM. In this study, ISM is defined as a systematic process of effectively coping with information security threats and risks in an organization, through the application of a suitable range of physical, technical or operational security controls to protect information assets and achieve business goals. Building on the IS literature and ISM standards, this study attempts to fill the void in the understanding of ISM effectiveness by identifying critical success factors (CSFs) of ISM and

developing an ISM performance model to empirically test the validity of the identified CSFs. More specifically, this study tries to answer the following questions:

Q1. What are the critical factors that must be present to make ISM effective?

Q2. How do these factors contribute to the success of ISM?

The rest of the paper is organized as follows. In the next section, the research background and theoretical foundation of this study are presented. Then a research model is developed, along with relevant hypotheses. The related methodology for model verification is discussed. Finally, following data analysis, discussion and conclusions highlight implications of this work for future research and practice.

2. Research background

2.1 Value conflict and value alignment for information security management

According to Lynn (2007), values are defined as peoples' preferences and priorities that reflect what is important to them. Values are the foundation on which organizations are built. Although organizational values were defined as the values shared by its members, it is possible that not every member of the organization shares all its values to the same extent. Conflict may occur when people have different ideas about what is important, as well as different answers for something that requires resolution. Conflict can be either productive or unproductive, depending on how collaboration is managed. Without a higher order organizing principle, an organization may self-organize into various structural conflicts (Fritz, 1999). To avoid unproductive conflict, there must be enough alignment between ends and means values for progress toward the overall mission and vision to occur (Hultman and Gellermann, 2002). In the case of ISM, value conflict may exist among managers, IT departments, employees and consumers because of different priorities and a lack of security awareness. Researchers have identified value conflict phenomena such as self-defense of security violations with neutralization theory (Siponen and Vance, 2010) and conflict resolving approaches such as sanctions to stop security violations based on deterrence theory (D'Arcy *et al.*, 2009). However, this approach may not be effective (Hu *et al.*, 2011). Reactive problem-solving approaches generally address symptoms rather than causes and the "flurry of activity hides what is really going on" (Fritz, 1999, p. 9). A proactive value alignment approach recognizes the importance of strategic alignment between a company's overall business strategy and its ISM strategy. This strategic alignment will tend to promote top management support and bolster organizational awareness of security risks, thus enhancing the implementation of security controls. This will result in achieving successful ISM measured from balanced and interrelated perspectives including business value, stakeholder orientation, internal processes and future readiness.

Current studies on ISM focus on the conceptual understanding of ISM, the performance evaluation of ISM and the factors that affect the success of ISM. A few papers have provided conceptual view of ISM at the organizational level from different perspectives: as an integrated component in corporate governance (Johnston and Hale, 2009; Posthumus and von Solms, 2004; Tsohou *et al.*, 2015; von Solms and von Solms, 2006), as a form of risk management (Chang *et al.*, 2011; Dhillon and Backhouse, 2001; Webb *et al.*, 2014) and as a life cycle of dynamic multiple-phase decision-making (Ma *et al.*, 2009; Nazareth and Choi, 2015; Nyanchama, 2005; Pipkin, 2000). A group of researchers has called for investigating the quality of information security programs (Choobineh *et al.*, 2007). Some scholars have developed performance indexes for ISM based on a balanced scorecard (BSC) model with limited testing (Herath *et al.*, 2010). However, the comprehensive performance measurement

of ISM success needs to be further developed and empirically verified. Other papers have tried to examine the influence of organizational factors on the effectiveness of ISM implementation (Singh *et al.*, 2014) in a specific context such as e-government (Smith and Jamieson, 2006) or small- and medium-sized businesses (Chang and Ho, 2006; Singh and Gupta, 2014; Smith and Jamieson, 2006; Yildirim *et al.*, 2011). Indeed, some organizational factors in ISM have been recognized in the literature (Kayworth and Whitten, 2010; Singh *et al.*, 2014; Soomro *et al.*, 2016). However, there is a lack of empirical evidence or general theoretical frameworks for ISM success especially from strategic value alignment perspective. It has been suggested that empirical studies in relation to the issues of security management and the development of secure IS based on suitable reference theories, are particularly necessary (Siponen and Oinas-Kukkonen, 2007).

2.2 Critical success factor analysis of information security management

CSFs are defined as key areas in the firm that, if they are satisfactory, will assure successful performance for the organization (Rockart, 1979). CSFs are a widely used approach to identify performance requirements upon which the success of the firm depends (Rockart, 1982). They were one of the earliest and most actively researched management tools (Lee and Ahn, 2008) and have been used as management measures in different areas such as manufacturing industry (Mohr and Spekman, 1994; Psomas, 2016), project management (Ahimbisibwe *et al.*, 2017; Davies, 2002), quality management (Singh and Gupta, 2014) and business intelligence system implementation (Yeoh and Popovič, 2016).

Identifying suitable CSFs for ISM requires a holistic view of the organization (Smith and Jamieson, 2006). To integrate knowledge from academic study and industry practice in the field of ISM, we reviewed both relevant literature and information security standard ISO/IEC 27001: 2013. Trying to bridge the gap between literature and ISM practice, we identify the socio-organizational issues which are often viewed as critical to the successful implementation of ISM in both literature and information security standard. By combining the results of our review and the perspective of value alignment, we group these issues into four key factors: business alignment, top management support, organizational awareness and security controls (Aksorn and Hadikusumo, 2008; Chang *et al.*, 2011; Choobineh *et al.*, 2007; Herath *et al.*, 2010; Hu *et al.*, 2012; ISO/IEC, 2013; Kayworth and Whitten, 2010; Ma *et al.*, 2009; Maarop *et al.*, 2016; Nazareth and Choi, 2015; Siponen and Oinas-Kukkonen, 2007; Smith and Jamieson, 2006; Spears and Barki, 2010; Van Niekerk and Von Solms, 2010; Von Solms, 1999; Werlinger *et al.*, 2009; Yildirim *et al.*, 2011).

Although some CSFs have been recognized in literature and industry security standards, the existing critical factor analysis approach does not provide a way to analyze the relationships between factors and empirically verify how these factors affect the organizations performance. Spears and Barki (2010) examined user participation in IS security risk management (SRM) and its influence in the context of regulatory compliance via a multi-method study at the organizational level. Their model examines the relationship between certain organizational factors of SRM. It indicates that an alignment between SRM and the business context contributes to greater organizational awareness of IS security, which in turn contributes to perceived improvements in control development and the perceived performance of security controls. In addition, improvements in control development may influence the performance of security controls. Maarop *et al.* (2016) reviewed literature on ISM system (ISMS) implementation success factors. Based on 20 of the most relevant and recent studies, ten factors were extracted which can be considered important in the ISMS implementation. In particular, staff awareness and training and top management support are found to be the most crucial factors in determining the successful

implementation of ISMS and the rating of the importance for both factors are almost equal. They suggested that all factors identified can be hypothesized to influence the successful implementation of ISMS in organizations; thus, all factors identified can be further evaluated empirically by both qualitative and quantitative methodology.

2.3 A balanced scorecard for information security management performance measurement

Prior literature has indicated the importance of performance evaluation for ISM (Erkan, 2005; Herath *et al.*, 2010; Huang *et al.*, 2006; Martin *et al.*, 2011; Nazareth and Choi, 2015). How to measure the performance of ISM from an organizational perspective is a big challenge. Performance measurement should reflect common values shared by managers, stakeholders, employees and consumers. The BSC (Kaplan and Norton, 1992; Kaplan and Norton, 1993) is a common organizational performance measurement system, which is widely used in practice and has been extensively researched (Marr and Schiuma, 2003). The generic BSC model has been applied in the IS domain to measure performance of IT management (Bremser and Chung, 2005; Huang *et al.*, 2006; Kaplan and Norton, 2004).

Huang *et al.* (2006) developed a general BSC model of ISM, translating the ISM strategy map into a Scorecard model with four perspectives: financial, customer, internal process and learning and growth. In their study, the 80 performance indicators acquired from previous studies were transferred into 35 key performance indicators, 12 strategic themes and one generic model of ISM strategy map. Herath *et al.* (2010) also established a conceptual framework for strategic implementation of information security performance management using a BSC approach. Four interrelated perspectives were presented: business value, stakeholder orientation, internal process and future readiness. However, approaches that use the BSC model for ISM need further empirical investigation and validation. In our study, we will adapt the BSC model for evaluation of ISM and empirically verify it.

2.4 IT-business strategic alignment model

IT-business strategic alignment refers to the fit between IS strategy and business strategy in terms of addressing the needs, demands, goals, objectives and/or structures of each strategy and management (Gerow *et al.*, 2014). In the industrial environment, chief information officers have identified IT-business strategic alignment as the top management issue along with security and privacy as the second (Luftman *et al.*, 2006). Aligned firms are more likely to invest in IT and allocate resources to projects tied to overall business objectives and thus leverage IT to create competitive advantage (Cumps *et al.*, 2009; Rivard *et al.*, 2006). A meta-analysis confirmed the positive relationships between the alignment dimensions and performance outcomes (Gerow *et al.*, 2014). Following the same logic, we expect that in the ISM context when an organization's information security strategy is better aligned with the organization's business strategy, more organizational support will be given to ISM and at the operational level organizational awareness of information security will be improved, security controls can be better developed and finally the organization's ISM will be more successful. According to the foregoing literature review, business alignment was found to be one of the CSFs of ISM success and it is also correlated with other CSFs. Because ISM should be viewed strategically from the top (Dutta and McCrohan, 2002), security–business strategic alignment in ISM could be a starting point to organize all the CSFs toward ISM success. Therefore, this model provides us with a solid theoretical basis to study the relationships among business alignment, other CSFs and ISM performance. It also fits well with the value alignment as a proactive approach to manage value conflict and promote coordination between different parties in ISM.

3. Research model and hypothesis development

Our research model (Figure 1) investigates how the CSFs contribute to the success of an organization's ISM from a strategic value alignment perspective. This ISM success model has five constructs, business alignment, top management support, organizational awareness, security controls and ISM performance, which are measured from four dimensions: business value, internal process, user orientation and future readiness.

Business alignment refers to the fit between ISM strategy and business strategy in terms of addressing the needs, demands, goals, objectives and/or structures of ISM. An effective ISM strategy should be strategically focused and thus information security is perceived as an important core business issue (Kayworth and Whitten, 2010). It must secure information assets while still enabling the business. Scholars have pointed out that the protection of information assets from potential threats should be a part of business strategy because it can give the organization a competitive edge (Soomro *et al.*, 2016). The alignment component refers to the collaborative efforts between information security and business managers that can align ISM practices with business strategies of the organization (Chang *et al.*, 2011). This alignment could be achieved through information security planners' understanding of organizational objectives, mutual understanding between top management and information security planners and a heightened view of the information security function within the organization (Ma *et al.*, 2009).

Top management support refers to the commitment from top management. Through business alignment, information security initiatives are addressed at the strategic level and thus are more likely to be recognized and supported by top management (Johnston and Hale, 2009). Top management can thereby be more convinced of the importance of information security and more fully appreciate the importance of the ISM processes within the business framework (Smith and Jamieson, 2006; Werlinger *et al.*, 2009). Top management has a direct corporate governance responsibility of ensuring that all the information assets of the company are secure (Von Solms and Von Solms, 2004). A lack of fit between security objectives and business objectives may lead to situations where information security policies and budgets do not reflect the needs of the business (Kayworth and Whitten, 2010; Siponen and Oinas-Kukkonen, 2007). In such cases, investment decisions are driven by short-term priorities without well-conceived strategic priorities, and top management may pay little attention to information security and allocate insufficient resources to ISM (Kayworth and Whitten, 2010). Thus, the alignment helps to facilitate the acquisition and

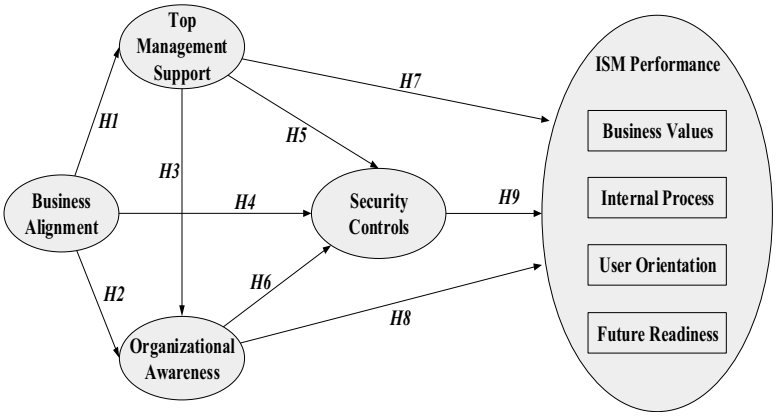

Figure 1.
Research model