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.