# Investigating the information security management role in smart city organisations

Mohamad Amin Hasbini
*College of Business Arts and Social Sciences, Brunel University, Uxbridge, UK*
Tillal Eldabi
*Brunel University, Uxbridge, UK, and*
Ammar Aldallal
*Department of Computer Engineering, Ahlia University, Manama, Bahrain*

## Abstract

**Purpose** – Information security management (ISM) is proving to be an important topic in the modern world; in environments that will rely a great deal on digital technologies, such as smart cities, ISM research is of high importance and needs to be well analysed. The paper aims to discuss these issues.
**Design/methodology/approach** – This paper indicates the criticality of ISM for smart cities through the literature, then focusses on top organisational factors influencing ISM in smart city organisations, which are embraced and justified from the literature.
**Findings** – This paper highlights the need for more research around ISM in the context of smart city organisations, also ISM-related organisational factors that are expected to most influence smart city organisational performance.
**Research limitations/implications** – This paper is proposed to influence more research in the area of ISM for smart cities among the research community. Additional research is also expected to further validate and examine the selected organisational factors.
**Originality/value** – This paper presents new information on ISM in smart city organisations, the lack of research in this area, and the criticality of the highlighted issues, creates high value for the conclusions and findings of this research. The paper also highlights top organisational factors that are expected to influence ISM in smart city organisations.

**Keywords** Corporate governance, Organizational performance, Information systems, Smart city, Information security management, Organizational factors

**Paper type** Research paper

## Introduction

Urbanisation is a globally intensifying phenomenon, by the year 2050, 2.5 billion more people will be living in cities, in which around 60 per cent of the infrastructure is yet to be build. Urban regions help better manage larger populations, while offering enhanced living quality, opportunities for growth and resources efficiency (Ramaswami *et al.*, 2016). With the global movement towards urbanisation and the widespread use of internet technologies, the concept of smart cities has drawn a lot of research interest and attention in recent years (Khatoun and Zeadally, 2016; Meijer and Bolívar, 2016; Angelidou, 2015). In particular, new technologies, such as the Internet of Things (IoT), Big Data, Data Analytics and cloud computing, are examples of supporting services and offerings for the future of urban life. Nonetheless, to ensure seamless operations for these smart cities, protecting information and infrastructure by maintaining robust information security

World Journal of Entrepreneurship, Management and Sustainable Development
Vol. 14 No. 1, 2018
pp. 86-98
Emerald Publishing Limited
2042-5961
DOI 10.1108/WJEMSD-07-2017-0042

becomes a necessity. Information security is considered to be of critical significance to the implementation and development of smart cities and one of its most serious challenges (Khatoun and Zeadally, 2016). The related governance processes and mechanisms also appear in the literature to be one of the most important pillars for the success of smart cities (Meijer and Bolívar 2016; Belissent, 2011), noting that such imply several challenges at the national and organisational levels.

The past few years have seen rapid development of the smart city concept. Numerous countries all around the world have already adopted smart city transformation programmes and are competing to achieve better and faster revolutions of their infrastructure. The IESE Cities in Motion Index (Berrone and Ricart, 2017) has also been developed since 2014 to annually update on cities progress and rank in the different smart city dimensions (human capital, economics, environment, social cohesion, urban planning, public management, etc.), current top-ranking cities include New York, London, Paris, etc.

Early studies on the smart city topic started with Komninos (2002) describing the different aspects of an intelligent city, but also discussing its competitive aspects, such as industrial, digital and learning capabilities. When discussing the characteristics of cities improvement, researchers such as Shapiro (2006) and Mulligan and Olsson (2013) discussed the impact on the quality of living and education by the increased urbanisation of metropolitan areas. In 2007, Giffinger *et al.*'s (2007) report on European smartness ranking expands the "smart city" concept to include evaluation measures and capabilities, to open the competition between European cities. Such measures include economy, people, governance, mobility, environment and living. Giffinger *et al.* (2007) developed 31 factors and 74 indicators for smart city ranking for 70 cities in the EU. Their main goal is reducing energy use and gas emissions by 2020. Hollands (2008) argues that smart cities should not be considered as large IT projects, whilst emphasising the human capital role in terms of education, creativity, innovation and entrepreneurship in determining the role and future of the city. Meijer and Bolívar (2016) also discussed the weight of smart city governance dimension and the need for strong infrastructure transformation abilities. Smart cities are proving to be an important phenomenon for urban living, promising better living for citizens; however, different challenges exist that need to be dealt with.

## ISM and related organisational factors in smart city organisations

Cyber security is well-researched topic in the literature, in their study, Cavusoglu *et al.* (2004) concluded that the cost of poor cyber security is high for stakeholders, with the breach impact not limited to a single organisation. They also concluded that the cost of a security breach for an internet only organisation is higher than for regular firms. Andoh-Baidoo and Osei-Bryson (2007) indicated that a security breach could have a negative impact on the organisation's performance, leading to lower revenues, higher expenses, a decrease in future prospects, in addition to a reduction in market value and investors trust. Goel and Shawky (2009) also investigated the cost of a security breach on an organisation that includes financial loss, client and partner loss, government sanctions, reputational loss and market value. In the context of smart cities, organisations are expected to be highly dependent on digital services and the ICT infrastructure, which, as per Cavusoglu *et al.* (2004), means that the impact of an information security breach will be larger than on any other type of organisations. The appropriate analysis of factors that impact information security issues in the smart city context requires careful consideration, being critical for the stability and sustainability of smart city organisational performance.

While information security has been justified to be of high importance for the safety of digital services, information security management (ISM) is noted to have an even higher significance in the context of smart cities being a combination of two of the smart city critical dimensions: information security and governance (Meijer and Bolívar 2016;

Sicari *et al.*, 2015). On the other hand, Chourabi *et al.* (2012) and Whitmore *et al.* (2015) confirm that little research has been done on smart cities' management and related organisational factors, even though previous research highlighted these as major challenges and success factors that need to be well examined. In addition, a literature assessment by Whitmore *et al.* (2015) indicated that literature is dominated by technology research, and that advanced technology services are not well represented in the management literature. On the other hand, as smart cities are purposed towards improved growth and development, it is imperative that smart city organisations deliver enhanced performance that matches the smart city objectives (Ahvenniemi *et al.*, 2017; Harrison *et al.*, 2010).

In an organisational environment, organisational performance is one of the most important aspects and is measured by different methods and characteristics. ICT technologies have long been known to have the potential of delivering important improvements in organisational performance (Brynjolfsson and Hitt, 1996; Sircar and Choi, 2007). They are also known to reshape organisational processes, structures, culture and even the job descriptions of employees (Fulford and Doherty, 2003; Markus, 2004). It has also long been identified that the real threat from information security issues lies in their consequential impact on organisational performance, such as reputation, productivity, financial loss or customer loss (Menzies, 1993). Smart cities are mainly composed of different types of organisations that rely a great deal on ICT technologies; smart cities' development evaluation will then come back to assessing an individual organisation's performance and efficiency.

Information assets protected by ISM represent a class of intangible capital, whose value is not easy to assess (Ittner and Larcker, 2003; Morgan and Strong, 2003). Multiple researchers have combined ISM with organisational performance to best understand its impact on organisational performance (Huang *et al.*, 2006; Hall *et al.*, 2011; Andoh-Baidoo and Osei-Bryson, 2007). The utilisation of the organisational performance angle in the context of this research is optimal to better understand organisational factors that influence ISM in smart city organisations, and therefore advance the aim of this research.

Drawing from the previously highlighted evidence on the importance of ISM in the smart city organisations, the lack of research in this area and the links in between OP and ISM, the aim of this research is to identify the ISM factors that most influence smart city organisational performance goals. It aims to assist towards developing a better understanding of ISM in the smart city organisational environment, whilst relying on research carried out in the ISM field for current and previous organisational environments.

## Selecting the ISM organisational factors that most influence the smart city organisation

As organisations drive online services mainstream to become the main enabler for a large share of their businesses, smart cities will have high mandates for reliability and CIA levels. ISM issues are expected to be more significant, leading the way towards the decisions and actions required to protect the smart city and its organisations. Research is needed to better examine ISM in smart cities, to identify factors and aspects that influence ISM in organisations, and how those reflect on performance. This research will be based on a literature analysis, or both "information security management factors in current organisations" and "smart cities organisational factors". The goal is to select the most influential factors that can impact ISM in the smart city organisations.

## The smart city organisation

As one of the smart city stakeholders, organisations are at the core of a city's operations. They are expected to offer quality living and opportunities for citizens; they are also expected to deliver services that are on the level of the city. Businesses are the main driver of a smart city, and are expected to leverage their infrastructure to offer better services; they

are also affected by the city's problems (Gann *et al.*, 2011). Businesses require long-term strategic studies and a vision of organisational evolution (Mulligan and Olsson, 2013). Kuk and Janssen (2011) highlight the need for a balanced approach between business models and information infrastructure to achieve short-term business goals without damaging innovation and service sustainability.

Anthopoulos and Fitsilis (2014) concluded that there were five types of organisations in smart city environments: public organisations handling state responsibilities; public-private partnerships where the government assigns the execution of projects to private companies; state-owned enterprises or new organisations that are created to develop or supervise a project; private companies that execute projects; and project companies that include alliances from different organisations to execute a project.

Research also highlights the important role of the citizen in a smart city, acting as the consumer but also using smart city participation utilities to send feedback and advance his quality of living, and acting as a developer of smart city services (Vilajosana *et al.*, 2013; Cardone *et al.*, 2013). While discussing smart city governance, Nam and Pardo (2014) describe the metrics for assessing smart governance initiatives by measuring efficiency, effectiveness, transparency and collaboration. They also categorise the smart governance challenges and opportunities as follows:

- technological factors that are needed to implement smart governance services running through the ICT infrastructure;
- organisational factors that consist of budgetary challenges, employees skills and organisational culture are to be considered to better enhance city efficiency and transparency; and
- cross-organisational challenges that mostly lie in inter-departmental or inter-agency information sharing, requiring a governance body to rule conflicts and control sharing agreements and cross-boundary collaboration.

Interaction with citizens is an important factor of collaboration in smart cities; feedback from the population is essential to best deliver transparent and efficient services.

*Organisational performance*

Organisational performance is a complex multi-dimensional phenomenon; it could be defined by multiple goals such as profit, growth and stakeholders' satisfaction, which are often in conflict with each other (Cameron, 1986; Chakravarthy, 1986; Venkatraman and Ramanujam, 1986). Researchers have proposed different measures of performance and evaluation of results; this has also opened the way to more difficulties, such as dealing with the different priorities that are assigned for organisational goals, and how each organisation could have different priorities. Other difficulties include the need to deal with fluctuating results, and how to define the success or failure of an organisation based on goals and priorities. Organisational performance in the context of complex smart city environments would bring new difficulties for the understanding of services, challenges, priorities and accountability, and in defining the key performance indicators that an organisation needs to attain. To cope with the smart city model, businesses need to adapt (Harrison *et al.*, 2010). ISM inside the smart city organisation therefore needs to be well-developed and maintained to meet maturity levels; failing to achieve this could cause a severe collapse of the organisational performance and therefore impact the success of smart city stakeholders.

## Information security and its management in the smart city

The smart city will run a highly interconnected infrastructure, which needs to be protected; it is a complex environment of interconnected systems. Threats to the critical infrastructure

could have devastating results on national security, the economy and citizens. Information security and privacy maturity must be taken to new levels before IoT and sensors can be deployed on a larger scale (Sicari *et al.*, 2015; Bekara, 2014; Gubbi *et al.*, 2013; Li *et al.*, 2012; Marias *et al.*, 2011; Kitchin, 2014; Ruiz-Romero *et al.*, 2014; Martinez-Balleste *et al.*, 2013; Elmaghraby and Losavio, 2014).

The management of information security is essential for protecting the interest of shareholders and the business. This relies on information-based services that are widely available today; information security maturity and control is not an investment but a necessity for survival in the modern world. The role of ISM within organisational governance is to define best practices, a means of managing costs efficiently, improve employee behaviour, strengthen business controls and define accountability. Establishing ISM requires the involvement of senior management, sharing of information and visibility on occurrences and incidents is not only important for business success, but also to ensure alignment with business goals; these include the prioritisation of selective security investments that best minimise risks (Williams, 2001; Nam and Pardo, 2014; Herath and Herath, 2009). While smart applications are expected to be widely deployed and reachable in a smart city (Zanella *et al.*, 2014), information security problems are expected to surge (Whitmore *et al.*, 2015), threatening not only the CIA triad of data protection but also the usability of digital services.

The impact of falling to ISM malpractices could have catastrophic results on an organisation's business. Von Solms and von Solms (2004) detail the impact that ISM could have on the organisational level; this includes resources and financial loss, mis-prioritised investments, a false sense of security, serious accountability on executive management, operational frustration and blame on information security departments for incidents, in addition to the non-compliance of users with the security policy. However, even though smart governance is a major aspect of the city, there is a lack of literature about smart cities that address smart governance issues (Chourabi *et al.*, 2012). The governance of the information security aspects will be highly delicate; the right decisions need to be made to protect not only the businesses, but also the resources and citizens. The lack of development in this area is another indicator of a need for more research and efforts to be exerted.

## Literature review on organisational factors and ISM

A review of the literature was conducted to gain more insight into factors that would influence ISM in the context of smart city organisations. The literature clearly highlights the influence of organisational factors on information security's conduct in organisational environments, and therefore their severe impact on organisational performance. The literature review conducted was systematic and attempted to identify and map most common organisational factors related to ISM inside organisations. Another literature review was then conducted to identify and map the organisational factors that influence smart city organisations. The literature quest was carried out using prevalent sources and an initial search for source identification was conducted in SCOPUS, Science Direct and Google Scholar. The queries that were used contained "smart city" and other research relevant terms (i.e. "information security", "ISM", "organisational factors", "organisational performance", "smart city", "smart city organisation", etc.).

### *Research scope and limitations*

While the literature is well-developed around ISM-related organisational factors in current world organisations, little research has been found in the literature around ISM in smart city organisations or smart city organisational factors. This is a research area that requires more exploration; this is being attempted in this research.

*ISM organisational factors in current organisations*

There is a wide range of organisational factors that impact information security in organisations. These are scattered in the literature and discussed in the context of each research paper. As shown in Table I, the most prevalent and cited organisational factors that impact modern organisations growth and prosperity had visibility over the literature emphasis and identified the most discussed aspects. The citation frequency is the number of scholarly documents in which the organisational factor was found.

*Smart city governance linked organisational factors*

There is a wide range of organisational factors that impact organisations in smart city environments. They are disseminated in the literature and discussed in the context of each research paper.

Table II shows the most prevalent and cited organisational factors that impact the growth of smart city organisations and their prosperity. The aim of the table is to have visibility over the literature emphasis and identify the most discussed aspects.

*Selected organisational factors that are expected to most influence ISM in smart city organisations*

After identifying the organisational factors that influence ISM and smart city organisations, ten factors were selected to be further analysed and investigated. Selected factors are expected to have a high influence on the smart city organisational ISM. The justification of the selection is then further rationalised.

*Leadership attitude*. Multiple researchers highlighted the importance of leadership attitude in smart city organisational environments (AlAwadhi and Scholl, 2013; Nam and Pardo, 2013; Giffinger *et al.*, 2007). Leadership attitude in matters of information security is also noted as an important aspect of organisational performance (Ashenden and Sasse, 2013). Therefore, in an

| Category/organisational factor | Organisational factor | Citation frequency |
|---|---|---|
| Business IT alignment | | 22 |
| Information security leadership issues | Employees engagement | 1 |
| | Organisational identity of the CISO | 1 |
| | Lack of confidence | 1 |
| Organisational size | | 8 |
| Organisational type of industry | | 4 |
| Uncertainty of environmental elements | Rapid change of technology and complexity of such | 4 |
| | Competitors' behaviour | 3 |
| | Customer security requirements | 1 |
| | Changes in legislation | 1 |
| Organisational support | Top management support | 16 |
| | Information security projects financing priority | 6 |
| | Organisational structure effectiveness | 10 |
| Organisational awareness | Staff and management, awareness and training | 13 |
| | Information security culture | 3 |
| | IT competencies | 11 |
| Security controls' development | Risk management | 7 |
| | Security policies implementation | 5 |
| | Standards compliance | 9 |
| | Performance evaluation, controls effectiveness and quality assurance | 14 |

**Source:** Devised by authors

**Table I.** ISM organisational factors in current organisations

| Organisational factor(s) | Citation frequency |
|---|---|
| Project size | 1 |
| Organisational diversity | 1 |
| Alignment of organisational goals with business | 1 |
| Compliance to change | 1 |
| Leadership, managers' attitudes and behaviour | 3 |
| Legislative compliance, reformed governance and regulations | 7 |
| Vendor independence | 5 |
| Financial resources | 2 |
| Human capital | 9 |
| Organisational innovation and transformation | 6 |
| Partners' and stakeholders' role and participation | 4 |
| Government role, influence and support | 1 |
| Complexity and rapid technological changes | 6 |
| Best utilisation of the ICT infrastructure | 4 |
| Type of organisation and business model | 2 |
| Type of industry | 2 |
| Bureaucracy | 1 |
| Organisational structure | 2 |
| Collaboration, cross/inter-organisational or inter-agency factors and interdependencies | 8 |
| Inter-departmental governance and collaboration | 3 |
| Inter-organisational competition | 3 |
| Organisational risk management | 2 |

**Source:** Devised by authors

**Table II.**
Smart city linked organisational factors

environment such as smart cities, which rely a great deal on digital infrastructure that is more criticality assigned to information security issues (Sicari *et al.*, 2015; Bekara, 2014; Gubbi *et al.*, 2013), leadership attitude towards ISM is expected to have higher consequences on overall business continuity and growth.

*Legislative compliance and government influence*. Smart city governments are expected to have high levels of engagement with city components and stakeholders, ensuring that government and citizen data does not get misused. Legislative compliance in matters of information security is then extremely important for the organisations (Backhouse *et al.*, 2006; Chang and Ho, 2006; von Solms, 2005; von Solms and von Solms, 2004). Compliance should have higher priority in the context of smart city environments due to the higher criticality of information security issues (Sicari *et al.*, 2015; Bekara, 2014; Gubbi *et al.*, 2013). Non-compliance with legislation might be the source of great damage to organisational performance and national security (Gubbi *et al.*, 2013; Amin, 2002; Ruiz-Romero *et al.*, 2014; Naphade *et al.*, 2011); this could lead to government sanctions (Goel and Shawky, 2009) and serious accountability for executives (von Solms and von Solms, 2004).

*Adaptation to rapid technology development*. In fast paced complex environments, such as smart cities, organisational changes need to follow the pace of the environment. It is essential to stay up-to-date with legislative, structural and processes adaptation to rapid technological developments (Zanella *et al.*, 2014; Hernández-Muñoz *et al.*, 2011 Gil-Garcia *et al.*, 2014). ISM is expected to follow the pace of the changes, adapting to new services and features, defending against new types of threats and weaknesses.

*Vendor selection and management*. Research has discussed the importance of the selection of smart city vendors and their independence (Mulligan and Olsson, 2013; Kitchin, 2014; Hollands, 2008, 2015). This is to protect organisations against monopolies, push for standardisation and protect competitiveness between technology vendors. Managing

information security technology requirements and selection is expected to be more challenging for ISM departments in smart city organisations.

*Human capital*. Human knowledge and skills are major influence factors of advanced environments such as smart cities. Managing the development of human capital inside organisations is of great importance for the protection of an organisation and for maintaining safe production services (Chang *et al.*, 2011; Eloff and Eloff, 2003; Bassellier *et al.*, 2001; Gil-Garcia and Pardo, 2005). Information security aspects are expected to have high importance in smart city environments; citizens' and workers' awareness of information security threats and challenges are expected to be different. Smart cities are expected to do their best to attract skilled labour (Caragliu *et al.*, 2011; Hollands, 2008; Toppeta, 2010).

*Better utilisation of the ICT infrastructure*. ICT technologies have long been known to positively impact organisational performance (Brynjolfsson and Hitt, 1996; Sircar and Choi, 2007). They also have a role in reshaping organisational processes, structures and cultures, and even the job descriptions of employees (Fulford and Doherty, 2003; Markus, 2004). As smart city organisations are expected be highly dependent on the ICT infrastructure (Dameri, 2013), it is anticipated that smart city organisations will research how to benefit more from that infrastructure (Nam and Pardo, 2011; Mulligan and Olsson, 2013; Gil-Garcia and Aldama-Nalda, 2013; Gann *et al.*, 2011). This is not only for better performance and more features but also to protect the information flows and availability, which need to be adapted and controlled adequately.

*Type of organisation and business model*. Developing strategies to protect the information assets in an organisation is the role of the ISM (Williams, 2001; Moulton and Coles, 2003; Zafar and Clark, 2009; Johnston and Hale, 2009); however, the information security role is different from one organisation to another. Smart city organisations are also expected to be different from current organisations (Kuk and Janssen, 2011; Anthopoulos and Fitsilis, 2014), therefore requiring modified strategies towards the protection of their data, services and businesses.

*Bureaucracy*. Excessively complicated procedures inside organisations are the cause of delays, clients' disappointment and loss of business. In smart city organisations, bureaucracy is anticipated to have a higher impact on the business and its safety (Toppeta, 2010; Nam and Pardo, 2013). Not being able to approve a decision, a change, a test or a budget in a timely manner could be the cause of a breach or loss of competitive edge and reputation; this could then result in the imposition of government sanctions (Goel and Shawky, 2009; von Solms and von Solms, 2004).

*Organisational support*. As organisations in smart cities are anticipated to be more dependent on the digital infrastructure, being a core tool in modern economies (Dutta and Mia, 2010; Audretsch and Welfens, 2013), the overall support of the organisation to the information security department role in the context of smart city organisations is expected to be higher; this is because the department is in charge of protecting the business goals and objectives (Johnston and Hale, 2009; Chang and Ho, 2006; Posthumus and von Solms, 2004).

*Inter- and intra-organisational collaboration*. The collaboration between different departments inside an organisation is essential for achieving its objectives through efficient decision making, conflicts resolution (Sila, 2010), etc. Intra-organisational collaboration is expected to be of higher importance for the development of a smart city organisation, especially in the context of ISM, where innovation and problem solving needs to be delivered quickly (Kitchin, 2014). Therefore, this requires timely decision making and highly efficient communication skills and tools, all prioritisation to be performed by top management. On the other hand, collaboration between organisations is important for sharing experience and learning about new threats and challenges (Bekara, 2014); such collaboration would

also enhance defence capabilities against attackers. In the context of smart city organisations, inter-organisational collaboration is anticipated to be of utmost importance for the overall defence of organisations against new threats and weaknesses (Hawryszkiewycz, 2014). Inter-organisational collaboration is also expected to happen directly between business clients and partners, to secure data communication, share latest threat information and guarantee safe collaboration: this is a mutual benefit.

## Conclusions

Analysing the efforts being put into the development of smart city and IoT solutions, a great deal is being done to define technologies and solutions to deal with the ICT infrastructure, to develop services and tools for the businesses and the infrastructure, which will benefit smart city advanced services, performance and sustainability. The lack of security consideration in the development of smart city solutions should not be justified by sustainability and cost effectiveness goals. It will be a root cause for problems that could only cause damage and losses and therefore delay the diffusion of the smart city concept globally. Information security issues will also place more dependence and accountability on robust and wise management of ICT security threats; smart governance will be significant in strategically driving business assurance and security to run over safe environments mitigating the smartness digital downsides.

More research is needed to solve the current issues with information security governance for smart cities; this is in order to best comply with needs and requirements, also helping the control and management of future cyber threats. In this paper we discussed smart city issues related to information security governance, we highlighted the significance of information security and ISM issues for smart city organisations and the lack of research in this area, we also selected the ISM-related organisational factors that are expected to be most influential on the smart city organisational performance.

## References

Ahvenniemi, H., Huovila, A., Pinto-Seppä, I. and Airaksinen, M. (2017), "What are the differences between sustainable and smart cities?", *Cities*, Vol. 60, Part A, pp. 234-245.

AlAwadhi, S. and Scholl, H.J. (2013), "Aspirations and realizations: the smart city of Seattle", *46th Hawaii International Conference in System Sciences (HICSS), IEEE, January*, pp. 1695-1703.

Amin, M. (2002), "Security challenges for the electricity infrastructure", *Computer*, Vol. 35 No. 4, pp. supl8-supl10, available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=1012423

Andoh-Baidoo, F.K. and Osei-Bryson, K.M. (2007), "Exploring the characteristics of internet security breaches that impact the market value of breached firms", *Expert Systems with Applications*, Vol. 32 No. 3, pp. 703-725.

Angelidou, M. (2015), "Smart cities: a conjuncture of four forces", *Cities*, Vol. 47, September, pp. 95-106.

Anthopoulos, L. and Fitsilis, P. (2014), "Exploring architectural and organizational features in smart cities", *Advanced Communication Technology (ICACT), 16th International Conference, IEEE, February*, pp. 190-195.

Ashenden, D. and Sasse, A. (2013), "CISOs and organisational culture: their own worst enemy?", *Computers & Security*, Vol. 39, Part B, pp. 396-405.

Audretsch, D.B. and Welfens, P.J. (Eds) (2013), *The New Economy and Economic Growth in Europe and the US*, Springer Science & Business Media, Berlin.

Backhouse, J., Hsu, C.W. and Silva, L. (2006), "Circuits of power in creating De Jure standards: shaping an international information systems security standard", *MIS Quarterly*, Vol. 30, August, pp. 413-438.

Bassellier, G., Reich, B.H. and Benbasat, I. (2001), "Information technology competence of business managers: a definition and research model", *Journal of Management Information Systems*, Vol. 17 No. 4, pp. 159-182.

Bekara, C. (2014), "Security issues and challenges for the IoT-based smart grid", *Procedia Computer Science*, Vol. 34 No. 2014, pp. 532-537.

Belissent, J. (2011), "The core of a smart city must be smart governance", available at: www.forrester.com/Jennifer-Belissent%2C-Ph.D.

Berrone, P. and Ricart, J.E. (2017), *IESE Cities in Motion Index*, IESE Business School, University of Navarra, Navarra, available at: www.iese.edu/research/pdfs/ST-0442-E.pdf

Brynjolfsson, E. and Hitt, L. (1996), "Paradox lost? Firm-level evidence on the returns to information systems", *Management Science*, Vol. 42 No. 4, pp. 541-558.

Cameron, K. (1986), "Effectiveness as paradox: consensus and conflict in conceptions of organizational effectiveness", *Management Science*, Vol. 32 No. 5, pp. 539-553.

Caragliu, A., Del, Bo, C. and Nijkamp, P. (2011), "Smart cities in Europe", *Journal of Urban Technology*, Vol. 18 No. 2, pp. 65-82.

Cardone, G., Foschini, L., Bellavista, P., Corradi, A., Borcea, C., Talasila, M. and Curtmola, R. (2013), "Fostering participation in smart cities: a geo-social crowdsensing platform", *IEEE Communications Magazine*, Vol. 51 No. 6, pp. 112-119.

Cavusoglu, H., Mishra, B. and 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*, Vol. 9 No. 1, pp. 70-104.

Chakravarthy, B.S. (1986), "Measuring strategic performance", *Strategic Management Journal*, Vol. 7 No. 5, pp. 437-458.

Chang, S.E. and Ho, C.B. (2006), "Organizational factors to the effectiveness of implementing information security management", *Industrial Management & Data Systems*, Vol. 106 No. 3, pp. 345-361.

Chang, S.E., Chen, S.-Y. and Chen, C.-Y. (2011), "Exploring the relationships between it capabilities and information security management", *International Journal of Technology Management*, Vol. 54 Nos 2/3, pp. 147-166.

Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J.R., Mellouli, S., Nahon, K., Pardo, T.A. and Scholl, H.J. (2012), "Understanding smart cities: an integrative framework", *Proceedings of the 45th Hawaii International Conference on System Sciences*, pp. 2289-2297.

Dameri, R.P. (2013), "Searching for smart city definition: a comprehensive proposal", *International Journal of Computers & Technology*, Vol. 11 No. 5, pp. 2544-2551.

Dutta, S. and Mia, I. (2010), "The global information technology report 2009-2010", World Economic Forum and INSEAD, SRO-Kundig, Geneva.

Elmaghraby, A.S. and Losavio, M.M. (2014), "Cyber security challenges in smart cities: safety, security and privacy", *Journal of Advanced Research*, Vol. 5 No. 4, pp. 491-497.

Eloff, J.H.P. and Eloff, M. (2003), "Information security management: a new paradigm", *Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology (SAICSIT 2003), South African Institute for Computer Scientists and Information Technologists*, pp. 130-136.

Fulford, H. and Doherty, N.F. (2003), "The application of information security policies in large UK-based organizations", *Information Management and Computer Security*, Vol. 11 No. 3, pp. 106-114.

Gann, D.M., Dodgson, M. and Bhardwaj, D. (2011), "Physical-digital integration in city infrastructure", *IBM Journal of Research and Development*, Vol. 55 Nos 1/2, pp. 8:1-8:10.

Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanovic, N. and Meijers, E. (2007), "Smart cities: ranking of European medium-sized cities", final report, Centre of Regional Science, Vienna UT.

Gil-Garcia, J.R. and Aldama-Nalda, A. (2013), "Making a city smarter through information integration: angel network and the role of political leadership", *46th Hawaii International Conference on System Sciences (HICSS), IEEE, January*, pp. 1724-1733.

Gil-Garcia, J.R. and Pardo, T.A. (2005), "E-government success factors: mapping practical tools to theoretical foundations", *Government Information Quarterly*, Vol. 22 No. 2, pp. 187-216.

Gil-Garcia, J.R., Helbig, N. and Ojo, A. (2014), "Being smart: emerging technologies and innovation in the public sector", *Government Information Quarterly*, Vol. 31, Supplement 1, pp. I1-I8.

Goel, S. and Shawky, H.A. (2009), "Estimating the market impact of security breach announcements on firm values", *Information & Management*, Vol. 46 No. 7, pp. 404-410.

Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M. (2013), "Internet of things (IoT): a vision, architectural elements, and future directions", *Future Generation Computer Systems*, Vol. 29 No. 7, pp. 1645-1660.

Hall, J.H., Sarkani, S. and Mazzuchi, T.A. (2011), "Impacts of organizational capabilities in information security", *Information Management & Computer Security*, Vol. 19 No. 3, pp. 155-176.

Harrison, C., Eckman, B., Hamilton, R., Hartswick, P., Kalagnanam, J., Paraszczak, J. and Williams, P. (2010), "Foundations for smarter cities", *IBM Journal of Research and Development*, Vol. 54 No. 4, pp. 1-16, doi: 10.1147/JRD.2010.2048257.

Hawryszkiewycz, I.T. (2014), "Cloud requirements for facilitating business collaboration: a modeling perspective", *Journal of Organizational Computing and Electronic Commerce*, Vol. 24 Nos 2/3, pp. 174-185.

Herath, H. and Herath, T. (2009), "Investments in information security: a real options perspective with Bayesian post-audit", *Journal of Management Information Systems*, Vol. 25 No. 3, pp. 337-375.

Hernández-Muñoz, J.M., Vercher, J.B., Muñoz, L., Galache, J.A., Presser, M., Gómez, L.A.H. and Pettersson, J. (2011), "Smart cities at the forefront of the future internet", *The Future Internet Assembly*, Springer, Berlin, Heidelberg, pp. 447-462.

Hollands, R.G. (2008), "Will the real smart city please stand up? Intelligent, progressive or entrepreneurial?", *City*, Vol. 12 No. 3, pp. 303-320.

Hollands, R.G. (2015), "Critical interventions into the corporate smart city", *Cambridge Journal of Regions, Economy and Society*, Vol. 8 No. 1, pp. 61-77.

Huang, S.M., Lee, C.L. and Kao, A.C. (2006), "Balancing performance measures for information security management: a balanced scorecard framework", *Industrial Management & Data Systems*, Vol. 106 No. 2, pp. 242-255.

Ittner, C.D. and Larcker, D.F. (2003), "Coming up short on nonfinancial performance measurement", *Harvard Business Review*, Vol. 81 No. 11, pp. 88-95.

Johnston, A.C. and Hale, R. (2009), "Improved security through information security governance", *Communications of the ACM*, Vol. 52 No. 1, pp. 126-129.

Khatoun, R. and Zeadally, S. (2016), "Smart cities: concepts, architectures, research opportunities", *Communications of the ACM*, Vol. 59 No. 8, pp. 46-57.

Kitchin, R. (2014), "The real-time city? Big data and smart urbanism", *GeoJournal*, Vol. 79 No. 1, pp. 1-14.

Komninos, N. (2002), *Intelligent Cities: Innovation, Knowledge Systems and Digital Spaces*, 1st ed., Routledge, London.

Kuk, G. and Janssen, M. (2011), "The business models and information architectures of smart cities", *Journal of Urban Technology*, Vol. 18 No. 2, pp. 39-52.

Li, W., Chao, J. and Ping, Z. (2012), "Security structure study of city management platform based on cloud computing under the conception of smart city", *Fourth International Conference on Multimedia Information Networking and Security (MINES), IEEE*, pp. 91-94.

Marias, G., Barros, J., Fiedler, M., Fischer, A., Hauff, H., Herkenhoener, R., Grillo, A., Lentini, A., Lima, L., Lorentzen, C., Mazurczyk, W., Meer, H., Oliveira, P., Polyzos, G., Pujol, E., Szczypiorski, K., Vilela, J. and Vinhoza, T. (2011), "Security and privacy issues for the network of the future", *Security and Communication Networks*, Vol. 5 No. 9, pp. 987-1005.

Markus, M.L. (2004), "Technochange management: using IT to drive organizational change", *Journal of Information Technology*, Vol. 19 No. 1, pp. 4-20.

Martinez-Balleste, A., Perez-Martinez, P. and Solanas, A. (2013), "The pursuit of citizens' privacy: a privacy-aware smart city is possible", *IEEE Communications Magazine*, Vol. 51 No. 6, pp. 136-141.

Meijer, A. and Bolívar, M.P.R. (2016), "Governing the smart city: a review of the literature on smart urban governance", *International Review of Administrative Sciences*, Vol. 82 No. 2, pp. 392-408.

Menzies, R. (1993), "Information systems security", *IT Strategy for Business*, Pitman Publishing, London.

Morgan, R.E. and Strong, C.A. (2003), "Business performance and dimensions of strategic orientation", *Journal of Business Research*, Vol. 56 No. 3, pp. 163-176.

Moulton, R. and Coles, R. (2003), "Applying information security governance", *Computers & Security*, Vol. 22 No. 7, pp. 580-584.

Mulligan, C.E. and Olsson, M. (2013), "Architectural implications of smart city business models: an evolutionary perspective", *IEEE Communications Magazine*, Vol. 51 No. 6, pp. 80-85.

Nam, T. and Pardo, T.A. (2011), "Smart city as urban innovation: focusing on management, policy, and context", *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance, ACM, September*, pp. 185-194.

Nam, T. and Pardo, T.A. (2013), "Building understanding of municipal service integration: a comparative case study of NYC311 and Philly311", *46th Hawaii International Conference on System Sciences (HICSS), IEEE, January*, pp. 1953-1962.

Nam, T. and Pardo, T.A. (2014), "The changing face of a city government: a case study of Philly311", *Government Information Quarterly*, Vol. 31, Supplement 1, pp. S1-S9.

Naphade, M., Banavar, G., Harrison, C., Paraszczak, J. and Morris, R. (2011), "Smarter cities and their innovation challenges", *Computer*, Vol. 44 No. 6, pp. 32-39.

Posthumus, S. and von Solms, R. (2004), "A framework for the governance of information security", *Computers & Security*, Vol. 23 No. 8, pp. 638-646.

Ramaswami, A., Russell, A.G., Culligan, P.J., Sharma, K.R. and Kumar, E. (2016), "Meta-principles for developing smart, sustainable, and healthy cities", *Science*, Vol. 352 No. 6288, pp. 940-943.

Ruiz-Romero, S., Colmenar-Santos, A., Mur-Pérez, F. and López-Rey, Á. (2014), "Integration of distributed generation in the power distribution network: the need for smart grid control systems, communication and equipment for a smart city – use cases", *Renewable and Sustainable Energy Reviews*, Vol. 38, October, pp. 223-234.

Shapiro, J. (2006), "Smart cities: quality of life, productivity, and the growth effects of human capital", *The Review of Economics and Statistics*, Vol. 88 No. 2, pp. 324-335.

Sicari, S., Rizzardi, A., Grieco, L. and Coen-Porisini, A. (2015), "Security, privacy and trust in internet of things: the road ahead", *Computer Networks*, Vol. 76, January, pp. 146-164.

Sila, I. (2010), "Do organisational and environmental factors moderate the effects of internet-based interorganisational systems on firm performance?", *European Journal of Information Systems*, Vol. 19 No. 5, pp. 581-600.

Sircar, S. and Choi, J. (2007), "A study of the impact of information technology on firm performance: a flexible production function approach", *Information Systems Journal*, Vol. 19 No. 3, pp. 313-330, doi: 10.1111/j.1365-2575.2007.00274.x.

Toppeta, D. (2010), *The Smart City Vision: How Innovation and ICT Can Build Smart, "Livable", Sustainable Cities*, The Innovation Knowledge Foundation, Milano.

Venkatraman, N. and Ramanujam, V. (1986), "Measurement of business performance in strategy research: a comparison of approaches", *Academy of Management Review*, Vol. 11 No. 4, pp. 801-814.

Vilajosana, I., Llosa, J., Martinez, B., Domingo-Prieto, M., Angles, A. and Vilajosana, X. (2013), "Bootstrapping smart cities through a self-sustainable model based on big data flows", *IEEE Communications Magazine*, Vol. 51 No. 6, pp. 128-134.

von Solms, B. (2005), "Information security governance: COBIT or ISO 17799 or both?", *Computers & Security*, Vol. 24 No. 2, pp. 99-104.

von Solms, B. and von Solms, R. (2004), "The 10 deadly sins of information security management", *Computers & Security*, Vol. 23 No. 5, pp. 371-376.

Whitmore, A., Agarwal, A. and Da Xu, L. (2015), "The internet of things – a survey of topics and trends", *Information Systems Frontiers*, Vol. 17 No. 2, pp. 261-274.

Williams, P. (2001), "Information security governance", *Information Security Technical Report*, Vol. 6 No. 3, pp. 60-70.

Zafar, H. and Clark, J.G. (2009), "Current state of information security research in IS", *Communications of the Association for Information Systems*, Vol. 24 No. 34, pp. 557-596.

Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014), "Internet of things for smart cities", *IEEE Internet of Things Journal*, Vol. 1 No. 1, pp. 22-32.

## Further reading

Atzori, L., Iera, A. and Morabito, G. (2010), "The internet of things: a survey", *Computer Networks*, Vol. 54 No. 15, pp. 2787-2805.

Ross, J.W., Beath, C.M. and Goodhue, D.L. (1996), "Develop long-term competitiveness through IT assets", *Sloan Management Review*, Vol. 38 No. 1, pp. 31-42.

## About the authors

Mohamad Amin Hasbini joined Kaspersky Lab in 2013 as a Senior Security Researcher in the Global Research & Analysis Team. He is responsible for the Kaspersky expert positioning in the Middle East and Africa, research development and knowledge support of the regional office in Dubai, UAE. Prior to joining Kaspersky Lab, Amin was a Senior Information Security and a Privacy Consultant at Deloitte & Touche Middle East, and before that a Security Network Engineer at Data Consult Lebanon. He also taught multiple official information security courses (Cisco, Ec-Council). Amin is specialised in cyber and advanced persistent threats and defence, penetration testing and malware landscape. Mohamad Amin Hasbini is the corresponding author and can be contacted at: mohamad.hasbini@brunel.ac.uk

Dr Tillal Eldabi is a Senior Lecturer at Brunel Business School, Brunel University, UK, and the Director of the PhD Degree without Residence Programme. He has received PhD Degree in Simulation Modelling. Since the late 1990s, Dr Eldabi has published over 100 articles in highly accredited journals and refereed conferences. He has successfully supervised 15 PhD students to completion. He led and co-investigated several research projects with ranges amounting to more than a £1M. His consulting expertise includes developing a modelling approach to enable stakeholder engagement, modelling to identify bottlenecks, modelling to support A&E departments, brainstorming sessions to identify information requirements. Dr Eldabi has led a number of international collaborative projects by United Nations Development Programme (UNDP) and the UK.

Ammar Aldallal, an Assistant Professor, a Member of Computer Engineering Department, Ahlia University. He received his PhD Degree in Information Systems and Computing at the Brunel University in 2012. In 1997, he received his Master's Degree in Computer Science, College of Engineering at the Kuwait University, State of Kuwait. In 1995, he received a Bachelor Degree in Computer Engineering at the Kuwait University, State of Kuwait. Dr Ammar joined Ahlia University of Bahrain in September 2012 as an Assistant Professor of the Computer Engineering Department. He conducted research in the area of information retrieval, genetic algorithm and its applications in optimisation problems and computer security. He also serves as a Paper Reviewer for a number of international journals. Aldallal has ten published papers, two accepted papers, and two research in progress articles.