

*INVESTIGATING THE
ORGANIZATIONAL FACTORS
INFLUENCING INFORMATION
SECURITY MANAGEMENT IN THE
CONTEXT OF SMART CITY
ORGANIZATIONS*



Mohamad Amin Hasbini

Business School

Brunel University London

This dissertation is submitted for the degree of Doctor of Philosophy

April 2019

Dedication

I dedicate this work to the most important pillars of my life, first and foremost, my unconditionally caring parents (AbdelKarim, Amneh) who sacrificed their lives and all effort to pursue the smarter choices towards our education and personal development, lessons for life; and to my precious wife Houda and children (Yasmin, Karim) for their extended patience and support during this lengthy journey. I would also like to dedicate this work to some of my first mentors and philosophic influencers, namely Dr Riyad Bazo, Mr Ghassan AbulNasr (RIP), Mr Rami Wehbe, Mr Marc Nader, Mr Fadi Aoun, Dr Tony Feghaly, Dr Mohammad AlHammouri, Mr Adnan Ibrahim, Mr Fadi Mutlak.

Quote

لا يزال المرء عالما ما طلب العلم، فإن ظن أنه عالم فقد جهل.

-ابن قتيبة (٨٢٨-٨٨٩ م.)-

An individual still seeks knowledge to become knowledgeable, if he then thinks he is knowledgeable then he has become ignorant.

-Ibn Qutaiba (828-889 A.D.)-

Acknowledgements

All praise is due to Allah, the Lord of the Worlds. The Generous, the Merciful. Master of the Day of Judgment. Thee do we serve and Thee do we beseech for help. Keep us on the right path.

I would like to thank the many people in many countries who allowed this work to reach its current standing. Special mention goes to my PHD supervisor, Dr Tillal Eldabi, for an excellent supervision and unlimited support throughout the PhD. The guidance and support received have helped shape this work and maximize the learning experience.

Similarly, profound gratitude goes to Dr Ramzi Elhaddadeh, Professor Mansour AIAli, Dr Ammar Aldallal, Dr Anjum Razzaque, Dr Osama AIAli, Hasan Ghorra. Their comments and pointers helped me find the way during this long and rough journey.

Lastly I would like to thank my country, Lebanon, the piece of heaven on earth and my pride, for passing me the philosophy and the mindset of being what I am today.

Appreciation and Recognition

Symposium Presentations – presented

Certificate of appreciation, PWR Doctoral symposium, 2016

Certificate of appreciation, PWR Doctoral symposium, 2017

Certificate of appreciation, PWR Doctoral symposium, 2018

Best Symposium presentation award, PWR Doctoral symposium, 2017

Certificate of appreciation, World Association for Sustainable Development, 2017

Symposium paper – accepted/published

Hasbini, MA., Eldabi T., Aldallal, A. (2017) 'Investigating the role of Information security management in smart city organizations' PWR Doctoral symposium, 2017

Journal paper – accepted/published

Hasbini, M.A., Eldabi, T. and Aldallal, A. (2018). Investigating the information security management role in smart city organisations. *World Journal of Entrepreneurship, Management and Sustainable Development*, 14(1), 86-98.

Other published reports/whitepapers

Cerrudo, C., Hasbini, M.A., Russell, B. (2015). Cyber security guidelines for smart city technology adoption. *Cloud Security Alliance*.

Hasbini, M.A., Ayoub, R., Tom-Petersen, M., Falletta, L., Jordan, D. and Seow, A. (2017). Smart Cities Cyber Crisis Management. *Securing Smart Cities*.

Hasbini, M.A., Cerrudo, C., Jordan, D., El-Haddadeh, R., Seow, A. and Pawaskar, S. (2016). The Smart City Department Cyber Security role and implications. *Securing Smart Cities*.

Hasbini, M.A. and Tom-Petersen, M. (2017). The Smart Cities Internet of Access Control, opportunities and cybersecurity challenges. *Securing Smart Cities*.


Hasbini, M.A., Tom-Petersen, M., Cerrudo, C. (2017) Securing the Smart City Olympics. *Securing Smart Cities*.

Russell, B., Hasbini, M.A., Tom-Petersen, M. (2017). Establishing a Safe and Secure Municipal Drone Program. *Cloud Security Alliance*.

Declaration

This dissertation is the result of my own work and includes nothing that is the outcome of work done in collaboration except where specifically indicated in the text. It has not been previously submitted, in part or whole, to any university or institution for any degree, diploma, or other qualification.

In accordance with the Brunel College of Business, Arts and Social Sciences guidelines, this thesis does not exceed 80,000 words, and contains fewer than 150 figures.

Signed:  _____

Date:  _____

Mohamad Amin Hasbini

Brunel

Abstract

Smart city (SC) research has undergone remarkable advances in recent years. Smart cities have been touted as the next phase of urbanization, whereby cities efficiently deploy resources, rely on a high quality Information and Communication Technologies (ICT) infrastructure, develop human capital, and improve the quality of life of its citizens. However, the adoption of digital technologies poses challenges. Research confirms the criticality of the information security issues in smart cities where digital services are key for modern businesses. As such, organizations need to effectively manage their information security to meet the necessities of online services, to protect data, and to limit and control any possible damage if vulnerabilities are exposed. There are different organizational factors that influence Information Security Management inside organizations, including project size, management and leadership behaviour, business type and model, awareness, financial resources, and human capital. However, it can be inferred from the literature that little research has been conducted on smart city management issues. Therefore, to best meet the smart city performance goals, there is a need to investigate the organizational factors that influence Information Security Management in the smart city organization.

The aim of this paper is to identify and examine the organizational factors that are expected to influence Information Security Management of smart city organizations. First, the literature is explored to cultivate a better understanding of the literature; Information Security Management is highlighted as an important subject in smart cities. The research then consolidated the organizational factors that are expected to be most influential on organizations' Information Security Management (ISM) (Adaptation to rapid technology development (ARTD), Bureaucratic standing (BC), employees' compliance (EC), best utilization of the information and communication technologies infrastructure (ICT), inter-organizational collaboration (Inter), intra-organizational collaboration (Intra), leadership attitude (LA), legislative influence (LI), skilful workforce (SW), type of organization (TO), vendor selection (VS)). The research then proceeds to test the identified factors in the context of smart and non-smart cities. A questionnaire was developed, and 308 valid participations were documented. Data were then analysed and have shown indicators that the current smart cities around the world do seem distant from becoming smart as defined in the common literature. Significant evidence was found to validate the positive

influence of LI on ISM, and ISM on OP in smart and non-smart cities. Significant evidence was found to validate the positive influence of SW on smart cities only. Significant evidence was found to validate the positive influence of VS on ISM in non-smart cities only. The research then discusses research results and limitations to conclude on findings and future research choices.

TABLE OF CONTENTS

Chapter 1 Introduction	1
1.1 Introduction	1
1.2 Smart Cities	1
1.3 Information Security in Smart Cities.....	5
1.4 Organizational Performance.....	6
1.5 Research Problem.....	6
1.6 Research Aim and Objectives.....	8
1.7 Methodology	8
1.8 Thesis Structure.....	9
1.9 Summary	12
Chapter 2 Literature review.....	0
2.1 Introduction	0
2.2 Smart City Definitions and Components	1
2.3 The Emergence of Smart Cities.....	9
2.3.1 Opportunities and challenges.....	12
2.3.2 The smart city ICT infrastructure	14
2.4 Smart City Performance Evaluation	17
2.5 The Role of Governance and Management in the Smart City	20

2.5.1 Smart cities governance organizational factors in the literature	23
2.6 The Importance of Information Security.....	29
2.7 The Smart City Organizational setting.....	34
2.8 Information Security Management (ISM).....	38
2.8.1 ISM organizational factors in the literature.....	41
2.8.2 ISM challenges.....	60
2.9 Information Security in the Smart City.....	63
2.10 Research Gap: Information Security Management Impact on Organizational Performance in Smart Cities.....	68
2.11 Summary.....	70
Chapter 3 Conceptual model development.....	72
3.1 Introduction.....	72
3.2 The Use of Organizational Performance as a Theoretical Lens in this Research	73
3.2.1 The selection of organizational performance in this research	74
3.2.2 Measuring organizational performance.....	75
3.2.3 Organizational performance and corporate governance	76
3.2.4 ICT and organizational characteristics	77
3.2.5 IT/ICT and Governance.....	80
3.2.6 Organizational performance and Information security.....	81
3.3 Study Hypotheses.....	85
3.3.1 Adaptation to rapid technology development.....	85
3.3.2 Bureaucracy	85

3.3.3 Employee compliance with organizational policies	86
3.3.4 Improved utilization of the ICT infrastructure.....	86
3.3.5 Inter-organizational collaboration	87
3.3.6 Intra-organizational collaboration	88
3.3.7 Leadership attitude.....	88
3.3.8 Legislative influence	89
3.3.9 Skillful workforce.....	90
3.3.10 Type of organization and business model	90
3.3.11 Vendor selection.....	91
3.3.12 Information security management and organizational performance.....	91
3.4 Research Model.....	92
3.5 Summary	93
Chapter 4 Research methodology	94
4.1 Introduction	94
4.2 Research Design	95
4.3 Research Philosophy.....	96
4.4 Research Strategy	100
4.5 Time Horizon	102
4.6 Quantitative Data Collection methods.....	102
4.7 From Hypotheses to Constructs	103
4.8 Research questions.....	104
4.9 Research questionnaire	113

4.10 Research Ethics	113
4.11 Research Population and Sample	113
4.11.1 Research data and target population.....	114
4.11.2 Sampling technique.....	114
4.11.3 Sample size and selection.....	115
4.12 Pilot Study	116
4.12.1 Comments received.....	117
4.12.2 Pilot study data analysis in IBM SPSS	118
4.13 Main Study.....	122
4.14 Data Analysis assumptions and justification.....	123
4.15 Summary.....	123
Chapter 5 Data analysis and results.....	124
5.1 Introduction.....	124
5.2 Respondents' Profiling.....	125
5.2.1 Gender	126
5.2.2 Age	127
5.2.3 Security Role.....	129
5.2.4 Organizational Size.....	130
5.2.5 Organizational Sector.....	132
5.2.6 Smart City Standing	133
5.2.7 Response Base.....	134
5.2.8 Organizational Base	138

5.2.9 Reporting City	143
5.3 Descriptive Statistics	148
5.3.1 Adaptation to Rapid Technology Development	148
5.3.2 Bureaucracy	149
5.3.3 Employee Compliance.....	149
5.3.4 Information and Communication Technologies (ICT).....	150
5.3.5 Inter-Organizational Collaboration.....	151
5.3.6 Intra-Organizational Collaboration.....	151
5.3.7 Leadership Attitude	152
5.3.8 Legislative Influence.....	152
5.3.9 Skilful Workforce	153
5.3.10 Type of Organization	154
5.3.11 Vendor Selection.....	154
5.4 PLS Evaluation.....	155
5.4.1 Construct Validity and Reliability Analysis (Cronbach’s Alpha and Composite Reliability)	165
5.4.2 Discriminant validity (Fornell-Larcker, Cross Loadings, HTMT).....	168
5.4.3 Structural equation modelling and hypothesis testing (R^2 , f^2 , Q^2)	176
5.4.4 Comparison between Smart and Non-Smart Cities	182
5.4.5 Model Significance comparison between Smart City, Non-Smart City and complete (P values)	191
5.5 Summary	192
Chapter 6 Discussions	193

6.1 Introduction	193
6.2 Adaptation to Rapid Technology Development	193
6.3 Bureaucracy	194
6.4 Employee Compliance	195
6.5 Information and Communication Technologies (ICT)	196
6.6 Inter-Organizational Collaboration	197
6.7 Intra-Organizational Collaboration	198
6.8 Leadership Attitude	199
6.9 Legislative Influence	200
6.10 Skilful Workforce	200
6.11 Type of Organization	201
6.12 Vendor Selection	202
6.13 Information Security Management and Organizational Performance	203
6.14 Ranking of Organizational Factors Influencing ISM in Smart Cities	203
Chapter 7 Research conclusions	206
7.1 Research objectives revisited	206
7.2 Research implications and recommendations	207
7.3 Contributions to the literature	208
7.4 Research limitations and future directions	209
REFERENCES	211
APPENDICES	255
Appendix I Smart city table of definitions	255

Appendix II LinkedIn message	260
Appendix III Research survey/questionnaire	261
Appendix IV: Research ethics approval.....	270

List of Tables

TABLE 2.1: SUMMARY AND SYNTHESIS OF THE SMART CITY COMPONENTS	3
TABLE 2.2: TABLE OF SMART CITIES GOVERNANCE ORGANIZATIONAL FACTORS	23
TABLE 2.3: TABLE OF INFORMATION SECURITY MANAGEMENT ORGANIZATIONAL FACTORS IN THE LITERATURE	42
TABLE 3.3.1: THE ORGANIZATIONAL ECONOMIC IMPACT OF A SECURITY BREACH.....	83
TABLE 4.1: COMPARISON BETWEEN THE RESEARCH MODELS	97
TABLE 4.2: COMPARING EFFECTS OF POSITIVISM AND SOCIAL CONSTRUCTIONISM (ADOPTED FROM EASTERBY- SMITH ET AL., 2002)	98
TABLE 4.3: ASPECTS OF POSITIVISM.....	100
TABLE 4.4: HYPOTHESES AND ASSOCIATED CONSTRUCTS	103
TABLE 4.5 SOURCES OF HYPOTHESIS RELATED QUESTIONS	106
TABLE 5.1: RESPONDENTS' DISTRIBUTION BY GENDER	126
TABLE 5.2: RESPONDENTS' DISTRIBUTION BY AGE GROUP	128
TABLE 5.3: RESPONDENTS' DISTRIBUTION BY SECURITY ROLE.....	129
TABLE 5.4: RESPONDENTS' DISTRIBUTION BY ORGANIZATIONAL SIZE	131
TABLE 5.5: RESPONDENTS' DISTRIBUTION BY ORGANIZATIONAL SECTOR.....	132
TABLE 5.6: RESPONDENTS' DISTRIBUTION BY SMART CITY.....	133
TABLE 5.7: RESPONDENTS' DISTRIBUTION BY RESPONSE BASE	134
TABLE 5.8: RESPONDENTS' DISTRIBUTION BY ORGANIZATIONAL BASE	139
TABLE 5.9: RESPONDENTS' DISTRIBUTION BY REPORTING CITY	143
TABLE 5.10: STANDARD DEVIATIONS RECOMMENDED VALUES	148
TABLE 5.11: DESCRIPTIVE STATISTICS FOR ADAPTATION OF RAPID TECHNOLOGY DEVELOPMENT	148

TABLE 5.12: DESCRIPTIVE STATISTICS FOR BUREAUCRACY	149
TABLE 5.13: DESCRIPTIVE STATISTICS FOR EMPLOYEE COMPLIANCE	150
TABLE 5.14: DESCRIPTIVE STATISTICS FOR INFORMATION AND COMMUNICATION TECHNOLOGIES	150
TABLE 5.15: DESCRIPTIVE STATISTICS FOR INTER-ORGANIZATIONAL COLLABORATION	151
TABLE 5.16: DESCRIPTIVE STATISTICS FOR INTRA-ORGANIZATIONAL COLLABORATION	151
TABLE 5.17: DESCRIPTIVE STATISTICS FOR LEADERSHIP ATTITUDE	152
TABLE 5.18: DESCRIPTIVE STATISTICS FOR LEGISLATIVE INFLUENCE	153
TABLE 5.19: DESCRIPTIVE STATISTICS FOR SKILFUL WORKFORCE	153
TABLE 5.20: DESCRIPTIVE STATISTICS FOR TYPE OF ORGANIZATION	154
TABLE 5.21: DESCRIPTIVE STATISTICS FOR VENDOR SELECTION.....	155
TABLE 5.22: TABLE INITIAL LOADINGS	156
TABLE 5.23: CRONBACH'S ALPHA, COMPOSITE RELIABILITY, AND AVE	160
TABLE 5.24 RELIABILITY ANALYSIS AND CONSTRUCT VALIDITY RECOMMENDED VALUES	161
TABLE 5.25 TABLE FACTOR LOADINGS OF THE CONSTRUCTS IN THE MODIFIED MODEL	161
TABLE 5.26 TABLE RELIABILITY ANALYSIS OF THE CONSTRUCTS	166
TABLE 5.27 CONVERGENT VALIDITY RECOMMENDED VALUES	167
TABLE 5.28 CONVERGENT VALIDITY (AVE)	167
TABLE 5.29 DISCRIMINANT VALIDITY RECOMMENDED VALUES	168
TABLE 5.30 FORNELL AND LARCKER CRITERION.....	169

TABLE 5.31 CROSS LOADINGS	171
TABLE 5.32 HETEROTRAIT-MONOTRAIT RATIO (HTMT)	175
TABLE 5.33 EFFECT SIZE FOR INDEPENDENT VARIABLES	178
TABLE 5.34 HYPOTHESES TESTING (ALL RESPONDENTS)	181
TABLE 5.35 EFFECT SIZE FOR INDEPENDENT VARIABLES FOR SMART CITIES	184
TABLE 5.36 HYPOTHESES TESTING FOR SMART CITY RESPONDENTS	185
TABLE 5.37 EFFECT SIZE FOR INDEPENDENT VARIABLES FOR NON-SMART CITY RESPONDENTS	187
TABLE 5.38 HYPOTHESES TESTING FOR NON-SMART CITY RESPONDENTS	189
TABLE 5.39 SIGNIFICANCE COMPARISON BETWEEN SMART CITY, NON-SMART CITY AND COMPLETE (P VALUES)	191
TABLE 6.1: SIGNIFICANCE EVIDENCE SORTED FOR ORGANIZATIONAL FACTORS IN THE COMPLETE PARTICIPANTS' SET	204
TABLE 6.2: SIGNIFICANCE EVIDENCE SORTED FOR ORGANIZATIONAL FACTORS IN THE NON-SMART CITY PARTICIPANTS' SET	204
TABLE 6.3: SIGNIFICANCE EVIDENCE SORTED FOR ORGANIZATIONAL FACTORS IN THE SMART CITY PARTICIPANTS' SET	205

List of Figures

FIGURE 1.1 THESIS STRUCTURE	12
FIGURE 2.1: GRAPHICAL REPRESENTATION OF THE SMART CITY PILLARS.....	8
FIGURE 2.2 HISTORIC AND FUTURE URBAN AND RURAL POPULATION GROWTH	11
FIGURE 3.1: STUDY FRAMEWORK: INVESTIGATING ORGANIZATIONAL FACTORS INFLUENCING INFORMATION SECURITY MANAGEMENT IN SMART CITY ORGANIZATIONS.....	92
FIGURE 5.1: RESPONDENTS' DISTRIBUTION BY GENDER	127
FIGURE 5.2: RESPONDENTS' DISTRIBUTION BY AGE GROUP.....	128
FIGURE 5.3 RESPONDENTS' DISTRIBUTION BY SECURITY ROLE	130
FIGURE 5.4: RESPONDENTS' DISTRIBUTION BY ORGANIZATIONAL SIZE.....	131
FIGURE 5.5: RESPONDENTS' DISTRIBUTION BY SMART CITY.....	134
FIGURE 5.6: SURVEY PLS MODEL.....	156
FIGURE 5.7: SEM HYPOTHESIS R ² TESTING ALL RESPONDENTS (ORIGINAL SAMPLE)....	177
FIGURE 5.8: SEM HYPOTHESIS TESTING ALL RESPONDENTS (T STATISTICS).....	182
FIGURE 5.9: SEM HYPOTHESIS TESTING FOR SMART CITIES RESPONDENTS (ORIGINAL SAMPLE).....	183
FIGURE 5.10: SEM HYPOTHESIS TESTING FOR SMART CITY RESPONDENTS (T STATISTICS).....	185
FIGURE 5.11: SEM HYPOTHESIS TESTING FOR NON-SMART CITY RESPONDENTS (ORIGINAL SAMPLE).....	187
FIGURE 5.12: SEM HYPOTHESIS TESTING FOR NON-SMART CITY RESPONDENTS (T STATISTICS).....	190

List of Abbreviations and Acronyms

ARTD: Adaptation to Rapid Technology Development

BC: Bureaucracy

EC: Employee Compliance

ICT: Information and communication technology

INTER: Inter-Organizational Collaboration

INTRA: Intra-Organizational Collaboration

IoT: Internet of things

IS: Information Security

ISM: information security management

IT: Information technology

LA: Leadership Attitude

LI: Legislative Influence

OP: Organizational performance

SC: Smart city

SW: Skilful Workforce

TO: Type of Organization

VS: Vendor Selection

List of Appendices

APPENDIX I SMART CITY TABLE OF DEFINITIONS

APPENDIX II LINKEDIN MESSAGE

APPENDIX I RESEARCH SURVEY/QUESTIONNAIRE

APPENDIX I RESEARCH ETHICS APPROVAL

Chapter 1 INTRODUCTION

1.1 Introduction

The recent population urbanization trends and the proliferation of Internet technologies has birthed the concept of smart cities. The notion of smart cities has drawn a great deal of research attention (Angelidou, 2015; Bakıcı et al., 2013), including how new technologies, such as the Internet of Things (IoT), the emergence of cloud computing, and supporting services influence urban living. To ensure the seamless operation of smart cities, information and infrastructure must be protected by establishing and maintaining robust information security mechanisms. Among other benefits, information security plays a crucial role in the protection of national interests and urban stability (Atzori et al., 2010). However, security is highly dependent on the Information and Communication Technology (ICT) infrastructure (Dameri, 2013), which faces several challenges (Belissent, 2011). To maintain the integrity of information security systems, security planning, management, and associated mechanisms require proficient stewardship, especially at the organizational level.

1.2 Smart Cities

The increasing importance of the smart city concept is the result of a range of technological, sociological, economic, demographic, environmental, political and cultural circumstances (Castells, 1996; Marceau, 2008; Dawes et al., 2009). Despite the strong debates around the “smart city” concept and its surrounding initiatives, there is still no specific or common definition of the smart city, only agreement on the characteristics and what needs to be sustained in future smart cities. For

example, there is wide agreement in the research community around the value of a pervasive ICT infrastructure (Chourabi et al., 2012; Allwinkle and Cruickshank, 2011), a resource that can improve the efficiency of city processes and businesses through enhanced information systems services and, in turn, catalyze economic growth and ensure urban sustainability (Hollands, 2008). However, smart city development in the last few years has also raised multiple discussions about the barriers to enhancing human efficiency, happiness, and prosperity in urban regions, including debate on how such issues should be explored by researchers. Ongoing issues are arising about how to help make cities more liveable and sustainable. This has made the smart city concept development highly researched in recent years.

Recent years have seen rapid development of the “smart city” concept. A smart city is defined as one that best employs its resources, is highly dependent on its ICT infrastructure, develops its human capital, and focuses on growth, efficiency, living quality, and citizen engagement. The evolution of the smart city concept originated with such concepts as the “intelligent city”, but also included a city’s competitive position amongst its peers, such as its differentiating industrial, digital, and learning capabilities (Komninos, 2002). In 2003, the smart city concept became more crystalized when Odendaal (2003) introduced new methods of city governance that not only integrated the e-government phenomenon, but also emphasized the governance benefits that cities could have from employing Information technologies, such as improved integration, maturation, and transparency. When discussing the smartness of cities Shapiro (2006), and Mulligan and Olsson (2013) discuss the impact on citizen’s quality of life with the increased urbanization of metropolitan areas; however, Shapiro’s (2006) research mostly focused on human capital aspects in relation to the development of urbanized regions, rather than the overall organizational factors that come into play in a modern organization. In 2007, Giffinger et al. (2007) report on European smartness ranking expanded the “smart city” concept to include evaluation measures and capabilities. This encouraged competition between European cities and enabled the assessment of the smartness of each city via the following dimensions: economy, the people, governance, mobility, environment, living quality. Meanwhile, Giffinger et al. (2007) also developed 31 factors and 74 indicators to rank 70 smart cities in the EU that had the goal of reducing energy use and gas emissions by 2020. Hollands (2008) subsequently argued that smart cities should not be highlighted as large IT projects and, instead, emphasized the importance of human capital in terms of education, creativity, innovation and entrepreneurship in the future of a city. Nam and Pardo

(2014) then discussed the importance of smart city governance and the changes needed to achieve the best governance efficiency and transparency. Performance indicators were later developed by Giffinger et al. (2007) to address six domains: smart economy, smart people, smart governance, smart mobility, smart environment, and smart living. These domains would play a major role in standardizing the assessment of smart city performance.

Smart cities are being positioned as the future of humans living, developed to support economic growth. Smart cities operations depend on the deployment of advanced communication systems to drive high efficiency and sustainability; they will then rely on the ICT infrastructure to deliver the city's services. Despite the possible advantages of smart city technology, the logistical issues relating to its adoption has become more evident. For example, the amount of IoT (Internet of Things) and smart sensors expected to be connected in smart cities is very large; Cisco expects there to be 26 billion IoT devices for a population of 7 billion (Gartner Inc., 2013), while another analyst prognosticated this figure to be 50 billion devices (Bekara, 2014). Regardless, there will be a need for enhanced practices, not only to manage, but also to secure such mass scale environments.

Gil-Garcia and Pardo (2005) discussed the challenges of relying on IT projects in advanced environments, identifying multiple organizational and managerial issues that could be of significance to the participating organization. Issues include the size of the project, the management of behaviour, the organizational diversity, alignment, and change resistance. While discussing success factors of smart city initiatives, Chourabi et al. (2012) also discuss managerial and organizational elements as major challenges and key success factors, ones that need to be discussed in the context of extensive e-government and IT projects literature. Chourabi et al. (2012) consider governance as a big challenge for smart cities, especially regarding the need to adapt laws, regulations, and policies to the smart city context; major changes are needed at the governance level. Researchers have also agreed that management and governance issues, especially in the smart city context, have only been addressed in a few studies (Chourabi et al., 2012; Gil-Garcia and Pardo, 2005). In the same context, Whitmore et al. (2014) justify the large number of studies on IoT technology a result of its lack of maturity, concluding that when technology reaches certain maturity levels, IoT and smart cities research should widen in focus to include broader issues related to management, law, and economics. The same could also be justified by the fact that technology research in

the context of smart cities is being pushed by international technology vendors and their marketing campaigns in order to gain long term markets for their products (Kitchin, 2014; Hollands, 2015; Mulligan and Olsson, 2013; Söderström et al., 2014). That is also why Hollands (2008, 2015) warned of the private sector leading smart city development, and recommended more consideration be granted to social concerns than commercial interests, such as education and human capital development. This perspective seeks to improve the quality of life for citizens, and not the bottom-line interests of corporations.

In recent years, information security has also gained increased attention, especially with the introduction, proliferation, and eventual ubiquity of the Internet. The purpose of information security is the protection of an organization's 'digital operations' assets, such as hardware, software and data. Information security also entails the protection of an organization's business, which relies on digital information to operate services and products, and where the lack of reliable communication and data would cause damage in the running of services, and harm operations and profitability. It is important to note the difference between "information privacy" and "information security" as they are sometimes confused. Information privacy is the right to have personal data kept safe and secure, while information security is about the methods used to secure that data (Bélanger and Crossler, 2011). Information security is also defined by the Organization for Economic Co-Operation and Development (OECD) using nine principles (OECD, 2002): awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management, re-assessment. Information security becomes a more pressing issue

In general, smart cities are proving to be the future of urban life, promising better living for citizens, helping them achieve better knowledge and performance. However, for smart cities to prosper, obstacles to their success such as information security must be attended to. The role of the next section is to expound on the protection requirements for a smart city. The smart city information security concept is detailed, then the concept of information security management is introduced, in order to connect the different concepts (the smart city, information security, information security management inside organizations).

1.3 Information Security in Smart Cities

In the information era, businesses tend to rely partially or completely on digital infrastructure to deliver their services and drive organizational growth. Information security is agreed and anticipated to be of major importance for a smart city's digital technologies and services. Information confidentiality, integrity and availability (CIA) are a must for survival and should be met now more than ever to ensure operations run unabated. Threats to information CIA have national security significance; a weakness or failure in core city systems could impact the city's liveability and society's well-being (Sicari et al., 2015; Bekara, 2014; Gubbi et al., 2013; Li et al., 2012; Baumeister, 2010; Marias et al., 2011; McDaniel and McLaughlin, 2009). Since a smart city runs highly interconnected ICT services, the power grid critical infrastructure will also be a function of this ecosystem that needs to be protected (Metke and Ekl, 2010; von Solms and von Solms, 2004); an ecosystem in the context of technology 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 could be deployed on a larger scale (Sicari et al., 2015; Bekara, 2014; Gubbi et al., 2013; Li et al., 2012; Baumeister, 2010; Marias et al., 2011; Kitchin, 2014; Ruiz-Romero et al., 2014; Naphade et al., 2011; Martinez-Balleste et al., 2013; Elmaghraby and Losavio, 2014; Roman et al., 2011; Bélanger and Crossler, 2011; McDaniel and McLaughlin, 2009).

The management of information security is highly required for guarding the interest of shareholders and the business. Information security maturity and control is not an investment but a necessity for survival in the modern world, the role of information security management within organizational governance is to define best practices, manage costs efficiently, improve employees' behaviour, strengthen business controls, and define accountability. Researchers have defined an organization's successful management of information security as a mix of confidentiality, integrity, and availability (CIA), and responsibility, integrity, trust and ethicality (RITE) (Dhillon and Backhouse, 2000). Establishing information security management also requires the involvement of senior management. The sharing of information and transparency regarding any incident is not only important for business success, but also to ensure alignment with business goals and, for example, the prioritization of selective security investments that best minimize risks (Williams, 2001; Nam and Pardo, 2014; Herath and Herath, 2009).

As a smart city will operate and rely on highly interconnected ICT services, it needs to be protected (Metke and Ekl, 2010). Therefore, the role of information security is undoubtedly one of the most important. The governance of information security will be highly delicate and intriguing, and the right decisions need to be made to protect not only the businesses, but also the resources and citizens. The security of information and its management in the oversight of smart city functions are proven to be significant responsibilities if smart cities are to develop efficiently and operate sustainably. The lack of empirical research in this area is an indicator of the need for more target attention directed towards understanding the best-practices to meet such ends.

1.4 Organizational Performance

Organizational performance is a complex multidimensional phenomenon. It has previously been defined using multiple goals such as profit, growth, and stakeholders' satisfaction, which often conflict (Cameron, 1986; Chakravarthy, 1986; Venkatraman and Ramanujam, 1986). Researchers proposed different measures of performance and evaluation of results that also opened the way to more difficulties, such as dealing with the different priorities that are assigned for each of the organizational goals and how each organization could have different priorities. Other difficulties also include the need to deal with fluctuating results and how to define a success or failure based on goals and priorities. Organizational performance in the context of complex smart city environments would bring new difficulties for the understanding of services, challenges, priorities and accountability, and defining the Key Performance Indicators (KPIs) that an organization needs to attain. To cope with the smart city model, businesses need to adapt (Harrison et al., 2010). The information security management inside smart cities needs to be well-developed and maintained to meet needed maturity levels. Failing to achieve that could convey a severe collapse of the organizational performance and therefore impact stakeholders' convenience and success.

1.5 Research Problem

The cost of poor cyber security is high for the organization and a breach might affect multiple organizations (Cavusoglu et al., 2004). Further, Cavusoglu et al. (2004) concluded that the cost of a security breach for an Internet only organization is higher than for conventional firms. While information security has been framed as of high importance for the safety of digital services, especially in the context of smart

cities (Sicari et al., 2015), information security management has been noted to be of greater significance (von Solms and von Solms, 2004; Belissent, 2011). On the other hand, Chourabi et al. (2012) and Whitmore et al. (2014) have confirmed that little research has been done on smart cities management and related organizational 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. (2014) indicates that the research literature is dominated by technology studies and that advanced technology services are not well represented in this body of work.

Information security mismanagement in smart cities could quickly escalate into the destruction of an organization's business and operations. Losses could impact business operations, financial capabilities, sanctions, and reputation. The impact of falling into information security management mis-practices could have catastrophic results on an organization. Von Solms and Von Solms (2004) also detail the impact that information security mismanagement could have at the organizational level. They concluded that resources and financial loss, mis-prioritized 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 security policies, could be blamed. However, even though smart governance is a major aspect of the city, there is a lack of literature exploring smart governance issues (Chourabi et al., 2012).

As smart cities are, in many cases, purposed towards improved growth and development, it is imperative that smart city organizations cope with the aforementioned challenges to deliver better performance (Harrison et al., 2010). Maintaining the proper information security status and the right governance over smart city organizations is vital for healthy organizational performance. As organizations push online services into the mainstream, smart cities will have high mandates for reliability and CIA levels, Information security management issues are expected to grow in importance, requiring evidence-based best practices to be well-established. In turn, research is needed to better examine information security management in smart cities, to identify factors and aspects that influence information security management in organizations, and how those might impact performance.

1.6 Research Aim and Objectives

Drawing from the previously highlighted evidence on the importance of information security management in smart city organizations and the sparsity of research in this area, the aim of this research is to investigate the organisational factors influencing information security management in the context of smart city organisations.

The definition issue concerns the identification of key factors that affect smart city organizations, which could be internal factors specific to the organization (e.g., employee awareness, organizational culture, top management support) or external factors (e.g., inter-organizational factors, information sharing). The modelling issue concerns the establishment of a tool to evaluate the impact of organizational factors on information security management in smart city organizations. The measurement issue concerns the methodology in which the model will be assessed to measure the impact of organizational factors on information security management in smart city organizations.

To achieve the aim of this research, the researcher will attempt to attain a thorough understanding of the research concepts (SC, IS, ISM) and their gaps, develop a model or framework to incorporate the different factors that impact information security management inside smart city organizations, assess and validate the model in a relevant environment to come out with a set of conclusions.

1.7 Methodology

To achieve the goals of this research, a thorough review of the literature has been conducted. This review was performed around the key topics being discussed:

- Smart cities and information security and privacy;
- Smart cities, management and governance;
- Information security and organizational performance;
- Smart cities and organizational performance aspects.

The literature review highlights the pressing issues of ISM in smart city organizations and then proceeds to identify the organizational factors that are expected to influence information security management in smart city organizations. The organizational factors are then used to develop a conceptual model in order to assess their influence on information security management and organizational performance in the context of smart cities. The current research uses surveys with

roots in the positivist research paradigm, attempting to achieve its aims and findings by using logical and mathematical research instruments such as questionnaires and experiments.

A survey instrument is then developed to better understand and measure the organizational factors influencing ISM in smart city organizations, relying on literature findings and previous studies. Eleven hypotheses were developed as the focus of this research and as correlated from the literature findings. An empirical examination of the developed survey instrument is followed in order to investigate and accumulate a better understanding of the information security management in smart city organizations. The survey instrument was ethically approved by the Brunel Ethics Committee.

A two-phase pilot study was organized in order to evaluate the developed survey instrument and then adapt it for the main study. The pilot study also served to examine the reliability and validity of the survey instrument and determine its readiness for the primary study. Subsequently, the primary study was distributed to thousands of people over the period of one month. Participants were addressed from different cultures, regions and information security backgrounds. The participants were selected as information security professionals with a current technical, leadership or management role inside organizations. The survey was sent to around 3,000 LinkedIn users that matched the survey participation rules. Of these, 322 respondents answered the survey, and 308 survey participations were validated.

The results of the empirical examination were then analysed using SPSS and Structural Equation Modelling using SMART-PLS. Validity and reliability were calculated to validate the data; structural equation modelling was also utilized to validate the previously defined hypotheses. After the data was analysed, conclusions were drawn about the most influential organizational factors on organizations operating in smart cities. Implications of the findings, including suggestions for future research, will be discussed.

1.8 Thesis Structure

The rest of this document is organized as follows. First, the literature review is conducted to identify and discuss the relevant variables, methods, and frameworks related to this research area. Key gaps in this literature are exposed to set the

rationale for the current investigation, from which hypotheses will be formulated. The research model and instrument are then discussed, developed, and tested. Finally, after the data analysis is conducted and the results reported, a discussion of the findings and study conclusions will be presented.

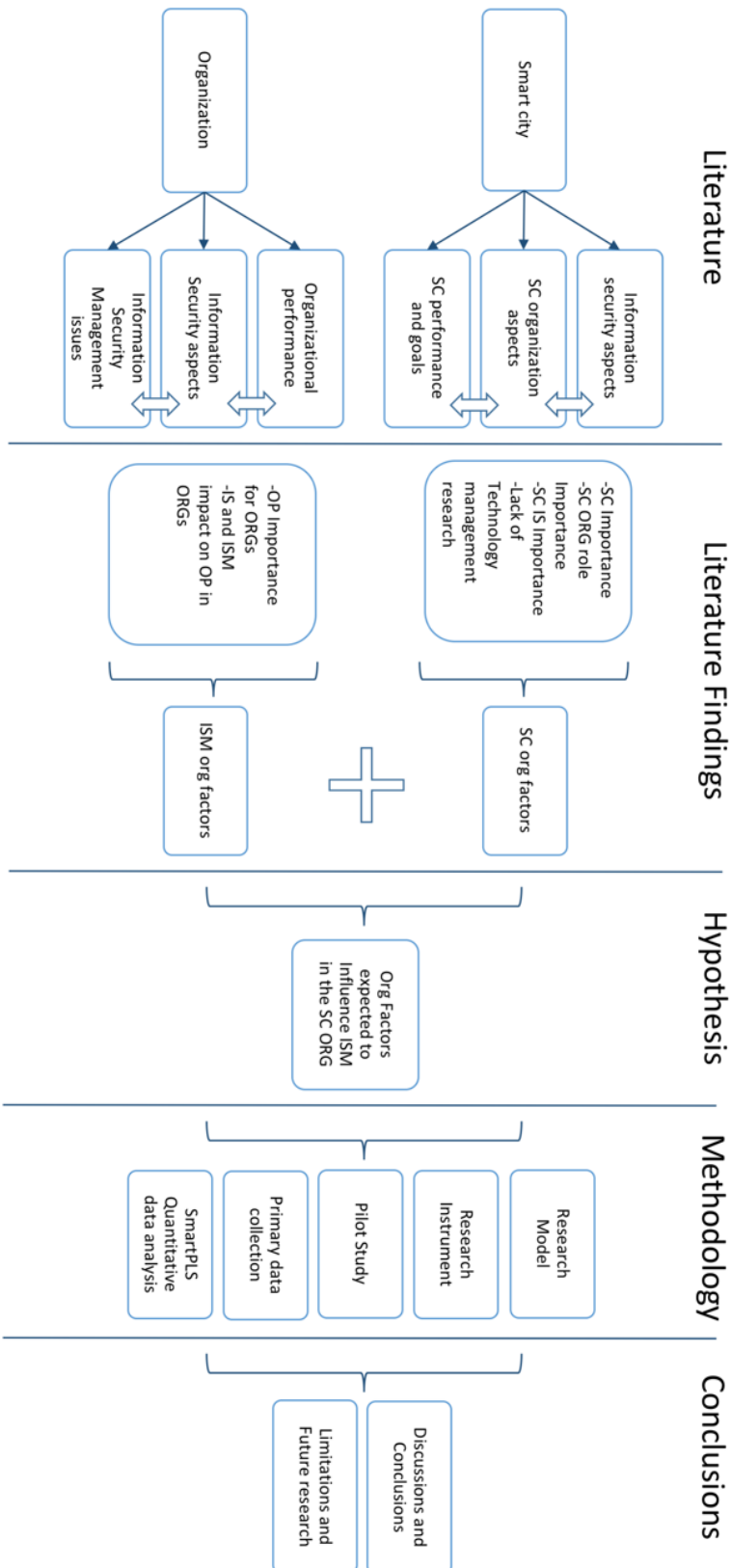


Figure 1.1 Thesis structure

Source: Devised by author

1.9 Summary

This chapter highlights the context and circumstances of this research study. The literature summary explains the gaps in the existing research. The research problem and objectives explain the goals of the research and the methods that will be followed to progress the research. The following chapter explores and discusses the existing research and theories pertinent to smart cities, information security and organizational factors.

Chapter 2 LITERATURE REVIEW

2.1 Introduction

The previous chapter outlined important information regarding security issues arising in the face of smart city organizations, and the lack of management research in this area. The purpose of this chapter is to identify the current knowledge about these issues and any corresponding evidence-based solutions. This chapter will also identify the knowledge around smart cities, their definitions, existence goals, stakeholders, challenges, opportunities and applications. It will then focus on smart city organizations in smart cities and the aspects around the influence of organizational information security management on organizational performance. The following subsections will provide analysis and discussions of the different smart city definitions, characteristics, dimensions, components, stakeholders, domains of evaluation and organizational aspects. In addition, there will be an analysis and discussions of the ICT infrastructure, information security and management definitions, roles, stakeholders, leaders and the different aspects that impact their effectiveness in an organization. The objective of this work is to lay solid ground for the research.

The literature review conducted in this chapter relies on different characteristics to assure the quality of the research findings and the relevant outcomes. The review has been conducted through trusted and quality literature sources such as Scopus, ScienceDirect and Elsevier. It focuses on key terms that directly reflect the topics at

play in this research (smart city, information security, information security management, organizational performance, organizational factors, etc.).

2.2 Smart City Definitions and Components

The development of the smart city concept requires the identification of smart components, their elements and characteristics. The previous section described the opportunities and challenges of the smart city; this section will review the literature around the components of the smart city, what they are, how they interrelate, their role and influence on smart city citizens.

Smart city research has described many elements that are expected to be part of smart cities in the future, describing their main characteristics and components as follows:

- the utilization of an ICT infrastructure to improve economic and governance efficiency not only in a business-oriented environment, but also for cultural and social development (Shapiro, 2006);
- the focus on smart governance and social inclusion to spot smart city needs, priorities and decisions that enable best growth and development options (Atzori et al., 2010; Giffinger et al., 2007; Chourabi et al., 2012);
- the focus on smart city human capital, leading and developing urban growth and how a city could attract creative people, which Florida (2002) describes as “The wave of the future” that shall be responsible for the city’s destiny;
- the focus on ecological efficiency, resources management and environmental sustainability. This point is required to guarantee balanced and stable living standards for the smart city population (Kourtit and Nijkamp, 2012).

The concept of the smart city has undergone many definitions, variations, and meanings, each serving different purposes based on its domain of application. The smartness term can be defined in many terms related to technology, economy, lifestyle and others. The most popular smart city definitions act as a guide for future research. The smart city dictionary definition is described in businessdictionary.com as “a developed urban area that creates sustainable economic development and high quality of life by excelling in multiple key areas; economy, mobility, environment, people, living, and government. Excelling in these key areas can be done through strong human capital, social capital, and/or ICT infrastructure”.

The smart city concept has become unprecedentedly important and popular in the last few years; it is broad, wide and envelops many definitions, dimensions and research themes (Mulligan and Olsson, 2013). The popularity of the smart city concept grew when it received support from technological and industrial vendors. IBM started the discussion through a live podcast on future prosperous and sustainable cities (Dirks and Keeling, 2009), then in 2010 (Harrison et al., 2010), IBM detailed the foundation for smart cities: technologies and research domains were triggered open to address the needs of the smart city, and research communities and institutions later started to research and advance. The following years proved different for the smart city concept as researchers accelerated research in smart citywide domains: ecological, technological, urban and civil, humanitarian, managerial, transport, etc. The concept of the smart city appears to have evolved in a way that it is now a template for future metropolitan areas, a sign of sustainable, efficient, growing, intelligent societies. Support for the concept was also received from international governmental organizations such as the European Union, Dubai, etc. (Anthopoulos and Fitsilis, 2013). The popularity boost is especially visible in the number of research journal papers published on smart cities in the last few years.

Kourtit et al. (2012) mention that the smart city could also be influenced by “negative externalities”. Caragliu et al. (2011) based an analysis of smart cities on the 2004 Urban Audit, which is a collection of statistics and indicators for European cities across the following domains: demographic, social aspects, economic aspects, civic involvement, training and education, environment, travel and transport, information society, culture and recreation. It is important to note that the majority of the smart city definitions feature the presence of ICT technologies to build and integrate with infrastructure and services, in order to offer better quality and more efficient services for citizens (Giffinger and Gudrun, 2010; Harrison et al., 2010; Hollands, 2008; Washburn et al., 2010).

A number of smart city definitions was found and collected from the literature, they can be found in Appendix I. The goal is to draw a better understanding of smart city components, challenges and goals.

There are multiple definitions of smart city components found in the literature. Table 2.2 is a summary of the most important components.

Table 2.1: Summary and Synthesis of the Smart City Components

Component of smart cities	References
Infrastructure and technology	Mahizhnan, 1999; Eger, 2009; Nam and Pardo, 2011a; Barrionuevo et al., 2012; Giffinger et al., 2007; Kourtit and Nijkamp, 2012; Chourabi et al., 2012; Marsal- Llacuna et al., 2014; Zygiaris, 2013; Bakıcı et al., 2013; Cretu, 2012; IDA, 2012; Lazaroiu and Roscia, 2012; Lombardi et al., 2012; Komninos, 2006; Caragliu et al., 2011; Gartner Inc., 2011 ; Thuzar, 2011; Harrison et al., 2010; Chen, 2010; Washburn et al., 2010; Toppeta, 2010;
Economic development and growth	Mahizhnan, 1999; Giffinger et al., 2007; Eger, 2009; Nam and Pardo, 2011a; Barrionuevo et al., 2012; Cretu, 2012; Thite, 2011; Thuzar, 2011;
Education and human capital	Mahizhnan, 1999; Giffinger et al., 2007; Barrionuevo et al., 2012; Kourtit and Nijkamp, 2012; Kourtit and Nijkamp, 2012; Chourabi et al., 2012; Lombardi et al., 2012 ; Komninos, 2006; Caragliu et al., 2011; Thite, 2011; Harrison et al., 2010;
Living quality/ Health	Mahizhnan, 1999; Giffinger et al., 2007; Thuzar, 2011; Barrionuevo et al., 2012; Guan, 2012; Caragliu et al., 2011; Thite, 2011; Chen, 2010;

Mobility	Giffinger et al., 2007
Public governance and participation	Nam and Pardo, 2011a; Giffinger et al., 2007; Barrionuevo et al., 2012; Kourtit and Nijkamp, 2012; Chourabi et al., 2012; Cretu, 2012; Caragliu et al., 2011; Gartner Inc., 2011;
Environment and ecological/natural resources usage efficiency	Giffinger et al., 2007; Thuzar, 2011; Nam and Pardo, 2011a; Barrionuevo et al., 2012; Chourabi et al., 2012; Zygiaris, 2013; Bakıcı et al., 2013; Guan, 2012; IDA, 2012; Lombardi et al., 2012; Caragliu et al., 2011; Thuzar, 2011; Hall, 2000;
Innovation/creativity	Eger, 2009; Nam and Pardo, 2011a; Komninos, 2006
Integration/Automation/interconnection	Nam and Pardo, 2011a
Social development and culture	Thuzar, 2011; Nam and Pardo, 2011a; Barrionuevo et al., 2012; Kourtit and Nijkamp, 2012; Zygiaris, 2013; Guan, 2012; Caragliu et al., 2011;
Job growth	Eger, 2009
Entrepreneurial capabilities	Kourtit and Nijkamp, 2012
Business models	Marsal- Llacuna et al., 2014

Urban performance	Marsal- Llacuna et al., 2014; Thuzar, 2011
Competition	Thite, 2011; Thuzar, 2011
Critical infrastructure	Washburn et al., 2010

Source: Devised by author

In the context of this research, the author of this study will consider the smart city as one that best employs its resources, is highly dependent on its ICT infrastructure, develops its human capital, and focuses on growth, efficiency, quality of life, and citizen engagement.

In one of the most common definitions of smart city components, Nam and Pardo (2011a) categorize the smart city in three strategic multi-dimensional principal components: technology, organization, and institutions/policies. Technology is referred to as a tool of innovation with examples including cloud e-services and an interconnected infrastructure; organization is adapted to manage, control and push the innovation in a business fashion, while also developing inter-organizational services and dependencies; policies are needed to enable the environment for innovation, especially modern governance through participation and collaboration.

The technologies are needed to install, develop and support a smart city's prosperity, while maintaining stability and monitoring smart city operations over its infrastructure. Examples of smart city concepts with a technological side include digital city, intelligent city, ubiquitous city, wired city, hybrid city, and information city. International institutions and think tanks have dedicated continuous efforts to prepare for ICT-driven smart urban areas. Smart city definitions have stressed the role of ICT tools in making the development of smart cities possible and in carrying innovation to the next levels. This role has also been emphasized by international initiatives such as the OECD/Eurostat Oslo Manual, 2005 (<http://www.oecd.org/science/inno/2367580.pdf>).

The ICT role is highly critical (Mulligan and Olsson, 2013); it is planned to be the nervous system of the smart city, which is expected to have many sensors distributed within it (Hall, 2000), and in which huge amounts of traffic (Big Data) is

expected to flow and be processed in real-time. In smart cities, ICT will provide many urban advantages such as location-based authentication and authorization, transport and traffic optimization, automated alerting and containment on incident occurrence, etc.

Human/People: the human intellectual capital in the smart city will be an important signal of its uniqueness, research, innovation, and democracy, which will all be ruled by its citizens. Examples of smart city concepts that belong to the human dimension include humane city, knowledge city, creative city, learning city.

Another smart city classification tool that is well known in the research community was developed by Giffinger et al. (2007), who segmented smart cities into six dimensions or axes, to develop a smartness ranking for European cities: smart economy, smart people, smart governance, smart mobility, smart environment and smart living. These six axes “connect with traditional regional and neoclassical theories of urban growth and development” (Caragliu et al., 2011), as they are based “on theories of regional competitiveness, transport and ICT economics, natural resources, human and social capital, quality of life, and participation of societies in cities” (Caragliu et al., 2011).

In a smart city environment, a smart economy is based on enterprises making the most of technologies and the throngs of information from various sources to develop high quality products and services for the population. Enterprises are also challenged into higher levels of innovation and being capable of transforming ideas into doable production processes. The importance of innovation is undeniable and has been considered since OECD’s report on the knowledge-based economy (OECD, 1996). This reported that industrial growth depends on knowledge as much as on capital and labour. Another aspect of the smart economy is the consideration of ecological aspects in the products and services, a green economy.

Smart technologies are also part of providing smart mobility for citizens that enable ease of use of services and products, better coordination about city services, and international accessibility. This is especially achievable using the smart city advanced ICT infrastructure, which is expected to be available and utilized (Giffinger et al., 2007). Environmentally aware products, services and technologies are expected to be of high importance to attain clean healthy living quality for citizens.

Renewable energy is also highlighted by European initiatives for future development. These initiatives include the SEAP (Sustainable Energy Action Plan) (Covenant of Mayors, 2010), which is a signed agreement that European cities will achieve a 20% reduction in gas emissions by 2020. Social and human smartness is defined by the capabilities of learning and innovating. Environments to nurture social and human factors are expected to be prepared by the smart cities through continuous educational opportunities. High educational opportunities enable citizens to become more skilled, qualified and influence the city's development. On the other hand, a smart environment is also connected to the participation of the citizens in the public benefit (Giffinger et al., 2007; Cardone et al., 2013).

Smart governance enables enhanced collaboration and communication between the smart city government and its citizens; other terms also referencing such improved interactions are e-governance and e-democracy. A smart city will enable enhanced governance through the advanced ICT infrastructure; it should encourage and support citizens' involvement by using their skills for consultation, but also by using their feedback, criticism and complaints to help shape city decisions (Nam and Pardo, 2011a).

The model by Giffinger et al. (2007) is highly influential in the smart city literature, primarily because the six dimensions are realistic and observable. Important aspects for each of the six smart city dimensions are presented in Figure 2.2 below.

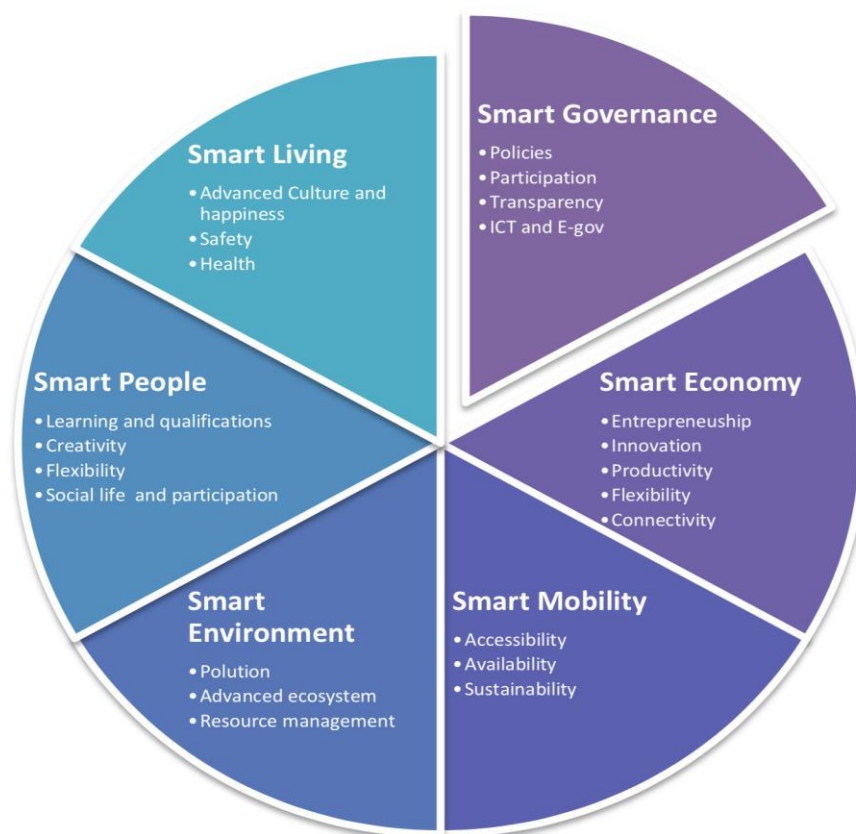


Figure 2.1: Graphical representation of the smart city pillars

Source: Devised by author

The triple helix (Lombardi et al., 2012) has also manifested itself as a reference framework for the analysis of innovation systems based on knowledge in urban regions; it relates the three main knowledge process agencies relationships (University, Government, Industry). This model is often used for the performance assessment of the smart city (Etzkowitz, 2008). A revised triple helix has been proposed by Lombardi et al. (2012) adding “civil society” to the agencies’ relationships. Lombardi et al. (2012) proposed 60 indicators for the ranking of smart cities performance, classified in 5 categories (smart governance, smart human capital, smart environment, smart living and smart economy). They also concluded on the prime conceptual relationships for the smart city concept being respectively: entrepreneurial city (48%), pioneer city (20%), liveable city (17%) and the connected city (13%).

The smart city definitions are numerous and have focused on the development of different aspects of the cities, namely economic, ecological, humanitarian and

technological. It will then be upon each city to define its own goals and targets, as per its population needs and desires. Nevertheless these cities need to be careful not to fall prey for the different mistakes a city can do such as the development of the city infrastructure but not the human capital; or relying on the technological vendors to care by themselves about the city goals and needs without strict monitoring and auditing.

2.3 The Emergence of Smart Cities

In previous sections, the evolution of urbanization in modern economies and the role of ICT in enhancing the human living and economic development were introduced, the smart city definitions were also detailed. The challenges posed by ICT in the form of information security and information security management were also detailed. In this section the knowledge around smart cities, the definitions, existence goals, stakeholders, challenges, opportunities and applications are identified. In addition, this section will analyse the role of smart city organizations and their specifics. The goal of this section is to develop an understanding of smart city specifics, in addition to highlighting the impact of governance and information security aspects on smart city performance.

The term “smart city” first appeared in 1998 in the Proceedings of the 4th EDC Conference on Digital Cities (Van Bastelaer, 1998), and implied a shift from non-digital to digital smarter city operations. This shift was needed to solve challenges of public leadership and efficiency, address the trends of process automation, and meet the growth expectations of its citizens. The concept became more mainstream with the Smart Growth Movement of the late 1990s (Harrison and Donnelly, 2011). At the same time, the smart city was portrayed by Mahizhnan (1999) as the shift from the industrial urban economy to an Information Technology (IT) based economy. Mahizhnan (1999) also described IT education of utmost importance for enabling the smart city through the human intelligence capital and the “bandwidth of the mind” instead of the “bandwidth in networks”. Such transformative goals have inspired progress in different research areas of urban development (i.e., industrial, managerial, technological, services) and influenced a race amongst researchers to satisfy the urban development requirements.

The process of urbanization is the exercise of populations shifting from distributed rural areas with agriculture-based economies to condensed urban areas characterized by industrial and urban services (Cohen et al., 2003; Mulligan and

Olsson, 2013). Historically, urban transitions were connected to economic evolutions; urbanization in Europe and North America was accompanied by the industrial revolution in the 19th and 20th centuries. As per the 2014 report “Revision of World Urbanization Prospects” (United Nations, 2014), 54% of the world’s population now live in urban areas, an increase from 30% in 1950. This number is projected to reach 66% by 2050. The report also mentions that these changes require considerable planning and governance for the maintenance of sustainable urban development and growth. Approximately 80% of global gross domestic product (GDP) is generated in cities (Grübler and Fisk, 2013).

On the other hand, as stated by Daniels (2004), high density cities present challenges to the infrastructure and basic services such as transport, water, drainage, housing, power consumption. These services are put under constantly increasing pressure and must be effectively managed and continuously optimized through sustainable development, policies and regulations for control and monitoring, to achieve growth potentials. Smart city solutions are expected to address urban density in cities, optimize the city’s capabilities in handling populations, and help manage infrastructure needs and efficiency (transport, waste, power, education, etc.).

Smart cities have recently been positioned as the future of human cities, developed to support growth and economic development, and have attracted a lot of research. Smart cities require the deployment of advanced communication systems to drive high efficiency and automation; they will then rely on the ICT infrastructure to deliver the city’s services. This will therefore highlight the need for the protection of such an infrastructure keeping it connected.

Current cities are complicated environments that implement technologies to connect businesses, governments, citizens, transportation, and many systems and devices (Zanella et al., 2014). Population growth in current cities has raised various concerns on the social, technical, economic and organizational status (United Nations, 2014); the UN report proves that the accelerated population growth in current cities is causing pollution, congestion, development difficulties and inequality. Such events have encouraged a great deal of research that could help cities better manage their population and resources to assure smarter solutions are developed and in place to support good quality living in future cities (Dirks and

Keeling., 2009; AlAwadhi and Scholl, 2013; Nam and Pardo, 2011a; Kaye Nijaki and Worrel, 2012; Zanella et al., 2014).

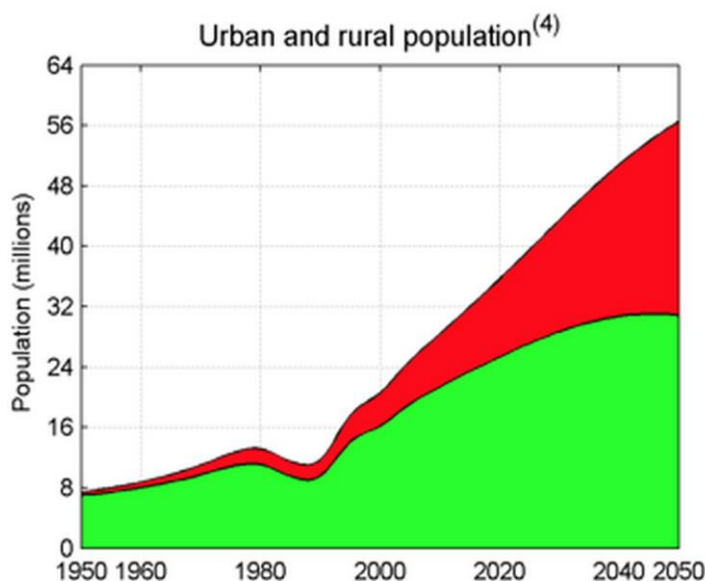


Figure 2.2 Historic and future urban and rural population growth

Source: United Nations, 2014

While migrating to smarter environments, and being of higher priority, cities and organizations will adopt transformation phases to integrate modern services into their ecosystem and satisfy the smart city (Earley, 2015). There is a need to understand its own maturity, understand its capabilities and the potential services that need to be offered, understand the value of Data Analytics, and how they could be used to correlate mass events, then rethinking the business and operational models to evolve with the city.

Identifying the stakeholders and their roles is important for researching the smart city: there are multiple researchers who described stakeholders. Yoshikawa (2012) classifies them into three categories: consumers (users, organizations), city managers (organizations), and world opinion (groups responsible for maintaining policies). Dameri (2012) takes another approach and defines two subjects, actors and stakeholders. Actors are further segmented into three categories:

- solution vendors that are interested in developing solutions to satisfy the needs of the city: for them, the digital city drives business;

- governments, responsible for developing and enforcing rules and policies to guide the implementation of the digital city: for them the digital city is a driver for society's prosperity;
- educational systems, that are especially important for the knowledge transfer and development of the intellectual capital within the smart city.

Stakeholders are also classified into three categories:

- enterprises that benefit from the presence of the digital city to improve their businesses, offer better products and services;
- public administration that uses the digital city to offer high efficiency, high quality, low cost services that are of positive outcome to the public benefit;
- citizens and civil society, the beneficiaries of digital cities, that can benefit from its smart services and products as long as they are skilled enough to use them.

2.3.1 Opportunities and challenges

Conceptually speaking, smart cities are hard to define. Many definitions and conceptual relatives have been detailed that target the smart city, but in real life, each city will have its own customized take on smart technology based on the needs that require addressing. Technologically speaking, many technologies need to be developed to address smart city needs; systems that manage other systems are also being discussed to operate ranges of complex environments.

A challenge being highlighted in the literature as a potential threat for smart cities is the technological domination by vendors, where a sole vendor is pushed and standardized over a city scale, through long term commitment that benefits the vendor more than it does for the city itself (Kitchin, 2014). The migration difficulties from current intelligent cities to smart cities are also reflected in Deakin and Al Waer (2011) where anxiety is expressed that the smart city concept development is moving towards "meeting the corporate needs of marketing campaigns rather than the social intelligence required for them to be smart", which was also mentioned by Hollands (2008, 2015) and Söderström et al. (2014). Deakin and Al Waer (2011) and Hollands (2015) express concerns that the smart city would end up as a branding and marketing ploy used by corporates for their own benefit rather than developing into the next best urban living experience for the citizens.

The role of creativity in the growth of smart cities has also been critically analysed in Nijkamp (2008). Nijkamp (2008) shows that creativity is not only an increasing determinant of smart city success and performance, but also an influence on the development of the creative population and skills migration. On the other hand, smart city governance is also too technocratic by nature, which is why international corporates are trying to position them for their own benefits. They do this by promoting themselves as the sole saviours in order to gain long term markets for their products (Kitchin, 2014). Concerns arise around the marketization of smart city services, where the city would then be directed for private profit and not for the benefit of the citizens (Hollands, 2008).

Naphade et al.'s (2011) view on smart cities' challenges and opportunities is more detailed, being a "system of systems". Naphade et al. (2011) describe smart cities' challenges as matters of efficiently operating the infrastructure and data, in addition to real-life challenges such as managing the implementation and operation of the sensors. Not only do they also need to conduct sophisticated analytics to correlate and respond to smart city events, such as traffic congestion and emergencies, but they also have to secure the sharing of the data, protect citizens' security and privacy, city access control, security and availability of services.

The technologies and quality of the ICT infrastructure are not the only important aspects of the smart city; research has also emphasized the importance of the human capital and education in urban growth (Glaeser and Berry, 2006). Glaeser and Berry (2006) also describe the importance of the human aspect in urban development as managed by innovators and entrepreneurs; this leads the creativity in products and services, also detailing that cities with high intellectual capital are also capable of attracting more skilled labour than other cities. Winters (2011) mentions that the development of human capital in a smart city is almost entirely driven by people seeking higher education, wanting a better standard of living and salaries, but also adapting and learning new skills that might only be relevant in the city in which they live.

Meanwhile, there have been some negative portrayals of the smart city concept. Some researchers describe smart cities as a fashion. For example, Batty et al. (2012) state that the attention wave for smart cities is only a fashion linked to drivers of smart city projects. Baron (2012) also states: "In general Smart City is a kind of buzzword that refers to implementing ICT in metropolitan services". Giffinger and

Gudrun (2010) go even further stating that cities are only trying to get a better rank in worldwide ranks, without seriously planning or putting action to the strategic and governance requirements for becoming smart. Schaffers et al. (2011) also mention that governments are not in real need of adopting the smart city concept, and that the “smart city” is only the result of marketed and boosted ideas by international IT vendors. Kourtiti et al. (2012) also add that no city will ever be ideal for everyone. Negative aspects of being smart, technologically advanced and sustainable are also evident; some constituents prefer less technological and pervasive environments for cultural or even political reasons. According to De Wilde (2000), “visions of the future create little room for dissensus and politics”.

The above review demonstrates that the smart city phenomenon is the result of a complex worldwide evolution forged through:

- worldwide economic competition;
- environmental and resources management priorities;
- urban governance challenges (equality, living standards);
- modern social challenges (cultural and educational development);
- efficiency challenges and the need to integrate technologies.

The literature suggests that a smart city is not one simple type of governance or management approach; it is a wide movement of changes in the human definition of urban habitat that includes the consideration of culture, resources, wealth and development.

2.3.2 The smart city ICT infrastructure

Information and communication technology (ICT) is a key driver for smart city initiatives (Hollands, 2008), and the integration of ICT in a smart city helps enhance aspects of operations and management (Chourabi et al., 2012). “Information and communication technologies have become the nervous system of all modern economies” (Hernández-Muñoz et al., 2011), and are expected to connect modern organizations and services to maximize the quality and efficiency of citizens lives (Anthopoulos and Fitsilis, 2010; Lynggaard and Skouby, 2015). The Internet of Things (IoT) is also one of the major concepts of ICT, enabling the communication of all the sensors around citizens (Borgia, 2014); life is improved in a smart city by the use different technological advancements such as ICT to deliver a better quality of life for the citizens; this extends to the different life aspects such as health,

transport, culture, housing, security, and efficiency. ICT is a big part of smart cities and a major concern (Mulligan and Olsson, 2013) as they are heavily relied on to drive and deliver all classes of smart services, standing as critical infrastructure (Markovic et al., 2012) and being part of city production processes (Giuffrè et al., 2012).

Research literature stresses the importance of the ICT infrastructure in supporting smart city planning and control. It is also described as a city's digital nervous system that is not only capable of receiving information from different numerous sources (sensors, systems, organizations, etc.), but is also capable of analyzing and correlating actions from the sensed data through sophisticated systems (Hall, 2000; Marsa-Maestre et al., 2008). ICT is expected to solve many problems of urban living and growth, such as traffic congestion, waste of resources, etc. Extensive ongoing research on wireless possibilities is examining the effects of integrating a large number of sensors in smart cities through LTE, Wimax or WAVE (Piro et al., 2014; Lynggaard and Skouby, 2015). The role of ICT integration and development will be of high benefit for the smart city (Mulligan and Olsson, 2013); Lynggaard and Skouby (2015) also discuss the implementation of 5G technologies on a smart city scale and the benefits that they could bring to the ecosystem in terms of power efficiency and better connectivity to IoT devices, in addition to opening new opportunities for big-data communication and smart services. Zanella et al. (2014) for example, discuss the complexity of the smart city and how the IoT could support the smart city infrastructure, such as buildings, waste management, noise levels monitoring, traffic management, air quality, energy efficiency, parking, and lighting.

Trying to define the role of ICT, Batty et al. (2012) discuss seven project areas for the development of smart city ICT. These areas include:

- “integrated databases”, that can consolidate mobility data from multiple sources, enabling better coordination and management;
- “sensing, networking and the impact of new social media”, that can support better response and interpretation of data from social media networks (transport, incidents, health, etc.);
- “modelling network performance, mobility and transport behaviour”, to better track mobile objects, better monitoring of the infrastructure using ICT (water, roads, energy, etc.);

- “modelling urban land use and transport”, that support better land usage efficiency to reach better transport;
- “modelling urban transactional activities in labour, housing and transportation markets”, that support new ways of how land and properties are developed, acquired or sold in the urban domain;
- “decision support as urban intelligence: real time modelling and participation in policy making”, that support the tools that could be used to support citizens’ participation and government decision-making;
- “City governance structures for the smart city”, that support governance frameworks to be used by governments to deal with big data capabilities.

Multiple issues involving transport and traffic congestion are expected to be solved using ICT-based enhanced mobility (Lynggaard and Skouby, 2015), through communication between moving vehicles, and between vehicles and the infrastructure; such would enable decreasing the requirements for user mobility and simplifying mobility options for citizens. Smart mobility would also help enhance the mobility experience of citizens by dynamically optimizing distribution of traffic load with respect to timing, capacity, incidents, etc. (Correia and Viegas, 2009). It would also support power efficiency and better connection signals between connected devices and services in the city (Lynggaard and Skouby, 2015).

Concerning the economy, the ICT infrastructure is expected to play an important role in smart city business environments. Many businesses will be offering services that are based on, and only possible through, the ICT infrastructure: ICT has already become an essential segment of competing economies (Dutta and Mia, 2010). In regard to the environment, the ICT infrastructure is expected to help the smart city better deal with environmental changes, especially in an economy that needs to be adapted for climate changes through the use of distributed sensors (OECD, 2009). Benefits also include better management of resources (e.g. power, water, etc.) and waste, leading to less pollution and better utilization of city resources.

ICT’s role in the development of human capital has already been deemed widely beneficial: E-learning portals, e-books are becoming standard for the new age learning, and content development. In addition, social networking platforms support better socialization and communication between people. Furthermore, online collaboration tools are helping run projects and distant cooperation through cloud computing technologies, reducing time and effort needed to achieve goals.

The maturity of the city governance, e-governmental services and citizens' identification are critical for smart city operations. Also, the development of the authentication and authorization systems that integrate with e-government services to operate successfully, while also guaranteeing citizens' data security and privacy, in all smart city operations. The development of solid policies and frameworks will give the smart city government the capability of monitoring, controlling and responding to events, and dealing with the use of personal data (Codagnone and Wimmer, 2007). Standardization and interoperability are highly important for the smart city components to integrate and communicate. The "Open Data Movement" is a global initiative trying to open government generated and collected metadata for usage and benefit of the public, and where applications could be run to use such for the public benefit.

Some researchers state that the ICT infrastructure should not be positioned as part of the smart city concept, but more as a general-purpose technology (Bresnahan and Traitenberg, 1995) that is complementary to humans and organizations, and that is developed and changed as needed by the city; they also state that ICT cannot evolve a city without the human capital. It is nevertheless well documented in the literature that ICT plays a major role in the development and evolution of the smart city. Even though that role should be governed by the needs of the human beings and their innovation, one cannot ignore the recent technological advancements that open many progress possibilities for the smart city and shape humanity's future (Angelidou, 2015). Merging the digital and physical worlds opens big opportunities to enable "really smart" devices with smarter automation and services (Want et al., 2015). By the use of ICT technologies, many citizens' activities are made much more efficient and productive. Examples include, but are not limited to, transport, work, learning, collaboration, socialization, and public services.

2.4 Smart City Performance Evaluation

In the previous sections, the role of ICT in modern world organizations and urbanization was analyzed. The development of smart cities and their different components was described. This section addresses the need to evaluate the performance of the smart city, identifying the most important pillars and enabling world scale competition and comparison between the urban cities.

The definitions of smart components proposed by researchers such as Nam and Pardo (2011a), Giffinger et al. (2007), and Lombardi et al. (2012) have been used to

develop key performance indicators, allowing smart cities to compare themselves to each other and rate their capabilities and “smartness”. Having these various definitions of components and goals set for the smart city concept, researchers have tried to develop evaluation capabilities for the testing of smart cities and measuring their capabilities. For example, Dameri (2013) developed a list of measurable goals of the smart city concept that could help compare the cities smartness and strength. There are several indicators for which to make such comparisons.

- Environmental efficiency and sustainability: one of the most important goals of smart cities is the ability to reduce energy consumption, pollution and waste. Utilizing ICT, results can be quantified and measured to enable a smart city to challenge and customize its ecological impact to levels not seen before.
- Life quality and well-being: an improved life quality for citizens is essential in smart cities. The ICT infrastructure, Government smart rules, policies and services, the smart economy, and energy efficiency will all play different roles to enhance the citizens’ living quality and ease.
- Participation: the people’s participation in the smart city’s governance is expected to be of high priority. Using the ICT-based e-democracy, citizens are expected to drive the decisions of the city by interacting and voting on goals, actions and priorities (Cardone et al., 2013).
- Knowledge and intellectual capital: one of the most important starting points of a smart city that reminds people that a smart city is not only about infrastructure and automated services. The intellectual capital of a smart city will be a major indicator of its innovation, economic and social development; it is also a major differentiator when comparing it with other smart cities.

A modified version of the “Triple Helix” (a system for the evaluation of knowledge-based innovation systems) was developed by Lombardi et al. (2012). They later modified the model to have a four-helix model: universities, industry, government and civil society. They also developed 60 indicators for the helices. Giffinger et al. (2007) developed 31 factors and 74 indicators for evaluating smart cities; they also tested their ranking system on 70 cities in the EU, which have a reduction in energy use and gas emissions by 2020 as their main goal.

Synthetic qualitative indicators are also receiving attention from smart city leaders, not only to best drive their decisions in terms of focus, time and resources, but also

to calculate and report smartness performance back to their citizens (Berardi, 2013a, 2013b).

Zygiaris (2013) identified six smart city layers for the measurement of city performance:

- the city layer;
- the green city layer (urban environment sustainability);
- the interconnection layer;
- the instrumentation layer (real-time processing of sensor data);
- the open integration layer (data sharing among city applications); and
- the innovation layer (encouraging environments for new ideas and businesses).

A methodology was also proposed by Lazaroiu and Roscia (2012) for the computation of smart city indicators; this methodology, based on fuzzy logic, is valid for both citizens and decision makers, and uses 18 indicators to measure the city's smartness. The Japanese Institute for Urban Strategies also developed the Global Power City Index to measure smart city strengths and weaknesses.

Neirotti et al. (2014) further identified the main application domains and subdomains for smart city integration and operations. Six main domains were determined ("natural resources and energy, transport and mobility, buildings, living, government, as well as economy and people"), including their corresponding subdomains. Neirotti et al. (2014) concluded that the main domains and subdomains for a city will vary and are highly dependent on the localization context. Therefore, policy makers are expected to generate their own contextually relevant studies to understand and evaluate a city's key domain and interests. Albino et al. (2015) also highlighted the smart initiatives that are ongoing in multiple cities (Seattle, Quebec, Friedrichshafen). Albino et al. (2015) noted the difficulty with which smartness can be measured, stating that measurements should take into consideration the city's priorities and visions towards their objectives, in addition to the qualities of people and communities. They conclude that it would be difficult to develop a universal smart city measurement tool.

Bakıcı et al. (2013) also explored the smart city strategy in the case of Barcelona in terms of infrastructure, living labs, open data, initiatives, and services. Sanchez et al. (2014) and Lanza et al. (2015) describe the deployment and experimentation of

the IoT at an experimentation facility in Santander (smart Santander). They developed a framework with the main components to be considered for the deployment of large scale IoT testbeds and concepts under real-life situations. Dubai city is another new example of the smart city initiative, developing telecom, transportation, healthcare, buildings, utilities, tourism, education and public safety to meet higher standards and smartness needs (KPMG, 2015).

In a competitive world, smart cities require huge development and planning efforts. The continuous evaluation and assessment of a smart city's evolution and progress is essential to its success and for minimizing the time and cost needed for its growth. The efforts should help it become successful and more appealing to the skilled human capital when compared to other cities.

2.5 The Role of Governance and Management in the Smart City

In previous sections, we identified the large role of ICT in the context of future smart cities. This section focuses on the aspects of technology management. Of course, technology itself cannot build the future; it is just a useful tool. The right management of technology towards the development and growth of smart cities is essential. While many scholars do not treat governance and management as separate, by definition, there is a difference. Governance is the act of planning and strategically driving an entity or organization towards its goals, scope of operation and maturity. Meanwhile, management is the act of controlling resources and capabilities to best achieve goals and follow the planned strategy.

Governance has also been identified as a core aspect of the smart city (Belissent, 2011). While discussing success factors of smart city initiatives, Chourabi et al. (2012) discuss managerial and organizational factors as major challenges and key success factors, but ones that also need to be discussed in the context of extensive e-government and IT projects literature. Chourabi et al. (2012) also consider governance as a big challenge for smart cities, especially regarding the need to adapt laws, regulations and policies to the smart city context: changes are needed at the governance level. Gil-Garcia and Pardo (2005) discussed the challenges of advanced environments relying on IT projects, identifying multiple organizational and managerial issues that could be of significance to organizations. These include the size of the project, management behaviour, organizational diversity, alignment, and change resistance.

Researchers have also agreed that management and governance issues, especially related to the smart city context, have only been addressed in a few studies (Chourabi et al., 2012; Gil-Garcia and Pardo, 2005). In the same context, while Whitmore et al. (2014) justify the large amount of research in IoT technology due to its lack of maturity, they conclude that when technology matures, IoT and smart cities' research will broaden to include management issues and other aspects such as law and economics. The same could also be justified by the fact that technology research in the context of smart cities is being pushed by international technology vendors and marketing campaigns in order to gain long term markets for their products (Kitchin, 2014; Söderström et al., 2014; Hollands, 2015; Mulligan and Olsson, 2013). That is also why Hollands (2008, 2015) and Söderström et al. (2014) warned of vendors leading smart cities, and enticed the consideration of other smart city aspects such as education and the human capital development to sustain future growth for the people, not the corporations.

Past research divides governance of smart cities in multiple ways. Smart cities differ in their principles on the smart governance and varying requirements on the amount of changes needed to achieve a "smart city" or "smart governance" status. The opinion of some researchers is that no changes are needed, that there will be no need for changing government structure and processes, and that managing a city that calls itself smart is the result of smart decisions that are right for such a city and which is doable by governmental management institutions (Batty et al., 2012). Giffinger et al. (2007) state that smart governance incorporates political participation, citizens' services and administrative functions.

Researchers have emphasized aspects unrelated to government operations to build a smart city. Alkandari et al. (2012) indicate that government should approve and prioritize the development tasks and missions in the smart city. Nam (2012) links smart governance to the contribution to smart city initiatives. Winters (2011) argues that a government can build a smart city only by further advancing higher education.

Other researchers state a need for little changes, stressing the need for new decision-making processes in smart city environments. UNESCAP (2007), for example, describes smart governance as "the process of decision-making" and then how these decisions are undertaken. Walravens (2012) further develops the discussion by stating that smart governance could be renewed and innovated through network technologies. Schuurman et al. (2012) defines smart governance

as the process of the smart city collecting all sorts of data feeds from operations, citizens and smart sensor networks, and that advanced technologies, such as cloud computing, are utilized to decide on decisions that are needed for the evolvement of smart cities.

The opinion of another group of researchers is that medium changes are required, conceptualizing smart governance as the need for developing smart administration of the city. Gil-Garcia (2012) defines that as the need for new processes utilizing advanced, sophisticated ICT that are capable of integrating data from all smart city components (organizations, citizens, sensors, etc.) to develop a smart administration capable of choosing the best decisions for benefit of the smart city. Caragliu and Del Bo (2012) state that “space-specific characteristics could influence on the smart cities development and therefore, there is a need for geographically differentiated policy actions”. Batty et al. (2012) state that, “smart governance is a much stronger intelligence function for coordinating the many different components that comprise the smart city. It is a structure that brings together traditional functions of government and business”.

A third and last group of researchers suggest that major changes of the government role and positions should be considered to create a smart governance status. Tapscott and Agnew (1999) indicate that future governance is the result of collaboration between the different communities using technologies to achieve facilitated enhanced decision-making. Bătăgan (2011) defines smart governance as the collaboration between government departments, institutions and communities to promote economic development and to make the city operations “citizen-centric”. Schuurman et al. (2012) stress that smart city governments are asked to play a central role by involving all smart city stakeholders into creating an information- and communication-based participatory environment for decision making. Kourtit et al. (2012) and Cardone et al. (2013) stress that “smart governance is the pro-active and open-minded governance structures, with all actors involved, in order to maximize the socio-economic and ecological performance of cities through feedback and stakeholder participation, and to cope with negative externalities and historically grown path dependencies”.

Nam and Pardo (2014) focused on government changes needed for smart governance on management and service delivery: innovation in management to best use resources that are available for the city, but also for better collaboration

between organizations; innovation in service delivery for the government to offer the best services and satisfy citizen's needs. Ferro et al. (2013) expected smart city development to drive significant changes in the management of smart cities through innovative ICT based participatory "extended governance". The role of ICT during the migration to the smart city in relation to the governance, is also described in three roles by Ferro et al. (2013) and Kramers et al. (2014): "The enablement of new production, distribution and governance processes", "The transformation of organizational and institutional arrangements", and "The information of individual choices and behaviours".

2.5.1 Smart cities governance organizational factors in the literature

There is a wide range of organizational factors that impact smart city organizations. These factors are scattered in the literature. The following table presents the most prevalent and cited organizational factors that impact smart city organizations' growth and prosperity. The purpose of this table is to enhance the visibility of these factors.

Table 2.2: Table of Smart Cities Governance Organizational Factors

Organizational factor	Definitions	Literature reference
Project size	The management of larger projects increases the complexity and aspects that need to be monitored and tested, therefore requiring more governance	AlAwadhi and Scholl, 2013
Leadership, managers' attitudes and behaviour	Leadership intelligence and attitude is essential towards the adoption of smart operations and smart behaviour by the employees	AlAwadhi and Scholl, 2013 Nam and Pardo, 2013 Giffinger et al., 2007

Organizational diversity	Organizational diversity helps in enriching the organizational culture and growth development	AlAwadhi and Scholl, 2013
Alignment of organizational goals with business	Alignment of business and organizational goals with the business is essential for the organization's employees to best know where it is going and what it needs to reach	AlAwadhi and Scholl, 2013
Legislative compliance, reformed governance and regulations	Legislations are developed in order to define a baseline for organizations to have a minimal level of safe and stable operations; they also need to be met to sustain normal business operations in the smart city	AlAwadhi and Scholl, 2013 Chourabi et al., 2012 Bătăgan, 2011 Schuurman et al., 2012 Ferro et al., 2013 Kourtit et al., 2012 Cardone et al., 2013
Compliance to change	The smart city concept requires organizational changes and transformations; the intention and capability of meeting the required changes is essential for sustaining business growth in smart city environment	AlAwadhi and Scholl, 2013
Vendor independence	Vendor independence is an important aspect of smart city operations; organizations are expected to	Mulligan and Olsson, 2013

	independently assess and evaluate vendors' solutions and adopt the ones that match their own needs	Kitchin, 2014 Hollands, 2008 Hollands, 2015
Financial resources	Financial resources are key for advancing an organization, which needs to position itself as competitive in order to gain market share and gain benefits	Nam and Pardo, 2013 Gil-Garcia et al., 2014
Human capital	Staff skills and training are essential for the most efficient organizational production and development; the more skilled the employees the better quality are the products and the production, helping the organization gain client satisfaction and lowering costs	Nam and Pardo, 2013 Longworth and Osborne, 2010 Shapiro, 2006 Hollands, 2008 Zygiaris, 2013 Kourtit and Nijkamp, 2012 Lombardi et al., 2012 Toppeta, 2010 Giffinger et al., 2007
Organizational innovation and transformation	Innovation is key for maintaining a competitive edge in smart city organizations, which are expected to keep adapting and offering new	Vilajosana et al., 2013 Nam and Pardo, 2013

	attractive solutions to solve client needs	Gil-Garcia et al., 2014 Nam and Pardo, 2011b Gann et al., 2011 Giffinger et al., 2007 Rios, 2012
Partners and stakeholders role and participation	Organizational stakeholders, partners and clients need to share feedback on organizations' services and offerings, that is expected to be a major method for organizations to know which changes are needed to apply and invest in	Vilajosana et al., 2013 Cardone et al., 2013 Giuffrè et al., 2012 Pardo and Nam, 2016
Government role, influence and support	Government is expected to be highly involved in smart city operations; they are also expected to require compliance for the different organizations	Nam and Pardo, 2014
Complexity and rapid technological changes	Organizations are expected to be flexible in adopting new needed technologies to help increase client base and increase "smartness"	Zanella et al., 2014 Hernández-Muñoz et al., 2011 Gil-Garcia et al., 2014 Domingo et al., 2013

		Bakıcı et al., 2013 Gil-Garcia, 2013
Best utilization of the ICT infrastructure	Organizations are expected to best utilize the smart city ICT infrastructure in order to offer the best quality services to clients	Nam and Pardo, 2011b Mulligan and Olsson, 2013 Gil-Garcia and Aldama-Nalda, 2013 Gann et al., 2011
Type of organization and business model	The type of organization will define the needed governance, to service other businesses/organizations and/or home clients, etc.	Kuk and Janssen, 2011 Anthopoulos and Fitsilis, 2014
Type of industry	The type of industry would help identify the characteristics to best match an organization; some industry types might have different needs, especially in terms of service quality, service defense and protection, etc.	Vilajosana et al., 2013 Kitchin, 2014
Bureaucracy	Smart city organizations are expected to minimize bureaucracy's negative aspects inside their organizations to increase efficiency and growth	Nam and Pardo, 2013
Organizational structure	Smart city organizations are expected to have highly efficient and adaptive	Gil-Garcia and Aldama-Nalda, 2013

	structures to meet smartness requirements	Gil-Garcia et al., 2014
Collaboration, cross/inter-organizational or inter-agency factors and interdependencies	Collaboration in between organizations is expected to reach new levels in smart city organizations to maintain high levels of communication, synchronization and efficiency; information integration and sharing among agencies could reduce complexities of end user services; sharing resources between organizations can also help reduce costs	Nam and Pardo, 2014 Nam and Pardo, 2011b Nam and Pardo, 2013 Hawryszkiewicz, 2014 Naphade et al., 2011 Vilajosana et al., 2013 Gil-Garcia and Aldama-Nalda, 2013 Gil-Garcia et al., 2014 Ahmad and Mehmood, 2015 Gil-Garcia, 2013
Inter-departmental governance and collaboration	Inter-departmental collaboration is expected to be governed by highly efficient controls inside smart city organizations to guarantee efficiency and business goals alignment	Nam and Pardo, 2013 Ahmad and Mehmood, 2015 Gil-Garcia, 2013

Inter-organizational competition	Smart city organizations need to stay competitive to be beneficial; they are also expected to be highly competitive	Nam and Pardo, 2013 Ahmad and Mehmood, 2015 Longworth and Osborne, 2010
Organizational risk management	Smart city organizations are expected to do continuous risk analysis to be able to proactively control assets and mitigate threats	Nam and Pardo, 2011b Kitchin, 2014

Source: Devised by author

While researchers have different opinions around the variety and size of changes needed to achieve the promised smart governance status, certain researchers define “smart governance” in short- to medium-term goals while others look at it more idealistically by suggesting the need for larger-scale, longer-term changes to the government’s role and its structure. This ambitious, yet critical, perspective aligns well with the highly competitive attitudes that appear to be influencing smart city planning (Hollands, 2008; Giffinger et al., 2007).

2.6 The Importance of Information Security

In the previous section, we introduced the evolution of modern urbanization and how the world is moving towards complex, highly urbanized regions that rely highly on digital technologies in the name of offering services and better living. In this section, we identify the knowledge in the literature around ICT and its role in modern economies and new technological developments. This section also details the issues of information security and the challenges posed for organizations. It then examines the information security management role in modern world organizations, and the difficulties organizations face to protect their business and clients while also detailing the consequences of mismanaging information security. This section also details the organizational factors that are likely to influence information security management in international organizations.

The term ICT emerged from information technology and communication technology. Information technology describes the hardware and software components that allow us to read and write information by digital methods. Communication technology is the term used to describe equipment, infrastructure, and software through which information can be sent, received and accessed, for example phones, Internet lines, etc. As per Dutta and Mia (2010), and Audretsch and Welfens (2013), ICT is a core tool of modern economies. The advances in ICT are transforming most modern economies while presenting new challenges to labour markets, the traditional learning environment, and everyday life in industrialized and developing countries. ICT also has pervasive effects influencing the evolution of economies and the people, generating new needs and challenges while at the same time furthering the interaction between them.

The rate at which organizational changes take place and new technologies emerge have led to an increased demand for human capital to promote the knowledge society in which the development, application of ICT, and continuous training to employees and citizens is crucial. In this document, the definition from OECD (2004) will be utilized: the term ICT is used to refer generically to the family of related technologies that process, store and transmit information by electronic means.

Big Data (also big data analytics) is one of the newest trends in ICT, as per McAfee et al. (2012). It is the capability of using advanced ICT tools to do the analysis of heterogeneous large amounts of digital information (e.g. Petabytes). Big Data also assists in correlating key trends and issues in real-time or near real-time that could, in the case of a business for example, provide data evidence to help business leaders enhance service performance and perform better decision making.

IoT (Internet of Things) refers to the interconnection of everyday things and objects, which are often equipped with digitized intelligence. IoT will increase the ubiquity of the Internet by integrating every object for interaction via embedded systems. This leads to a highly distributed network of devices communicating with human beings as well as other devices. Thanks to rapid advances in underlying technologies, IoT is opening tremendous opportunities for a large number of novel applications that promise to improve the quality of our lives. Cloud computing refers to the applications delivered as services over the Internet and the hardware and software in datacentres that provide those services (Armbrust et al., 2010). Cloud computing has also emerged in the last few years as an alternative for maintaining expensive

computing hardware. Clouds promise to address a large user base with different needs with the same shared set of physical resources; therefore, clouds promise to be an alternative to clusters, grids, and supercomputers for organizations and researchers.

The European Union and other international institutions have dedicated increasing efforts to shaping their strategies on future urban growth and prosperity; it is agreed that future cities would involve ICT driven forms of evolution. The OECD and Eurostat Oslo Manual (2005) stress the role of innovation in ICT sectors and provide indicators for analysing urban innovation. The development of the communication infrastructure is having a larger role in determining the economic performance of the future cities. In recent years, multiple ICT trends have gained attention. Big data analytics is also one that is expected to change the way businesses operate (McAfee et al., 2012); Internet of Things (IoT) and cloud computing have also gained much attention from researchers and practitioners from around the world, being two of the latest and most popular advances in ICT (Suciu et al., 2013).

The aim of information security is to ensure business continuity and minimize business damage by limiting the impact of security incidents (Von Solms, 1998). The international standard, ISO/IEC 27002 (2005), defines information security as the preservation of the confidentiality, integrity and availability of information (CIA). Information security is therefore the process and controls put in place to guarantee data access is protected for reading by authorized personnel only, writing by authorized personnel only, and its readiness is protected when needed by authorized parties, etc. In another definition of the information security concept, researcher Thomas Peltier (Peltier, 2002) defines it as based on the following aspects: information security should be of support for business goals and objectives. Senior management is assigned two main duties, duty of loyalty (decisions made in the interest of the enterprise), and duty of care (commitment and decisions for the protection of the business enterprise). Information security and protection controls should only be introduced when a risk is confirmed; they need to be cost-effective. Information security roles and responsibilities should be made public to all employees through the utilization of the information security policy. The information/asset owner is responsible for the monitoring and control of the information/asset usage in addition to the authorization of the users. They should also verify compliance with the information security policy and ensure that the system is appropriately secured.

Information protection requires a comprehensive approach that follows a system development lifecycle. Information security should be periodically re-assessed and verified, based on objectives and requirements. In addition, information protection is directly impacted by the organizational culture. Information security management should be involved with business units to best understand their needs and determine the solutions that best protect assets.

Information security has been identified as an important aspect of the smart city concept (Whitmore et al., 2014) where billions of sensors will be running and generating traffic that need to be controlled and monitored and where each sensor could be important for the life of citizens. Threats to critical infrastructure could have devastating results to the city's national security, economy and citizens (Amin, 2002; Ruiz-Romero et al., 2014).

Securing digital services is a major concern for modern organizations. While businesses do their best to build their services strength, cyber criminals are looking for their own illegal benefit; crime has been moving to the digital realm and cyber attackers are more powerful than ever in the last few years. Carefully choosing targets and maximizing damage, they are organized and skilled (Dlamini et al., 2009; Roman et al., 2011; McDaniel and McLaughlin, 2009). Technological advances in the IoT and the migration to smart cities will bring changes and benefits to the quality of life, services for citizens and organizations. However, connecting things also has an impact on the security and privacy of the stakeholders' more devices are expected to generate more risks and without standards or regulations to rule providers and beneficiaries, threats to the realm become inevitable.

Researchers are also considering that future networks will be based on different models from current networks, and for security to be built from within, not as an add-on. Marias et al. (2011) identify multiple "security by design" concepts that could be useful for future networks. These concepts are summarized in multiple concepts.

First, the physical layer security: correct physical security would help in providing hassle-free lower error environments for the transport of information; it will also support in the protection against criminal activity.

Second, network coding security: robust, secure coding will help the status of information security for smart city solutions, also helping solutions to contain and self-defend against potential threats.

Third, the network infrastructure security: network security is not only essential for the protection of all network components against cyber threats, but also for alerting against sources of attacks and for the logging/auditing of the network traffic.

Fourth, the security in Information Centric Networking (ICN): ICN has been defined as a possible replacement for the current Internet (Ahlgren et al., 2012), seamlessly embedding new technology and security features to enhance mobility, flexibility, and scalability. Fabian and Günther (2009) also detailed the need for an enhanced international legal framework to address IoT characteristics, particular globality, verticality and the personality of the future world; they also detail Privacy Enhancing Technologies that could support in satisfying privacy requirements.

Fifth, the Virtual Private Network (VPN): the VPN tunnels traffic and helps provide integrity and confidentiality of data; however, this solution is not scalable for global information exchange.

Sixth, the Transport Layer security (TLS): this is implemented at the connection level to provide confidentiality and integrity; it also causes an overload of traffic because of the different traffic layers.

Seventh, DNSSEC: DNS has long been used to resolve hostnames to IP addresses on global systems. DNSSEC couples DNS with Public Key Infrastructure (PKI) to secure and guarantee safe name resolution to correct IP addresses; however, deployment of DNSSEC on a worldwide scale is needed for effectiveness.

Eighth, onion routing: this is used to protect privacy and anonymity, which enables traffic to be hidden and routed through multiple nodes before reaching its destination; it also adds multiple layers of encryption, scalable but layers of encryption could affect delay and performance.

Ninth, Private Information Retrieval (PIR): PIR is used to keep client requests for information private, enabling an anonymous exchange of information. Although scalable, key management and performance issues make this technology more difficult to implement.

Researchers already determined Information Security and privacy issues to be one of the biggest obstacles to the rapid large-scale adoption and upgrade of current urban cities to smart environments. Cyber threats include blocking or crashing services in smart cities. Being practical about the risks and security/privacy

problems that may arise, and how to deal with them, would be essential for smart city costs, environment effectiveness and continued liveability (Gubbi et al., 2013; Weber, 2010; O'Neill, 2014; Bekara, 2014; Naphade et al., 2011; Martinez-Balleste et al., 2013; Elmaghraby and Losavio, 2014; Roman et al., 2011; Bélanger and Crossler, 2011; Kitchin, 2014; McDaniel and McLaughlin, 2009).

2.7 The Smart City Organizational setting

As one of the smart city stakeholders, organizations are at the core of the city's operations; they are expected to offer job opportunities for citizens and deliver the smart services that are expected from today's cities (i.e., services that are advanced, efficient and sustainable). However, to align with the smart city model, businesses need to adapt. There are several factors that impact the businesses in smart cities. Harrison et al. (2010) propose the need for instrumented enterprise business processes to have visibility over the smart city world in real-time (e.g., data, sensors), using interconnected enterprise computing platforms to process smart city real-time data through complex analytics, and to collaborate with other city operations, services and businesses. Intelligent operational processes are then expected to deliver optimized services with high efficiency, engaging interaction with the citizens, and supporting better decisions. Cloud-based architecture, for example, is an important aspect of the smart city premise. Cloud-based solutions are capable of delivering much needed processing power to achieve better process optimization, data access and exploitation. This achievement needs to be obtained at a reasonable energy cost, while ensuring the strong, uninterrupted performance essential for building and sustaining smarter enterprises (Chelliah, 2014). The following is a description of the business identity in the smart city and how such could be defined and tested.

The selection of the smart city as the context of this research brings in multiple novel aspects. On one side, as per the literature review, the ISM related organizational factors have not been tested before in a smart city context, which uncovers a new research area and then potential for contribution to theory. The context will also include organizations which are highly demanding and demanded, therefore creating a new environment for employees and the management of information security issues, which emphasizes high efficiency and automation. The research also needs to evaluate organizational factors influencing ISM in smart cities, comparing them to evaluation of organizational factors influencing ISM in non smart

cities. On the other side, the smart city organizational context also opens up challenges and complexities for this research, the study needs to be able to select study participations from cities, which need to be classified as smart. Another challenge is that world cities have different priorities and are therefore smarter than others in specific areas but not others.

Businesses are the main driver of smart cities; they are expected to leverage its infrastructure to offer world class services that enhance its citizens' quality of life. They are also affected by the city problems and should be involved in the city's decision-making processes (Gann et al., 2011). Businesses should be informed by evidence-based practices and have a vision of organizational evolution (Mulligan and Olsson, 2013). Most businesses will fall under at least one of the six business categories described by Mulligan and Olsson (2013):

- organizations that study and operate environmental improvements;
- organizations that develop economy and growth;
- organizations that study and analyse cost efficiency;
- organizations that care about safety;
- organizations responsible for the quality of life; and
- organizations that care of the ICT infrastructure, best mobility and connectivity options.

Kuk and Janssen (2011) also discussed the business models that could be adopted by businesses in the migration to smart cities, concluding that when business models are prioritized and precede the information architecture, a business is capable of delivering new services to the public faster. On the other hand, if the information architecture precedes the business model, the delivery of new services is slower and more resource intensive, even if better, more sustainable services are achieved over time.

Kuk and Janssen (2011) identified multiple business models that fit the smart city:

- 1) the content providers, which are organizations that deliver data services and news;
- 2) the direct-to-customer, which deliver services directly to users or businesses;
- 3) the value-net-integrators, which collect and perform data analytics on information from multiple sources, then deliver correlated information based on the analysis;

- 4) the full-service providers, which develop multiple departments or organizations to offer a full end-to-end service to its clients;
- 5) infrastructure service providers that offer the infrastructure as an enabler for smart businesses and citizens to run the services;
- 6) market analysis providers, which help to match supply and demand of services, products, human capital;
- 7) collaboration providers, which offer the services that enable citizens' participation in the smart city decision-making; and
- 8) virtual community providers that help create and develop communities based on interests, but also encourage the sharing of content inside such communities.

Kuk and Janssen (2011) concludes by highlighting the need for a balanced approach between business models and information infrastructure to achieve short term business goals without damaging innovation and service sustainability in the long term.

Anthopoulos and Fitsilis (2014) also concluded that there were five types of organizations in smart city environments:

- 1) public organizations handling state responsibilities;
- 2) public-private-partnerships where the government assigns project execution to private companies;
- 3) state owned enterprises or new organizations that are created to develop or supervise a project;
- 4) private companies that execute projects; and
- 5) project companies that include alliances from different organizations to execute a project.

Vilajosana et al. (2013) analysed the difficulties that businesses face in smart city environments and proposed a procedure for big data utilization through API stores, "google-maps-like" that offer extended data for a license fee. They also highlight the need for smart city departments (similar to IT departments) inside organizations to build smart city capabilities. Further, Vilajosana et al. (2013) highlight the growth of a smart city business as three dimensional: 1) political, calling for the development of smart city departments, 2) technological, calling for platforms capable of managing and processing the huge amounts of data available in the smart city, and 3)

financial, calling for a sustainable business model enabling the smart city business to succeed and sustain growth.

The research by Vilajosana et al. (2013) also proposes a three-phase smart city business growth model: 1) the bootstrap phase, where services are offered for revenue, initiating future developments, 2) the growth phase, where investments are put into the expansion of new services, and 3) the wide adoption phase, where services are offered on a wide scale. The research also highlights the important role of the citizen in the process, as not only the consumer of smart services, but also having a voice in smart city utility development.

While discussing smart city governance, Nam and Pardo (2014) describe the metrics for assessing smart governance initiatives by measuring efficiency, effectiveness, transparency and collaboration. Nam and Pardo (2014) also categorize governance challenges and opportunities as:

- 1) technological factors, which are the technical aspects and technologies needed to implement smart governance services running through the ICT infrastructure;
- 2) organizational factors, which consist of budgetary challenges, employees' skills and organizational culture; these are to be considered to better enhance city efficiency and transparency; and
- 3) cross-organizational challenges that mostly lie in interdepartmental or interagency information sharing, requiring a governance body to rule over conflicts and control sharing agreements and cross boundary collaboration.

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

Smart cities are mainly composed of organizations and the people employed or benefiting from these organizations. Smart city information security then applies this directly to its organizations. This research is focused on identifying organizational aspects that influence information security management, which, in the context of smart city organizations, are represented and measured in how they influence organizational performance.

The inter-organizational aspects are also expected to be more developed in smart city environments; organizations have to adapt to deal with a set of issues that are more social and organizational than technical or physical (Nam and Pardo, 2011b). Nam and Pardo (2011b) described issues that are associated with a variety of smart city stakeholders, high levels of interdependence between services and organizations, and competing values amongst them (Nam and Pardo, 2011b; Naphade et al., 2011). Smart city innovation requires interoperability and data sharing among organizations. Strong leadership is expected to drive such measures within organizations to fulfill cross-boundary collaboration capabilities, particularly applying ICT driven organizational and structural changes.

There are different levels of complexity in dealing with such challenges related to the type of task being implemented or developed, whether it is intergovernmental, interorganizational or intraorganizational, or whether it is programme/project specific or enterprise/organization specific. Such smart city activities require the cooperation of different stakeholders, including governmental, private, non-profit firms or citizens (Nam and Pardo, 2011b). In the scope of smart city organizational collaboration, Hawryszkiewicz (2014) proposes a cloud-based model “for a system of systems” to enable large scale collaboration to resolve issues such as space usage and to enact clearly defined communication flows. The present study may elucidate the complexity of such challenges further by exploring the organizational factors that influence information security management, enabling a better understanding and analysis of the dynamics in play and how they influence organizational performance.

2.8 Information Security Management (ISM)

Governance in an organizational context is the development of a management framework to strategically drive the business processes and support compliance with regulations. Governance is planning for effective management, where management is the application of operational decisions (von Solms, 2005). Information security management is a necessity for business survival in the new digital world; its main goals are to protect confidentiality, integrity and availability, and it has an essential role in today’s organizations (Johnston and Hale, 2009; Chang and Ho, 2006; Posthumus and von Solms, 2004). Information security management standards are core fundamentals that control the arrangements of information systems (Backhouse et al., 2006). There are multiple standards for addressing information security management in organizations (COBIT, ISO 27001/2,

etc.), and combinations of multiple standards that can help organizations define roles and govern information security (von Solms, 2005).

It is worth mentioning that management attention to information security has been low compared to other information security issues, such as the technical side. However, the different aspects of information security, such as economic, financial and management, are complements to the technical side and not substitutes (Hong et al., 2003; Chang and Ho, 2006).

Information Security management roles can be defined as follows (Williams, 2001; Moulton and Coles, 2003; Zafar and Clark, 2009; Johnston and Hale, 2009):

- Defining security roles, responsibilities and applications: relevant when discussing the accountability of users to specific information security occurrences within organizations.
- Defining goals for security: goals should be built using the business model and defined needs. The classification of systems and data could also come into play when defining the security goals; different organizations with different data will have different security goals.
- Strategies for Security: strategies should comply with business needs. This comes to play when planning the future of business services and legal/regulatory compliance.
- Risk assessment and management: especially useful when policies are being developed, it helps in defining and taking ownership of risks to later define the controls to avoid, mitigate/control, accept or transfer the risks. Risk assessment and controls definition are also highly connected to the asset classification.
- Resource management for security: defining the ISG structure needed is important for running safe operations (Boss et al., 2009), achieve information security goals, monitor the security status and respond to threats.
- Compliance with regulations and rules: organizations need to comply with regulations to be able to run their business; compliance is needed to ensure the correct security measures and responsibilities are implemented. Investor relations and communications activity (in relation to security goals).

Information security management is a prime component of almost every modern organization that needs to deal with digital information as a business asset.

Information security is a key component of such organizations, and the governance

of information security enables organizations to add value to products and services, reduce costs and meet customer requirements. The importance of information security was mainly driven by the penetration of the Internet and e-services (Chang and Ho, 2006).

In a smart city context, the governance of information security issues inside each organization is crucial, not only for defending against threats and hazards, but also in defining recovery and continuity methods in case of problems that not only affect the organization itself, but that could easily extend to partners and clients.

The impact and role of information on corporate governance was initially discussed by Lindup (1996) and Von Solms (2001) during the early years of IT infrastructure adoption into businesses operations. The role of information security within organizational governance is to define best practices, improve employees' behaviour, strengthen business controls, and define accountability. Establishing information security governance and management requires the involvement of senior management. The sharing of information and visibility on incidents and ongoing is important for business success in decision making; it does this by ensuring alignment with business goals and to the prioritization of security investments that best deal with risks (Williams, 2001; Baker and Wallace, 2007). Hollands (2008, 2015) and Söderström et al. (2014) repeatedly emphasized the importance of balanced governance in smart cities to best meet citizens' needs, and they warned of pro-business entrepreneurial governance models of urban development that are sponsored by corporate marketing and serve their benefit more than the citizen's; the same phenomenon is also described by Kitchin (2014) as "the corporatisation of city governance and a technological lock-in".

The role of ICT during the migration to the smart city in relation to the governance, is also determined in a conceptual framework in Ferro et al. (2013) as the development and execution of new production, distribution and governance processes, and the improvement of organizational and institutional operations. Researchers in Ferro et al. (2013) also note that smart city governance needs to be built through the collaboration of government stakeholders and partners. It is also noted that "most public policies fail due to lack of attention", and that governments could benefit from an ICT infrastructure that builds attention to policies and collaboration on influencing, monitoring and supervising governance and policy programme design. This would not be possible without the smart city ICT

infrastructure; researchers named the before mentioned as the “extended governance” and to be the result of people’s participation in decision making and policy building.

The role of ICT in smart city governance is undeniable; it is especially interesting during the urban evolution that cities are going through, and will go through in the future. What is certain is that it will be more elaborate than current cities and will have more impact on the development of the smart city and its organizations. To date, there has been a notable absence of research on technology governance, especially within smart cities, which rely critically on ICT and IoT; such could only be substance for failure.

2.8.1 ISM organizational factors in the literature

There is a wide range of organizational factors that impact the information security management of an organization. They are scattered in the literature and discussed in the context of each research paper. The most prevalent and cited organizational factors that impact modern organizations growth and prosperity are listed in following table.

Table 2.3: Table of Information Security Management Organizational Factors in the Literature

Category	Organizational Factor	Definition	Supporting literature
Business efficiency issues	Business IT alignment	<p>Business and IT alignment is an essential aspect for the efficiency of defences and sustainable IT operations within a business with digital services. It also prioritizes investments and reduces costs of security implementation, thus enhancing the ROSI and protecting important assets.</p> <p>Success or failure determinants:</p> <ul style="list-style-type: none"> • Management role • Technology leadership role • Technology strategy • Trainings and socialisation • Size of the firm 	<p>Bruque and Moyano, 2007</p> <p>Hanan and McDowel, 1984</p> <p>Chang et al., 2011</p> <p>Williams, 2001</p> <p>Ross et al., 1996</p> <p>Dhillon and Backhouse, 2000</p> <p>Vermeulen and von Solms, 2002</p> <p>Bharadwaj, 2000</p> <p>Croteau and Raymond, 2004</p>

		<ul style="list-style-type: none"> • Need for Growth • Impact on power and hierarchies 	<p>So and Sculli, 2002</p> <p>Dutta and McCrohan, 2002</p> <p>von Solms and von Solms, 2004</p> <p>Santhanam and Hartono, 2003</p> <p>Choobineh et al., 2007</p> <p>Ittner and Larcker, 2003</p> <p>Herath et al., 2010</p> <p>Kayworth and Whitten, 2010</p> <p>Dehning and Stratopoulos, 2003</p> <p>Ma et al., 2009</p>
--	--	--	--

			<p>Siponen and Oinas-Kukkonen, 2007</p> <p>Smith and Jamieson, 2006</p> <p>Spears and Barki, 2010</p> <p>Van Niekerk and Von Solms, 2010</p> <p>von Solms, 1999</p>
	Bureaucratic aspects	<p>The bureaucratic standing is a strong determinant of the success of the changes and transformation that an organization decides to follow.</p> <p>Success or failure determinants:</p> <ul style="list-style-type: none"> • Workload pressure • Organizational function • Client requirements 	<p>Scott, 1997</p> <p>Bertelli, 2006</p>

		<ul style="list-style-type: none"> • Organizational culture • Organizational external environment • Rules and constraints 	
	Vendor selection	<p>Technology selection is essential a determinant to an organization's success. The right technologies enable adequate control and protection, in addition to introducing new functions and features.</p> <p>Success or failure determinants:</p> <ul style="list-style-type: none"> • Purchasing team characteristics and psychology • Interpersonal influence of organizational members • Organizational variables (such as finances) • Environmental variables (such as legal) • Quality/prive ratio 	Wind and Robinson, 1968 Weber et al, 1991

		<ul style="list-style-type: none"> • Vendor reliability and support • Vendor location/presence • Vendor reputation • Vendor resources and innovation • Vendor history 	
Information Security leadership issues	Organizational identity of the CISO	Identification of the CISO role as one that has to be directly or indirectly involved in all business operations to insure adequate protection of assets and people	Ashenden and Sasse, 2013
	Leadership aspects	Leadership confidence is important to drive the culture and the changes needed. Success or failure determinants: <ul style="list-style-type: none"> • Experience • Human capital 	Ashenden and Sasse, 2013 Arvey et al, 2006 Kayworth and Leidner, 2002

		<ul style="list-style-type: none"> • Social potency • Innovation and mentoring role • Coordination and clarification role • Monitoring and influence role 	
Organizational size		The size of an organization is a large determinant of the security defences' complexity, the resources needed and the cost of protection	<p>Kankanhalli et al., 2003</p> <p>Chang and Ho, 2006</p> <p>Goes and Park, 1997</p> <p>Yang et al., 2005</p> <p>Raymond, 1990</p> <p>Hoffer and Straub, 1989</p> <p>David, 2002</p>

<p>Inter-organizational and Intra-organizational collaboration</p>		<p>Inter-organizational and Intra-organizational collaboration have been a challenge for organizations due to logistical, trust, legal, bureaucracy or other reasons. Organizations and governments need frameworks to enforce collaboration through information sharing, especially around information security issues. The collaboration between teams of a single organization and between different organizations is important for sharing experiences and learning about new threats and challenges.</p> <p>Success or failure determinants:</p> <ul style="list-style-type: none"> • Financial resources support • Formally appointed personnel • Compatibility and standards • Clarity of goals and common interest • Incentives • Trust 	<p>Sayogo and Gil-Garcia, 2014 Page Hocevar, 2006 Yang and Maxwell, 2011</p>
--	--	---	--

		<ul style="list-style-type: none"> • Power and political influence 	
Organizational type of industry		<p>The organization type is a large determinant of the type and cost of assets that need to be protected, and therefore the cost of securing those assets.</p> <p>Success or failure determinants on industry influence on ISM:</p> <ul style="list-style-type: none"> • Organization sufficient awareness of industry related threats • Asset management capabilities of an organization • Dependence of the organization on information security 	<p>Kankanhalli et al., 2003</p> <p>Chang and Ho, 2006</p> <p>Goodhue and Straub, 1991</p> <p>Stanton et al., 2005</p>
Uncertainty of environmental elements	Rapid change of technology and complexity of such	Rapid technological and complexity changes need to be resolved by organizations in order to maintain the competitive edge and security efficiency	<p>Chang and Ho, 2006</p> <p>Audestad, 2005</p> <p>Jivnani and Zelkowitz, 2002</p> <p>Chou et al., 1999</p>

	Competitors' behaviour	Competitive behaviour could indicate new types of challenges and threats to the business	Chang and Ho, 2006 Bharadwaj, 2000 Croteau and Raymond, 2004
	Customer security requirements	Customers' data and assets have security requirements that should be met in order to be compliant and maintain client satisfaction	Chang and Ho, 2006
	Changes in legislation	Changes in legislation could indicate actions and technologies that must be implemented or customized to sustain business compliance and operations	Chang and Ho, 2006
Organizational support	Top management support	Top management support is one of the main factors to lead security efficiency inside an organization; without top management support, projects may not be fully implemented and employees may not comply with security requirements, resulting in devastating results	Aksorn and Hadikusumo, 2008 Kankanhalli et al., 2003 Barling et al., 2002 Chang and Ho, 2006

			<p>Chang and Lin, 2007</p> <p>Knapp et al., 2006</p> <p>Posthumus and von Solms, 2004</p> <p>Kayworth and Whitten, 2010</p> <p>Ma et al., 2009</p> <p>Smith and Jamieson, 2006</p> <p>Straub, 1988</p> <p>Straub and Collins, 1990</p> <p>Barlette and Fomin, 2009</p> <p>von Solms, 1999</p> <p>Werlinger et al., 2009</p> <p>Yildirim et al., 2011</p>
--	--	--	--

	Information security projects financing priority	The priority of security investments could be urgent in some cases in order to maintain business success; this is due to new types of attacks	Williams, 2001 Gil-Garcia and Pardo, 2005 Aksorn and Hadikusumo, 2008 Herath and Herath, 2009 Smith and Jamieson, 2006 Baker and Wallace, 2007
Organizational structure effectiveness	Organizational structure highly influences the efficiency of large scale cross-departmental security implementations and the compliance of users with security requirements	Boss et al., 2009 Williams, 2001 Moulton and Coles, 2003 Knapp et al., 2009 Kayworth and Whitten, 2010	

		<p>Employees' interest in security measures, understanding the need and willingness to participate</p> <p>Success or failure determinants:</p> <ul style="list-style-type: none"> • Work environment and culture • Team or co-workers relationship • Leadership role • Training and career development 	<p>Ma et al., 2009</p> <p>Zafar and Clark., 2009</p> <p>Seetharaman et al., 2006</p> <p>Straub, 1988</p> <p>Straub and Collins, 1990</p>
Organizational awareness	Employee engagement		<p>Ashenden and Sasse, 2013</p> <p>Anitha, 2014</p>

		<ul style="list-style-type: none"> • Compensation • Organizational policies 	
	<p>Staff and management, awareness and training</p>	<p>Training and awareness on modern types of attacks and how cyber criminal could cause damage to an organization are essential in order to prepare employees to have security alertness when something happens</p>	<p>Aksorn and Hadikusumo 2008 Culnan et al. 2008 Straub and Welke, 1998 Kayworth and Whitten, 2010 Ma et al., 2009 Gil-Garcia and Pardo, 2005 Siponen et al., 2009 Smith and Jarnieson, 2006 van Niekerk and von Solms, 2010</p>

			von Solms, 1999 von Solms and von Solms, 2004 Werlinger et al., 2009 Yildirim et al., 2011
	Information security culture	Developing a security culture that is supportive for security behaviour and the overall security status inside an organization	Chan et al., 2005 Chang and Lin, 2007 Martins and Eloff, 2002
	IT Competencies	Staff IT skills are a big influencer of security maturity, in order to find and block cyber threats inside or outside an organization	Chang et al., 2011 Eloff and Eloff, 2003 Bassellier et al., 2001 Gil-Garcia and Pardo, 2005

			Alshawaf et al., 2005 Davies, 2002 Dehning and Stratopoulos, 2003 Kayworth and Whitten, 2010 Stewart, 2005 von Solms, 1999 Florida, 2002
	Risk management	The role of risk management is essential in identifying the sources of the threats, the rank of the threats, the at-risk assets and then the needed measures	Herath et al., 2010 von Solms and von Solms, 2004 Straub and Welke, 1998 von Solms, 1999
Security controls development			

			Williams, 2001 Moulton and Coles, 2003 Zafar and Clark, 2009
	Security policies implementation	Security policies represent organization specific information security practices that employees are expected to meet; they also define ownership of assets and therefore responsibilities	Siponen and Oinas-Kukkonen, 2007 von Solms, 2001 Straub and Welke, 1998 von Solms, 1999 Yildirim et al., 2011
	Standards compliance	Security standards represent best practices and rules that each healthy organization is expected to meet, and could act as guidelines for the development of company policies Success or failure determinants:	Murithi et al, 2011 Backhouse et al., 2006 Chang and Ho, 2006

		<ul style="list-style-type: none"> • Financial means • Complex requirements • Lack of trainings and assistance • Strategy and realistic conditions 	<p>von Solms, 2005</p> <p>von Solms and von Solms, 2004</p> <p>Hanseth and Braa, 2001</p> <p>Gil-Garcia and Pardo, 2005</p> <p>Smith and Jamieson, 2006</p> <p>von Solms, 1999</p> <p>Yildirim et al., 2011</p>
	Performance evaluation, controls effectiveness and quality assurance	Monitoring the information security risk and progress within an organization is essential for the determination of the security maturity status and required measures to move forward.	<p>Kahraman, 2005</p> <p>Nam and Pardo, 2011b</p> <p>Herath et al., 2010</p> <p>Ithner and Larcker, 2003</p>

			Morgan and Strong, 2003 von Solms, 2005 Seetharaman et al., 2006 Santhanam and Hartono, 2003 Croteau and Raymond, 2004 Gil-Garcia and Pardo, 2005 Kankanhalli et al., 2003 Huang et al., 2006 Martinsons et al., 1999 Mercuri, 2003
--	--	--	---

Source: Devised by author

The above table presented the categories and classes of the organizational factors that impact the information security of an organization as defined in the literature. The table has listed the factors that impact organizations; the goal is then to contrast such on the smart city related organizational factors defined in the literature.

2.8.2 ISM challenges

Information security products and technologies cannot defend an organization without the appropriate strategies and policies. Organizational aspects have a direct impact on the behaviour and efficiency of information security management.

However, it is confirmed, but repeatedly forgotten, that security is not principally a technical matter but a management or business issue (Dhillon and Backhouse, 2000; Vermeulen and von Solms, 2002; Dutta and McCrohan, 2002; So and Sculli, 2002; von Solms and von Solms, 2004).

Information security management in smart city organizations is expected to be impacted by many factors. First, technological factors, where solutions are needed to best meet organizational governance strategy for effectiveness and transparency, and protect against cyber threats in a connected world dependent on the confidentiality, integrity and availability of communication capabilities. Second, human and organizational factors, where the organization's size and culture, employees' diversity, skills and training, the organization's budgeting and financial capabilities, and management priorities are all factors that highly impact organizational performance and capabilities (Werlinger et al., 2009; Baker and Wallace, 2007; Herath and Herath, 2009; Ittner and Larcker, 2003; Morgan and Strong, 2003). Third, cross-organizational factors are also expected to impact information security management, availability and stability of services for partners, clients and interdependent organizations. The security requirements on interdependent organizations show the need for threat intelligence sharing and collaboration. Different challenges for information security management are detailed in von Solms and von Solms (2004). They describe ten information security management mistakes that count as "deadly sins" for organizations:

- not being aware that information security is a corporate governance responsibility;
- not being aware that information security is a business issue not a technical one;

- not being aware that information security corporate governance is a complex multidimensional issue that does not have a single solution;
- not building security planning based on business and organizational identified risks;
- not using or being aware of the international information security standards, guidelines and best practices;
- not having an information security policy;
- not having a mature information security corporate governance;
- not being aware of the need of doing user awareness on information security issues;
- not being aware of information security compliance requirements;
- not realizing information security managers cannot perform well without the right tools, infrastructure and commitment/support.

There are different organizational issues that challenge information security management in organizations. For example, Ashenden and Sasse (2013) discuss the struggles that Chief Information Security Officers (CISO) face as representers of organizational information security management when dealing with organizational issues. The research focuses on management issues in the context of information security and investigates the factors that most influence CISO success in an organization: enabling or disabling a healthy information security management status through business strategy and compliance, marketing, employees' engagement, CISO identity in the organization, lack of confidence, effectiveness evaluation, organizational structure, and social responsibility (Ashenden and Sasse, 2013; Boss et al., 2009). Ashenden and Sasse (2013) also emphasized organizational behaviour, where they prove that employee's reaction to information security management is positive when well informed and educated; however, this cannot always be true because human behaviour cannot be controlled or predicted. Ashenden and Sasse (2013) also indicated that autocratic attitude in an organization is highly damaging to the CISO role and is one of the biggest obstacles.

There are many other organizational issues that impact ISM in modern organizations that present serious challenges to the information security status. Information technology and information security's strategic alignment with business objectives is one that is well documented in the literature. Chang et al. (2011), for example, established its importance by stating that IT systems become more adopted for core modern enterprise activities. Doing so would stabilize systems and

smooth operations, enabling better performance. The alignment of the business with IT is also important for external business changes and the introduction of new challenges and business opportunities (Chang and Ho, 2006). That is, rapid technological development can introduce new threats and vulnerabilities to data (Chou et al., 1999).

The size of the organization is another factor that is documented in the literature to have an impact on the ISM status. Chang and Ho (2006) discuss that organizational size has positive relationship to technological innovation and technology implementation, stating that larger organizations usually have better human, technological and financial resources to better utilize information systems; they are also able to handle information security better with better resources, expertise, and training. In addition, David (2002) found that vendors are more willing to cooperate with larger organizations.

Industry type has long been used by researchers to investigate quality assurance, information and change management, and using IT systems for competitive behaviour (Chang and Ho, 2006). Goodhue and Straub (1991) initially proposed industry type as an important factor affecting ISM, and Stanton et al. (2005) found large variations in information security related behaviour in organizations whose type of industry relied more on information security. Kankanhalli et al. (2003) also concluded, for example, that financial organizations needed more information security to drive business, and therefore such would have an impact on ISM efforts.

IT competencies enable an organization to plan, execute and invest in information security effectively. Various researchers have highlighted the importance of a shared management of IT and ISM between IT professionals and business managers in an organization (Bassellier et al., 2001). If knowledgeable of IT issues, they would provide a boost for information security management status inside the organization, as found by Alshawaf et al. (2005) in a study on 62 executives.

Another examination of organizational capabilities was also undertaken by Hall et al. (2011), which examined the relationship between IS strategy and organizational performance. The study developed a survey instrument that was used to collect data, and hypotheses were tested utilizing structural equation modelling. The study found that the ability to develop quality situational awareness of the current and future threat environment, the ability to possess appropriate resources, and the ability to orchestrate the resources to respond to information security threats, are

positively associated with the effective implementation of information security strategy, which in turn positively affects an organization's performance. Similarly, Chang and Ho (2006) also investigated organizational factors on the effectiveness of ISM, and found that the IT competence of business managers, environmental uncertainty, industry type, and organization size, have a positive impact on the effectiveness of implementing ISM.

While there are a number of researchers who addressed the organizational factors that impact information security management in modern organizations and how these could be developed and maintained, there is no research focusing on exploring these factors in smart city development and performance. This is an important absence because smart cities are different. Organizations within them have a higher dependency on ICT, therefore requiring more ISM attention and research. Therefore, such a gap needs to be filled for a better understanding of how organizations can (or should) plan to deal with future IS and ISM issues. While most organizational factors that influence ISM in the context of smart cities may not be much different from current organizations, there may be new aspects that are specific to the smart city context alone.

2.9 Information Security in the Smart City

Previous sections have outlined the importance of the ICT infrastructure and its role in future cities. However, the wide adoption and dependence on digital solutions makes cities more vulnerable to digital threats. Information security is expected to be of major importance for all smart city operations; information confidentiality, integrity and availability (CIA) are essential if operations are to run efficiently and uninterrupted. Threats to information CIA are expected to have national significance. Any weakness or failure in core city operations could threaten the urban ecosystem and society's well-being at large (Sicari et al., 2015; Bekara, 2014; Gubbi et al., 2013; Li et al. 2012; Baumeister, 2010; Marias et al., 2011; McDaniel and McLaughlin, 2009).

Cavusoglu et al. (2004) concluded that the cost of poor cyber security is high for investors, with the breach impact not limited to a single organization. Cavusoglu et al. (2004) also concluded that the cost of a security breach for an Internet-only organization is higher than for conventional firms. Since a smart city will run with

highly interconnected ICT services, the critical power grid infrastructure will also be a function of this ecosystem. To date, the protection of technologies, challenges and strategies of critical infrastructure from cyber-attacks have been analyzed across a variety of studies (Metke and Ekl, 2010; von Solms and von Solms, 2004). Threats to the critical infrastructure could have devastating results for national security, the economy, and citizens. Information security and privacy maturity must be more crystallized than before IoT, and sensors could be deployed on a large scale (Gubbi et al., 2013; Amin, 2002; Ruiz-Romero et al., 2014; Naphade et al., 2011; Martinez-Balleste et al., 2013; Elmaghraby and Losavio, 2014; Roman et al., 2011; Bélanger and Crossler, 2011; Kitchin, 2014; McDaniel and McLaughlin, 2009).

Bekara (2014) identified security concerns and challenges that are threatening the smart city. Bekara (2014) segmented these concerns into three larger categories; security concerns, authorization and access control problems, and security challenges:

- security concerns;
 - identity spoofing: faking an identity that could be used for different types of attacks that could result in financial loss, and could be used as part of larger attacks to compromise systems and networks;
 - eavesdropping: communication interception that could be used to collect data and launch further malicious attacks;
 - data integrity: manipulation of content that could be used in attacks to perform unwanted malicious modifications;
 - availability issues: services availability and reliability are some of the most important for critical infrastructure and smart environments, relying on digital services to operate services;
- authorization and access control concerns;
- privacy issues: pervasive users' data collection by smart sensors could be maliciously used to perform malicious activities, therefore there is a need for its protection;
- security challenges:
 - scalability: the large number of sensors and smart grid systems spread over large areas need to be managed by flexible, scalable, compatible solutions. the security of these scalable solutions is therefore critical as their disruption could have a huge impact on the status of the smart city;

- mobility: in flexible mobile environments, there will be a challenge to comply with the need for continuous verification and identification of mobile devices and systems in order to resume mobile communication and services;
- deployment: since the physical monitoring of all sensors may not be possible in order to guarantee physical security, there is a need to define solutions to verify deployed smart grid systems are not tampered with;
- legacy systems: current and old running systems, found especially in critical infrastructure operations, have security challenges that need to be met before they are connected to the smart grid networks; this is to guarantee security and reliability;
- constrained resources: systems with limited resources need to run security functions that could be challenging, especially when talking about cryptographic algorithms;
- heterogeneity: there will be challenges for different systems from different vendors to run compatible encrypted communication;
- interoperability: even though similar to heterogeneity, interoperability is about the negotiation of functions and possible protocols/connections that are needed after communication is established;
- bootstrapping: how to securely load system firmware, encryption and security keys while devices are loading, without endangering content or the confidentiality of data;
- trust management: guaranteeing certain levels of trust is needed to permit the communication and analyses of data in between online services in the smart grid;
- latency/time constraints: services operating in the smart grid all need to respond to requests for the smart city to run smoothly without disruption in real-time.

One example of a critical component in a smart city is the smart grid. Its protection from threats is crucial for the survival of the city and its citizens. Baumeister (2010) and Wang and Lu (2013) specified the smart grid components that need to be protected for a self-healing, resilient environment, and the security architecture of the different power grid components that could be vulnerable. The first component is the process control system, used in smart environments to control and monitor the

different aspects of the electrical power grid. One of the biggest concerns would be the numerous entry points to the network, since the power grid has to be reachable everywhere. The second vulnerable component is smart meter security. Smart meters are used to monitor different aspects in smart environments and will be communicating data, which should be protected from being maliciously surveyed or manipulated. The third component is the power system state estimation security. This component is capable of controlling physical aspects of the power grid; the security here is important because it is used to maintain stable electric power systems. The fourth component, smart grid communication protocol security, is heavily relied upon as a smart city relies on communication with all different components. As such, communication should be secured and available in an effort to protect the status of the power grid. Finally, smart grid simulation for security analysis enables the testing of new solutions and methods for security issues, without having to test on the live power grid network. In such cases, the restart or disruption of services is also not possible, limiting the testing options to simulations only.

Smart sensors also have a crucial role in smart cities; they are integral components of almost any intelligent control system and have a wide variety of roles. They are evolving continuously in terms of technology and functions, but also in terms of cost, power efficiency and sustainability. In application, they are expected to support smart transport, smart buildings and smart homes (Hancke et al., 2012; Ding et al., 2011). Sensors need to be secure to run safe, stable operations. Smart sensors would rely on advanced communication technologies, wired or wireless, to communicate with control systems. Example technologies could be Dash7, Zigbee, 5G, LTE/4G, 3G, RFID, NFC, Bluetooth, or Cloud computing (Hancke et al., 2012, Want et al., 2015; Lynggaard and Skouby, 2015), and their role in enhancing urban living in the smart city or at home (GhaffarianHosseini et al., 2013).

Smart cities are expected to utilize natural resources and manage waste more effectively (Lombardi et al., 2012). Researchers have highlighted several challenges of planning water facilities and infrastructure. Challenges include security and integration with the ICT, guaranteeing water resources, intelligent water flow control, minimized water infrastructure risks, and energy efficiency (Lee et al., 2014; Lazaroiu and Roscia, 2012). The power grid or electrical grid is also one of the main components of a smart city. Future cities have increasing power demands but need decreasing power utilization. Having the smart grid connected, automated,

integrated, controlled, and managed is expected to be of high importance for improving eco-efficiency and resource utilization through the more effective monitoring practices (Moreno et al., 2014; Vassileva et al., 2013; Kramers et al., 2014; Battista et al., 2014). Securing such an infrastructure would then become indispensable for grid operation (Shuaib et al., 2013; Chourabi et al., 2012).

Privacy issues are also of major concern for smart cities. Services operate through the sharing and analysis of pervasive information from users. Research has been conducted to define the requirements and approaches to address privacy issues in smart environments (Bettini and Riboni, 2015), such as user transport tracking privacy issues (Avoine et al., 2014), and how to decouple sensors' data from user-identifying data (Bartoli et al., 2011; Martinez-Balleste et al., 2013). Bettini and Riboni (2015) further consider the information collected by pervasive applications in smart environments. In addition to technical requirements, Bettini and Riboni (2015) also emphasize the importance of individual awareness and the need for privacy that does not affect profitable business models. This is in addition to the need for new regulations to push privacy preserving solutions to become practical. As IoT devices will be able to collect and communicate pervasive information about users Bettini and Riboni (2015) performed a survey classifying pervasive IoT applications. These applications were as follows:

- location based services: mainly for mobile applications and of benefit to location customized services;
- participatory sensing application: based on services that require participation from a considerable number of users, to collect, analyze and correlate data from these users and offer services based on the findings;
- healthcare and well-being applications: based on services that collect data from sensors used to monitor physical and health signals from the user.

Bettini and Riboni (2015) then identified the privacy preserving approaches (access control, obfuscation, anonymity, cryptography, privacy preserving data-mining) and their effects on service quality, while also discussing the technical, legal and economic challenges to best meet privacy requirements. A solution was also proposed by Gope and Hwang (2015) for the protection of smart city IoT sensor privacy in terms of anonymity, untraceability, resistance to replay attacks and cloning attacks. Sicari et al. (2015) performed a survey to identify the requirements for a safer IoT environment, addressing main security challenges (authentication,

access control, confidentiality, privacy, policy enforcement, trust, mobile security, secure middleware), open issues and existing solutions. Sicari et al. (2015) also emphasized the importance of more research on “the insurance of security and privacy requirements in such a heterogenous environment, involving different technologies and communication standards is still missing. Suitable solutions need to be designed and deployed, which are independent from the exploited platform and able to guarantee: confidentiality, access control, and privacy for users and things, trustworthiness among devices and users, compliance with defined security and privacy policies” (Sicari et al., 2015).

The research clearly suggests that information security and privacy issues are highly important for smart city survival. Information security issues need to be identified for the different application domains and their utilization of advanced ICT, such as cloud computing and IoT. These issues need to be controlled and properly managed from the early stages of the smart city in all its components. It is also noteworthy that technical research in the smart city literature is more developed than management research (Whitmore et al., 2014). As smart city organizations will be a major component of smart cities, it would then be valuable to evaluate the information security aspects inside smart city organizations to check how they could be controlled and managed.

2.10 Research Gap: Information Security Management Impact on Organizational Performance in Smart Cities

While information security is paramount for the safety of digital services, especially in the context of smart cities (Sicari et al., 2015), information security management has been noted to have an even greater significance, the reason being that just deploying and running technology is not sufficient to protect an organization; orchestrating technologies and teams are essential for information security efficiency (von Solms and von Solms, 2004), especially in the context of smart cities which rely more on technology and require more information security (Belissent, 2011). However, Chourabi et al. (2012) and Whitmore et al. (2014) confirm that little research has been done on smart city management and related organizational factors, even though previous research highlighted these as major challenges and

success factors that need to be better examined. In addition, a research audit by Whitmore et al. (2014) determined that the management literature is dominated by technology research and that advanced technology service research is under-represented.

In smart cities, performance and efficiency are prioritized. Meanwhile, the same priorities exist for organizations. Organizational performance is the output of an organization when measured to its predetermined goals and objectives; it is a predecessor to organizational success or failure, and researchers have confirmed that it is supported by the IT function. This directly impacts productivity, profitability, cost, and simplicity, and contributes to competitive positioning (Devaraj and Kohli, 2003; Melville et al., 2004).

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 organization. They also concluded that the cost of a security breach for an Internet-only organization is higher than for conventional firms, and the damage has more impact on small businesses than large ones. The higher impact of a security breach on Internet-only firms is also confirmed by Hovav and D'Arcy (2003). Andoh-Baidoo and Osei-Bryson (2007) indicate that a security breach could have a negative impact on the organization'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 organization that includes financial loss, client and partner loss, government sanctions, reputational loss and market value.

In the context of smart cities, organizations are expected to be highly dependent on digital services and the ICT infrastructure, which, as per Cavusoglu et al. (2004) and Hovav and D'Arcy (2003), means that the impact of an information security breach will be larger than for any other type of organization. The right analysis and management of factors that impact information security issues in the smart city context requires careful consideration, as they will be critical for the stability and sustainability of smart city organization's performance and growth. Then, however, organizational factors are a major influencer of information security management in organizations; the organizational attitude ultimately determines its progress towards better security and security management (von Solms, 2005).

The impact of information security mismanagement has also been considerably researched; security technologies cannot defend an organization without the correct strategy and policies. Organizational aspects have a direct impact on the behaviour and efficiency of information security management. Security is not principally a technical matter but a management or business issue (Dhillon and Backhouse, 2000; Vermeulen and von Solms, 2002; Dutta and McCrohan, 2002; So and Sculli, 2002; von Solms and von Solms, 2004). In the context of smart cities, it would then be significant to a smart city's organizational future to identify the organizational factors that most influence information security management.

One solution for the identified research problem could be to enhance understanding of the information security management related organizational factors that are expected to influence smart city organizations. This knowledge can be applied to help tackle challenges of information security that are expected to be exacerbated in the smart environment. This solution requires the identification of the most relevant factors towards better information security management standing inside organizations, and consequently a better opportunity for modern-day organizations to prepare for forthcoming smart cities.

In light of the trends in the literature highlighted in this chapter, two research questions emerge:

- how does the influence of information security management compare between smart and non-smart cities?
- what are the organizational factors that are expected to most influence information security management inside smart city organizations?

2.11 Summary

Information security management is a rapidly evolving component of any modern organization, and, as with any developing practice, the sooner gaps and progress prospects are identified, the sooner they are given the right attention. This chapter presented a review of the relevant literature with the objective of identifying key gaps and to highlight the research problem. Security management organizations will be facing serious issues in the smart city era. There is a need for a better understanding of how smart city organizations can deal with such challenges from an information security management perspective and an organizational perspective.

Elucidating such challenges will lead to solutions to help organizations successfully navigate the complex smart city environment.

Chapter 3 CONCEPTUAL MODEL DEVELOPMENT

3.1 Introduction

As mentioned previously, the aim of this research is to identify and rank the information security management (ISM) factors that influence a smart city organization's performance goals and improve its information security. To do so, the organizational performance goals, in addition to ISM and smart city related organizational factors, need to be researched in greater depth. The purpose of research is to gain knowledge, learn (Denzin, 1978; Chadwick et al., 1984), and to put it in conversational terms, "finding out" about the world (Gergen, 1992). In this way it produces theory (i.e., a fact-based framework or model to explain a certain phenomenon) and proposes solutions to problems or resolutions to unsolved questions. According to Kerlinger (1979), a theory encompasses a group of interrelated constructs, descriptions, and propositions that provide a methodical perspective of phenomena by specifying associations among variables, with the ultimate objective of clarifying a specific phenomenon (Creswell et al., 2003). The primary goal of theoretical development is to answer questions of how, when, where, and/or why (Bacharach, 1989).

In the previous chapter, an elaborate literature review exercise was completed to highlight the aspects of smart city and its organizations; the literature review also highlighted the importance of information security management and its organizational aspects. This Chapter builds on the overall findings from the previous

chapter especially the literature synthesis on the smart cities governance organizational factors list built under section 2.5.1 and the literature synthesis on the information security management related organizational factors list under section 2.8.1. The findings from Chapter two will be used to develop a list of organizational factors that best portrays information security management influence on smart city organizations.

According to Creswell et al. (2003), a research methodology outlines the process of tackling the research. A study's methodology is best described as the methodical, formal, rigorous and specific procedures used to obtain resolutions to challenges and/or to find and translate new facts and relationships (Waltz and Bausell, 1981). A methodology is also described as "...the architectural blueprint of a research project, linking data collection and analysis activities to the research questions and ensuring that the complete research agenda will be addressed" (Bickman and Rog, 2008).

The focus in this chapter is on the research design strategy, philosophy, and the research methods used, detailing the basis on which key decisions were made. It demonstrates the choice of a philosophical position, the use of a proper methodology to address the research questions, followed by different research procedures for collecting data and for its analysis.

3.2 The Use of Organizational Performance as a Theoretical Lens in this Research

Efforts to describe and analyse organizational performance go back to investigations of "organizational effectiveness" by Cameron and Whetten (1981) and Steers (1975). Organizations are considered effective if they accomplished their projected goals (Lewin and Minton, 1986). However, organizational performance is a complex, multidimensional phenomenon. Organizational performance goals, such as profit, growth, and stakeholders' satisfaction, have been inconsistently defined and often conflict (Cameron, 1986; Chakravarthy, 1986; Venkatraman and Ramanujam, 1986). Due to stakeholders conflicting agendas and competing organizational goals, researchers have found it difficult to craft a specific definition for an effective organization and how to best measure it (Cameron, 1986; Chakravarthy, 1986; Zammuto, 1984). Consequently, the adoption definition of organizational performance will be one that has been broadly rationalized as the social and economic outcomes resulting from interactions between organizational elements, actions and the environment (Andrews, 1971; Hrebiniak et al., 1989).

In strategic management research, Venkatraman and Ramanujam (1986) tried to define the organizational performance measurements in a model with three concentric circles. These circles consisted of the largest circle of organizational effectiveness, then operational performance with non-financial indicators and at the center, the economic outcome factors such as growth, ROI, and stock price. Venkatraman and Ramanujam (1986) also implored researchers to give more value to the two inner circles (operational performance and economic outcome), as organizational effectiveness is broad in scope and almost impossible to measure, while the two other circles have lower difficulty but are still complex due to the numerous indicators of operational performance and economic outcome involved. The following sections will explain why organizational performance was selected for this research, its relationship to the primary themes of this research (namely smart cities, organizations and information communication technologies), then proceeds to explain how organizational performance could be measured in the context defined in this research.

3.2.1 The selection of organizational performance in this research

Organizational performance is one of the most important aspects of an organization and is measured using different methods. Information and communication technologies (ICT) have long been known to have the prospective of delivering important improvements in organizational performance (Brynjolfsson and Hitt, 1996; Sircar and Choi, 2007), and are known to reshape organizational processes, structures and cultures, 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 problems lies in their consequential impact on organizational performance, such as reputation, financial loss or customer loss (Menzies, 1993). Smart cities are mainly composed of different types of organizations that highly rely on ICT; the evaluation of smart cities' development will then come back to assessing individual organizations' performance and efficiency. Linking information security initiatives to financial investment helps firms evaluate the ratio of costs to benefits and thus improve the effectiveness of ISM (Huang et al., 2006).

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). To measure ISM performance, Huang et al. (2006) combined information security and organizational performance research to help organizations assess the value of

information security projects, and to help infer how to link a project's performance to future business strategies. Hall et al. (2011) also examine the relationship between information security strategy and organizational performance, and how organizational capabilities influence the successful implementation of information security strategy and organization performance. Hall et al. (2011) also identified a positive relationship between the successful implementation of an information security strategy and organizational performance. Andoh-Baidoo and Osei-Bryson (2007) also researched ISM and organizational performance by analysing the impact of a security breach towards the market value of firms.

The literature suggests that the utilization of the integration of an organizational performance perspective in the context of this research would be optimal to further understand organizational factors that influence ISM in smart city organizations. The organizational performance angle is not only convenient but advantageous to better understand the most important ISM organizational factors that influence smart city organizational performance.

3.2.2 Measuring organizational performance

Organizational performance researchers have attempted to classify the organizational dimensions of organizational performance. For example, Murphy et al. (1996) identified five dimensions: efficiency (ROE – Return on Equity), growth (sales), profit (net income), size (net sales), and survival (failure/bankruptcy). Woo and Willard (1983) also analysed 14 performance indicators from the profit impact of marketing strategy (PIMS) database, distilling them down to 4 dimensions: profitability, relative market position (quality, competition), changes in profit and cash flow (ROI variability); growth in sales and market share. Meanwhile, Rowe and Morrow (1999) identified three dimensions: subjective return (market reputation), financial returns, and market performance. Tosi et al. (2000) also analysed 30 performance indicators from Compustat data, and identified 8 domains: absolute financial performance levels, changes in financial performance, stock performance, long-term and short-term return on equity, return on assets, market returns, and internal performance indicators. Finally, Maltz et al. (2003) interviewed senior managers and proposed five performance dimensions based on the emergent themes: financial revenue, market satisfaction, project management process quality, employee satisfaction and leadership development, and future planning (strategy and readiness).

As multiple researchers proposed different measures of performance and evaluation of results, certain challenges became apparent. For example, each organization may have different priorities for each of the organizational goals, need to deal with fluctuating results, or struggle to clearly define success or failure. Rumelt et al. (1994) states organizational performance is the most important construct in strategic management research. Therefore, it is imperative to understand the factors that affect organizational performance to help improve organizational performance (Meyer, 1991; Carlson and Hatfield, 2004; Rumelt et al., 1994). Clearly, there are different perspectives on the concept of organizational performance; for example, some organizations prefer to empower and satisfy employees to be more productive, while other organizations push employees to perform difficult work, resulting in higher productivity but also high employee turnover.

Based on the existing themes in the literature, and the context in which the current study takes place, the definition of organizational performance will be adopted from Venkatraman and Ramanujam (1986). Venkatraman and Ramanujam (1986) break performance down into financial aspects; these are represented by:

- accounting and financial returns;
- stock prices;
- growth;
- hybrids (cash flow, market value);
- survival aspects (failure, bankruptcy);
- operational performance aspects (marketing, outbound logistics, operation and process/project management, technology/infrastructure development and effectiveness, customer satisfaction, employee satisfaction, leadership development/effectiveness).

3.2.3 Organizational performance and corporate governance

Corporate governance is the methodologies, processes and practices by which a corporate organization is controlled and managed in order to achieve its goals (Baker and Anderson, 2010). The role of corporate governance is also to balance the relationships and interests of the organization's stakeholders, such as management, shareholders, partners, clients, suppliers, government, the public or others. Good organizational and inter-organizational corporate governance is essential for maintaining the integrity of corporations, markets and financial systems,

but is also core to the stability and health of world economies (Baker and Anderson, 2010; Hernández-Espallardo et al., 2010).

Corporate governance is highly connected to organizational performance, especially in the context of strategic management. This link is highly supported by research on corporate strategies (Heracleous, 2001; Rumelt, 1991; McGahan and Porter, 1997). Even in tough industries, characterized by intense competition and low profits, strategic management is considered of highest priority and is usually most effective (Heracleous, 2001). For example, Nickerson and Silverman (2003) found that firms that have poorly established governance processes and inappropriate conduct achieve lower financial profit than organizations with well-established governance. They also identified other factors that impact the flexibility of firms to change, such as firms dealing with large investments, firms with unions. Nickerson and Silverman (2003) also found that firms cannot adapt easily due to the fact that change requires investing resources. In the context of IT governance, Simonsson et al. (2010) found a positive relationship between IT governance maturity and IT governance performance: a clear indicator of the need for the right governance implementation and optimization inside an organization.

3.2.4 ICT and organizational characteristics

There are multiple organizational factors that influence the usage and adoption of the ICT infrastructure. Clegg et al. (1997) studied the failure of IT departments, and highlighted that performance was influenced most by the following organizational elements:

- the performance and impact of IT investments (Herath and Herath, 2009; Ittner and Larcker, 2003; Morgan and Strong, 2003);
- the significance of the IT entity within the organization;
- the complexity of the IT entity and systems within the organization;
- the development and implementation of IT;
- organizational change and politics;
- the role of end users in the company development strategy;
- the role of managers awareness of new technology;
- learning and continuous innovation.

Meanwhile, Bai and Lee (2003) investigated the organizational factors and concluded with the influencers of the information systems strategic planning process

being organizational relations (CEO and CIO relationship, task coordination, stakeholder interaction and involvement), organizational IT context (IT maturity and computer aided planning), and organizational structure (centralization of the organizational structure).

Furthermore, Wiengarten et al. (2013) developed a framework to demonstrate the IT business value, and how the synergy and alignment among the IT and organizational factors could lead to enhanced overall organizational performance. They emphasize that for managers to evaluate IT resources, they must take into consideration organizational factors that have a direct and indirect impact on the IT business value (Wiengarten et al., 2013). Researchers in Hameed et al. (2012) also tried to identify the main organizational factors that impact the adoption and innovation of IT. They found the following factors to influence the organization's adoption of IT:

- organization size (business size);
- IT expertise (knowledge, experience, maturity);
- top management support (commitment) (Barlette and Fomin, 2009);
- resources (economic and financial resources) (Herath and Herath, 2009);
- information systems department size (development or IT functions);
- information systems infrastructure (technological capabilities);
- organizational readiness (awareness, commitment); and
- the existence of an innovation champion (i.e., someone to promote innovation).

Bordonaba-Juste et al. (2012) also researched the impact of multiple organizational factors on the e-business operations and adoption (organization size, IT knowledge, IT outsourcing and external knowledge, IT staff education), and confirmed their importance for conducting an online business. They concluded that IT outsourcing is only suitable when used by small enterprises. Similarly, Lee et al. (2007) investigated and confirmed the influence of the organizational learning processes and educational capabilities on the success of e-business implementation. Lee et al. (2011) also researched the connection between the ICT infrastructure and business performance, investigating the adoption of organizational factors and their impact on different types of organizations. They concluded that:

- organizational learning and growth is impacted by internal process performance and has an impact on customer satisfaction;
- customer satisfaction is impacted by organizational internal process performance and has an impact on organizational financial performance.
- business process reengineering has a significant impact on internal process performance and on organizational financial performance;
- ICT adoption has a significant impact on business process reengineering and organizational learning and growth;
- organizational environment flexibility (dynamism) and capabilities have a significant impact on ICT adoption;
- the organizational environment dynamism is impacted by the competition intensity, market pressure and the complexity in an industrial setting;
- the organizational environment is impacted by environment capabilities, innovativeness and dynamism;
- the organizational environment determinants are impacted by environment knowledge sharing.

Gil-Garcia and Pardo (2005) mapped organizational factors that affect the e-government, and summarized the main challenges for e-government initiatives as quality control, standards compliance, and projects sponsorship. Gil-Garcia and Pardo (2005) also identified the main challenges that affect organizational and managerial status as the size of the project, the diversity of the users, a lack of alignment between IT projects and organizational goals, conflicting goals, and the existence of internal conflicts or resistance to change due to lack of interest. They also emphasized the importance of security and privacy in government IT initiatives.

Inter-organizational issues have also been considered in the literature to be a challenge to organizational performance. For example, Sila (2010) investigated the factors that most influence the adoption of Internet-based inter-organizational systems (IBIS) (pressure from partners, pressure from competitors, costs, top management support, trust, network reliability, data security, scalability, complexity), but also organizational factors (firm type, firm age, firm ownership type) and environmental factors (dynamism, complexity, hostility). They found that organizational factors were significant influencers and that complexity and hostility were not. Top management support is imperative to the purpose of ISM because only top management is capable of pushing the changes that are challenged by organizational culture and creating a productive organizational security culture

(Barlette and Fomin, 2009; Chang and Lin, 2007; Barling et al., 2002; Posthumus and von Solms, 2004).

Sila (2013) also investigated the factors that influence the adoption of Internet-based technologies into “Business to Business” e-commerce applications. Using the technology-organization-environment (TOE) framework adapted for knowledge learning and knowledge management, they found the influencing factors to be: costs, network reliability, data security, scalability, top management support, pressure from trading partners, and pressure from competition. The relationship between ICT characteristics and organizational performance is strongly described in the literature, giving more justification to involve organizational performance as a lens to evaluate ICT related organizational factors.

3.2.5 IT/ICT and Governance

IT governance was likely first discussed in the 1960s by Garrity (1963) while studying top management’s influence on IT. It has since been well defined by Brown (1997), Sambamurthy and Zmud (1999), Loh and Venkatraman (1992), and Henderson and Venkatraman (1993), and commonly referred to as “information systems governance frameworks”. IT governance is a branch of corporate governance (Weill and Ross, 2004) that reflects the decision makers and their accountabilities. In essence, IT management is about who implements IT decisions and projects (Weill and Ross, 2004). Weill and Ross (2004) define IT governance as “specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT”. Bradley et al. (2012, p. 157) define IT governance as “the capacity of top management to control the formulation and implementation of the IT strategy via organizational structures and processes that produce desirable behaviours, which will ensure that IT initiatives sustain and extend the organization’s strategy and objectives”.

The adoption of IT and ICT in current world organizations is understood; its presence highly influences corporate governance; information systems also affect key organizational measures that are core to governance, such as economic growth, performance (monitoring, evaluation and development), flexibility, efficiency, production, development and operational cost effectiveness, communication channels, competition, speed of delivery, and automation. In fact, the impact of the information revolution has been sensed at each level of organizations, industries and society (Gurbaxani and Whang, 1991; Brynjolfsson and Hitt, 2000). Since the

ICT infrastructure is key for operations, its governance becomes even more demanding and critical in a smart environment; the right decisions for controlling and managing the ICT infrastructure are crucial for its success and growth. Poor decision-making could result in services becoming obsolete, or slow, or even increase the risk of successful cyber-attack.

As modern organizations continue to rely heavily on information technologies to deliver services, operate production lines, drive communication with partners and clients, and monitor quality and performance, effective IT governance has grown in priority (De Haes and Van Grembergen, 2009). There is a need to manage IT complexities to achieve best efficiency and ROI, and to maintain proper healthy economic growth in line with corporate governance goals (Brynjolfsson and Hitt, 2000). Melville et al. (2004) also confirmed the impact of IT on flexibility, quality improvement, cost reduction and productivity development. Research has shown that organizations utilizing mature IT governance practices are capable of achieving better alignment between IT operations and business goals. Researchers also identify the lack of research in the IT governance area (De Haes and Van Grembergen, 2009). In a smart environment, organizational performance capabilities are key for deploying the best services, bypassing bureaucracies and politics to focus on outcomes that benefit the business and drive its growth.

3.2.6 Organizational performance and Information security

The impact of information security on organizational performance is understood. Even though information security investments are a cost for the organization, they are the first line of defence against cybercrime and advanced cyber-attacks that target organizations for financial, reputational, intelligence or intellectual property purposes. Researchers have analysed the cost of lack of security on an organization, its impact on productivity, the impact of breaches on organizations; it was found that information security maturity was of high importance for e-businesses sustainability, and that the right analysis of impact factors within each organization is required to identify the right security investment needs to maximize efficiency, the mitigation of risk and ROSI (return on security investment) (Davis, 2005; Sonnenreich et al., 2006).

However, Cavusoglu et al. (2004) concluded that the cost of poor cyber security is high for investors, with the breach impact not limited to a single organization. They also concluded that the cost of a security breach for an Internet-only organization is

higher than for conventional firms, and the damage has more impact on small businesses than large businesses. Cavusoglu et al. (2004) also added that the denial of service attacks has less financial impact on organizations as they affect the availability of public services and not the internal infrastructure. The higher impact of a security breach on Internet-only firms is also confirmed by Hovav and D'Arcy (2003).

Information security investments in an organizational context could be evaluated using the framework developed by Westerlind (2004) using the following steps:

- currency: the availability, accessibility and reliability of the latest information/data;
- content: the accuracy of the available data;
- quality: considerations for managers to better perform their role and the need for business managers' involvement;
- importance: how much business is dependent on information security and the level of security required;
- scalability: the system flexibility to adhere to business changes and needs

Brink (2001) and Pipkin (2000) also discussed the cost of security investment, first, through the need to insure the protection of the right assets, and second, to analyse the size of the investment against the value of the information being protected.

Tsiakis and Stephanides (2005) analysed the economics of information security investments inside organizations in order to avoid additional costs and risks of security breaches, and the security process to evaluate a risk probability, loss impact and expectancy and the ROSI. They also segmented the differences in the degree of impact of information security breaches. An immediate economic impact requires the repair and restoration of services to an operationally healthy status. A short-term economic impact includes the loss of contracts and existing clients because of unreliable services and reputational loss. Finally, long-term economic impact is characterized by a loss in market value and stock prices. Tsiakis and Stephanides (2005) identified key information security economics that need to be addressed in economic information security research: the frequency of security breaches, the cost of security breaches, the investments in security operations, and security levels needed.

Information security problems occur in modern connected organizations, and impact organizational performance and business: damage is immediately classified by its impact on the main security pillars: confidentiality, integrity and availability. Damage could also vary in impact and reach; examples include data leak, business services disruption, customers' data and privacy affected, etc. The following table summarizes data collected through the literature and shows the consequences of an information security breach inside an organization.

Table 3.3.1: The organizational economic impact of a security breach

Impact	Damage	Sources from the literature
Financial loss		
	Direct Financial loss	Goel and Shawky, 2009 Gordon et al., 2011 Thomas et al., 2013 Cavusoglu et al., 2004 Andoh-Baidoo and Osei-Bryson, 2007 Ettredge et al., 2001 Hovav and D'Arcy, 2003
	Client and partners loss Similar technological companies loss	Goel and Shawky, 2009 Gordon et al., 2011 Cavusoglu et al., 2004
	Government sanctions	Goel and Shawky, 2009
	Market value	Goel and Shawky, 2009

		Gordon et al., 2011 Cavusoglu et al., 2004
Decreased productivity		Cavusoglu et al., 2004 Andoh-Baidoo and Osei-Bryson, 2007
Reputational loss		Goel and Shawky, 2009 Gordon et al., 2011 Thomas et al., 2013
Trade secrets or Intellectual property loss		Thomas et al., 2013

Source: Devised by author

3.3 Study Hypotheses

The role of this section is to identify the ISM-related organizational factors that impact organizational performance the most. This review examines such factors in the context of smart city organizations. This section benefits most of the literature synthesis on the smart cities governance organizational factors list built under section 2.5.1 and the literature synthesis on the information security management related organizational factors list under section 2.8.1. Identifying these unique factors will help excavate the most pertinent issues in a smart city organization's ISM practices. These issues, itemized below, will subsequently inform the hypotheses informing the current investigation.

3.3.1 Adaptation to rapid technology development

In fast paced complex environments such as smart cities, organizational change cannot lag behind the advances of the environment. Legislative, structural and procedural adaptation to technological developments are essential for staying up-to-date, competitive and secure (Zanella et al., 2014; Hernández-Muñoz et al., 2011; Gil-Garcia et al., 2014). Information security management is expected to follow the pace of the changes, adapting to new services and features, and defending against the new types of threats and weaknesses, especially in the context of smart cities (Udo and Edoho, 2000; Ejiaku, 2014; Gil-Garcia and Pardo, 2005; Chourabi et al., 2012). The state of the literature on rapid technology development yields Hypothesis 1.

Hypothesis 1:

The positive ability to adapt to rapid technology changes has a significant and positive impact on organizational ISM in smart cities.

3.3.2 Bureaucracy

The primary challenge generated by bureaucracies is that they can create change-resisting monopolies; these limit the competitive pressure to innovate and the efficiency of internal structures in performing core organizational tasks (Nam and Pardo, 2011b). Excessively complicated procedures inside organizations can cause delays, client disappointment, and loss of business. In smart city organizations, bureaucracy is anticipated to have a higher impact on the businesses and their safety (Toppeta, 2010; Nam and Pardo, 2013). The inability to timely approve a decision, a change, a test or a budget could be the cause of a breach or loss of

competitive edge and reputation, or government sanctions (Goel and Shawky, 2009; von Solms and von Solms, 2004). Smart cities are expected to be highly automated and provide fast services; that is also why they are sometimes referred to as “real-time” cities, as outlined in the previous chapter. Tolerance against bureaucracy is expected to be small in smart city organizations because smart cities offer speedy services, focus on client satisfaction, and provide competitive services (Toppeta, 2010; Nam and Pardo, 2013; Chourabi et al., 2012; Allwinkle and Cruickshank, 2011).

Hypothesis 2:

Bureaucracy has a significant negative impact on organizational ISM in smart cities.

3.3.3 Employee compliance with organizational policies

While top management support is important for organizational success, organizational compliance of information security also needs to be enforced, usually through different means such as employee awareness (Ashenden and Sasse, 2013), competencies development (Kayworth and Whitten, 2010), organizational culture (Chang and Lin, 2007), structure effectiveness (Boss et al., 2009), and employee engagement (Ashenden and Sasse, 2013). Top management support without organizational compliance with information security requirements is not enough to satisfy the obligations for safe organizational operations of services. The enforcement of information security behaviour inside the organization is a necessity to fight threats using normal employees, but also to identify rogue ones (Puhakainen and Siponen, 2010; Gil-Garcia and Pardo, 2005; Zafar and Clark, 2009; Kayworth and Whitten, 2010). The body of evidence in the literature on compliance underpins Hypothesis 3.

Hypothesis 3:

Employees' compliance to ISM policies has a significant and positive impact on organizational ISM in smart cities.

3.3.4 Improved utilization of the ICT infrastructure

The proper integration of the organization with the smart city's ICT infrastructure enables the organization to better benefit from available features and, in turn, to enhance service quality. ICT has long been known to not only positively impact organizational performance (Brynjolfsson and Hitt, 1996; Sircar and Choi, 2007), but

also to reshape organizational processes, structures and cultures (Fulford and Doherty, 2003; Markus, 2004). As smart city organizations are expected to be highly dependent on the ICT infrastructure (Dameri, 2013), it is anticipated that smart city organizations benefit from a stronger ICT infrastructure (Nam and Pardo, 2011b; Mulligan and Olsson, 2013; Gil-Garcia and Aldama-Nalda, 2013; Gann et al., 2011). The benefits are not only expected for performance but also to protect the information flows and availability, which need to be adapted and controlled adequately. ISM departments need to be involved in defining the extent of integration with the city's infrastructure, determining risks and threats, and reflecting on organizational strategy (Chourabi et al., 2012; Puhakainen and Siponen, 2010). Therefore, the current investigation also seeks to examine the following hypothesis:

Hypothesis 4:

The better use of the ICT infrastructure has a significant and positive impact on organizational ISM in smart cities.

3.3.5 Inter-organizational collaboration

Inter-organizational collaboration has been a challenge for organizations due to logistical, trust, legal, bureaucracy or other reasons. In smart cities, organizations and governments are expected to establish frameworks to enforce collaboration through information sharing, especially to share threat-related data. The collaboration between organizations is important for sharing experiences and learning about new threats and challenges (Bekara, 2014); it is also important for enhancing the defence capabilities against attackers. In the context of smart city organizations, inter-organizational collaboration is anticipated to be of utmost importance for the overall defence of organizations against new threats and weaknesses (Hawryszkiewicz, 2014). Inter-organizational collaboration is also expected to occur directly between business clients and partners to secure data communication, share mutually beneficial threat information and guarantee safe collaboration. In the organizations themselves, organizations are expected to seek the best performance out of the different teams, made most possible through collaboration and communication options available (Yang and Maxwell, 2011; Gil-Garcia and Pardo, 2005; Chourabi et al., 2012; Kayworth and Whitten, 2010; Chang and Lin, 2007; Kożuch and Sienkiewicz-Małyjurek, 2016; Patel et al., 2012). Therefore, Hypothesis 5 is as follows:

Hypothesis 5:

Inter-organizational collaboration between ISM departments has a significant and positive impact on organizational ISM in smart cities.

3.3.6 Intra-organizational collaboration

Intra-organizational collaboration has been a challenge for organizations for logistical, trust, and bureaucratic reasons, among others. In smart cities, organizations and governments are expected to establish frameworks to enforce collaboration inside the organizations on information sharing, especially to share threat related data. Collaboration between the different departments inside an organization is essential for achieving its objectives through efficient decision making and conflict resolution (Sila, 2010). Intra-organizational collaboration is expected to be of higher importance in a smart city organization, especially in the context of ISM, where innovation and problem-solving needs to be delivered quickly (Kitchin, 2014). Therefore, timely decision-making and highly efficient communication skills and tools are likely to be prioritized by top management (Yang and Maxwell, 2011; Zang et al, 2005; Gil-Garcia and Pardo, 2005; Chourabi et al., 2012; Kayworth and Whitten, 2010; Chang and Lin, 2007). This inference from the literature frames Hypothesis 6:

Hypothesis 6:

Intra-organizational collaboration between ISM and other departments has a significant and positive impact on organizational ISM in smart cities.

3.3.7 Leadership attitude

Top management compliance with requirements is needed to allocate the required investments and priorities for the ISM functions and human resources. On one hand, top management commitment to information security and management issues is essential for the performance of the smart city organization; they are expected to have higher impact on the smart city organization, with higher consequences for failure. On the other hand, government involvement and legislative compliance could cause the prioritization of, and investment in, information security, allowing less influence from the top management side. Multiple studies highlight the importance of leadership attitude in smart city organizational environments (Giffinger et al., 2007). Leadership attitude and top management support in matters of information security is also noted as an important aspect of organizational performance (Ashenden and Sasse, 2013). The primary challenge in ISM in smart

city organizations is for leadership to become more efficient, to cope with fast paced technological changes and communication/collaboration skills required to best manage information security.

Information security issues are expected to have a stronger influence on smart city organizational performance in a smart city. Therefore, in an environment such as smart cities, which rely highly on digital infrastructure with 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 (Puhakainen and Siponen, 2010; Chang and Lin, 2007; Hu et al., 2012; Gil-Garcia and Pardo, 2005; Chourabi et al., 2012; Williams, 2001; Kayworth and Whitten, 2010; Chang et al., 2011; Bassellier et al., 2001). This expectation is fulfilled in Hypothesis 7 below:

Hypothesis 7:

Leadership attitude has a significant and positive impact on organizational ISM in smart cities.

3.3.8 Legislative influence

Government imposed controls are expected to help organizations better manage information security and digital assets, technology selection or other aspects, and to better protect users and national data. Meanwhile, ISM leadership should know the organizational needs and challenges well, which means they probably know how to protect data effectively. Smart city governments are also expected to have high levels of engagement with city components and stakeholders, defending government and citizen's data. Legislative compliance in matters of information security is therefore important for the organizations (Backhouse et al., 2006; Chang and Ho, 2006; von Solms, 2005; von Solms and von Solms, 2004). It is expected to be of higher priority in smart city environments due to the more critical nature of information security issues (Sicari et al., 2015; Bekara, 2014; Gubbi et al., 2013). Non-compliance with legislations might be the source of significant damage to organizational performance and national security (Gubbi et al., 2013; Amin, 2002; Ruiz-Romero et al., 2014; Naphade et al., 2011), which could lead to government sanctions (Goel and Shawky, 2009) and serious accountability on executives (von Solms and von Solms, 2004; Gil-Garcia and Pardo, 2005). As such, the current investigation seeks to examine Hypothesis 8 below:

Hypothesis 8:

Legislative influence has a significant and positive impact on organizational ISM in smart cities.

3.3.9 Skillful workforce

A skillful workforce is a major component of advanced environments, including smart cities, and managing the development of human capital inside organizations is paramount to the protection of an organization and for maintaining safe production services (Chang et al., 2011; Eloff and Eloff, 2003; Bassellier et al., 2001; Gil-Garcia and Pardo, 2005). Therefore, information security is expected to have great importance in smart city environments. Smart cities are expected to do their best to attract skilled labour (Caragliu et al., 2011; Hollands, 2008; Toppeta, 2010). ISM departments in smart city organizations are subsequently expected to require more skilled human capital to operate services and functions. On one hand, it might be possible that organizations would need the best information security human capital to better ensure best services' quality. On the other hand, automation, machine learning and artificial intelligence would help organizations lower their human capital requirements (Chang et al., 2011; Bassellier et al., 2001; Gil-Garcia and Pardo, 2005; Fulford and Doherty, 2003; Chourabi et al., 2012; Williams, 2001). Hypothesis 9 reflects these inferences.

Hypothesis 9:

Human resources that are skilful in IS and ISM have a significant and positive impact on organizational ISM in smart cities.

3.3.10 Type of organization and business model

Developing strategies for the protection of information assets in an organization is the role of the information security management (Williams, 2001; Zafar and Clark, 2009; Johnston and Hale, 2009). However, information security is different from one organization to another. Furthermore, smart city organizations are expected to be different from current organizations (Kuk and Janssen, 2011; Anthopoulos and Fitsilis, 2014), and therefore require modified strategies for the protection of data, services and the business. The role of ISM departments is expected to be impacted by the different smart city business model as organizations need to adapt to risks and threats specific to their business type and role (Chang and Ho, 2006; Johnson and Goetz, 2007).

Hypothesis 10:

The organizational type and business model has a significant and positive impact on organizational ISM in smart cities.

3.3.11 Vendor selection

Technology selection is essential and could be a determinant to an organization's success. The right technologies enable adequate control and protection, in addition to introducing new functions and features. In turn, ISM leadership needs the right technological exposure, resources and skills to be able to recommend positive changes and ideal technologies. Government influence might be able to support such activities, but is also questionable from an enforcement and bias perspective. Several studies reinforce the importance of smart cities' vendor selection and independence (Mulligan and Olsson, 2013, Kitchin, 2014, Hollands, 2008, 2015) to guard organizations against monopolies, push for standardization, and protect competitiveness between technology vendors. In general, managing information security technology requirements is expected to be more challenging for the ISM departments in smart city organizations (Weber et al., 1991; Parthiban et al., 2013; Chourabi et al., 2012; Allwinkle and Cruickshank, 2011; Hollands, 2008; Söderström et al., 2014; Calzada and Cobo, 2015).

Hypothesis 11:

Vendor selection ability has a significant and positive impact on organizational ISM in smart cities.

3.3.12 Information security management and organizational performance

Information security management (ISM) is an important factor for any modern organization. Its main goals are to protect confidentiality, integrity and availability, and it has an essential role in today's organizations and their performance (Chang and Ho, 2006; Posthumus and von Solms, 2004). ISM in smart cities is expected to have more influence on organizational performance, mainly due to smart cities being more dependent on ICT (Dameri, 2013; Chang et al., 2011; Chourabi et al., 2012). The literature then warrants the following hypothesis for the current investigation:

Hypothesis 12:

ISM has a significant and positive influence on organizational performance in smart city organizations.

3.4 Research Model

As mentioned earlier in the introduction chapter, this research aims at the identification and ranking of the top organizational factors that are expected to influence ISM in smart city organizations. However, these factors need to be explored further and tested. The model below summarizes the hypothesized relationships between organizational factors and ISM: this model will guide the verification. On completion, a ranked list of organizational factors affecting ISM will be formed.

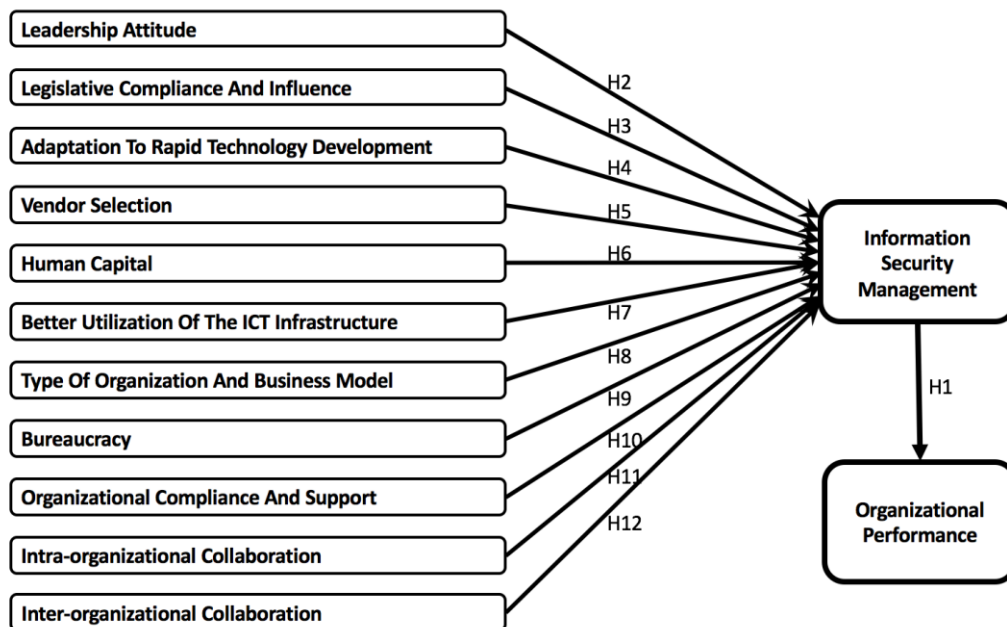


Figure 3.1: Study framework: Investigating organizational factors influencing information security management in smart city organizations

Source: Devised by author

The factors portrayed in Figure 3.1 have been drawn from the literature. When examined in smart city organizations, this research instrument is expected to measure and test the organizational abilities to deal with smart city organizational issues related to ISM, as defined by the literature.

3.5 Summary

This chapter presented the concepts and tools that will be used in the testing development of this research, being the integration of organizational performance as a lens to look at the organizational factors, the exploration of these organizational factors that influence ISM in current organizations, also the classification of these organizational factors that influence smart cities. The researcher selected 10 organizational factors that are expected to influence the smart city organizational ISM and positioned these into a conceptual model, to be evaluated and tested. The next chapter will discuss the evaluation options of the proposed model and hypotheses.

Chapter 4 RESEARCH METHODOLOGY

4.1 Introduction

In the previous chapter, the integration of organizational performance in the scope of this research was justified. Also, the organizational factors expected to influence information security management (ISM) in the context of smart cities were drawn, and the hypotheses and research model were developed. This chapter describes the rationale behind the specific strategic planning employed in this research effort. Some of the methodological considerations include sampling techniques, the sample size of the pilot study and of the data, as well as the design and implementation of interviews and the questionnaire (including organizational theory and distribution techniques).

Following the description of these areas, which will constitute the majority of the chapter; additional segments will describe the post-compilation stage of data analysis, research ethics, validity and reliability. These sections will further relate theory to strategic design, while also revealing the potential limitations of the analysis and results. The chapter also discusses the details of the research and analysis methodology being selected as quantitative, followed by the framework considered for addressing the research inquiries. The research direction is outlined in detail, the significance of the research is emphasized with a focus on the relationships to context (and the importance of the organizational) characteristics, and data sources are demonstrated.

4.2 Research Design

Literature on the research methodology offers varied approaches and methods to research design. However, it is not clear as to how to combine these methods when conducting a specific type of study, and how to examine the data. According to Churchill (1979), research design is a general guidance for the gathering and evaluation of information for a particular study. The meaning of research design is implied from its function as a crucial connection linking the theory and argument that supported the study, and the empirical data gathered (Frankfort-Nachmias and Nachmias, 2007). A research design facilitates the pursuit of answers to the queries being studied for a research project, in addition to supporting a concise research structure, with clear identification of limitations and ethical matters that will inevitably occur and need to be considered (Saunders et al., 2009).

Additionally, there is a difference inside and between methodologies in the manner in which research design is defined. For instance, in one study, research design can mirror the complete process, from conceptualising a research problem to reviewing the literature, techniques and conclusions, while in another study, the design might just refer to the methodology of the research (e.g., data gathering and analysis). In this research, the design follows Harwell's (2001) description as he describes a research design as qualitative, quantitative, or as involving both qualitative and quantitative methods, in which case it is referred to as mixed methods. Nonetheless, an area covering design is one that reflects on the study procedure, data gathered (numbers, signs, words) in varying manners and for varying uses. Consequently, quantitative researches collect and analyse quantitative data, while qualitative studies collect and analyse qualitative data.

As mentioned earlier in the first chapter, this research adopts a quantitative approach to collect data. Since it initially expects to conceptualise a research model, which involves the development of an instrument that employs quantitative metric units and that measures abstract concepts, the use of a quantitative design then becomes necessary at this particular stage of the research. Identifying and understanding the elements comprising such a process as well as offering the appropriate associations between the method and the study area will support the task of gathering required information for developing the research.

4.3 Research Philosophy

When undertaking a scientific research, it is important to study different relevant branches of philosophy, as it defines opinions, principles, conclusions and the nature of reality, which affects the approach in which the study is carried out. From design to conclusion, it is essential to guarantee the researcher's approaches are coherent with the type and objectives of the enquiry to ensure that researcher biases are known, disclosed, and minimised. In addition, the researcher should adopt a philosophy, which follows practical considerations (Saunders et al., 2009). Methods used must also be well-suited with the researcher's philosophical stance, guaranteeing that the final work is not undermined through lack of coherence (Easterby-Smith et al., 2002).

Different models and frameworks are used to analyse the relationship between the research methodology elements found in the literature. These frameworks provide the conceptual background for managing research. A major number of researchers exerted efforts to research the conceptual aspects and elements of this task, such as Ticehurst and Veal's (2000) methodologies, Kolb's (1984) Learning Cycle, Karl Knox's (2004) Research Needs, Sexton's (2003) PhD Research Methodology Model and Dawood and Underwood's (2010) Research Life Cycle.

Kagioglou et al. (2000) also developed the nested approach, a significant framework for research modelling. The external layer shows the research philosophy, which controls the research approaches and methods shown in the internal layer. Research approaches refer to the techniques for theory development and testing, such as experiments, case studies, action researches, and surveys. Research methods refer to the data collection techniques used, such as interviews, questionnaires, and observations. Saunders et al. (2009) deployed a similar research design approach to Kagioglou et al. (2000), and proposed what they called the 'research onion'. The research onion provides an appropriate structure within which to shape a research inquiry. It has multiple layers, with each layer becoming more comprehensive from the outside to the inside.

The model by Saunders et al. (2009) introduces three extra levels to the nested model. The research onion has six layers resembling the rings of an onion. It starts with philosophies at the outer layer, progressing through approaches, strategies, choices, time horizons, and with techniques and procedures at the core. Even though a "research approach" level is available in the "nested research" model as

well as in the “research onion”, each represents different perceptions. The research techniques within the nested model resemble the research strategies in the research onion. In addition to showing the components of each model, Figure 4.1 illustrates the mode in which the research design features overlap within the models suggested by Kagioglou et al. (2000) and Saunders et al. (2009).

Table 4.1: Comparison Between the Research Models

Nested model	Research Onion	Notes
Research Philosophy	Research Philosophy	E.g. Positivism vs Interpretivism
Research Approach	Research Strategies	E.g. Case study vs experiments
	Time Horizons	E.g. Cross-sectional vs Longitudinal
	Research Choices	E.g. Quantitative vs Qualitative, Multi-method vs Mono-method
	Research Approaches	E.g. Inductive vs Deductive
Research Techniques	Techniques and Procedures	E.g. Interviews vs Questionnaire Surveys

Source: Devised by author

Ontology – “the branch of philosophy concerned with the articulating, the nature and structure of the world” (Wand and Weber, 1993: p.220) – discusses the claims can be made about the nature of reality and how these claims interact with each other (Guba and Lincoln, 1994). The most popular examples of ontological positions are objectivism and subjectivism (constructivism) (Perera and Sustrina, 2011; Grix, 2002). Objectivism portrays the position that social bodies are present in a reality independent from the social actors related to their presence. Subjectivism in

contrast, affirms that a social phenomenon is formed from the opinions and subsequent activities by those social actors related to its presence.

Epistemology – represents “the theory or science of the method or grounds of knowledge” (Blaikie, 2007: p.18), being an alternative philosophical branch associated with ontology. Epistemology concerns the claims of what is assumed to exist and can be known by the “knower or to-be-knower” (Guba and Lincoln, 1994: p.3). It considers the concept of knowledge, with regard to its techniques, verification and the likely methods of attaining information in the believed reality. Two main schools of thought have dominated the epistemological dispute on how to carry out studies, outlining two paradigms that can be positioned at extreme ends of a continuum: positivism and interpretivism (Easterby-Smith et al., 2012; Creswell, 1994). Positivism the social world is external and its characteristics should be measured by objective methods other than being understood subjectively by awareness, consideration or instinct. Interpretivism (Social Constructivism) on the other side postulates that the researcher is independent of and neither influences or is influenced by the matter of the study (Easterby-Smith et al., 2008).

Table 4.2: Comparing effects of positivism and social constructionism (adopted from Easterby- Smith et al., 2002)

	Positivism	Social Constructionism
The observer	Should be independent	Is part of what is being observed
Human Interest	Should be irrelevant	Is the main driver of the science
Explanations	Should demonstrate causality	Aims to increase general understanding of the situation
Research progress through	Hypotheses and deductions	Gathering rich data from which ideas are induced
Concepts	Need to be operationalised so to be measured	Should incorporate stakeholder perceptions

Units of analysis	Should be reduced to simple terms	May encompass the complexity of whole situation
-------------------	-----------------------------------	---

Robson (2002) identified five stages on how positivist research should be conducted:

- Inference of hypothesis from theory;
- Expression of hypothesis in operational terms;
- Testing the hypothesis;
- Examination of the outcome of the test inquiry;
- If required, modification of the theory.

The current study uses surveys with roots in the positivist research paradigm. Positivism emphasizes that it is possible to grasp reality by using research instruments such as questionnaires and experiments (Blaxter et al., 2006). It is a method of deductive reasoning that proves or disproves the hypotheses of a researcher (Greener, 2008). Positivistic approaches are defined by individuals' views, an external reality exists independent from the researcher's views. As a result, the researcher separates himself from the research environment and takes the role of an independent observer that is not interfering with the research (Kulatunga et al., 2007). In positivist disciplines, results are evaluated through logical examination, quantification, the consistency of control and prediction, and through the application of comprehensive methodologies regarding reflexivity and focus on enhancing techniques and their implementation (Johnson and Duberley, 2000).

The strength of positivism lies in its use of quantitative approaches (Blaxter et al., 2006). A quantitative approach has been selected for examining the influence of selected organizational factors on the ISM in smart city organizations.

The following presented characteristics confirm that this research falls in the positivist paradigm. These characteristics align with the conditions identified by Easterby-Smith et al. (2002) for such research. Table 4.2 also presents the requirements of a successful positivism-based study that must and will be followed in this research.

Table 4.3: Aspects of Positivism

Component	Condition
The viewer	Must be independent
Human interest	Inexistent
Explanation	Must exhibit causality
Research progress	Hypothesis and conclusions
Concepts	Need to be operationalized
Unit of analysis	Reduced to simple forms
Generalization	Statistical probability
Required sampling	Random selection, sizeable sample

Source: Adopted from Easterby-Smith et al., 2002

Being positivist, this research uses measurement and aims to verify its findings via logical or mathematical proof. The following sections will be inspired by the research onion model layered strategies, and will detail the different steps with which this positivist research will utilize to develop the research model and achieve the intended goals. The research onion provides an elaborate and structured method with which this research inquiry could be planned and then conducted.

4.4 Research Strategy

Following the selection of the research philosophy and part of the selected research onion model, this research requires an overall strategy to integrate the different components of this study, ensuring the following sections and efforts will effectively address the research problem. The research strategy can be thought of as the “master plan” of a research that elucidates how the study should be conducted. The research design is required to identify the way in which the necessary data can be gathered and analysed to achieve a solution to the research problem (Sekaran, 2003). The selection of the research strategy is directed by the research questions, the available information, the available time, and the chosen philosophical path. As recommended by Gill and Johnson (1991), research strategies could be classified

as realist (nomothetic) and idealist (ideographic) ontologies, nomothetic being the method that utilises measured techniques for data analysis, and ideographic techniques being the analysis of subjective data produced through personal positions and concerning oneself interactions with the daily flow of life.

Burrell and Morgan (1994) indicate that nomothetic techniques emphasises the significance of establishing research using methodical methods, approaches used for example in natural sciences which concentrate on the practice of testing assumptions. Importance is thus given to covering explanations and expectations, and employing reasonable operationalisation of theories. As also explained by Burrell and Morgan (1994), ideographic methodologies, otherwise also emphasise the evaluation of subjective accounts that are created by entering a certain circumstance. The emphasis is on theory founded in the empirical observations utilized in the goal of achieving interpretation by comprehension.

Common research strategies used in business and management are explained while being referred to their relationship to the quantitative, qualitative or mixed research methods in the form of experiments, case studies, surveys, grounded theory, focus group, phenomenological search, action research, and narrative research (Easterby-Smith et al., 2008; Collis and Hussey, 2003; Saunders et al., 2009).

The two most used quantitative research methods are experiments and surveys (Saunders et al., 2009). Experimental research is done in laboratories or fields where there is complete control on the variables and it aims to test the relationships between specific variables, while holding all variables constant and changing only one variable to observe the effects on the dependent variable (Fellows and Liu, 2009). The experimentation is considered a trial since the result is not known beforehand, and also an observation since the result is cautiously documented (Melville and Goddard, 1996).

The second most popular type of quantitative research is surveys, which is a research strategy that emphasises the structured gathering of data from a significant portion of a population. Surveys are one of the most important approaches in applied social research (Fellows and Liu, 2009). Even though the term 'survey' is usually employed to define the collection of information using questionnaires, it also incorporates other methods like structured observation and structured interviews.

In this research, surveying is the strategy that will be carried out to collect quantitative data. Surveying is practical in defining the characteristics of a large sample, and no alternative approach offers such a wide perspective (DeVaus, 2002). Surveys are also regarded as a flexible way of collecting data since they may be achieved in different ways such as online, email, social media, paper, mobile, telephone, and face-to-face interviews (Blumberg et al., 2005). An important parameter of data collection method is validity. The anonymity of participants, particularly the ones that are ran online, allow respondents to answer with more truthful and useable answers which provide an opportunity for more honest and unambiguous results compared to other strategies, especially when clearly stated that survey data will remain completely confidential (Neuman, 2005).

4.5 Time Horizon

The time horizon is one of the research items part of the research onion model and part of the current research strategy. Subject to the research questions and objectives, the time horizon of the practiced research strategy would be taken as either a snapshot at a particular time (cross-sectional) or as a series of snapshots of events over a specified period of time (longitudinal) (Saunders et al., 2009).

This research will be conducted following the cross-sectional methodology, due to time constraints. Cross-sectional studies often employ surveys and focus group strategies, such as questionnaires and interviews conducted over a short period of time (Easterby-Smith et al., 2008; Robson, 2002).

4.6 Quantitative Data Collection methods

This research is an incorporation of constructs in a model that will be the foundation of an investigation in relation to the data collected through a survey from information security professionals, managers, and executives throughout organizations from around the world. The first major action to be undertaken in this research effort is the pilot study. Once this has been designed and carried out, the results will be analysed to inform the next phase of this research. After the pilot study, the main study will be undertaken, surveys in the form of a questionnaire will be sent out to professionals and managers in information security roles within organizations in smart and nonsmart cities. The participants will be approached via the LinkedIn social platform

The data analysis section comprises a description of techniques to be employed in explaining the nature of the elements in the analysis, and describe the development of the resulting data. It also blends observation (including relationships, correlations, and particularly significant or implicative findings), in addition to generating quantifiable figures. The validity and reliability section will explain potential limitations, biases, or other similarly influential factors, while the research ethics section will overview the important ethical consideration undertaken in the design and implementation of this study, such as confidentiality, awareness and freedom of the respondents, and academic policies.

4.7 From Hypotheses to Constructs

The purpose of this section is to identify questions from the literature that relate to the previously identified constructs. The goal is to link the hypotheses to the research constructs, showing their influence direction, and the identified research questions that will be used in the collection of research data.

As introduced in Chapter 3, Table 4.3 below shows the hypotheses and associated constructs to be measured.

Table 4.4: Hypotheses and Associated Constructs

No	Hypothesis	Constructs
1	The positive ability to adapt to rapid technology changes has a significant and positive impact on organizational ISM in smart cities	ARTD → ISM
2	Bureaucracy has a significant negative impact on organizational ISM in smart cities	BC → ISM
3	Employees' compliance with ISM policies has a significant and positive impact on the organizational ISM in smart cities	EC → ISM
4	Better use of the ICT infrastructure has a significant and positive impact on organizational ISM in smart cities	ICT → ISM

5	Inter-organizational collaboration between ISM departments and others has a significant and positive impact on the organizational ISM in smart cities	INTER → ISM
6	Intra-organizational collaboration between ISM departments and others has a significant and positive impact on the organizational ISM in smart cities	INTRA → ISM
7	Leadership attitude has a significant and positive impact on organizational ISM in smart cities	LA → ISM
8	Legislative influence has a significant and positive impact on organizational ISM in smart cities	LI → ISM
9	IS and ISM skilful human resources have a significant and positive impact on organizational ISM in smart cities	SW → ISM
10	The organizational type and business model have a significant and positive impact on organizational ISM in smart cities	TO → ISM
11	Accurate vendor selection ability has a significant and positive impact on organizational ISM in smart cities	VS → ISM
12	ISM has a significant and positive influence on OP in smart city organizations	ISM → OP

Source: Devised by author

4.8 Research questions

Employing the literature findings and the research model, a questionnaire was developed to address the main research questions around the previously identified organizational factors. The goal is to identify and highlight the important organizational factors towards ISM in smart city organizations. The literature sources of the survey questions have been described previously in this chapter. The defined questionnaire items for the profiling of participants and identification of their thoughts around the organizational factors follow. The questionnaire also included participants' profiling data, which required participants to answer non-invasive and

non-anonymity threatening questions on demographic and professional information (age, gender, information security role category, job location, and industry type).

The language selected for the questionnaire is clear and easy to facilitate the answering of the questions (Bhattacharjee, 2012). Participants had to select the best choices as they see suitable, based on their perception of the constructs of the conceptual model. The questionnaire did not ask participants for any identifying information. Also, the participants were informed that the collected information will only be used for this research, and that it will be kept confidential.

The identified and discussed organizational factors in Chapter 3 have long been researched in the literature in different contextual research examinations. Table 4.5 details how the research survey questions are inferred from the literature. The identified organizational factors are also listed with the relevant questions and the literature sources for the organizational factors and the research questions.

Table 4.5 Sources of Hypothesis Related Questions

Constructs	Question	Source
Organizational Performance (OP)	1. My organization is experiencing an integral improvement in finance and performance (e.g. sales, profits, or return on investment, etc.)	Maltz et al. (2003)
	2. My organization is experiencing an integral improvement in its relationship with its customers (e.g. market share, customer retention rates, customer satisfaction, etc.)	Germain et al. (2001)
	3. My organization is experiencing an integral improvement in human resources development (e.g. employee skills, commitment to technological leadership, personnel development, etc.)	Chakravarthy (1986)
	4. My organization is experiencing an integral improvement in preparing for the future (e.g. quality/depth of strategic planning, indicators of partnerships and alliances, anticipating and preparing for changes in the environment, products and services, etc.)	Kaplan and Norton (1996) Fliaster, 2004
Information Security Management (ISM)	<ol style="list-style-type: none"> 1. My organization has a well-documented and continuously updated information security policy that clearly defines the information security objectives of the organization. 2. My organization routinely conducts internal and external (third party) organizational information security audits 	Narain Singh et al, 2014

	<ol style="list-style-type: none"> 3. My organization has a continuously updated inventory record of all the information assets (hardware and software) 4. My organization has an access control policy that specifies which users have access to what data 5. My organization has a well-documented disaster recovery and business continuity plan 6. My organization takes disciplinary action against employees violating the information security rules/policy 7. My organization can survive a disaster that may result in the loss of systems, premises, etc. 	
<p>Leadership Attitude (L-A)</p>	<ol style="list-style-type: none"> 1. Senior executives regard the significance of information security 2. Senior executives attend information security related meetings 3. Senior executives are involved in information-security-related decisions 4. Senior executives allocate a reasonable budget for operations 5. Senior executives allocate reasonable manpower for organizational information security functions 	<p>Narain Singh et al, 2014</p>
	<ol style="list-style-type: none"> 1. Senior executives are able to inspire employees to attain set goals 2. My direct supervisor provides me with regular feedback on my job performance and behaviour 3. Senior executives praise good performance in blocking attacks or handling incidents 	<p>Ritz, 2009</p>

	4. Senior executives are open to change	
Legislative Influence (LI)	<ol style="list-style-type: none"> 1. My organization complies with information security legislations 2. Employees in my organization could be legally liable in case of information security failure 3. Senior leadership regard the significance of complying with information security legislations 4. There is a team/committee in my organization for monitoring compliance with data protection laws/legislations 	Q4: Narain Singh et al, 2014
Adaptation to Rapid Technology Development (ARTD)	<ol style="list-style-type: none"> 1. The rapid adoption of smart/e-business technologies helps in increasing our revenues/profits 2. The rapid adoption of smart/e-business technologies helps in reducing our direct and indirect costs 3. Management is supportive of the use of the latest smart/e-business technologies in our operations 4. Management communicates the need for the latest smart/e-business technologies usage in the firm 5. We know our customers are ready to accept the latest smart/e-business technologies 6. Our customers and partners are demanding the use of the latest smart/e-business technologies in doing business with them 	Ifinedo, 2011

	<p>7. We know our suppliers and partners are ready to do business over using the latest smart/e-business technologies</p>	
Vendor Selection (VS)	<ol style="list-style-type: none"> 1. My organization emphasizes the vendor solutions quality rather than the cost of purchase 2. My organization selects technology vendors based on their potential to support a competitive advantage and position 3. My organization selects technology vendors based on their support for quality and efficiency 4. My organization evaluates different vendors to find best matching solutions and most secure offerings for the organization 	<p>Dalvi and Kant, 2015</p>
Skilful Workforce (SW)	<ol style="list-style-type: none"> 1. My organization conducts regular information security training for employees 2. My organization conducts advanced information security training for technical employees 3. The information security training programmes offered by my organization are useful 4. My organization makes sure all employees are vigilant towards information security 5. My organization employs personnel with the right skills in the right positions 6. My organization does not face a shortage of information security skilled labour 	<p>Narain Singh et al, 2014</p>

<p>Better Utilization of the ICT Infrastructure (ICT)</p>	<ol style="list-style-type: none"> 1. My organization acknowledges the need to best utilize the Information and Communication Technologies (ICT) infrastructure to help in information security defence 2. My organization encourages the best utilization of the ICT infrastructure 3. My organization analyses the quality of service received from the ICT infrastructure provider (ISP/DSP) 4. My organization has a team/committee to evaluate Internet/data service provider service quality 	<p>Nam and Pardo, 2011a Mulligan and Olsson, 2013</p>
<p>Type of Organization (TO)</p>	<ol style="list-style-type: none"> 1. The type of industry my organization belongs to influences the information security procedures needed to protect online services 2. The type of industry my organization belongs to influences the data protection measures needed to protect customer data 3. The type of industry my organization belongs to influences the speed with which cyber security incidents need to be handled 4. The type of industry my organization belongs to influences the information security legislations my organization needs to comply with 5. The type of industry my organization belongs to influences the information security skills level needed to defend services 	<p>Chang and Ho, 2006</p>

<p>Employees Compliance to Organizational Policies (EC)</p>	<ol style="list-style-type: none"> 1. Employees inside my organization are required to comply with the information security policy and legislations 2. Employees inside my organization believe the information security policies are well developed to help in the protection of assets 3. Employees in my organization will comply with the information security policy, even if faced with urgent or critical issues 	<p>Hu et al., 2012</p>
<p>Bureaucracy (BC)</p>	<ol style="list-style-type: none"> 1. My organization's speed of change is on a par with leading organizations 2. My organization exerts tight control in delivering its core products/services 3. My organization tends to apply standardized administrative practices to monitor and control core operations 4. My organization is adopting innovative solutions to reduce internal processes complexity (e-documents, automated workflow, business intelligence) 	<p>Keung, 2009 Toppeta, 2010</p>
<p>Intra-Organizational Collaboration (INTRAC)</p>	<ol style="list-style-type: none"> 1. My organization considers individuals as an asset and tries to appreciate them continuously 2. The preservation of different points of view internally is encouraged in my organization 3. Everybody's opinions and contributions are respected in my organization 4. Collaboration and co-operation among the different duties and departments are encouraged 	<p>Pérez López et al., 2004</p>

	<p>5. My organization has a team/committee for conducting regular meetings between the different teams to consolidate efforts against cyber threats</p>	
<p>Inter-Organizational Collaboration (INTER)</p>	<ol style="list-style-type: none"> 1. The preservation of different points of view externally is encouraged in my organization 2. Collaboration and co-operation with other organizations are encouraged 3. Collaboration and co-operation with other organizations are allowed but also carefully monitored 4. My organization has a team/committee for conducting regular meetings with other organizations towards better threat information sharing and collaboration 	<p>Pérez López et al., 2004</p>

Source: Devised by author

4.9 Research questionnaire

The research questionnaire intended for data collection is divided into multiple sections. The first section introduces the research theme and goals in addition to the responsibilities and ethics behind its distribution. The second section asks the participants profiling questions around their age, gender, information security role category, and the size of the organization. The goal for doing profiling is to later gain the ability to anonymously segment the participants' data by role, location, size of the organization, or personal information such as age or gender. This is in an attempt to identify opinion patterns that could help achieve the goals of this research. The following sections of the questionnaire are established to answer the questions related to each of the hypotheses. The questions followed multiple phases to achieve full maturity (2-phase pilot study) and a 5-point Likert scale is adopted to answer the questions, which allows much better measurement of opinions and attitudes than Yes/No or True/False questions.

4.10 Research Ethics

As this research collected primary data from human beings, ethics approval was necessary before proceeding with the data collection. The goal was to ensure the research data are collected in an ethical manner that protects both the researcher and the participants. The submitted application included a description of the intended research aim and objectives, and the methodology and tools by which the data collection will be achieved from the target audience. Moreover, the researcher explained how the participants' data would be collected, used, and later discarded when the research is completed. Ethics approval was requested from the Brunel University research ethics committee, and was obtained on 3 August 2017, reference 7296-LR-Aug/2017- 8023-1 (see Appendices III and IV for full details on the survey and the Brunel university research ethics approval).

4.11 Research Population and Sample

Population refers to the complete group of people, events, or things of interest that the researcher wishes to investigate (Sekaran, 2003). The population of this research is information security-related personnel, who are working inside organizations inside cities that are among the smartest in the world following the IESE (2017) cities ranking. Demographics will, therefore, be collected from the participants. The goal is to be able to compare results between smart city

organizations and non-smart city organizations to identify discrepancies and better understand the differences that lead to enhanced ISM standing.

As this research aims to investigate information security management related organizational factors, the research unit of analysis is personnel with an information security role. The participants were divided into multiple groups by size of the organization (small, medium, large), the type organization industry, the type of job role (technical, management, executive), gender, age group, working city, reporting city, and organization's base city. Respondents in the study were asked to provide information about the size of the organization they are working for in terms of the number of employees. The response was categorized into three categories, namely <50, 50-250, and 250+, following the Europa Eurostat enterprise size guidelines.

4.11.1 Research data and target population

There are two types of possible research data, primary and secondary. Primary research data are those collected by the researcher to achieve the research aim and objectives (Collis and Hussey, 2003). Examples include surveys, case studies, and laboratory experiments (Bryman and Bell, 2007; Orlikowski and Baroudi, 1991). On the other hand, secondary data are those where the collected data are not directly connected to the research at hand. Examples include published summaries, reports, and statistics (Collis and Hussey, 2003). The selection of primary or secondary data or both is based on the research questions being addressed. For instance, some research may need to use primary data, while others only need secondary data. In order to address the specifics of this research, primary research data will be collected. In particular, data related to every defined construct within the conceptual model of this study will be collected from people with a current information security role.

4.11.2 Sampling technique

There are two types of sampling techniques, probability and non-probability. Using the probability sampling technique, all the units of the sampling frame have the probability of being a part of the sample. Non-probability is defined in contrary (Bhattacharjee, 2012; Saunders et al., 2011). The utilization of one or more sampling techniques is based on the research aim and objectives.

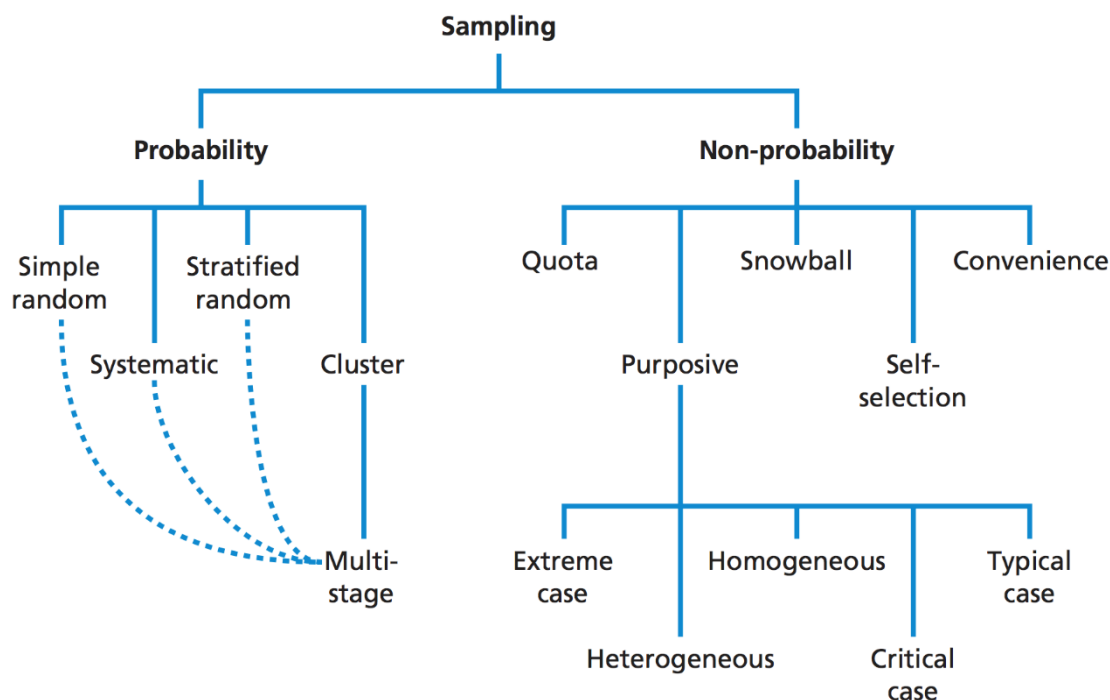


Figure 4.2: Sampling Techniques

Source: Saunders et al., 2011

Since this research captures the perceptions of information security professionals, the probability random sampling technique would fit best to ensure equal and satisfactory contributions to the study. Random sampling is typically used with data collection methods such as online surveys, postal surveys, and/or telephone surveys (Saunders et al., 2011; Dashti et al., 2009; Nam and Sayogo, 2011; Weerakkody et al., 2013).

Since information security professionals are generally tech-savvy and use the Internet regularly, this research uses online random sampling for data collection, as long as the selected survey participant has a valid LinkedIn profile with a current information security professional or manager role.

4.11.3 Sample size and selection

Researchers have not agreed on a definite number for a research sample size, as that changes based on multiple factors (Fowler, 2002; Muthen and Muthen, 2002). Nevertheless, it is generally preferred to have a large number of samples for better accuracy. The sampling size for the current research is 308, which is considered as satisfactory (Comrey and Lee, 1992; Tabachnich et al., 2001).

The researcher has chosen the Google Forms survey platform, a trusted platform that can guarantee participants' anonymity and data integrity.

A message was developed and sent to the LinkedIn users matching the required sample population, inviting them to participate in the research inquiry. The LinkedIn message can be found in Appendix II.

This research was conducted utilising a random discovery of information security related participants, primarily using the professional social networking platform, LinkedIn. The participants needed to be strictly information security professionals or managers with a current information security role. The researcher initially had 1,800 contacts on LinkedIn (relevant and non-relevant), and added around 9,000 people on LinkedIn during the survey period (8 August 2017 to 9 September 2017). At the end of the survey, the researcher had around 4,000 contacts on LinkedIn in total. The survey was therefore sent to around 3,000 LinkedIn users. Of these, 322 respondents answered the survey, and 308 survey participations were validated. The survey participants will then be divided into two groups, the ones that belong to smart cities and those who do not. The identification of smart cities will be based on the top 100 cities of the IESE (2017) world cities ranking, which is based on the evaluation of each world city parameters such as economy, human capital, social cohesion, environment, governance, urban planning, international outreach, technology, mobility and transportation.

4.12 Pilot Study

The pilot study for this research is organized in two rounds. All invited participants belong to the previously specified target population (information security related academics and professionals). The number of valid participations totalled 25 out of the 37 invited (67%), an acceptable rate as per the literature (Baruch, 1999; Dommeyer et al., 2002 Ogier, 2005). The questionnaire was set up on Google forms, and was communicated directly via email or WhatsApp, a social networking platform.

Pilot study round 1:

The questionnaire contained 48 questions, all mandatory for the questionnaire to be considered complete. The questionnaire was sent to 18 people (9 Information technology/security academics and 9 information security professionals). A total of

11 responses and 4 comments were received, and minor changes were made to the location questions.

Pilot study round 2:

A questionnaire was sent to 19 new people. a total of 14 responses (+1 falsified survey), and 2 comments were received. Further minor changes to the participants' selection section were made (in relation to smart city context with IESE). There were 25 validated pilot surveys.

4.12.1 Comments received

In the pilot rounds one and two, the participants were asked to input comments in text on the survey quality and clarity; such a practice allowed some qualitative feedback from the participants' side towards enhancing the overall survey status. It was left to the participants if they wished to complete the comments' section (see Table 4.5).

Table 4.6: Comments Received by Participants on Questionnaire

No	Comment type	Comment
1	Pilot1	The survey was well-prepared and designed to evaluate different aspects of information security within an organization. The length of the survey was acceptable as well. I feel that there some questions that need to be clarified to get a better measurement of each individual's view.
2	Pilot1	None.
3	Pilot1	This survey consisted of relevant questions and the answer options are very clear and not biased. Easy to understand, apt timing, well designed. Altogether, an excellent piece of the survey.
4	Pilot1	Good quality, clear and quite long.
5	Pilot1	Great questions!

6	Pilot1	Survey a little bit long and some questions are not clear for participants. Good luck!
7	Pilot2	I'm missing how this series of questions relate specifically to smart cities or what smart cities are defined as the opening premise.
8	Main study	Great survey. Good luck with your research topic. A hint to give to the survey taker: it's better to flip the mobile horizontally in case he is taking the survey from his smart phone.
9	Main study	Excellent quality, very clear and not too long to bore the person taking the survey.
10	Main study	Good quality survey, it touches the key aspects of Information Security, not lengthy at all. Good luck!
11	Main study	My country is still light years late on InfoSec awareness.
12	Main study	The survey was well organized and classified. I enjoyed completing it and it gives me an overall vision of how organizations should verify their threat intelligence overview with a high-quality survey like this. Thank you for inviting me.
13	Main study	Compliance is looked upon as a burden by senior management.

Source: Devised by author

4.12.2 Pilot study data analysis in IBM SPSS

Data analysis was then conducted on the pilot study data using the IBM Statistical Package for the Social Sciences (SPSS) version 23.0. Descriptive (Minimum, Maximum, Mean, Standard deviation) and reliability statistics (Cronbach's alpha) were calculated.

Following the pilot data analysis, and considering that Q10 and Q29 are negative questions, descriptive and reliability statistics were generated. Not all tests were possible to perform due to the low sample size. An elaborate number of participations is required to complete other tests.

Descriptive statistics

Table 4.7: Pilot Study Descriptive Statistics

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
Q1	25	2	5	3.96	.978
Q2	25	3	5	4.20	.816
Q3	25	1	5	3.44	1.446
Q4	25	1	5	4.24	1.012
Q5	25	1	5	4.16	1.214
Q6	25	1	5	4.32	1.069
Q7	25	1	5	3.84	1.214
Q8	25	1	5	4.04	1.207
Q9	25	1	5	3.88	1.166
Q10	25	1	5	2.32	1.345
Q11	25	2	5	4.48	.770
Q12	25	3	5	4.32	.690
Q13	25	2	5	4.00	1.225
Q14	25	3	5	4.36	.860
Q15	25	3	5	4.48	.770
Q16	25	1	5	3.60	1.225
Q17	25	2	5	4.24	.970
Q18	25	2	5	4.20	.913
Q19	25	2	5	4.36	.907
Q20	25	1	5	3.88	1.054
Q21	25	2	5	3.64	1.075
Q22	25	1	5	3.72	1.400
Q23	25	2	5	4.44	.821
Q24	25	2	5	4.08	.997
Q25	25	1	5	4.36	.995
Q26	25	2	5	4.20	.957
Q27	25	3	5	4.40	.764
Q28	25	1	5	3.80	1.225
Q29	25	1	5	3.08	1.288
Q30	25	2	5	4.00	1.118
Q31	25	2	5	4.00	1.000
Q32	25	1	5	3.76	1.165
Q33	25	3	5	4.56	.651
Q34	25	4	5	4.80	.408
Q35	25	2	5	4.40	.866
Q36	25	3	5	4.40	.707
Q37	25	1	5	3.52	1.327
Q38	25	1	5	3.92	1.222
Q39	25	1	5	3.76	1.451
Q40	25	3	5	4.72	.542
Q41	25	2	5	3.88	1.013
Q42	25	1	5	3.72	1.308
Q43	25	1	5	3.84	1.281
Q44	25	2	5	4.12	1.130
Q45	25	1	5	3.60	1.354
Q46	25	1	5	3.60	1.225
Q47	25	1	5	3.40	1.080
Q48	25	1	5	3.24	1.422
Valid N (listwise)	25				

Source: Devised by author

All answers had mean values of more than three, an indicator of agreement to a certain extent in the opinions of the respondents. All standard deviation values were less than half the mean value.

Reliability statistics

Table 4.8: Pilot Study Reliability Statistics

Questions Group	Questions	Cronbach's Alpha reliability	Comments
B	Q1->Q4	0.684	
C	Q5->Q10	0.805	Q10 reverse question
D	Q11->Q13	0.575	Without Q13 value=0.716
E	Q14->Q17	0.878	
F	Q18->Q21	0.772	
G	Q22->Q25	0.765	
H	Q26->Q29	0.816	Q29 reverse question
I	Q30->Q32	0.877	
J	Q33->Q36	0.764	
K	Q37->Q39	0.816	
L	Q40->Q42	0.729	
M	Q43->Q45	0.822	
N	Q46->Q48	0.862	

Source: Devised by author

In the reliability statistics analysis, Cronbach's Alpha factor was calculated to check for data reliability as per Tavakol and Dennick (2011). It was noted that question groups B and D had a Cronbach's Alpha reliability value of <0.7, which is

questionable. It was also noted that for question group D, the Cronbach's Alpha reliability value could be enhanced if Q13 was removed. Nevertheless, it was decided that no changes would be made to the questions' format as the overall average Cronbach's Alpha reliability for all questions groups was 0.782, which is an acceptable result for demonstrating the internal consistency of the questionnaire.

Table 4.9: Cronbach's Alpha Score Results Interpretation

Cronbach's alpha	Internal consistency
$\alpha \geq 0.9$	Excellent
$0.9 > \alpha \geq 0.8$	Good
$0.8 > \alpha \geq 0.7$	Acceptable
$0.7 > \alpha \geq 0.6$	Questionable
$0.6 > \alpha \geq 0.5$	Poor
$0.5 > \alpha$	Unacceptable

Source: Adapted from Tavakol and Dennick (2011)

In general, a Cronbach's alpha score higher than 0.7 is considered acceptable (Tavakol and Dennick, 2011).

In this pilot study, data were gathered quantitatively through the survey and qualitatively through the comments. The development and utilization of a pilot study are advantageous for the initial evaluation of the survey questions and content, enabling the improvement of questionnaire content, focus, and reliability. It also enables the determination of the questions' validity and internal consistency.

4.13 Main Study

This research is restricted to personnel with a current information security role in an organization. The appropriate number of participants was set to be around 300 validated surveys, with the goal being to provide a sufficient amount of data, where additional data do not provide additional information. According to Roscoe (1975), for perceptual studies, an acceptable sample size ranges between 200 and 500 samples. The questionnaire was implemented utilizing the Google forms format, which provides a popular, trusted, and convenient platform to execute data surveys (Denton, 2012). The survey was open from 8 August 2017 to 9 September 2017 for participants to complete the survey (pilot and main study). It is believed that the survey reached around 3,000 people.

4.14 Data Analysis assumptions and justification

Before data results are analysed, they need to be checked for layout, coding, and errors (Churchill and Iacobucci, 2004; Saunders et al., 2011; Sekaran, 2000). As this research selected an online survey method (Google Forms) for data collection from participants, the data layout, coding, and error checking was done automatically once the survey method was designed. Data were presented to the researcher in a spreadsheet format, downloadable in XLS format. This research adopted SPSS for the data analysis as it is flexible, effective, and includes a number of options for graphs and modelling (Field, 2013; Green and Salkind, 2010; Pallant, 2013). The data collected via online survey were exported to an SPSS file. Using an online survey method saved time and effort while also helping to avoid errors and mistakes when compared to a manual approach.

The selection of the PLS-SEM algorithm for the data analysis in this research is based on the fact that theory is less developed in the context of smart cities in addition to the lack of current-day presence of ready smart cities, all inferring an exploratory context where the research objective is the identification of key “driver” constructs. The primary objective of this research is to “maximize explained variance in the dependent constructs but additionally to evaluate the data quality on the basis of measurement model characteristics” (Hair et al., 2011; Hair et al., 2012; Hair et al., 2014). There are also no assumptions tests needed to conduct PLS-SEM (unlike CB-SEM), the SEM will also present the reliability and validity of the data and the measurement instrument into multiple calculations. Chapter 5 will detail the steps performed in the data analysis in this research.

4.15 Summary

This chapter provided information on the methodology and techniques for conducting this research. It started by clarifying the selection of a positivist research philosophy. The research philosophy and structure were then explained, and the steps that needed to be followed to achieve the research goals were listed. A quantitative approach was selected. Also, the sampling format, size, techniques, tools and scope were defined, and the use of SEM and SMARTPLS software was explained and justified. The next chapter presents the data analysis protocols and findings.

Chapter 5 DATA ANALYSIS AND RESULTS

5.1 Introduction

This research targets the identification and measurement of the influence of organizational factors on information security management (ISM) in the context of smart city organizations. After the proposition of the conceptual framework model presented in Chapter 3, and the research methodology provided in Chapter 4, this chapter provides detailed data analysis of the questionnaire data to verify and validate the proposed model. Therefore, the purpose of this chapter is to provide a full analysis of the data collected from the questionnaire surveys. Results from descriptive statistics, multivariate analysis, and hypotheses testing are presented. This chapter will address the phase of data analysis and report results using SPSS and the Structural Equation Modelling method using SMART-PLS.

The goal of the model in this study is to investigate the impact of the different organizational factors (namely leadership attitude (LA), legislative influence (LI), adaptation to rapid technology development (ARTD), vendor selection (VS), skilful workforce (SW), information and communication technologies (ICT), type of organization (TO), employee compliance (EC), bureaucracy (BC), inter-organizational collaboration (INTER), and intra-organizational collaboration (INTRA) on information security management (ISM)). The study further assesses the impact of information security management on organizational performance (OP).

The data analysis of this study is divided into four parts:

1. the presentation of the descriptive statistics for the profiling of the respondents;
2. the presentation of the descriptive statistics for the different constructs in the study;
3. the analysis of the results of the measurement model involving the assessment of reliability and construct validity, including convergent and discriminant validity;
4. the analysis of the results of the structural model to substantiate the hypotheses. The structural model is the analysis of the results of the relationship among the latent variables or constructs. This analysis includes the coefficient of determination (R^2), the path coefficients, and the predictive relevance Q^2 .

5.2 Respondents' Profiling

In the present study, respondents were asked some personal and work/business specific questions. The first goal of the respondents' profiling is to get to know and understand the participants better while keeping their anonymity protected. The second goal of respondents' profiling is to identify any mistaken participation in the research survey, which could lead to the collection of false data. The third goal of data profiling is to leave space for the profiling variables to be used in future differential tests. The fourth goal of data analysis, and which is particular to this research, is to collect demographic data to classify the participants as belonging to smart cities or not, as per the IESE (2017) cities ranking.

The study required:

1. gender;
2. age;
3. security role;
4. organizational size;
5. organizational sector;
6. smart city status;
7. residential base;
8. organizational base;
9. reporting city.

The following section will provide details of the responses on each of the aforementioned demographic variables.

5.2.1 Gender

Respondents in the study were asked to state their gender. The majority of the respondents were male (287, 93.2%), while a total of 21 (6.8%) of the respondents were female. The number of respondents based on gender is shown in Table 5.1 and Figure 5.1. The gender population inequality is a known and discussed phenomena in the literature as more males have a presence in the information technology domain (Reinen and Plomp, 1997)

Table 5.1: Respondents' Distribution by Gender

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Male	287	93.2	93.2	93.2
	Female	21	6.8	6.8	100.0
	Total	308	100	100.0	
Total		308	100.0		

Source: Devised by author

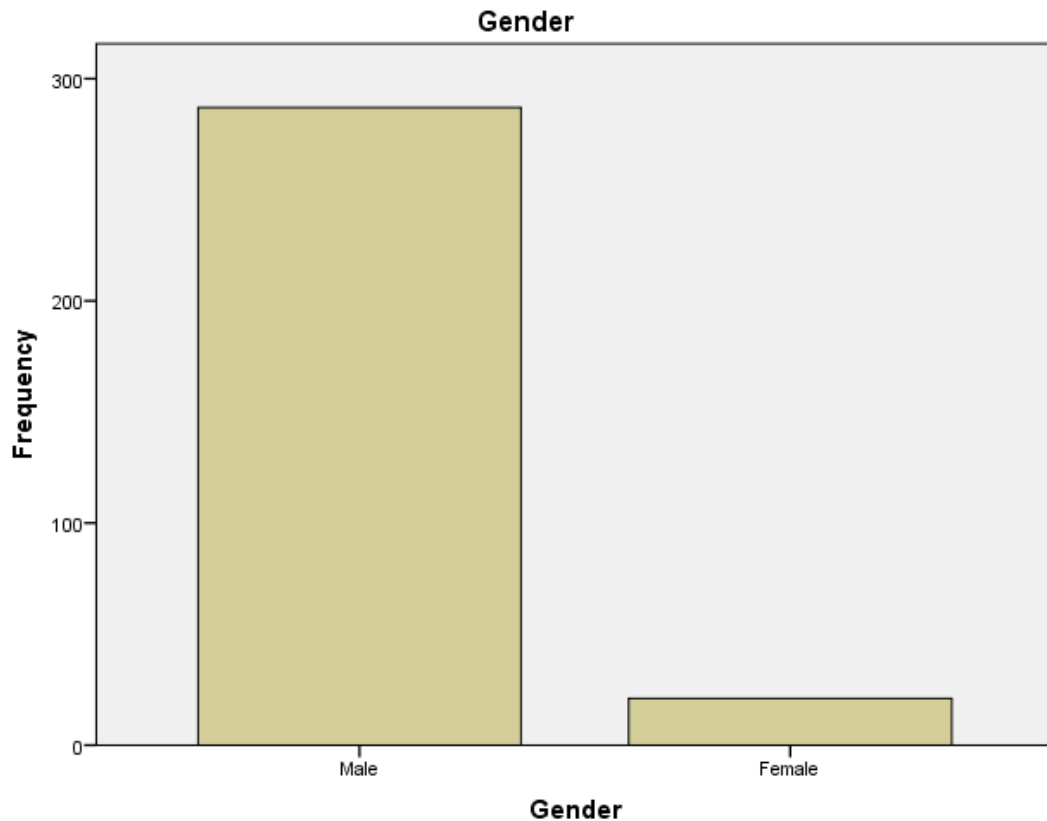


Figure 5.1: Respondents' Distribution by Gender

Source: DeVised by author

5.2.2 Age

Respondents in the study were asked to provide their age. Age was categorized into a total of three different groups, namely less than 25, Between 25 and 35, and more than 35. The majority of the respondents were middle aged and belonging to the age group between 25 and 35 (176, 57%), while the minority of the respondents were in the age group less than 25 (22, 7.1%). The number of respondents per each age group and their respective percentages are shown in Table 5.2 and Figure 5.2. The lowest number of participants from the group "Less than 25" could be caused by the fact that the age window after graduation is small (e.g. 22 to 25), compared to the other age windows (e.g. 25 to 35, 35 or more).

Table 5.2: Respondents' Distribution by Age Group

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Less than 25	22	7.1	7.1	7.1
	25-35	176	57.1	57.1	64.3
	More than 35	110	35.7	35.7	100.0
	Total	308	100	100.0	
Total		308	100.0		

Source: Devised by author

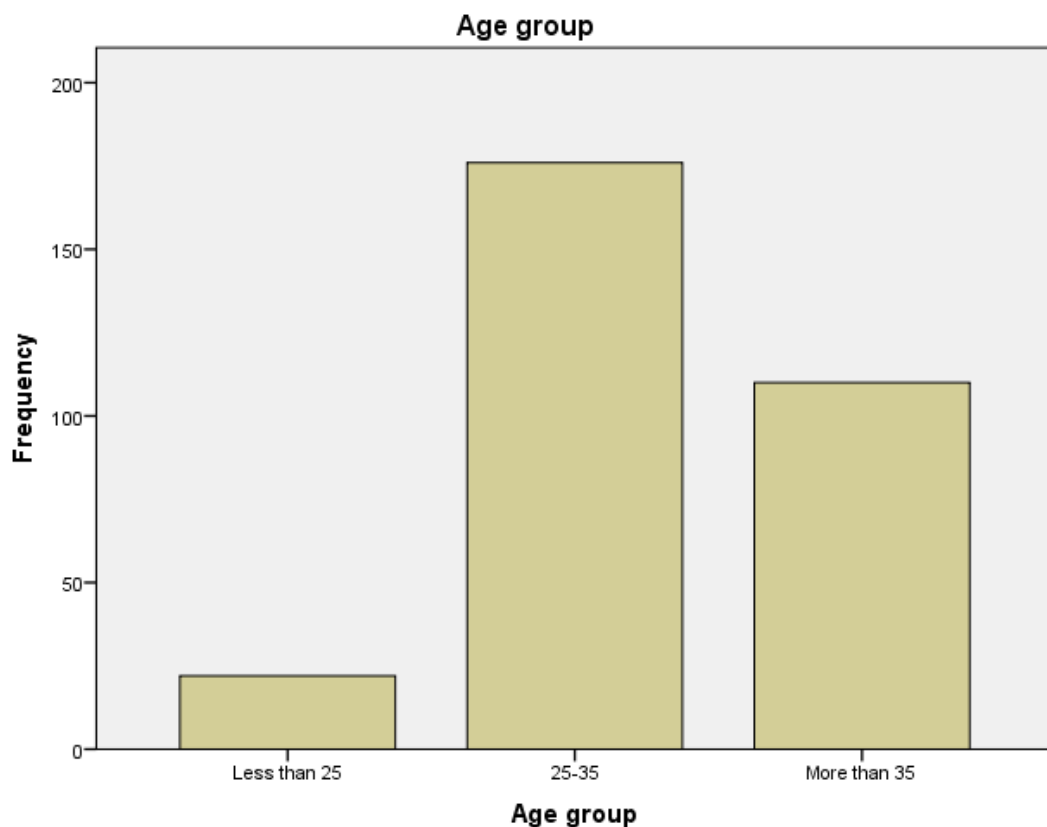


Figure 5.2: Respondents' Distribution by Age Group

Source: Devised by author

5.2.3 Security Role

Respondents in the study were asked to provide information about their information security role. Roles were categorized into three different categories, namely:

“Security management, Risk, Audit, Policy”, “Technical, Specialist, Architect”, and “Chief, Executive, Director”. The majority of the respondents were in the Technical, Specialist, Architect category (174, 56.3%), while the minority of the respondents were in the group entitled Chief, Executive, Director (49, 15.9%). The number of respondents in each age group and their respective security role are shown in Table 5.3 and Figure 5.3. The reason behind the majority of the respondents being from the “Technical, Specialist, Architect” group is probably because the management and executive information security roles are usually fewer than those in the “Technical, Specialist, Architect” area.

Table 5.3: Respondents' Distribution by Security Role

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Security management, Risk, Audit, Policy	85	27.6	27.6	27.6
	Technical, Specialist, Architect	174	56.5	56.5	84.1
	Chief, Executive, Director	49	15.9	15.9	100.0
	Total	308	100	100.0	
Total		308	100.0		

Source: DeVised by author

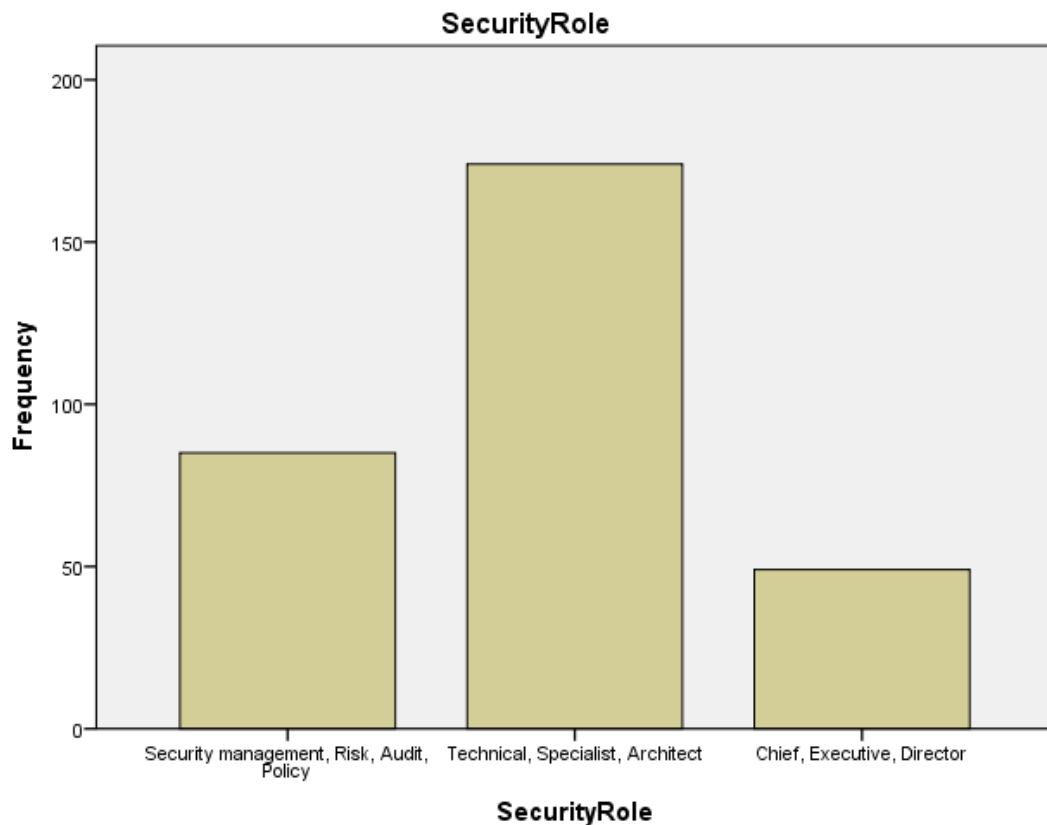


Figure 5.3 Respondents' Distribution by Security Role

Source: Devised by author

5.2.4 Organizational Size

Respondents in the study were asked to provide information about the size of the organization they work for in terms of the number of employees. The response was categorized into three categories, namely <50, 50-250, and 250>. The majority of the respondents worked for an organization that had over 250 employees (205, 66.3%), while the least number of respondents were in organizations with fewer than 50 employees (49, 15.9%). The number of respondents in each age group and their respective security role is shown in the Table 5.4 and Figure 5.4.

Table 5.4: Respondents' Distribution by Organizational Size

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	<50	49	15.9	15.9	15.9
	50-250	54	17.5	17.5	33.4
	250>	205	66.6	66.6	100.0
	Total	308	100	100.0	
Total		308	100.0		

Source: Devised by author

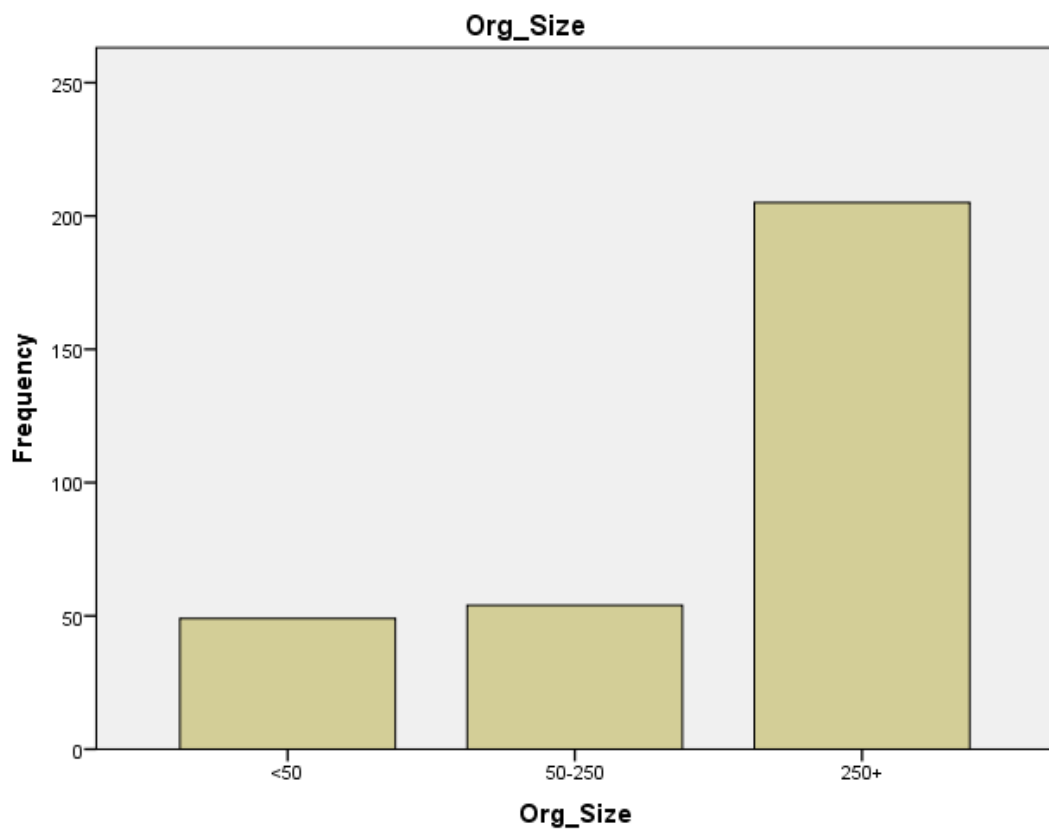


Figure 5.4: Respondents' Distribution by Organizational Size

Source: Devised by author

5.2.5 Organizational Sector

Respondents in the study were asked to provide information about the sector in which they are currently providing services, choosing from a total of 13 different sectors. The majority of the respondents were employed in an international or multinational organization (68, 22%). The number of respondents in each sector and their respective percentages are shown in Table 5.5.

Table 5.5: Respondents' Distribution by Organizational Sector

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Public Sector	36	11.7	11.7	11.7
	Financial Services	54	17.5	17.5	29.2
	Integrator services	37	12.0	12.0	41.2
	Telecommunications	43	14.0	14.0	55.2
	Industrial/manufacturing	11	3.6	3.6	58.8
	Engineering	10	3.2	3.2	62.0
	International or Multinational	68	22.1	22.1	84.1
	Professional Services	24	7.8	7.8	91.9
	Utilities	3	1.0	1.0	92.9
	Cyber security services/vendor	17	5.5	5.5	98.4

	Aviation	3	1.0	1.0	99.4
	Media	1	0.3	0.3	99.7
	Transportation	1	0.3	0.3	100.0
	Total	308	100	100.0	
Total		308	100.0		

Source: Devised by author

5.2.6 Smart City Standing

Respondents' location information in the study was matched to the latest IESE cities ranking. The top 100 on the IESE rank were considered smart cities. The majority of the respondents worked in smart cities (168, 54.4%), while 139 (45%) worked in non-smart cities. The number of respondents in each category and their respective percentages are shown in Table 5.6 and Figure 5.5.

Table 5.6: Respondents' Distribution by Smart City

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Not Smart	139	45.1	45.1	45.1
	Smart	169	54.9	54.9	100.0
	Total	308	100.0	100.0	
Total		308	100.0		

Source: Devised by author

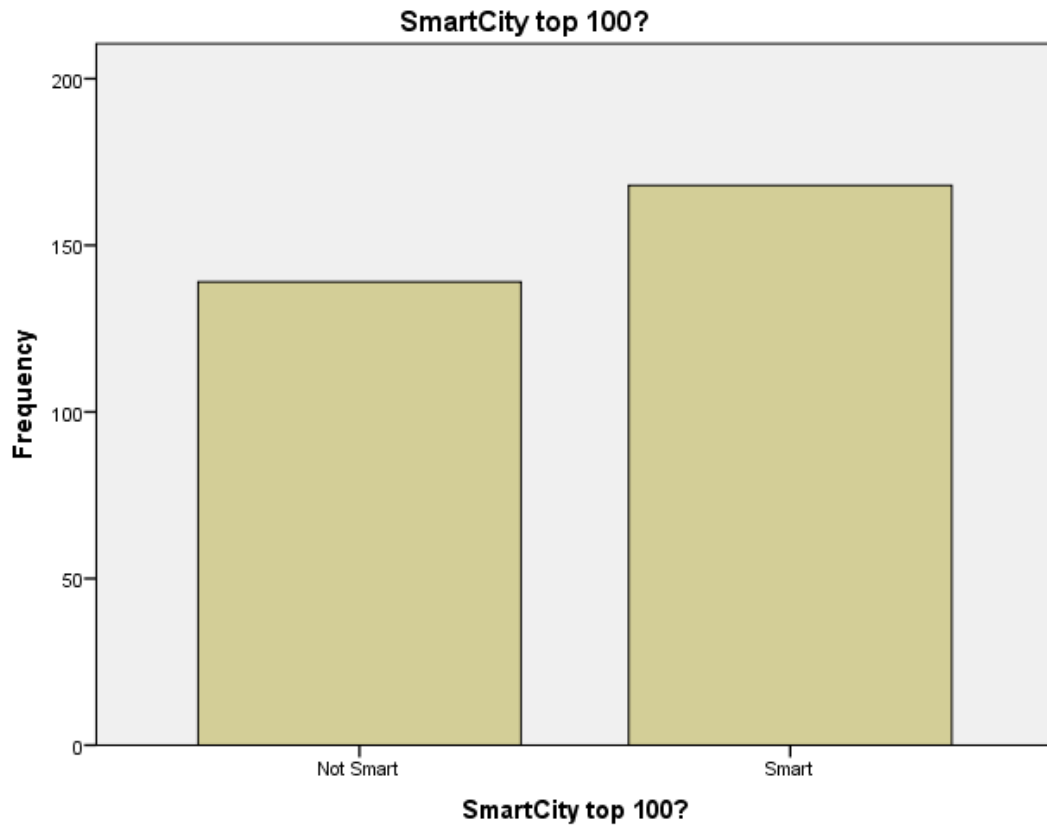


Figure 5.5: Respondents' Distribution by Smart City

Source: Devised by author

5.2.7 Response Base

Respondents in the study were asked to provide information about their response base. The majority of the respondents' response base was Dubai (53, 17.2%). The different response bases and the number of respondents in each base, as well as their respective percentages, are shown in Table 5.7.

Table 5.7: Respondents' Distribution by Response Base

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Abu Dhabi	12	3.9	3.9	4.2
	AL Fortville	1	0.3	0.3	4.5
	Algeria	1	0.3	0.3	4.9

Algiers	3	1.0	1.0	5.8
Amman	18	5.8	5.8	11.7
Atlanta	1	0.3	0.3	12.0
Bahrain	1	0.3	0.3	12.3
Bangalore	1	0.3	0.3	12.6
Barcelona	3	1.0	1.0	13.6
Beirut	31	10.0	10.0	23.6
Bologna	1	0.3	0.3	23.9
Bonn	1	0.3	0.3	24.3
Boston	1	0.3	0.3	24.6
Brescia	1	0.3	0.3	24.9
Brisbane	1	0.3	0.3	25.2
Cairo	17	5.5	5.5	30.7
California	1	0.3	0.3	31.1
Casablanca	2	0.6	0.6	31.7
Chicago	1	0.3	0.3	32.0
Dammam	1	0.3	0.3	32.4
Delhi	1	0.3	0.3	32.7
Doha	6	1.9	1.9	34.6
Dubai	53	17.2	17.2	51.8
Essen	1	0.3	0.3	52.1

Giza	1	0.3	0.3	52.4
Hartford CT	1	0.3	0.3	52.8
Indiana	1	0.3	0.3	53.1
Islamabad	3	1.0	1.0	54.0
Issy-les-Moulineaux	1	0.3	0.3	54.4
Jakarta	1	0.3	0.3	54.7
Jeddah	3	1.0	1.0	55.7
Khartoum	1	0.3	0.3	56.0
Khobar	1	0.3	0.3	56.3
Kuwait	1	0.3	0.3	56.6
Lebanon	1	0.3	0.3	57.0
London	5	1.6	1.6	58.6
Los Angeles	2	0.6	0.6	59.2
Madrid	2	0.6	0.6	59.9
Malaysia	1	0.3	0.3	60.2
Manama	2	0.6	0.6	60.8
Manchester	2	0.6	0.6	61.5
Melbourne	2	0.6	0.6	62.1
Miami	1	0.3	0.3	62.5
Milan	11	3.6	3.6	66.0
Modena	1	0.3	0.3	66.3

Montreal	3	1.0	1.0	67.3
Munich	2	0.6	0.6	68.0
Muscat	3	1.0	1.0	68.9
New Delhi	1	0.3	0.3	69.3
New York	1	0.3	0.3	69.6
Oxford	2	0.6	0.6	70.2
Paris	23	7.4	7.4	77.7
Punjab	1	0.3	0.3	78.0
Rawalpindi	1	0.3	0.3	78.3
Reading	1	0.3	0.3	78.6
Riyadh	16	5.2	5.2	83.8
Rome	4	1.3	1.3	85.1
San Diego	1	0.3	0.3	85.4
San Mateo	1	0.3	0.3	85.8
Saudi	1	0.3	0.3	86.1
Seattle	1	0.3	0.3	86.4
Sharjah	1	0.3	0.3	86.7
Singapore	10	3.2	3.2	90.0
Sulaymaniyah	1	0.3	0.3	90.3
Swansea	1	0.3	0.3	90.6
Sydney	8	2.6	2.6	93.2

Taichung	1	0.3	0.3	93.5
Tallahassee	1	0.3	0.3	93.9
Tehran	3	1.0	1.0	94.8
Tel Aviv	1	0.3	0.3	95.1
Tenerife	1	0.3	0.3	95.5
Texas	1	0.3	0.3	95.8
Tirana	1	0.3	0.3	96.1
Trieste	1	0.3	0.3	96.4
Turin	3	1.0	1.0	97.4
Valletta	1	0.3	0.3	97.7
Venice	1	0.3	0.3	98.1
Vienna	1	0.3	0.3	98.4
Washington	4	1.3	1.3	99.7
Yokohama	1	0.3	0.3	100.0
Total	308	100.0	100.0	

Source: Devised by author

5.2.8 Organizational Base

Respondents in the study were asked to provide information about their organizational base. The majority of the respondents had Dubai as their response base (45, 14.6%). Different organizational bases and the number of respondents in each base and their respective percentages are shown in Table 5.8.

Table 5.8: Respondents' Distribution by Organizational Base

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Abu Dhabi	10	3.2	3.2	3.6
	Algeria	1	0.3	0.3	3.9
	Algiers	2	0.6	0.6	4.5
	Amman	15	4.9	4.9	9.4
	Amsterdam	2	0.6	0.6	10.0
	Atlanta	1	0.3	0.3	10.4
	Austin	1	0.3	0.3	10.7
	Baghdad	1	0.3	0.3	11.0
	Bahrain	1	0.3	0.3	11.3
	Bangalore	1	0.3	0.3	11.7
	Barcelona	1	0.3	0.3	12.0
	Beirut	29	9.4	9.4	21.4
	Boston	2	0.6	0.6	22.0
	Brisbane	1	0.3	0.3	22.3
	Cairo	16	5.2	5.2	27.5
	California	2	0.6	0.6	28.2
	Cambridge UK	1	0.3	0.3	28.5
	Casablanca	1	0.3	0.3	28.8
	Chicago	1	0.3	0.3	29.1

Darmstadt	1	0.3	0.3	29.4
Dhahran	1	0.3	0.3	29.8
Doha	6	1.9	1.9	31.7
Dubai	45	14.6	14.6	46.3
Dublin	1	0.3	0.3	46.6
Emilia Romagna	1	0.3	0.3	46.9
Essen	1	0.3	0.3	47.2
Florence	1	0.3	0.3	47.6
Geneva	1	0.3	0.3	47.9
Giza	1	0.3	0.3	48.2
Herndon VA	1	0.3	0.3	48.5
Indiana	1	0.3	0.3	48.9
Internet	1	0.3	0.3	49.2
Islamabad	3	1.0	1.0	50.2
Issy-les- Moulineaux	1	0.3	0.3	50.5
Italy	1	0.3	0.3	50.8
Jakarta	1	0.3	0.3	51.1
Japan	1	0.3	0.3	51.5
Jeddah	3	1.0	1.0	52.4
Jordan	1	0.3	0.3	52.8

Khobar	1	0.3	0.3	53.1
Lancashire	1	0.3	0.3	53.4
Lebanon	1	0.3	0.3	53.7
London	12	3.9	3.9	57.6
Los Angeles	2	0.6	0.6	58.3
Madrid	2	0.6	0.6	58.9
Malaysia	1	0.3	0.3	59.2
Manama	2	0.6	0.6	59.9
McLean	1	0.3	0.3	60.2
Melbourne	3	1.0	1.0	61.2
Milan	12	3.9	3.9	65.0
Montreal	4	1.3	1.3	66.3
Moscow	2	0.6	0.6	67.0
Munich	2	0.6	0.6	67.6
Muscat	3	1.0	1.0	68.6
Netherlands	1	0.3	0.3	68.9
New Delhi	1	0.3	0.3	69.3
New York	2	0.6	0.6	69.9
Northwich	1	0.3	0.3	70.2
Oxford	1	0.3	0.3	70.6
Paris	20	6.5	6.5	77.0

Punjab	1	0.3	0.3	77.3
Qatar	1	0.3	0.3	77.7
Rawalpindi	1	0.3	0.3	78.0
Reading	2	0.6	0.6	78.6
Reston	1	0.3	0.3	79.0
Riyadh	15	4.9	4.9	83.8
Rome	4	1.3	1.3	85.1
San Diego	1	0.3	0.3	85.4
San Francisco	2	0.6	0.6	86.1
San Jose	2	0.6	0.6	86.7
Saudi	1	0.3	0.3	87.1
Seattle	1	0.3	0.3	87.4
Singapore	6	1.9	1.9	89.3
Stockholm	1	0.3	0.3	89.6
Sulaymaniyah	1	0.3	0.3	90.0
Sunnyvale CA	1	0.3	0.3	90.3
Switzerland	1	0.3	0.3	90.6
Sydney	7	2.3	2.3	92.9
Taichung	1	0.3	0.3	93.2
Tallahassee	1	0.3	0.3	93.5
Tehran	3	1.0	1.0	94.5

	Tel Aviv	1	0.3	0.3	94.8
	Tenerife	1	0.3	0.3	95.1
	Texas	1	0.3	0.3	95.5
	Tirana	1	0.3	0.3	95.8
	Tokyo	1	0.3	0.3	96.1
	Turin	2	0.6	0.6	96.8
	USA	3	1.0	1.0	97.7
	Valletta	1	0.3	0.3	98.1
	Vienna	1	0.3	0.3	98.4
	Virginia	1	0.3	0.3	98.7
	Washington	4	1.3	1.3	100.0
	Total	308	100.0	100.0	

Source: Devised by author

5.2.9 Reporting City

Respondents in the study were asked to provide information about their reporting city. The majority of the respondents' response base was Dubai (46, 14.9%).

Different reporting cities, the number of respondents in each reporting city and their respective percentages are shown in Table 5.9.

Table 5.9: Respondents' Distribution by Reporting City

		Frequency	Percentage	Valid Percentage	Cumulative Percentage
Valid	Paris	1	0.3	0.3	0.6
	Abu Dhabi	12	3.9	3.9	4.5

Algeria	1	0.3	0.3	4.9
Algiers	3	1.0	1.0	5.8
Amman	14	4.5	4.5	10.4
Amman	1	0.3	0.3	10.7
Amsterdam	2	0.6	0.6	11.3
Atlanta	1	0.3	0.3	11.7
Baghdad	1	0.3	0.3	12.0
Bahrain	1	0.3	0.3	12.3
Bangalore	1	0.3	0.3	12.6
Barcelona	4	1.3	1.3	13.9
Beirut	29	9.4	9.4	23.3
Bologna	1	0.3	0.3	23.6
Boston	2	0.6	0.6	24.3
Brisbane	1	0.3	0.3	24.6
Cairo	16	5.2	5.2	29.8
California	2	0.6	0.6	30.4
Casablanca	2	0.6	0.6	31.1
Chicago	1	0.3	0.3	31.4
Darmstadt	1	0.3	0.3	31.7
Dhahran	1	0.3	0.3	32.0
Doha	6	1.9	1.9	34.0

Dubai	1	0.3	0.3	34.3
Dubai	46	14.9	14.9	49.2
Essen	1	0.3	0.3	49.5
Florence	1	0.3	0.3	49.8
Geneva	1	0.3	0.3	50.2
Giza	1	0.3	0.3	50.5
Indiana	1	0.3	0.3	50.8
Islamabad	3	1.0	1.0	51.8
Issy_les_moulineau x	1	0.3	0.3	52.1
Italy	1	0.3	0.3	52.4
Jakarta	1	0.3	0.3	52.8
Jeddah	3	1.0	1.0	53.7
Khobar	1	0.3	0.3	54.0
Lancashire	1	0.3	0.3	54.4
Lausanne	1	0.3	0.3	54.7
Lebanon	1	0.3	0.3	55.0
Levallois-Perret	1	0.3	0.3	55.3
London	1	0.3	0.3	55.7
London	7	2.3	2.3	57.9
Los Angeles	2	0.6	0.6	58.6
Madrid	2	0.6	0.6	59.2

Malaysia	1	0.3	0.3	59.5
Manama	3	1.0	1.0	60.5
Melbourne	2	0.6	0.6	61.2
Milan	13	4.2	4.2	65.4
Montreal	3	1.0	1.0	66.3
Moscow	3	1.0	1.0	67.3
Mumbai	1	0.3	0.3	67.6
Munich	2	0.6	0.6	68.3
Muscat	3	1.0	1.0	69.3
NA	1	0.3	0.3	69.6
New Delhi	1	0.3	0.3	69.9
New York	3	1.0	1.0	70.9
Northwich	1	0.3	0.3	71.2
Oxford	1	0.3	0.3	71.5
Paris	23	7.4	7.4	79.0
Punjab	1	0.3	0.3	79.3
Rawalpindi	1	0.3	0.3	79.6
Reading	1	0.3	0.3	79.9
Riyadh	15	4.9	4.9	84.8
Rome	4	1.3	1.3	86.1
San Diego	1	0.3	0.3	86.4

San Francisco	2	0.6	0.6	87.1
Saudi	1	0.3	0.3	87.4
Seattle	1	0.3	0.3	87.7
Shariah	1	0.3	0.3	88.0
Singapore	8	2.6	2.6	90.6
Sulaymaniyah	1	0.3	0.3	90.9
Sydney	7	2.3	2.3	93.2
Taichung	1	0.3	0.3	93.5
Tallahassee	1	0.3	0.3	93.9
Tehran	3	1.0	1.0	94.8
Tel Aviv	1	0.3	0.3	95.1
Tenerife	1	0.3	0.3	95.5
Texas	1	0.3	0.3	95.8
Tirana	1	0.3	0.3	96.1
Tokyo	1	0.3	0.3	96.4
Trieste	1	0.3	0.3	96.8
Turin	2	0.6	0.6	97.4
US	1	0.3	0.3	97.7
Valletta	1	0.3	0.3	98.1
Vienna	1	0.3	0.3	98.4
Virginia	1	0.3	0.3	98.7

	Washington	4	1.3	1.3	100.0
	Total	308	100.0	100.0	

Source: Devised by author

5.3 Descriptive Statistics

This section presents a detailed descriptive analysis of the different constructs. Sample size, value, measure of central tendency, and standard deviations are also presented. The recommended values of standard deviations are shown in Table 5.10.

Table 5.10: Standard Deviations Recommended Values

Variable	Recommended Value
Standard deviations	Less than half of the mean value

Source: Devised by author

5.3.1 Adaptation to Rapid Technology Development

Adaptation to rapid technology development measured the perception of the respondents pertinent to whether or not the organization and its members are adapting to the rapid changes in technology. The purpose of this factor is to understand the level of adaptation to rapid technological development. In order to develop an understanding of this factor, descriptive statistics have been carried out to analyse the factor to assess the overall perception among the respondents pertinent to the adaptation to rapid technological development.

Descriptive statistics results for adaptation to rapid technology development are presented in Table 5.11, showing that the respondents agreed that the organization is adapting to the changing technology.

Table 5.11: Descriptive Statistics for Adaptation of Rapid Technology Development

	N Statistic	Mean Statistic	Std. Deviation Statistic

ARTD1	308	4.15	0.903
ARTD2	308	4.09	0.982
ARTD3	308	3.90	1.083
ARTD4	308	3.85	1.057

Source: Devised by author

5.3.2 Bureaucracy

Bureaucracy measured the perception of the respondents pertinent to whether the organization has a high bureaucratic structure and procedures. In order to develop an understanding of this factor, descriptive statistics were carried out to analyse the factor to assess the overall perception among the respondents pertinent to the level of bureaucracy in the organization.

Descriptive statistics results for bureaucracy are presented in Table 5.12, showing that the respondents agreed that the organization promotes change and innovation under compliance to rules and regulations

Table 5.12: Descriptive Statistics for Bureaucracy

	N Statistic	Mean Statistic	Std. Deviation Statistic
BC1	308	3.77	1.110
BC2	308	3.94	1.037
BC3	308	3.85	1.151

Source: Devised by author

5.3.3 Employee Compliance

Employee compliance measured the perception of the respondents pertinent to employee compliance with organizational policies. In order to develop an understanding of this factor, descriptive statistics were carried out to analyse it to assess the overall perception among the respondents pertinent to the level of compliance that employees show towards organizational policies.

Descriptive statistics results for employee compliance are presented in Table 5.13 below, which shows that the respondents agreed that the employees comply with the organizational policies.

Table 5.13: Descriptive Statistics for Employee Compliance

	N Statistic	Mean Statistic	Std. Deviation Statistic
EC1	308	4.51	0.841
EC2	308	3.92	1.048
EC3	308	3.85	1.118

Source: Devised by author

5.3.4 Information and Communication Technologies (ICT)

Information and Communication Technologies measured the respondents' perception pertinent to whether or not the organization is appropriately utilizing the ICT infrastructure. In order to develop an understanding of this factor, descriptive statistics were carried out to analyse the factor to assess the overall perception among the respondents.

Descriptive statistics results for ICT are presented in Table 5.14 below, showing that the respondents agreed that the organization is appropriately utilizing and benefiting from ICT infrastructure.

Table 5.14: Descriptive Statistics for Information and Communication Technologies

	N Statistic	Mean Statistic	Std. Deviation Statistic
ICT1	308	3.98	0.975
ICT2	308	3.95	0.971
ICT3	308	3.60	1.219

Source: Devised by author

5.3.5 Inter-Organizational Collaboration

Inter-organizational collaboration measured the respondents' perception pertinent to whether the organization has a high collaboration with other organizations. In order to develop an understanding of this factor, descriptive statistics were carried out to analyse the factor to assess the overall perception among the respondents pertinent to the level of collaboration with other organizations.

Descriptive statistics results for inter-organizational collaboration are shown in Table 5.15 below, showing that the respondents agreed that the organization has high inter-organizational collaboration.

Table 5.15: Descriptive Statistics for Inter-Organizational Collaboration

	N Statistic	Mean Statistic	Std. Deviation Statistic
INTER1	308	3.89	1.136
INTER2	308	3.75	1.117
INTER3	308	3.40	1.321

Source: Devised by author

5.3.6 Intra-Organizational Collaboration

Intra-organizational collaboration measured the perception of the respondents pertinent to whether there is a high collaboration within the organization. In order to develop an understanding of this factor, descriptive statistics were carried out to analyse the factor to assess the overall perception among the respondents pertinent to the level of collaboration.

Descriptive statistics results for intra-organizational collaboration are presented in Table 5.16 below, showing that the respondents agreed that the organization has high intra-organizational collaboration.

Table 5.16: Descriptive Statistics for Intra-Organizational Collaboration

	N Statistic	Mean Statistic	Std. Deviation Statistic
INTRA1	308	4.10	1.048

INTRA2	308	4.21	0.994
INTRA3	308	3.70	1.233

Source: Devised by author

5.3.7 Leadership Attitude

The first factor that the subjects in the study responded to was leadership attitude. Leadership attitude measured the perception of the respondents pertinent to attitudes of leadership regarding information security and job performance. The purpose of this factor is to understand the level of positive attitude shown by the leaders. In order to develop an understanding of this factor, descriptive statistics were carried out to analyse the factor to assess the overall perception among the respondents pertinent to the leadership attitude.

Descriptive statistics results for leadership attitude are presented in Table 5.17, showing that there was a belief among the respondents that the attitude of their leadership is conducive towards information security and are performance-oriented.

Table 5.17: Descriptive Statistics for Leadership Attitude

	N Statistic	Mean Statistic	Std. Deviation Statistic
LA1	308	4.31	0.959
LA2	308	4.18	1.023
LA3	308	4.04	1.033

Source: Devised by author

5.3.8 Legislative Influence

Legislative influence measured the perception of the respondents pertinent to legislative influence regarding information security. The purpose of this factor is to understand the level of legislative influence in terms of whether the organization complies with information security legislation. In order to develop an understanding of this factor, descriptive statistics were carried out to analyse the factor to assess the overall perception among the respondents pertinent to the legislative influence.

Descriptive statistics results for legislative influence are presented in Table 5.18, showing that there was a belief among the respondents that the organization complies with the regulations pertinent to information security management.

Table 5.18: Descriptive Statistics for Legislative influence

	N Statistic	Mean Statistic	Std. Deviation Statistic
LI1	308	4.40	0.869
LI2	308	4.38	0.847
LI3	308	3.82	1.143
LI4	308	4.05	1.135

Source: Devised by author

5.3.9 Skilful Workforce

Skilful workforce measured the perception of the respondents regarding whether or not the organization has a skilful workforce at its disposal. In order to develop an understanding of this factor, descriptive statistics were carried out to analyse the factor to assess the overall perception among the respondents pertinent to a skilful workforce.

Descriptive statistics results for skilful workforce are presented in Table 5.19, showing that the respondents agreed that the organization has a skilful workforce, although there was a slight disagreement with the statement.

Table 5.19: Descriptive Statistics for Skilful Workforce

	N Statistic	Mean Statistic	Std. Deviation Statistic
SW1	308	4.05	1.103
SW2	308	4.20	0.975
SW3	308	3.99	1.043
SW4	308	3.14	1.358

Source: Devised by author

5.3.10 Type of Organization

The type of organization measured the respondents' perception pertinent to the impact of the type of industry to their organization. In order to develop an understanding of this factor, descriptive statistics were carried out to analyse the factor to assess the overall perception among the respondents pertinent to the impact to the organization by the type of organization.

Descriptive statistics results for the type of organization are presented in Table 5.20, showing that the respondents were in agreement that the organization was impacted by the type of organization.

Table 5.20: Descriptive Statistics for Type of Organization

	N Statistic	Mean Statistic	Std. Deviation Statistic
TO1	308	4.50	0.776
TO2	308	4.53	0.792
TO3	308	4.28	0.965
TO4	308	4.31	0.895

Source: Devised by author

5.3.11 Vendor Selection

The next factor that the subjects in the study responded to was vendor selection. Vendor selection measured the respondents' perception and their assessment of how much their organization takes concrete steps before the selection of a technology vendor. The purpose of this factor is to understand the initiatives taken by the organization before selecting its vendors. In order to develop this understanding, descriptive statistics were carried out to analyse the factor.

Descriptive statistics results for vendor selection are presented in Table 5.21, showing that the respondents believed that, overall, their organization takes concrete steps before selecting a vendor.

Table 5.21: Descriptive Statistics for Vendor Selection

	N Statistic	Mean Statistic	Std. Deviation Statistic
VS1	308	3.87	1.051
VS2	308	4.35	0.877
VS3	308	4.19	0.862
VS4	308	4.34	0.879

Source: Devised by author

5.4 PLS Evaluation

The model developed in this study examines the relationship between thirteen factors. The model is shown in Figure 5.6.

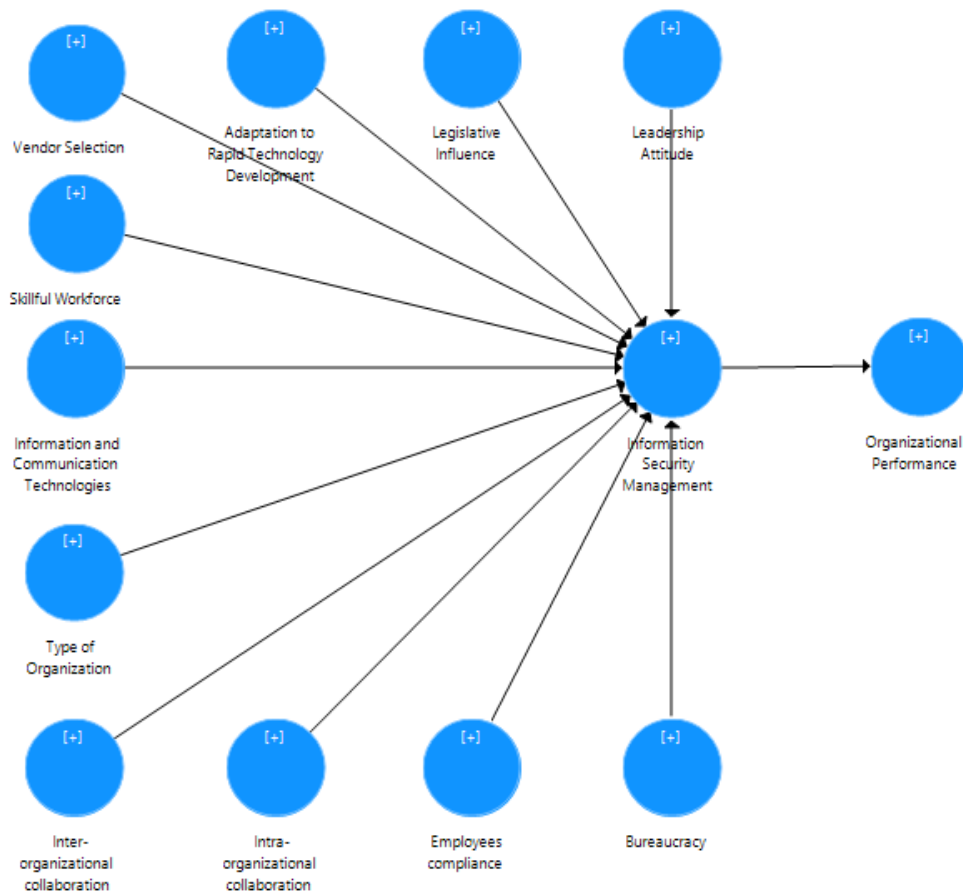


Figure 5.6: Survey PLS model

Source: Devised by author

The PLS model shown above in Figure 5.6 is composed of blue interconnected circles, which represent the variables of the research that are being measured in this section. The arrows represent the influence direction being measured from the organizational factors towards information security management and then towards organizational performance.

The next step is to present the resulting initial loadings, which will help in calculating and establishing constructs' validity and reliability. The rows represent the indicators in relation to each of the variables being measured via the survey questions, while the columns represent the variables themselves (see Table 5.22).

Table 5.22: Table Initial Loadings

	ART D	BC	EC	IC T	Int er	Intr a	LA	LI	OP	S W	TO	VS	IS M
ARTD 1	0.71												
ARTD 2	0.82												
ARTD 3	0.81												
ARTD 4	0.82												
BC1		0.8 0											
BC2		0.8 8											
BC3		0.7 3											

EC1			0.8 0										
EC2			0.8 6										
EC3			0.8 5										
ICT1				0.8 1									
ICT2				0.8 8									
ICT3				0.8 8									
INTE R1					0.8 4								
INTE R2					0.8 7								
INTE R3					0.8 2								
INTR A1						0.8 8							
INTR A2						0.8 7							
INTR A3						0.7 8							
LA1							0.7 9						

LA2							0.8 8						
LA3							0.8 3						
LI1							0.8 8						
LI2							0.8 4						
LI3							0.7 1						
LI4							0.8 1						
OP1								0.7 0					
OP2								0.7 6					
OP3								0.8 5					
OP4								0.7 9					
SW1									0.8 2				
SW2									0.8 5				
SW3									0.7 7				

SW4										0.5 0			
TO1											0.8 0		
TO2											0.8 4		
TO3											0.8 0		
TO4											0.8 3		
VS1												0.7 7	
VS2												0.7 9	
VS3												0.8 2	
VS4												0.8 3	
ISM1													0.8 3
ISM2													0.7 3
ISM3													0.7 2
ISM4													0.8 1

ISM5													0.75
ISM6													0.18

Source: Devised by author

Table 5.23 below details the results of multiple tests carried out to measure construct reliability and validity of the variables:

Table 5.23: Cronbach's Alpha, Composite Reliability, and AVE

	Cronbach's Alpha	Composite Reliability	Average Variance Extracted (AVE)
ART	0.802	0.868	0.623
D			
BC	0.735	0.845	0.647
C	0.784	0.874	0.699
ISM	0.77	0.844	0.501
ICT	0.821	0.893	0.735
Inter	0.798	0.88	0.71
Intra	0.798	0.882	0.713
LA	0.78	0.872	0.695
LI	0.824	0.884	0.657
OP	0.786	0.858	0.603
SW	0.724	0.83	0.558
TO	0.832	0.888	0.664
VS	0.817	0.878	0.642

Source: Devised by author

The results from the initial model analysis in SMART-PLS revealed that all factors had a good Cronbach's Alpha value (≥ 0.7), Composite Reliability (\geq), and AVE. An analysis of factor loadings for each of the constructs in the study revealed that two items, ISM6 (Loading: 0.184) from information security management and SW4 (Loading: 0.50) from skillful workforce, had low loadings. Only ISM6 was removed from further analysis due to its significantly low loading. Skillful workforce was kept for further analysis as deleting the item would not have improved the reliability or validity. Also, deletion would have resulted in only three items in the construct. After removal of the item ISM6, the model was re-run. Table 5.24 shows the recommended values.

Table 5.24 Reliability Analysis and Construct Validity Recommended Values

Variable	Recommended Value	Reference
Cronbach's Alpha	≥ 0.7	Sekaran, 2000
Composite Reliability (CR)	≥ 0.7	Nunnally and Bernstein (1994)

Source: Devised by author

The factor loadings for each of the constructs in the modified model are presented in Table 5.25. The loadings represent the contribution of the indicator to the definition of its latent variable.

Table 5.25 Table Factor Loadings of the Constructs in the Modified Model

	ART D	BC	EC	IC T	Int er	Intr a	LA	LI	OP	S W	TO	VS	IS M
ARTD 1	0.70												
ARTD 2	0.82												

ARTD 3	0.81												
ARTD 4	0.82												
BC1		0.8 0											
BC2		0.8 7											
BC3		0.7 3											
EC1			0.7 9										
EC2			0.8 6										
EC3			0.8 5										
ICT1				0.8 1									
ICT2				0.8 8									
ICT3				0.8 8									
INTE R1					0.8 4								
INTE R2					0.8 7								

INTE R3					0.8 3								
INTR A1						0.8 8							
INTR A2						0.8 7							
INTR A3						0.7 8							
LA1							0.7 9						
LA2							0.8 8						
LA3							0.8 3						
LI1								0.8 7					
LI2								0.8 4					
LI3								0.7 1					
LI4								0.8 1					
OP1									0.7 0				
OP2									0.7 6				

OP3									0.8 5			
OP4									0.7 9			
SW1									0.8 2			
SW2									0.8 4			
SW3									0.7 7			
SW4									0.5 0			
TO1										0.8 0		
TO2										0.8 3		
TO3										0.8 0		
TO4										0.8 3		
VS1											0.7 8	
VS2											0.7 8	
VS3											0.8 2	

VS4												0.8 2
ISM1												0.8 3
ISM2												0.7 3
ISM3												0.7 3
ISM4												0.8 2
ISM5												0.7 5

Source: Devised by author

5.4.1 Construct Validity and Reliability Analysis (Cronbach's Alpha and Composite Reliability)

The factors presented in the revised model were evaluated for reliability and validity. A reliability analysis was then conducted to determine the internal consistency for each construct. According to Mark (1996), "Reliability is defined as the extent to which a measuring instrument is stable and consistent. The essence of reliability is repeatability. If an instrument is administered over and over again, will it yield the same results" (Mark, 1996, p. 285). Validity is established when the concepts that should be related to each other are, in fact, related.

5.4.1.1 Cronbach's alpha and composite reliability

Reliability in the present study was assessed using two different techniques, namely Cronbach's Alpha and Composite Reliability (CR). Composite reliability refers to the consistency of the group of items measuring a latent construct. Traditionally, the Cronbach's Alpha has been widely used to measure the reliability of a construct. However, Cronbach and Shavelson (2004) recognized that using an Alpha coefficient alone to determine reliability may not be sufficient: therefore, CR is used. The results of the Alpha and Composite Reliability are shown in Table 5.26. The

Cronbach's Alpha of the constructs in the present study ranged between 0.724 and 0.832 while the CR values ranged between 0.83 and 0.892. The results indicate that both the Cronbach's Alpha and the composite reliability of all the constructs were well above 0.70, an indicator of good reliability. Cronbach's Alpha and CR values for each of the constructs in the present study are summarized in Table 5.26. The calculations are a possible part of the PLS algorithm in smart PLS.

Table 5.26 Table Reliability Analysis of the Constructs

	Cronbach's Alpha	CR
ARTD	0.802	0.868
BC	0.735	0.846
EC	0.784	0.874
ISM	0.832	0.881
ICT	0.821	0.892
Inter	0.798	0.881
Intra	0.798	0.882
LA	0.78	0.872
LI	0.824	0.884
OP	0.786	0.858
SW	0.724	0.83
TO	0.832	0.888
VS	0.817	0.877

Source: Devised by author

Construct validity is defined broadly as the degree to which a construct/measure/operationalization measures the concept it is supposed to

measure; it is determined once convergent and discriminant validity is established (Bagozzi et al., 1991).

5.4.1.2 Convergent validity (AVE)

One of the two forms of validity established in the present study is convergent validity. Bagozzi et al. (1991) state:

Convergent validity is the degree to which multiple attempts to measure the same concept are in agreement. The idea is that two or more measures of the same thing should converge highly if they are valid measures of the concept.

Convergent validity is established when the concepts that should be related to each other are, in fact, related. Statistically, convergent validity is established if an AVE of 0.50 or greater is achieved for the constructs (Fornell and Larcker, 1981). Based on the factor loadings, convergent validity was calculated. The establishment of convergent validity shows that the latent variable explains half, or more than half, of the variance of its indicators on average or, alternatively, measurement errors account for relatively less variance in the indicators than the latent variables (Reverte et al., 2016). The AVE statistic for the constructs in the current study was found to be over the required value of 0.50. Hence, convergent validity was established. Table 5.27 shows the AVE value for each of the constructs in the present study. AVE calculations are a possible part of the PLS algorithm in smart PLS. Table 5.28 then illustrates the calculated AVE values for each of the research constructs.

Table 5.27 Convergent Validity Recommended Values

Variable	Reference
Average Variance Extracted (AVE)	Fornell and Larcker (1981)

Source: Devised by author

Table 5.28 Convergent Validity (AVE)

Constructs	Average Variance Extracted (AVE)
ARTD	0.624
BC	0.648

EC	0.698
ISM	0.598
ICT	0.735
Inter	0.711
Intra	0.713
LA	0.695
LI	0.657
OP	0.603
SW	0.558
TO	0.664
VS	0.641

Source: Devised by author

5.4.2 Discriminant validity (Fornell-Larcker, Cross Loadings, HTMT)

Discriminant validity assesses the extent to which distinct constructs are not strongly associated with each other. According to Bagozzi et al. (1991), “Discriminant validity is the degree to which measures of different concepts are distinct. The notion is that if two or more concepts are unique, then valid measures of each should not correlate too highly” (Bagozzi et al., 1991, p. 425). In the current study, and to assess discriminant validity, three different techniques were utilized (calculations are a possible part of the PLS algorithm in smart PLS).

1. Fornell-Larcker Criterion
2. Cross Loadings Analysis
3. Heterotrait-Monotrait Ratio (HTMT) (See Table 5.29)

Table 5.29 Discriminant validity recommended values

Variable	Recommended Value	Reference
----------	-------------------	-----------

Fornell and Larcker Criterion	The square root of AVE of each construct is greater than inter-construct correlations.	Fornell and Larcker (1981)
Cross Loadings	The diagonal loadings are significantly greater than the off-diagonal loadings in the corresponding rows and columns.	Hulland (1999)
Heterotrait-Monotrait Ratio	≥ 0.85 ≥ 0.90 (Teo et al., 2008)	Kline (2011), Teo et al. (2008)

Source: Devised by author

5.4.2.1 Fornell-Larcker criterion

According to the criterion defined by Fornell and Larcker (1981), discriminant validity is assessed when the square root of AVE for each of the constructs in the study is greater than the inter-construct correlation. The results indicate that the square root of AVE for each construct is greater than inter-construct correlations. Thus, discriminant validity was established. This shows that the constructs in the present study have discriminant validity, and that the constructs in the model are different from the other constructs of that model and do not share a high correlation. This indicates that each construct measures a different phenomenon. Table 5.30 compares the AVE square roots and inter-construct correlations.

Table 5.30 Fornell and Larcker Criterion

	ART D	BC	EC	IS M	IC T	Inter	Intra	LA	LI	OP	S W	TO	VS
ART D	0.79												
BC	0.42	0.81											
EC	0.29	0.45	0.84										

ISM	0.26	0.5 2	0.4 9	0.7 7									
ICT	0.35	0.4 5	0.3 5	0.3 5	0.8 6								
Inter	0.39	0.5 3	0.4 7	0.3 9	0.4 0	0.8 4							
Intra	0.35	0.5 4	0.4 6	0.3 9	0.3 8	0.6 9	0.8 5						
LA	0.29	0.5 1	0.4 2	0.4 8	0.2 9	0.5 3	0.6 0	0.8 3					
LI	0.22	0.4 4	0.5 7	0.5 5	0.3 2	0.3 9	0.3 7	0.4 7	0.8 1				
OP	0.40	0.3 8	0.3 7	0.3 9	0.3 0	0.4 7	0.5 0	0.4 8	0.3 5	0.7 8			
SW	0.37	0.5 6	0.5 6	0.5 5	0.3 8	0.5 2	0.5 6	0.6 0	0.5 3	0.4 1	0.7 5		
TO	0.25	0.3 1	0.3 6	0.3 8	0.2 7	0.2 8	0.2 4	0.3 3	0.3 8	0.2 5	0.3 3	0.8 2	
VS	0.41	0.3 7	0.3 7	0.2 4	0.3 8	0.4 0	0.4 5	0.3 6	0.2 6	0.3 8	0.4 1	0.2 5	0.8 0

Source: Devised by author

5.4.2.2 Cross loadings

Another method utilized in the present study to assess discriminant validity is through cross loadings. Cross loadings assess if an item belonging to a particular construct loads strongly on another construct/measure in the study. Table 5.31 below reports details of correlations among the items with the latent constructs. According to Wasko and Faraj (2005), factor loadings of all indicators should be greater than the constructs of other factors in the loadings table to establish discriminant validity and convergent validity. The results indicate that all the factor

loadings for items in a particular construct are greater than their cross loadings, providing additional support for discriminant validity. According to Hulland (1999), discriminant validity is established when the diagonal loadings are significantly greater than the off-diagonal loadings in the corresponding rows and columns.

Table 5.31 Cross Loadings

	ART	BC	EC	IC	Int	Intr	LA	LI	OP	S	TO	VS	IS
	D			T	er	a				W			M
ARTD	0.70	0.3	0.1	0.2	0.2	0.2	0.1	0.1	0.3	0.2	0.2	0.3	0.1
1		1	8	2	9	2	5	8	0	4	2	1	3
ARTD	0.82	0.4	0.2	0.3	0.3	0.3	0.3	0.1	0.3	0.3	0.2	0.3	0.2
2		1	4	1	7	4	3	8	6	8	2	5	4
ARTD	0.81	0.2	0.2	0.2	0.2	0.2	0.1	0.1	0.2	0.1	0.1	0.2	0.1
3		6	4	5	7	1	6	5	9	9	5	5	8
ARTD	0.82	0.3	0.2	0.3	0.3	0.3	0.2	0.1	0.3	0.3	0.1	0.3	0.2
4		2	6	1	0	0	4	8	0	1	9	7	3
BC1	0.32	0.8	0.2	0.3	0.4	0.4	0.4	0.2	0.3	0.4	0.2	0.3	0.3
		0	8	2	5	6	1	8	0	0	0	1	5
BC2	0.28	0.8	0.4	0.3	0.4	0.3	0.4	0.4	0.2	0.4	0.3	0.2	0.5
		7	2	8	1	7	2	3	8	8	2	5	4
BC3	0.44	0.7	0.3	0.3	0.4	0.5	0.4	0.3	0.3	0.4	0.2	0.3	0.3
		3	7	9	5	1	2	1	6	8	1	8	3
EC1	0.19	0.2	0.7	0.2	0.3	0.2	0.2	0.5	0.2	0.4	0.4	0.2	0.3
		6	9	6	2	6	9	1	6	0	0	5	6
EC2	0.28	0.4	0.8	0.3	0.4	0.4	0.4	0.4	0.3	0.5	0.2	0.3	0.4
		3	6	3	3	5	0	9	4	1	3	6	5
EC3	0.26	0.4	0.8	0.2	0.4	0.4	0.3	0.4	0.3	0.4	0.2	0.3	0.4
		3	5	8	2	2	5	3	4	9	8	1	0

		0.3	0.3	0.8	0.3	0.3	0.2	0.2	0.2	0.3	0.2	0.4	0.2
ICT1	0.35	9	0	1	4	8	6	8	6	7	8	3	6
		0.3	0.2	0.8	0.3	0.3	0.2	0.2	0.2	0.2	0.2	0.3	0.2
ICT2	0.30	6	5	8	3	0	4	6	7	8	4	6	7
		0.4	0.3	0.8	0.3	0.3	0.2	0.2	0.2	0.3	0.2	0.2	0.3
ICT3	0.27	1	5	8	5	0	4	7	4	2	0	3	4
		0.4	0.4	0.3	0.8	0.7	0.5	0.4	0.5	0.5	0.2	0.3	0.3
INTE R1	0.33	8	3	0	4	0	4	0	2	0	0	9	6
		0.4	0.3	0.4	0.8	0.5	0.3	0.2	0.3	0.4	0.2	0.3	0.2
INTE R2	0.34	4	7	0	7	4	9	7	5	1	8	6	8
		0.4	0.3	0.3	0.8	0.5	0.3	0.2	0.2	0.3	0.2	0.2	0.3
INTE R3	0.31	1	8	2	3	0	9	9	9	8	4	5	2
		0.4	0.3	0.3	0.5	0.8	0.5	0.3	0.4	0.5	0.1	0.3	0.3
INTR A1	0.30	6	4	2	8	8	2	0	7	0	9	8	6
		0.4	0.4	0.3	0.5	0.8	0.5	0.3	0.3	0.4	0.2	0.4	0.3
INTR A2	0.32	5	1	4	8	7	2	0	9	5	0	3	2
		0.4	0.4	0.3	0.6	0.7	0.4	0.3	0.4	0.4	0.2	0.3	0.3
INTR A3	0.27	5	1	0	0	8	8	5	1	8	3	4	2
		0.3	0.3	0.1	0.3	0.3	0.7	0.4	0.3	0.4	0.2	0.3	0.3
LA1	0.26	4	7	7	6	8	9	4	3	9	9	2	5
		0.4	0.3	0.2	0.4	0.5	0.8	0.4	0.3	0.5	0.3	0.2	0.4
LA2	0.19	1	6	4	4	1	8	1	8	2	3	4	4
		0.5	0.3	0.3	0.5	0.6	0.8	0.3	0.4	0.5	0.2	0.3	0.4
LA3	0.29	2	2	0	2	0	3	3	8	1	2	4	1
		0.3	0.4	0.2	0.3	0.3	0.4	0.8	0.3	0.4	0.3	0.2	0.5
LI1	0.13	7	7	5	0	0	2	7	3	4	6	0	0

		0.3	0.4	0.2	0.2	0.2	0.4	0.8	0.3	0.4	0.3	0.2	0.4
LI2	0.24	5	6	8	9	8	3	4	2	4	8	7	3
		0.3	0.3	0.1	0.3	0.3	0.3	0.7	0.2	0.4	0.2	0.2	0.3
LI3	0.21	2	8	5	4	3	6	1	3	0	3	1	8
		0.3	0.5	0.3	0.3	0.3	0.3	0.8	0.2	0.4	0.2	0.1	0.4
LI4	0.15	7	1	3	3	1	2	1	5	5	7	7	8
		0.2	0.2	0.1	0.2	0.2	0.2	0.2	0.7	0.2	0.1	0.2	0.2
OP1	0.28	4	6	8	6	8	6	8	0	1	7	4	5
		0.2	0.2	0.1	0.3	0.2	0.2	0.1	0.7	0.2	0.1	0.2	0.1
OP2	0.26	2	2	8	1	9	8	4	6	0	5	1	9
		0.3	0.3	0.2	0.4	0.4	0.4	0.3	0.8	0.4	0.2	0.3	0.3
OP3	0.32	5	8	5	6	7	2	5	5	3	1	2	8
		0.3	0.2	0.2	0.3	0.4	0.4	0.2	0.7	0.3	0.2	0.3	0.3
OP4	0.36	2	6	8	8	5	6	7	9	5	2	7	2
		0.4	0.4	0.2	0.3	0.4	0.4	0.4	0.2	0.8	0.2	0.2	0.4
SW1	0.24	0	0	7	6	4	9	4	7	2	9	6	3
		0.4	0.5	0.2	0.3	0.4	0.5	0.5	0.2	0.8	0.3	0.3	0.4
SW2	0.25	1	3	8	6	4	3	5	9	4	6	5	7
		0.4	0.4	0.3	0.4	0.5	0.4	0.3	0.4	0.7	0.2	0.3	0.4
SW3	0.39	8	2	2	9	1	9	6	3	7	0	6	5
		0.4	0.2	0.2	0.3	0.2	0.2	0.1	0.2	0.5	0.0	0.2	0.2
SW4	0.23	0	9	6	3	6	3	8	2	0	8	3	7
		0.2	0.2	0.2	0.1	0.1	0.2	0.3	0.2	0.2	0.8	0.2	0.3
TO1	0.20	2	2	4	9	3	4	1	3	3	0	1	2
		0.2	0.2	0.1	0.2	0.2	0.3	0.2	0.1	0.2	0.8	0.2	0.2
TO2	0.18	2	7	8	2	1	0	6	7	5	3	3	6

		0.2	0.3	0.2	0.2	0.2	0.3	0.4	0.1	0.3	0.8	0.2	0.3
TO3	0.19	9	7	3	3	2	0	2	9	1	0	2	3
		0.2	0.3	0.2	0.2	0.2	0.2	0.2	0.2	0.2	0.8	0.1	0.3
TO4	0.23	8	0	2	8	3	5	4	1	7	3	7	0
		0.3	0.3	0.2	0.3	0.3	0.3	0.2	0.3	0.2	0.1	0.7	0.2
VS1	0.34	5	1	9	6	7	1	6	5	9	8	8	3
		0.2	0.2	0.2	0.3	0.3	0.2	0.1	0.2	0.3	0.2	0.7	0.1
VS2	0.32	5	4	5	0	1	6	9	9	0	2	8	4
		0.2	0.3	0.3	0.2	0.3	0.2	0.1	0.2	0.3	0.1	0.8	0.1
VS3	0.41	8	3	4	8	8	6	4	9	4	8	2	7
		0.2	0.3	0.3	0.3	0.3	0.2	0.2	0.2	0.3	0.2	0.8	0.2
VS4	0.25	8	0	4	2	7	9	2	7	8	4	2	1
		0.4	0.4	0.3	0.3	0.3	0.4	0.4	0.3	0.4	0.3	0.1	0.8
ISM1	0.23	7	3	5	5	9	2	8	4	9	0	9	3
		0.3	0.3	0.2	0.2	0.2	0.3	0.4	0.2	0.4	0.2	0.1	0.7
ISM2	0.17	6	4	4	3	7	7	5	5	1	6	5	3
		0.3	0.2	0.2	0.2	0.2	0.3	0.2	0.2	0.3	0.2	0.1	0.7
ISM3	0.17	5	8	5	8	3	0	9	8	6	3	9	3
		0.3	0.3	0.3	0.2	0.2	0.3	0.3	0.2	0.3	0.3	0.1	0.8
ISM4	0.20	9	3	1	7	4	2	9	9	8	0	5	2
		0.4	0.4	0.1	0.3	0.3	0.4	0.4	0.3	0.4	0.3	0.2	0.7
ISM5	0.21	3	6	8	4	6	4	9	2	7	5	5	5

Source: Devised by author

5.4.2.3 Heterotrait-Monotrait ratio (HTMT)

HTMT is an estimate of the correlation between the constructs. It is referred to as a new criterion for assessing discriminant validity in variance-based structural equation modelling. Its interpretation is straightforward. Using the HTMT as a criterion involves comparing it to a predefined threshold. According to Henseler et al. (2015), if the value of the HTMT is higher than this threshold, then there is a lack of

discriminant validity. The exact threshold level of the HTMT is debatable; some authors suggest a threshold of 0.85 (Kline, 2011), while others suggest a value of 0.90 (Teo et al., 2008). Table 5.32 below shows that the estimates do not exceed the recommended values, except for the value between inter-organizational collaboration and intra-organizational collaboration. The value is lightly over 0.85 but it is still less than the value of 0.90. Hence, discriminant validity is established.

Table 5.32 Heterotrait-Monotrait Ratio (HTMT)

	ART D	BC	EC	IS M	ICT	Inte r	Intr a	LA	LI	OP	SW	TO	V S
ART D	-												
BC	0.56												
EC	0.36	0.5 7											
ISM	0.30	0.6 3	0.5 9										
ICT	0.43	0.5 8	0.4 3	0.4 1									
Inter	0.48	0.7 0	0.5 8	0.4 6	0.4 9								
Intra	0.43	0.7 3	0.5 7	0.4 7	0.4 7	0.8 6							
LA	0.35	0.6 8	0.5 3	0.5 9	0.3 6	0.6 6	0.7 5						
LI	0.27	0.5 4	0.7 1	0.6 5	0.3 8	0.4 7	0.4 7	0.5 9					
OP	0.49	0.4 9	0.4 5	0.4 5	0.3 6	0.5 6	0.6 0	0.5 8	0.4 1				

SW	0.47	0.7 8	0.7 3	0.7 0	0.5 0	0.6 8	0.7 3	0.7 9	0.6 7	0.5 0			
TO	0.30	0.3 8	0.4 5	0.4 4	0.3 3	0.3 5	0.3 0	0.4 1	0.4 5	0.2 9	0.4 0		
VS	0.50	0.4 9	0.4 5	0.2 8	0.4 7	0.4 8	0.5 5	0.4 4	0.3 1	0.4 5	0.5 3	0.3 1	-

Source: Devised by author

5.4.3 Structural equation modelling and hypothesis testing (R^2 , f^2 , Q^2)

The structural model comprises the hypothesized relationship between independent and dependent variables in this research study. The structural model provides information as to how well the theoretical model predicts the hypothesized paths. The coefficient of determination (R^2), the effect size (f^2), and the predictive relevance measure (Q^2) were obtained in order to assess the proposed structural model in the present study.

The R^2 and f^2 measures are calculated part of the PLS algorithm in smart PLS. The results of the analysis show an R^2 value of 0.465 for information security management. This shows that 46.5% change in information security management can be attributed to leadership attitudes, legislative influence, adaptation to rapid technology development, vendor selection, skilful workforce, information and communication technologies, type of organization, employee compliance, bureaucracy, inter-organizational collaboration, and intra-organizational collaboration. Furthermore, the model also shows that the R^2 value for organizational performance is 0.149, which means that a 14.9% change in the organizational model can be attributed to information security management. The model with R^2 values for information security management and organizational performance is shown in Figure 5.7 below.

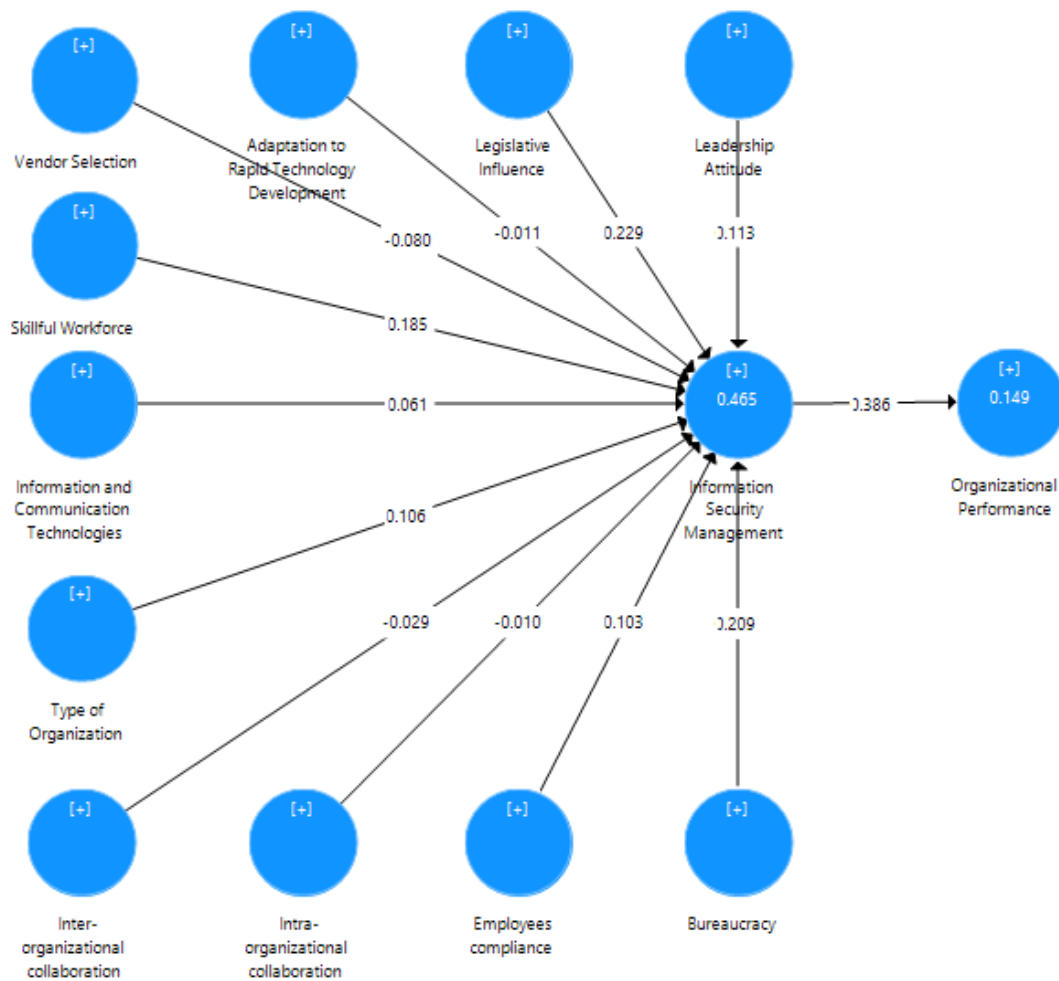


Figure 5.7: SEM hypothesis R^2 testing all respondents (original sample)

Source: DeVised by author

In addition to the evaluation of the R^2 value, the measure of f^2 effect size can also be assessed. The f^2 effect size statistic specifies whether the removal of an independent variable from a model can have a principal impact on the dependent variable (Hair Jr et al., 2013).

The results show that only the removal of information and security management (ISM) has a significant impact on organizational performance. However, if any of the predictors of ISM are removed, this would not significantly impact the model. The effect size for the independent variables and their significance values are shown in Table 5.33.

Table 5.33 Effect Size for Independent Variables

	Original Sample	STDEV	T Statistics	P Values
ARTD -> ISM	0	0.007	0.023	0.982
BC -> ISM	0.043	0.03	1.446	0.149
EC -> ISM	0.011	0.015	0.7	0.484
ICT -> ISM	0.005	0.01	0.484	0.629
Inter -> ISM	0.001	0.005	0.128	0.898
Intra -> ISM	0	0.006	0.014	0.989
LA -> ISM	0.012	0.013	0.907	0.365
LI -> ISM	0.055	0.031	1.767	0.078
SW -> ISM	0.029	0.023	1.254	0.21
TO -> ISM	0.016	0.02	0.84	0.401
VS -> ISM	0.008	0.012	0.689	0.491
ISM -> OP	0.175	0.054	3.232	0.001

Source: Devised by author

The predictive relevance measure (Q^2) effect size indicates a positive prediction ability between the variables. It is calculated via Blindfolding in Smart PLS. The Q^2 of ISM was found to be 0.244. The statistic indicates that the independent variables have a medium effect in producing the Q^2 for ISM. This shows that ISM has a medium predictive relevance in the model. As for organizational performance, the Q^2 statistic was 0.078. The statistic indicates that the ISM independent variables have a small effect in producing the Q^2 for organizational performance. This shows that organizational performance has a small predictive relevance in the model.

5.4.3.1 Path analysis

Further to the assessment of the R^2 value, the hypotheses were tested during the course of analysis.

H₁: Adaptation to rapid technology development (ARTD) has a significant impact on information security management (ISM)

H₁ seeks to assess the significance of the impact of ARTD on ISM. The results of hypotheses tests revealed that ARTD has an insignificant impact on ISM (B = -0.011, t = 0.183, p = 0.855). Hence hypothesis H₁ was not substantiated.

H₂: Bureaucracy (BC) has a significant impact on information security management (ISM)

H₂ seeks to assess the significance of the impact of BC on ISM. The results of hypotheses tests revealed that BC has a significant impact on ISM (B = 0.209, t = 3.096, p = 0.002). Hence, hypothesis H₂ was substantiated.

H₃: Employee compliance (EC) has a significant impact on information security management (ISM).

H₃ seeks to assess the significance of the impact of EC on ISM. The results of hypotheses tests revealed that EC has an insignificant impact on ISM (B = 0.103, t = 1.625, p = 0.105). Hence, hypothesis H₃ was not substantiated.

H₄: Information and communication technologies (ICT) has a significant impact on information security management (ISM)

H₄ seeks to assess the significance of the impact of ICT on ISM. The results of hypotheses tests revealed that ICT has an insignificant impact on ISM (B = 0.061, t = 1.093, p = 0.275). Hence, hypothesis H₄ was not substantiated.

H₅: Inter-organizational collaboration (INTER) has a significant impact on information security management (ISM)

H₅ seeks to assess the significance of the impact of INTER on ISM. The results of hypotheses tests revealed that INTER has an insignificant impact on ISM (B = -0.029, t = 0.457, p = 0.648). Hence, hypothesis H₅ was not substantiated.

H₆: Intra-organizational collaboration (INTRA) has a significant impact on information security management (ISM).

H₆ seeks to assess the significance of the impact of INTRA on ISM. The results of hypotheses tests revealed that INTRA has an insignificant impact on ISM (B = -0.01, t = 0.15, p = 0.881). Hence hypothesis H₆ was not substantiated.

H₇: Leadership attitudes (LA) has a significant impact on information security management (ISM).

H₇ seeks to assess the significance of the impact of LA on ISM. The results of hypotheses tests revealed that LA has an insignificant impact on ISM (B = 0.113, t = 1.847, p = 0.065). Hence, hypothesis H₇ was not substantiated.

H₈: Legislative influence (LI) has a significant impact on information security management (ISM).

H₈ seeks to assess the significance of the impact of LI on ISM. The results of hypotheses tests revealed that LI has a significant impact on ISM (B = 0.229, t = 3.78, p < 0.001). Hence, hypothesis H₈ was substantiated.

H₉: Skilful workforce (SW) has a significant impact on information security management (ISM).

H₉ seeks to assess the significance of the impact of SW on ISM. The results of hypotheses tests revealed that SW has a significant impact on ISM (B = 0.185, t = 2.857, p = 0.004). Hence, hypothesis H₉ was substantiated.

H₁₀: The type of organization (TO) has a significant impact on information security management (ISM).

H₁₀ seeks to assess the significance of the impact of TO on ISM. The results of hypotheses tests revealed that TO has an insignificant impact on ISM (B = 0.106, t = 1.788, p = 0.074). Hence, hypothesis H₁₀ was not substantiated.

H₁₁: Vendor selection (VS) has a significant impact on information security management (ISM).

H₁₁ seeks to assess the significance of the impact of VS on ISM. The results of hypotheses tests revealed that VS has an insignificant impact on ISM (B = -0.08, t = 1.528, p = 0.127). Hence, hypothesis H₁₁ was not substantiated.

H₁₂: Information security management (ISM) has a significant impact on organizational performance (OP).

H₁₂ seeks to assess the significance of the impact of ISM on OP. The results of hypotheses tests revealed that ISM has a significant impact on OP (B = 0.386, t = 7.971, p < 0.001). Hence, hypothesis H₁₂ was substantiated.

These results are summarized in Table 5.34 and Figure 5.8.

Table 5.34 Hypotheses Testing (all respondents)

Hypothesis Number		Original Sample (O)	STDEV	T Statistics	P Values	Supported?
1	ARTD -> ISM	-0.011	0.058	0.183	0.855	No
2	BC -> ISM	0.209	0.067	3.096	0.002	Yes
3	EC -> ISM	0.103	0.063	1.625	0.105	No
4	ICT -> ISM	0.061	0.056	1.093	0.275	No
5	Inter -> ISM	-0.029	0.063	0.457	0.648	No
6	Intra -> ISM	-0.01	0.069	0.15	0.881	No
7	LA -> ISM	0.113	0.061	1.847	0.065	No
8	LI -> ISM	0.229	0.06	3.78	0.000	Yes
9	SW -> ISM	0.185	0.065	2.857	0.004	Yes
10	TO -> ISM	0.106	0.059	1.788	0.074	No
11	VS -> ISM	-0.08	0.052	1.528	0.127	No

12	ISM -> OP	0.386	0.048	7.971	0.000	Yes
----	-----------	-------	-------	-------	-------	-----

Source: Devised by author

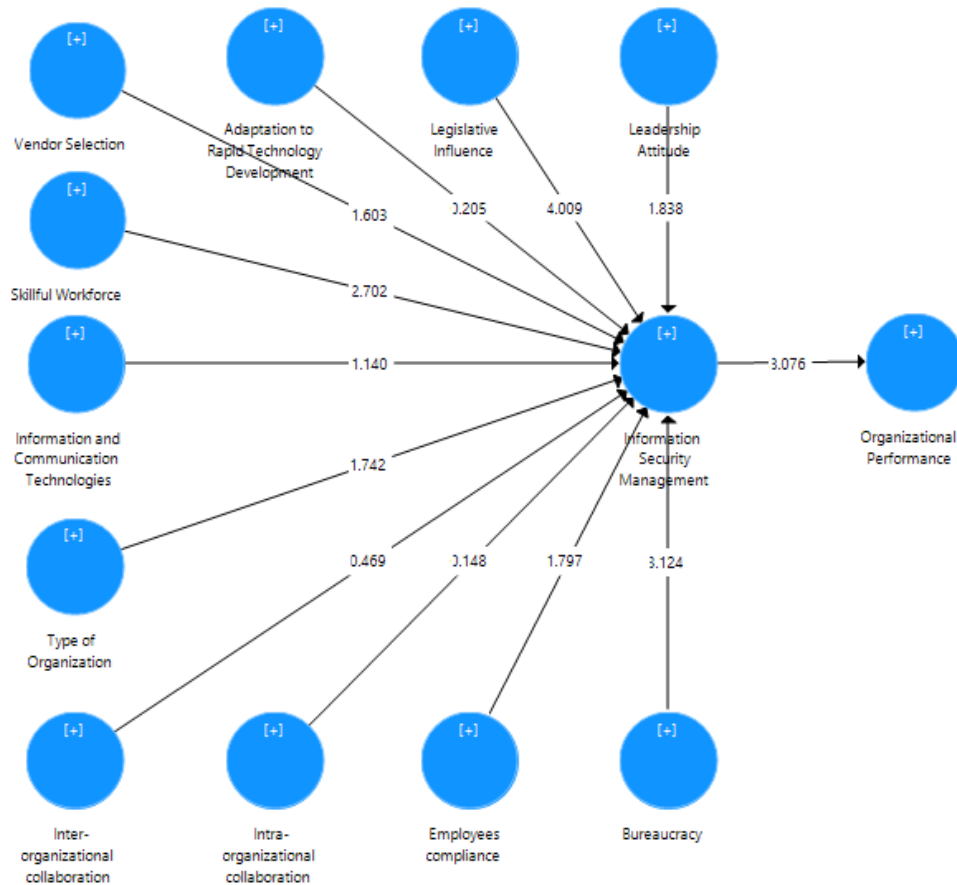


Figure 5.8: SEM hypothesis testing all respondents (T statistics)

Source: Devised by author

5.4.4 Comparison between Smart and Non-Smart Cities

5.4.4.1 Smart City

The results of the analysis for respondents from smart cities show an R^2 value of 0.419 for information security management. This shows that a 41.9% change in perception of information security management can be attributed to leadership attitude, legislative influence, adaptation to rapid technology development, vendor selection, skilful workforce, information and communication technologies, type of organization, employee compliance, bureaucracy, inter-organizational collaboration, and intra-organizational collaboration. Furthermore, the model also shows that the R^2 value for organizational performance is 0.103, meaning that a 10.3% change in

organizational performance can be attributed to information security management in the case of smart cities. The model with R² values for information security management and organizational performance is shown in Figure 5.9 below.

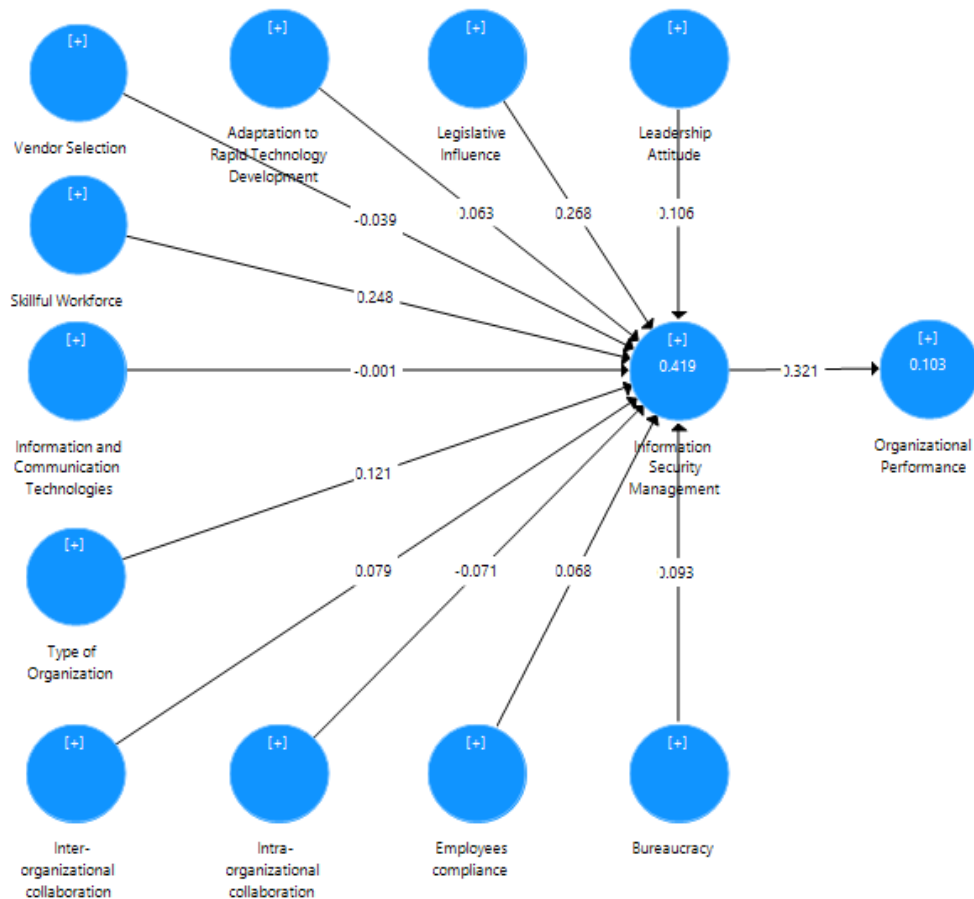


Figure 5.9: SEM hypothesis testing for smart cities respondents (original sample)

Source: Devised by author

In addition to the evaluation of the R² value, the measure of f² effect size can also be assessed. The f² effect size statistic specifies whether the removal of an independent variable from a model can have a substantive impact on the dependent variable (Hair Jr et al., 2013).

The results show that only the removal of ISM has a moderately significant impact on organizational performance. However, if any of the predictors of ISM are removed, this would not significantly impact the model. The effect size and their significance values are shown in Table 5.35.

Table 5.35 Effect Size for Independent Variables for Smart Cities

	Original Sample	STDEV	T Statistics	P Values
ARTD -> ISM	0.005	0.018	0.286	0.775
BC -> ISM	0.008	0.021	0.360	0.719
EC -> ISM	0.005	0.016	0.318	0.750
ICT -> ISM	0.000	0.010	0.000	1.000
Inter -> ISM	0.006	0.013	0.424	0.671
Intra -> ISM	0.004	0.013	0.307	0.759
LA -> ISM	0.011	0.024	0.466	0.641
LI -> ISM	0.089	0.056	1.588	0.113
SW -> ISM	0.053	0.043	1.235	0.217
TO -> ISM	0.022	0.038	0.567	0.571
VS -> ISM	0.002	0.012	0.157	0.875
ISM -> OP	0.115	0.065	1.768	0.078

Source: Devised by author

5.4.4.1.1 Path analysis smart cities

Relationship was assessed in smart city respondents for the significance of the impact of leadership attitude, legislative influence, adaptation to rapid technology development, vendor selection, skilful workforce, information and communication technologies, type of organization, employee compliance, bureaucracy, inter-organizational collaboration, and intra-organizational collaboration on information security management; and further, the impact of information security management on organizational performance. The results of the significance test for smart city subjects show that only legislative influence ($t = 3.478$, $p = 0.001$) and skilful workforce ($t = 2.804$, $p = 0.005$) have a significant impact on ISM. All other variables fail to impact ISM in smart cities. Moreover, the impact of ISM on organizational

performance was also found to be significant in smart cities ($t = 4.440, p < 0.001$). The results are shown in Figure 5.10 and Table 5.36.

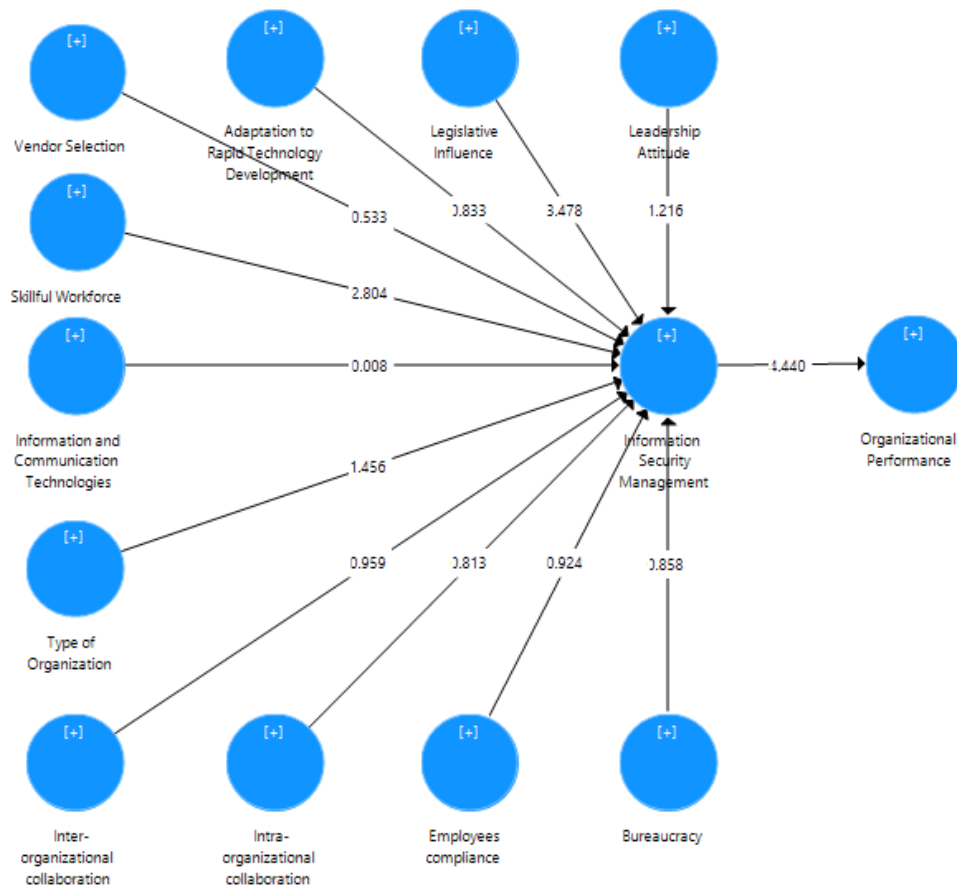


Figure 5.10: SEM hypothesis testing for smart city respondents (T statistics)

Source: DeVised by author

Table 5.36 Hypotheses Testing for Smart City Respondents

Hypothesis nb		Original Sample	STDEV	T Statistics	P Values	Supported?
1	ARTD -> ISM	0.063	0.076	0.833	0.405	No
2	BC -> ISM	0.093	0.108	0.858	0.391	No
3	EC -> ISM	0.068	0.074	0.924	0.356	No

4	ICT -> ISM	-0.001	0.075	0.008	0.994	No
5	Inter -> ISM	0.079	0.082	0.959	0.338	No
6	Intra -> ISM	-0.071	0.088	0.813	0.417	No
7	LA -> ISM	0.106	0.087	1.216	0.225	No
8	LI -> ISM	0.268	0.077	3.478	0.001	Yes
9	SW -> ISM	0.248	0.089	2.804	0.005	Yes
10	TO -> ISM	0.121	0.083	1.456	0.146	No
11	VS -> ISM	-0.039	0.072	0.533	0.594	No
12	ISM -> OP	0.321	0.072	4.440	0.000	Yes

Source: Devised by author

5.4.4.2 Non-smart City

The results of the analysis for respondents from non-smart cities show an R^2 value of 0.569 for information security management. This shows that a 56.9% change in perception of ISM can be attributed to leadership attitude, legislative influence, adaptation to rapid technology development, vendor selection, skilful workforce, information and communication technologies, type of organization, employee compliance, bureaucracy, inter-organizational collaboration, and intra-organizational collaboration. Furthermore, the model also shows that the R^2 value for organizational performance is 0.221, meaning that a 22.1% change in organizational performance can be attributed to ISM in the case of non-smart cities. The model with R^2 values for ISM and organizational performance is shown in Figure 5.11 below.

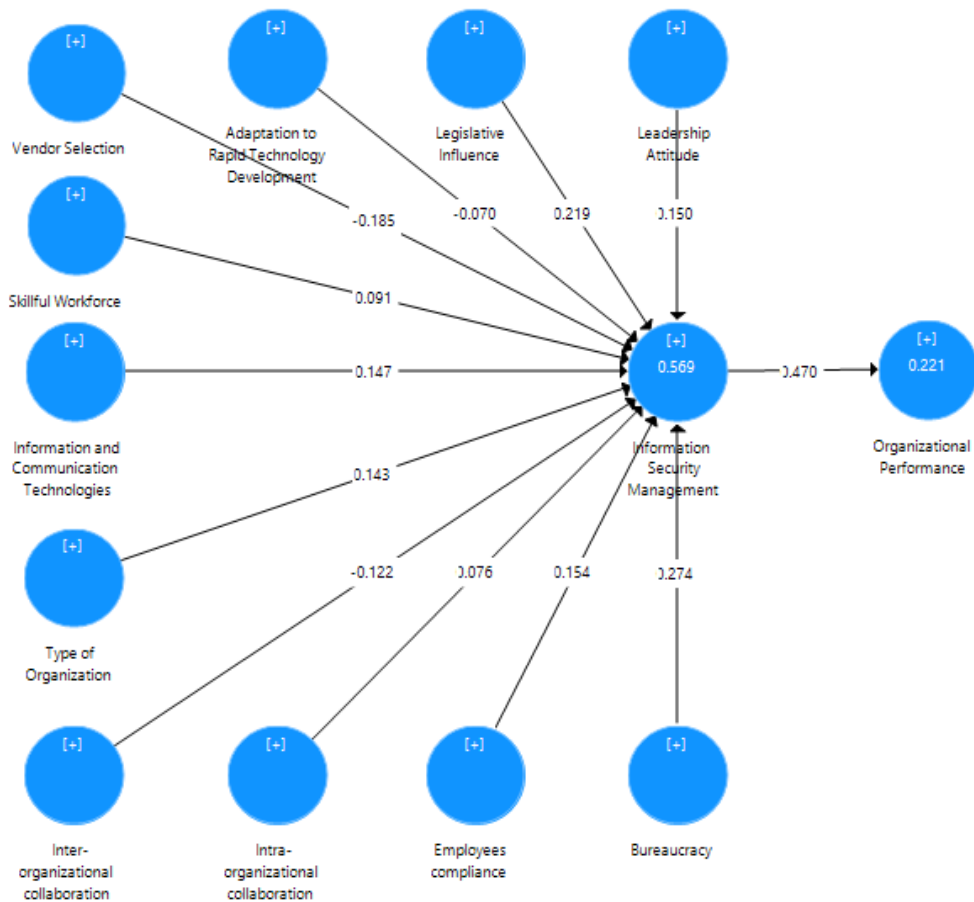


Figure 5.11: SEM hypothesis testing for non-smart city respondents (original sample)

Source: DeVised by author

In addition to the evaluation of the R^2 value, the measure of the f^2 effect size can also be assessed. The f^2 effect size statistic specifies whether the removal of an independent variable from a model can have a substantive impact on the dependent variable (Hair Jr et al., 2013).

The results show that only the removal of ISM has a moderately significant impact on organizational performance. However, if any of the predictors of ISM are removed, this would not significantly impact the model. The effect size and their significance values are shown in Table 5.37.

Table 5.37 Effect Size for Independent Variables for Non-smart City respondents

	Original Sample	STDEV	T Statistics	P Values

ARTD -> ISM	0.007	0.021	0.339	0.735
BC -> ISM	0.084	0.061	1.364	0.173
EC -> ISM	0.027	0.028	0.94	0.348
ICT -> ISM	0.029	0.036	0.794	0.428
Inter -> ISM	0.013	0.023	0.552	0.581
Intra -> ISM	0.004	0.016	0.270	0.787
LA -> ISM	0.017	0.024	0.709	0.479
LI -> ISM	0.048	0.039	1.232	0.218
SW -> ISM	0.007	0.022	0.337	0.736
TO -> ISM	0.030	0.041	0.730	0.465
VS -> ISM	0.039	0.031	1.252	0.211
ISM -> OP	0.283	0.108	2.613	0.009

Source: Devised by author

5.4.4.2.1 Path analysis non-smart cities

Relationship was assessed in non-smart city respondents for the significance of the impact of leadership attitude, legislative influence, adaptation to rapid technology development, vendor selection, skilful workforce, information and communication technologies, type of organization, employee compliance, bureaucracy, inter-organizational collaboration, and intra-organizational collaboration on information security management, and further the impact of information security management on organizational performance. The results of the significance test for smart city subjects show that only bureaucracy ($t = 3.008$, $p = 0.003$) and vendor selection ($t = 2.339$, $p = 0.02$) have a significant impact on ISM. All other variables fail to impact ISM in non-smart cities. Furthermore, the impact of ISM on organizational performance was also found to be significant in non-smart cities ($t = 7.351$, $p < 0.001$). The results are shown in Table 5.38 and Figure 5.12.

Table 5.38 Hypotheses Testing for Non-Smart City Respondents

Hypothesis #		Original Sample	Standard Deviation	T Statistics	P Values	Supported
1	ARTD -> ISM	-0.07	0.077	0.906	0.365	No
2	BC -> ISM	0.274	0.091	3.008	0.003	Yes
3	EC -> ISM	0.154	0.079	1.957	0.051	No
4	ICT -> ISM	0.147	0.084	1.744	0.082	No
5	Inter -> ISM	-0.122	0.092	1.327	0.185	No
6	Intra -> ISM	0.076	0.102	0.74	0.459	No
7	LA -> ISM	0.15	0.097	1.555	0.121	No
8	LI -> ISM	0.219	0.082	2.665	0.008	Yes
9	SW -> ISM	0.091	0.107	0.844	0.399	No
10	TO -> ISM	0.143	0.085	1.686	0.092	No
11	VS -> ISM	-0.185	0.079	2.339	0.02	Yes

12	ISM -> OP	0.47	0.064	7.351	.000	Yes
----	-----------	------	-------	-------	------	-----

Source: DeVised by author

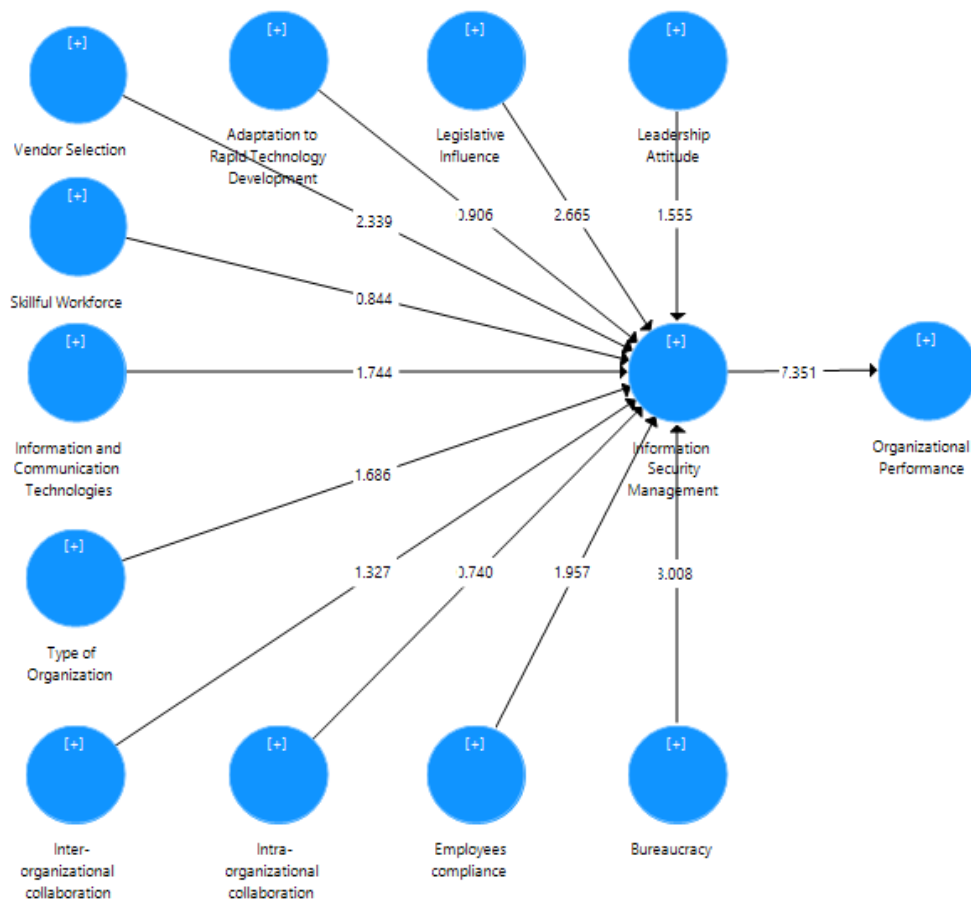


Figure 5.12: SEM hypothesis testing for non-smart city respondents (T statistics)

Source: DeVised by author

The comparison of significance of the impact of the factors namely: leadership attitude, legislative influence, adaptation to rapid technology development, vendor selection, skilful workforce, information and communication technologies, type of organization, employee compliance, bureaucracy, inter-organizational collaboration, and intra-organizational collaboration on information security management and furthermore, the impact of information security management on organizational performance between smart and non-smart cities is presented in Table 5.39. The results reveal that in smart cities, legislative influence and skilful workforce had a

significant impact on ISM while all other factors were insignificant. In non-smart cities, bureaucracy and vendor selection were found to have a significant impact while all other factors were insignificant. It is important to note that in both smart and non-smart cities, ISM had a significant impact on organizational performance. smart city, non-smart city and the overall complete analysis are presented in Table 5.39.

5.4.5 Model Significance comparison between Smart City, Non-Smart City and complete (P values)

After undertaking structural equation modelling and path analysis for the correspondents' data in different categories (full, smart and non-smart cities), Table 5.39 below shows the P values comparing the findings in the different respondents' categories.

Table 5.39 Significance comparison between Smart City, Non-Smart City and complete (P values)

Hypothesis nb		Smart City	Non-Smart City	Complete
1	ARTD -> ISM	0.405	0.365	0.855
2	BC -> ISM	0.391	(0.003)	(0.002)
3	EC -> ISM	0.356	0.051	0.105
4	ICT -> ISM	0.994	0.082	0.275
5	Inter -> ISM	0.338	0.185	0.648
6	Intra -> ISM	0.417	0.459	0.881
7	LA -> ISM	0.225	0.121	0.065
8	LI -> ISM	(0.001)	(0.008)	(0.000)
9	SW -> ISM	(0.005)	0.399	(0.004)
10	TO -> ISM	0.146	0.092	0.074
11	VS -> ISM	0.594	(0.020)	0.127

12	ISM -> OP	(0.000)	(0.000)	(0.000)
----	-----------	---------	---------	---------

Source: Devised by author

5.5 Summary

This chapter presented the data analysis. It started by illustrating the response rate and the sample size of the online survey. This was followed by a respondents' profiling analysis and descriptive statistics for the conceptual model constructs (construct means, standard deviations).

An SEM evaluation of the model and data followed, including construct validity, reliability analysis, convergent validity, and discriminant validity. This was followed by the coefficient of determination (R^2), the effect size (f^2), and the predictive relevance measure (Q^2) for the whole set of data; it then separated smart cities from non-smart cities. Path analysis confirmed three hypotheses in the smart cities dataset, four hypotheses in the non-smart cities data, and four hypotheses in the overall dataset.

Chapter 6 DISCUSSIONS

6.1 Introduction

The purpose of this research was to investigate the organizational factors that influence information security management (ISM) in smart-city organizations. This study first identified the most important organizational factors that influence information security management in the literature. Then, the organizational factors that influence smart cities governance were identified. Ten organizational factors were then recognized as being influential to ISM in smart city organizations; they were then tested in organizations from more than 70 cities worldwide, with 169 participants out of 308 from the top 100 smart cities. The study contained an empirical investigation into the organizational factors. It validated four hypotheses (two, eight, nine, and twelve) for the overall participants list, three were validated in the top 100 smart cities (eight, nine, twelve), and four validated in non-smart cities (two, eight, eleven, twelve). The goal of the current chapter is to discuss the findings in light of the data analysis results, highlighting interactions and comparisons in between the different respondents' categories.

6.2 Adaptation to Rapid Technology Development

Recent research has emphasized the importance of the rapid adoption of, and adaptation to, technological novelties for an organization to be competitive through innovation, better services and safer environments (Zanella et al., 2014). In this study, the test for the influence of “adaptation to rapid technology development” on information security management was not confirmed. There was no significant evidence to support the hypothesis (H_1) in question, meaning that organizations

might not be sufficiently planning and implementing processes to adapt to rapid technological changes.

The lack of adaptation to rapid technology development could be traced back to technology adoption challenges and difficulties, such as the government policy and inability to deploy and develop an ICT infrastructure that is able to serve the requirements of a fast-moving and growing economy (Laryea, 1999; Rexwhite Enakrire and Onyenania, 2007; Ejiaku, 2014). Another reason behind technology adoption difficulties is the non-presence of well-developed human capital and trainings that enable the growth of the different parties and the best usage of deployed technology (Udo and Edoho, 2000; Ejiaku, 2014). Another reason behind technology adoption difficulties is the absence of management strategies that could reflect management understanding of smart cities and translate smart city requirements into directions and actions inside the organizations. Such can also be caused by a lack of understanding from the leadership on how smart cities fulfill the need for growth inside organizations or on the other hand or limit them to resist change and not to impact power and hierarchies. (Bruque and Moyano, 2007; Hanan and McDowel, 1984)

6.3 Bureaucracy

Literature has previously discussed the advantages and disadvantages of bureaucracies inside organizations. Bureaucracies enable stronger processes inside organizations but can also be the cause of time wastage and inefficiencies (Toppeta, 2010; Nam and Pardo, 2011a). In this study, significant evidence was found to support the hypothesis (H₂) regarding the influence of bureaucratic standing on information security management in non-smart cities, and on the whole set of participants.

The positive bureaucratic standing inside the tested organizations has been found to lack supporting evidence in smart cities. A possible explanation is that smart city participants do not find the bureaucratic standing to be significantly satisfying due to fast organizational changes or rapid technological development requirements which are not being fulfilled. The lack of satisfaction with the bureaucratic standing from participants in smart cities could be traced back to the bureaucratic challenges of controlling complexity and performance by having the right processes in place inside organizations that enable a satisfying bureaucratic standing. This is especially relevant because smart cities are adopting more technologies and require more

human capital that is not simple to find or build, while still relying on the same bureaucratic functions that disrupt progress (Toppeta, 2010; Nam and Pardo, 2013). Other reasons behind a non-satisfying bureaucratic standing described in the literature is the workload pressure, smart cities are especially demanding and require continuous and rigorous follow up. The role an organization plays for its clients and its external influencers could also influence its bureaucratic standing, but that is not the case in the current research because organizations from a number of different industries were surveyed. (Scott, 1997; Bertelli, 2006)

6.4 Employee Compliance

Literature has previously discussed the importance of employees' compliance with information security policies and suggested methods to have that accomplished. In the case of smart cities, such measures are expected to be even more pressing as information security issues could be the cause of large-scale damage (Puhakainen and Siponen, 2010; Gil-Garcia and Pardo, 2005; Ashenden and Sasse, 2013). In this study, no significant evidence was found to support the hypothesis (H₃) regarding the influence of employees' compliance on information security management inside the participants' organizations. Nevertheless, employees' compliance with policies and regulations is an important matter and a major worry for modern organizations.

A different number of challenges could be behind the lack of sufficient employees' compliance, also going back to the literature around employee engagement part of an organizational culture. Hu et al. (2012) emphasized the critical importance of top management's commitment and participation towards the influence on the organizational compliance culture and shaping the intention of employees to comply with information security policies. Puhakainen and Siponen (2010) emphasized the need for the adoption of information security awareness training and continued communication processes to motivate the employees' systematic cognitive processing of the information they receive and achieve the best development of employees' compliance results. Another influencer of employees engagement is their preception of trainings and career development inside the organization, which highly reflect on smart cities requirements which demand smart people, though such cannot be achieved without strong skills development techniques employed in the workplace and presented in different forms of modern training methods like wargames or simulations. (Ashenden and Sasse, 2013, Anitha, 2014)

6.5 Information and Communication Technologies (ICT)

The importance of the best utilization of ICT has been discussed in the literature as an important factor towards the performance and security of online services (Sircar and Choi, 2007; Puhakainen and Siponen, 2010). In this study, no significant evidence was found to support the hypothesis (H₄) in either smart cities or non-smart cities around the organizational implementation of clear procedures and processes to evaluate the best utilization of the ICT infrastructure.

While the best utilization of the ICT infrastructure is a positive factor towards enhancing the quality of services, there seems to be a disconnect between organizations and Internet/data providers, rather than integration of what is better suited for smart cities. Current Internet/data providers take the least responsibility (in contracts and service level agreements) for any harm that happens to the client organization or its business. Such is a probable indicator that the role of the Internet/data providers might need to be re-evaluated in environments moving towards smart cities, especially now that the Internet/data infrastructure is being used to deliver harm towards the client organizations.

The resulting non-satisfaction of how the ICT infrastructure is being utilized could be traced back to multiple factors. A reason behind it is the lack of visibility over the advanced infrastructure and smart cities technology requirements from top management side and therefore weak top management support for the monitoring and evaluation of the ICT infrastructure quality, whether on the client's side or the provider's side (Chourabi et al., 2012; Williams, 2001; Kayworth and Whitten, 2010; Chang et al., 2011). Another reason behind a non-satisfactory ICT infrastructure is the lack of training for ICT employees, which does not permit the correct configuration, development and assessment of the ICT infrastructure (Zygiaris, 2013; Kourtiti and Nijkamp, 2012; Lombardi et al., 2012). A final reason behind non-satisfactory ICT utilization could be the lack of attention to ICT policy on the government or organizational side, especially because it is the only way to establish processes in place that enable the identification of quality deficiencies, legally finding the responsible party, and holding them accountable for ICT issues (Nam and Pardo, 2011b).

6.6 Inter-Organizational Collaboration

Past research has discussed the importance of inter-organizational collaboration in organizations. Enhancing the collaboration between organizations enables each to gain more knowledge and intelligence about new challenges and possible experiences that they might face (Bekara, 2014). In this study, no significant evidence was found to support the hypothesis (H₅) regarding the influence of inter-organizational collaboration on information security management. This is probably an indicator that these organizations are not yet fully aware of the importance of inter-organizational collaboration, and that more effort needs to be done to clarify and motivate top management support towards such activities. Collaboration between the different organizations inside the same city, country or different countries in matters of information security is essential towards better threat intelligence and overall safety, resiliency and sustainability of the smart city.

Several factors influencing inter-organizational collaboration were discussed in the literature and could be behind the lack of sufficient evidence to confirm inter-organizational collaboration. These include external environment factors, such as regulations and government policies, that influence organizations to maintain a level of openness and collaboration, demonstrating influence in the market and good reputation. Also, there are factors that relate to the type of organization and industry, which dictate how much external collaboration is needed. Furthermore, there are the people factors, where collaboration ability and trust is built between different people inside organizations. Others include the availability of communication and collaboration tools that enable inter-organizational collaboration, or organizational relational factors that vary depending on the organizational relationships with others, which could be based on needs or the stakeholders' capabilities (Yang and Maxwell, 2011; Patel et al., 2012; Kożuch and Sienkiewicz-Małyjurek, 2016). Another reason behind a lack of inter-organizational collaboration is the non-availability of financial resources supporting the development of such collaboration, especially in smarter cities because organizations will need to dedicate resources to develop frameworks that are accepted legally, defining the scope of trust, goals and compatibility concerns, following standards and classifying the types of data that could be shared with other organizations, also assigning project managers and performance indicators for such collaboration activities. (Sayogo and Gil-Garcia, 2014; Page Hocevar, 2006; Yang and Maxwell, 2011)

6.7 Intra-Organizational Collaboration

Past research has revealed the importance of intra-organizational collaboration in organizations. Enhancing collaboration between the different teams of an organization enables better performance and security of products and services, as the different teams get better visibility on product and services requirements (Sila, 2010). In this study, no significant evidence was found to support the hypothesis (H₆) regarding the influence of intra-organizational collaboration on information security management.

Although it is highlighted in the literature as a factor of major importance towards a smart city standing, no evidence was found of the influence of intra-organizational collaboration in the context of participants' organizations. This may indicate that these organizations are still not fully aware of the importance of intra-organizational collaboration, and that more effort needs to be made to clarify and motivate top management support towards such activities. Collaboration between the organization's departments is essential towards a better information security standing.

Several factors that influence intra-organizational collaboration were discussed in the literature and could be behind a lack of sufficient evidence to confirm intra-organizational collaboration. While these are sometimes similar to inter-organizational collaboration, high emphasis is put on organizational perspectives that address different complex social, cultural, political and bureaucratic abilities of an organization. Another reason behind a lack of intra-organizational collaboration is the non-availability of financial resources supporting the development of such collaboration. Organizations especially in smart cities require the investment of resources into the development of frameworks that define the collaboration needs and visibility each of the teams need in order to best deliver their performance, such is also pushed in policies and internal marketing campaigns that integrate the collaborative attitude between employees and encourage. Organizations need then to define and monitor performance indicators to guarantee the needed collaboration is continuously being applied and based on that define incentives for performing teams. (Sayogo and Gil-Garcia, 2014; Page Hocevar, 2006; Yang and Maxwell, 2011). Emphasis is also placed on the technological abilities inside an organization that enable faster and more efficient collaboration, management abilities in supporting the push such is a requirement of a successful organization (Gil-Garcia and Pardo, 2005; Yang and Maxwell, 2011).

6.8 Leadership Attitude

Previous research emphasized the importance of leadership attitude inside organizations (Aksorn and Hadikusumo, 2008). Top leadership support for information security management is essential for the implementation of a successful information security programme that is able to defend and protect an organization from information security issues. Leadership attitude could be sourced from top management or information security leadership (Ashenden and Sasse, 2013). Support could also come in different forms such as financial, political, and cultural or educational, among others. Negative leadership attitude towards information security could then negatively impact the organizational performance and goals. The influence of leadership attitude in this study was not confirmed in the contexts of the survey (smart city, non-smart city) and the hypothesis (H₇) cannot be validated with significant evidence.

Results show no significant evidence of a significant relationship between leadership attitude and information security issues. Such results could be explained in different ways. There are multiple determinants of leadership success or failure, starting from leadership's own human capital, skills and previous experiences, which would then influence leadership's own understanding of ISM issues and if not compatible or within shape, leading to lack of clarity for employees, lack of understanding of what needs to be done and decisions to be made, lack of monitoring of progress and ending with accelerated negative effects, furthermore inside smart city organizations. Another determinant is the social capacities of leadership and facilities employed in social and cultural influence inside the organization, critical for building an information security culture and employees engagement (Arvey et al, 2006; Kayworth and Leidner, 2002). Another possible reason is that leadership attitude is being not sufficiently involved in the process of understanding and influencing decision making around information security issues inside the organization. The literature is primarily focused on employees' influence as a major role of leadership attitude and in the context of information security, which is achieved through active involvement of the leadership in information security meetings, decision making, culture building... (Puhakainen and Siponen, 2010; Chang and Lin, 2007; Hu et al., 2012).

6.9 Legislative Influence

Previous research emphasized the importance of legislative influence on the enforcement of information security measures inside organizations; these measures protect them from cyber threats and breaches of data that could impact their business or endanger their clients (Chang and Ho, 2006; AlAwadhi and Scholl, 2013). In this study, the influence of legislation on information security management inside organizations was confirmed in both smart and non-smart cities. The hypothesis (H₈) was validated regardless of the context (smart city, non-smart city, complete set). Legislative influence was confirmed in all contexts of this research. The participants believed that they were being impacted by legislative measures related to information security. There are multiple determinants of legislative influence success or failure, such as the financial means an organization has to invest in information security technologies and ISM development, this is mostly present in cities being pushed to become smart as it starts with national level commitment towards progress via investment. Another determinant is the complexity of the requirements, which is also prevalent in smart cities, complexities of which were well described in the literature review. Another determinant is the strategy implemented towards the achievement of legislative changes and influence, such is key towards the achievement of efficient development of legislations, progress and monitoring of feedback, adoption and compliance. Another determinant is the training and educational offerings, which allow employees to stay up-to-date with latest technologies, standards and methods towards playing their roles efficiently, such goes back to the importance of human capital in smart cities, well described in the literature and one of the most important smart city dimensions. (Muriithi et al., 2011; Caragliu et al., 2007).

Interestingly, it is worth noting that non-smart city countries do not have cyber laws and controls that enable legislative influence, yet sometimes use the same methods for achieving political or cultural influence. An explanation is that non-smart city participants could be under the illusion of legislative influence coming from superior and smarter countries, especially through the media and information security news that has been highly intensive in the last few years.

6.10 Skilful Workforce

Human capital plays a major factor in advanced environments such as smart cities, especially in the information security domain. The literature discussed the

importance of human capital in the context of smart cities. Smart cities are not only expected to encourage and foster skilled workers, but to also hunt and attract skilled human capital (Chang et al., 2011). In this study, the testing of the “skilled workforce” variable revealed significant evidence to support the hypothesis (H_9) in the top 100 smart cities, an indicator that reasonable consideration is being given to human capital. The results were also valid in the context of the whole participants set. Human capital is one of the most important pillars of smart city development and growth. In this current research, the top 100 smart cities worldwide have demonstrated better attention to the importance of human capital and the need for human capital development for enhanced overall information security inside an organization when compared to smart cities outside the top 100. While the availability of skilled employees is found significant in both smart and non-smart cities, further research is needed towards exploring the methods by which skills are more likely to cause positive influence than others, and how such skills could best be diffused to the highest number of employees in smart city organizations.

6.11 Type of Organization

Previous literature discussed the influence of the type of organization on its processes and requirements. The same applies in the technological domain as each organization will have different needs and special requirements to protect its data and services (Kuk and Janssen, 2011; Anthopoulos and Fitsilis, 2014). In this study, no significant evidence was found to support the hypothesis (H_{10}) regarding the influence of the type of organization on the information security management in the participants’ organizations.

According to the findings, the type of organization influences the type of technologies and solutions it needs to protect its core data and production mechanisms. No significant evidence was found on the influence of the type of organization on information security management operations. Therefore, each organization may need to customize their own information security operations, designs, and solutions’ deployment to protect their specific environment and assets. Such is a strong deterrent measure when cyber-attacks occur as it makes victim infiltration much harder.

Various factors related to the type of organization were discussed in the literature, such as organizational behaviour and business goals. One determinant of such is the lack of leadership awareness about the industry specific threats related to the

organization, as that is a factor that enables the right reactions to be designed (solutions, trainings...). Another factor is that the organization does not have sufficient and efficient assets management capabilities, allowing for the right visibility of the organization over the data assets they are trying to protect, their criticality and thenforth the requirements to protect such assets. Another factor that influences organizational awareness of industry specific threats is awareness of its dependence on information security, sometimes caused by the slow emergence and transformation of organizations with technology and lack of holistic view over how to protect all the systems including legacy ones and what data do these systems hold in the first place (Chang and Ho, 2006). The lack of sufficient evidence to confirm a positive influence of the 'type of organization' on ISM in this research could be an indicator that organizations' ISM is being carried out in the same way for different organizations. Therefore, similarly designed solutions are being implemented as one-way solutions in different environments which is not optimal for efficient ISM (Johnsson and Goetz, 2007).

6.12 Vendor Selection

Literature on smart cities discussed the importance of technology vendor selection, process difficulties, and the dangers of vendor monopolies, especially in smart city environments (Hollands, 2008, 2015). In this study, the testing of the "vendor selection" abilities inside organizations revealed significant evidence to support the hypothesis (H₁₁) in the context of non-smart cities, although there was not enough evidence to support the hypothesis in smart cities or in the complete participants' set in this research.

Research results only confirmed the validity of the hypothesis in the context of non-smart cities. Therefore, participants from non-smart cities view the vendor selection processes inside their organizations as more adequate than those in smart cities. A possible explanation is that non-smart cities have smaller technological projects that require functions that have already been tested, validated or rejected and ranked in other regions worldwide. Smart cities demand larger projects with technology not well tested before, which leaves a lot of room for influence by vendors through social relationships or marketing to gain large projects that benefit the business.

Various determinants for vendor selection were discussed in the literature, such as the purchasing team characteristics and psychology, which is an important factor demonstrating human capital and HR practices of an organization inside smart

cities. Having the right team in place enables an organization transparent and correct vendor selection based on its own requirements. Another factor influencing vendor selection is organizational specific variables such financial capabilities and the quality/price ratio; nevertheless, smart city organizations are expected to agree and prepare for smart city level changes and upgrades that allow investments to be made into the right technologies. (Wind and Robinson, 1968; Weber et al., 1991; Parthiban et al., 2013). The dangers of vendor influence and monopolies in smart cities is a phenomenon that Hollands (2008) and Söderström et al. (2014) warned about from the early stages of the smart cities concept development.

6.13 Information Security Management and Organizational Performance

Previous research studied and analysed the influence of information security management on organizational performance (Goel and Shawky, 2009; Gordon et al., 2011; Cavusoglu et al., 2004). There is an agreement in the research community around the negative influence of information security problems on the organizational performance of different domains of influence, such as financial, market value (Goel and Shawky, 2009), productivity (Cavusoglu et al., 2004), reputation (Gordon et al., 2011), and intellectual property (Thomas et al., 2013).

The influence of information security management (ISM) has been confirmed in the context of this research. The hypothesis on ISM's influence on organizational performance (H_{12}) has been validated in the context of this research for all types of participants (both smart cities and non-smart cities). The results of ISM in the context of smart cities in this study are, therefore, consistent with previous research from the literature on the success of information security management inside organizations and its influence on organizational performance. Since the significance of this variable has been validated in both smart city and non-smart city context, this is indicator of proper awareness about the information security management influence on organizational performance in most of the organizations that were involved in this research.

6.14 Ranking of Organizational Factors Influencing ISM in Smart Cities

A smaller p value is an indicator of stronger evidence against the null hypothesis, so the null hypothesis is rejected. Below is a ranking of the organizational factors

identified in this study, organized by their evidence significance (p value ascending). The goal is to point out the most significant organizational factors influencing ISM in the different contexts of this research. The different results demonstrate a different understanding and evaluation of the organizational factors by the participants, and a different understanding of the challenges in their corresponding environments (see Tables 6.1-6.3).

Table 6.1: Significance evidence sorted for organizational factors in the complete participants' set

	Complete
ISM -> OP	0.000
LI -> ISM	0.000
BC -> ISM	0.002
SW -> ISM	0.004

Source: Devised by author

Table 6.2: Significance evidence sorted for organizational factors in the non-smart city participants' set

	Non-Smart City
ISM -> OP	0.000
BC -> ISM	0.003
LI -> ISM	0.008
VS -> ISM	0.020

Source: Devised by author

Table 6.3: Significance evidence sorted for organizational factors in the smart city participants' set

	Smart City
ISM -> OP	0.000
LI -> ISM	0.001
SW -> ISM	0.005

Source: Devised by author

This chapter discussed the data analysis results. It examined the findings in the context in which they occurred and considered various explanations for their occurrence. This included highlighting instances from relevant literature that not only supported the results but also refuted them. The next chapter offers a set of conclusions for this project.

Chapter 7 RESEARCH CONCLUSIONS

7.1 Research objectives revisited

The purpose of this research was to investigate the organizational factors influencing information security management in smart city organizations. The research aimed to fill the literature gap in this research area caused by the lack of research in smart cities management topics. The study started with an extensive review of the academic literature in Chapter 2 that focused on smart cities, information security, and information security management. It then proceeded towards exploring the organizational factors that influence information security management in the context of organizations, indicators of which are found in the smart cities literature. The literature review highlighted the importance of information security management for smart cities, the lack of management research in smart cities, and the criticality of the highlighted issues. The review then proceeded to identify the organizational factors that are expected to most influence information security management in the context of smart city organizations. The literature review findings and highlights fulfil the research objective of attaining a thorough understanding of the research concepts and their development in the literature.

The study then proceeded in Chapters 3 and 4 towards the development of the research methodology and a quantitative survey instrument to evaluate the previously identified organizational factors in the current smartest cities around the world. The survey was designed and initiated with a pilot study of two rounds, and

concluded with 308 valid participations from different backgrounds (technical, management, and executive); these are presented in Chapter 5. The research methodology and conceptual model development then fulfil the research objective of developing a model or framework to incorporate the factors influencing information security management in smart city organizations.

The study then highlights multiple conclusions in Chapter 6 and contextualizes them with previous studies in related fields. These included research on the influence of vendors on organizations, the role of leadership attitude in information security management issues, the noticeable legislative influence on organizations, and the role of employee skills in smarter cities. The study also highlighted leadership attitude, vendor selection, ICT infrastructure, adaptation to rapid technology development, type of organization, employees' compliance, inter- and intra-organizational collaboration as organizational factors that would need additional investigation as no significant evidence was found to support their positive existence in smart city organizations. The data analysis permitted the validation of the proposed model and data, fulfilling one of the research objectives. The data collection, analysis and conclusions also permitted the fulfilment of the research objective of accumulating a better understanding of information security management in smart city organizations and how they compare to other non-smart city organizations. Overall, current organizations in smart cities around the world fall short of being entirely "smart" as defined in the common literature on smart cities definitions. Different fragments of the literature have already highlighted the importance of the identified organizational factors towards advancing the cities and their organizations towards becoming smart in reality, not on the charts only. Nevertheless, a great deal of effort is expected to be generated in this regard. This research has mostly highlighted the importance of information security management in the smart cities context, consolidated the organizational factors that are expected to be most influential on organizations information security management, and then measured these in the context of current smartest cities worldwide.

7.2 Research implications and recommendations

This study offered multiple guidelines for organizations and management. The study highlighted the importance of information security management in the smart city. A lack of sufficient evidence was found for multiple organizational abilities that require more attention on the organizational level (i.e., adaptation to rapid technology

development, bureaucratic standing, employees' compliance, best ICT utilization, inter- and intra-organizational collaboration, leadership attitude, type of organization, and vendor selection). Existing literature has already emphasized the importance of realistic urban growth (Hollands, 2008), and how technological vendors can influence the smart cities hype, technology adoption, vendor selection, and employees' compliance with less advantage for the organization or the city itself. Firms should, therefore, find ways to enhance their abilities to the best readiness of their employees and services. Top management are also required to be more involved in information security issues as they seriously affect business performance and therefore stakeholders' objectives.

This research has highlighted important issues of current organizations around the world, identifying key factors that influence information security management for cities' organizations. This research has, therefore, developed a tool that could be used for future evaluations of information security management in smart cities' organizations. This research has also highlighted multiple issues that require attention from global decision makers. Smart cities are not supposed to be playgrounds for corporations looking for their own shareholders' profit. Real smart cities should focus on the actual development of their organizational abilities.

As such, business leaders and decision makers should focus on identified organizational factors, especially those highlighted in the context of smart cities to enable their businesses to achieve market-leading performance and competitive advantage.

7.3 Contributions to the literature

This study presented multiple contributions to theory, First the significance of information security management for smart cities was highlighted, an important factor of smart cities and which is expected to cause major stability or instability depending on how it is handled.

Second the lack of management research in the area of smart cities information security management is highlighted; without sufficient awareness of the threats and requirements to best manage smart cities information security issues correctly, smart cities risk wasting time, human and financial resources in order to achieve their best standing.

Third, this research identified and classified the organizational factors that influence information security management in smart city organizations. The goal is to then test and evaluate these factors inside smart and non-smart cities and study the results that come out. Such testing will enable the identification of where current smarter cities are in terms of information security management standing, what could be the problems and what can be done to accelerate the move of smart cities towards their defined goals.

Fourth, the study then proceeded to the design of a research methodology, and the development of a conceptual model to be evaluated in the context of smart and non-smart cities. The incorporation of both smart and non-smart cities in the data collection was done to allow comparison of results and data in following stages.

Fifth, after the data collection was completed from more than 300 participants from over 70 cities globally, analysis of the results was done and discussions followed to explain the outcome. Overall, results have shown indicators of lack of satisfaction from the information security professional and managers side in smart cities towards the strategies being employed by their organizations for the different technological aspects (adaptation to smart city technologies, adaptation to rapid technological development, bureaucratic strategies, internal and external collaboration efforts, vendor selection). Nevertheless, these same participants have demonstrated a strong understanding of the influence information security plays onto the organizational performance, have demonstrated satisfaction from the legislative influence they see onto their organizations, indicator of strong governments legislative pressure inside smart cities, possibly enriched by media and news on information security issues. Smart city participants have also demonstrated satisfaction from the human capital development inside their own organizations, indicator of strong push from top management in smart city organizations for the development of a skilled workforce that is able to handle the smart city requirements and successfully protect and defend against threats.

7.4 Research limitations and future directions

Research is constrained by schedules, resources and scope that limit that research. This implies limited research ability in finding and identifying the full truth. The present research was limited by its methodology being quantitative and allowing only limited options of responses for participants. Another limitation is the sample size which is the current research only represents a small percent of the target

population, the research was also limited to the LinkedIn platform to reach participants as dictated by the LinkedIn connections algorithms; such implies the inability to contact people outside of the LinkedIn platform, and the inability to contact all LinkedIn people. The research also had a better representation of some regions (the Middle East and GCC) than others due to researcher presence and access circumstances. The researcher also had less access to the female gender due to regional and research circumstances; such could imply lower accuracy in representing general organizational aspects on a larger scale. Additional limitations include the IESE ranking of smartest cities worldwide, which adapts new changes annually and which was used to classify those cities in the top 100 smartest; this implies an additional number of variables that classify cities.

There are multiple avenues for further research based on the present findings. Future research should consider a periodic re-evaluation of the organizational factors in the top 100 smart cities, especially while trying to better develop the factors that influence the measured variables that were found insignificant (adaptation to smart city technologies, adaptation to rapid technological development, bureaucratic strategies, internal and external collaboration efforts, vendor selection) and relying on the factors that were proven significant such as the strong understanding of participants of the information security influence on organizational performance, the organizations push towards having skilled employees and the governments legislative influence on organizations in smart cities. To better understand the results causality and the evolution of maturity among worldwide cities, this could create a new form of an evaluation methodology for smart city organizations and better classify top cities by what is happening inside their organizations rather than what they say is happening for the media. Future research might also consider other emerging organizational factors influencing information security management in smart city organizations. Future research might also consider the validity of the developed survey instrument in the evaluation of departments different from information security management, whether technology or non-technology focused. The goal would be to create different tools that can evaluate and compare organizational smartness of these departments and compare their maturity inside the company or among sectors or cities. Finally, further research should also explore bureaucratic requirements for better functioning smart cities. While bureaucracy enables better processes and strict controls around production environments, more research should be done to enhance the speed of such processes and their effectiveness to meet smart city goals.

REFERENCES

- Ahlgren, B., Dannewitz, C., Imbrenda, C., Kutscher, D. and Ohlman, B. (2012). A survey of information-centric networking. *IEEE Communications Magazine*, 50(7), 26-36. Available at: <http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6231276>
- Ahmad, N., & Mehmood, R. (2015). Enterprise systems: are we ready for future sustainable cities. *Supply Chain Management: An International Journal*, 20(3), 264-283.
- Aksorn, T. and Hadikusumo, B.H.W. (2008). Critical Success Factors Influencing Safety Program Performance in Thai Construction Projects, *Safety Science*, 46(4), 709-727.
- AlAwadhi, S. and Scholl, H.J. (2013). Aspirations and realizations: The smart city of Seattle. In System Sciences (HICSS), *2013 46th Hawaii International Conference* (pp. 1695-1703). IEEE.
- Albino, V., Berardi, U. and Dangelico, R.M. (2015). Smart cities: Definitions, dimensions, performance, and initiatives. *Journal of Urban Technology*, 22(1), 3-21.
- Alkandari, A., Alnasheet, M. and Alshekhly, I.F.T. (2012). Smart Cities: A Survey. *Journal of Advanced Computer Science and Technology Research*, 2(2), 79-90.
- Allwinkle, S. and Cruickshank, P. (2011). Creating Smart-er Cities: An Overview. *Journal of Urban Technology*, 18(2), 1-16.

Alshawaf, A.H., Ali, J.M.H. and Hasan, M.H. (2005). A benchmarking framework for information systems management issues in Kuwait, *Benchmarking: An International Journal*, 12(1), 30-44.

Amin, M. (2002). Security challenges for the electricity infrastructure. *Computer*, 35(4), 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*, 32(3), 703-725.

Andrews, K. (1971). *The concept of corporate strategy*. Homewood, IL: H. Dow Jones-Irwin.

Angelidou, M. (2015). Smart cities: A conjuncture of four forces. *Cities*, 47, 95-106.

Anitha, J. (2014). Determinants of employee engagement and their impact on employee performance. *International journal of productivity and performance management*, 63(3), 308.

Anthopoulos, L. and Fitsilis, P. (2010). From online to ubiquitous cities: The technical transformation of virtual communities. In Sideridis, A.B. and Patrikakis, C.Z. (Eds), *Next Generation Society: Technological and Legal Issues* (Proceedings of the Third International Conference, eDemocracy 2009, Athens, Greece, 23-25 September 2009) (Vol. 26, pp. 360-372). Berlin, Germany: Springer. Available at <http://www.springerlink.com/content/g644776482968k36/fulltext.pdf>.

Anthopoulos, L. and Fitsilis, P. (2013). Using Classification and Roadmapping techniques for Smart City viability's realization. *Electronic Journal of e-Government*, 11(2), 326-336.

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

Anthopoulos, L.G. and Tsoukalas, I.A. (2005). The implementation model of a digital city. The case study of the digital City of Trikala, Greece: e-Trikala. *Journal of EGovernment*, 2(2), 91-110.

- Armbrust, M., Fox, A., Griffith, R., Joseph, A.D., Katz, R., Konwinski, A., Lee, G., Patterson, D., Rabkin, A., Stoica, I. and Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM*, 53(4), 50-58.
- Arvey, R. D., Rotundo, M., Johnson, W., Zhang, Z., & McGue, M. (2006). The determinants of leadership role occupancy: Genetic and personality factors. *The Leadership Quarterly*, 17(1), 1-20.
- Ashenden, D. and Sasse, A. (2013). CISOs and organisational culture: Their own worst enemy? *Computers & Security*, 39, 396-405.
- Atzori, L., Iera, A. and Morabito, G. (2010). The Internet of Things: A survey. *Computer Networks*, 54(15), pp.2787-2805. Available at: <http://dx.doi.org/10.1016/j.comnet.2010.05.010>.
- Audestad, J.A. (2005). Four reasons why 100% security cannot be achieved. *Teletronikk*, 101(1), 38.
- Audretsch, D.B. and Welfens, P.J. (Eds) (2013). *The new economy and economic growth in Europe and the US*. Springer Science & Business Media.
- Avoine, G., Calderoni, L., Delvaux, J., Maio, D. and Palmieri, P. (2014). Passengers information in public transport and privacy: Can anonymous tickets prevent tracking? *International Journal of Information Management*, 34(5), 682-688. Available at: <http://www.sciencedirect.com/science/article/pii/S0268401214000620>
- Bacharach, S.B. (1989). Organizational theories: Some criteria for evaluation. *Academy of management review*, 14(4), 496-515.
- 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*, 30, Special Issue on Standard Making (August 2006), 413-438.
- Bagozzi, R.P., Yi, Y. and Phillips, L.W. (1991). Assessing construct validity in organisational research. *Administrative science quarterly*, 421-458.
- Bai, R.J. and Lee, G.G. (2003). Organizational factors influencing the quality of the IS/IT strategic planning process. *Industrial management & data systems*, 103(8), 622-632.

- Baker, H.K. and Anderson, R. (2010). An overview of corporate governance. *Corporate Governance: A Synthesis of Theory, Research, and Practice*, 8(1), 3-17, Robert W. Kolb Series in Finance.
- Baker, W.H. and Wallace, L. (2007). Is Information Security under Control?: Investigating Quality in Information Security Management. *IEEE Security & Privacy*, 5(1), 36-44.
- Bakıcı, T., Almirall, E. and Wareham, J. (2013). A smart city initiative: The case of Barcelona. *Journal of the Knowledge Economy*, 4(2), 135-148.
- Barlette, Y. and Fomin, V.V. (2009). The Adoption of Information Security Management Standards: A Literature Review.
- Barling, J., Loughlin, C. and Kelloway, E.K. (2002). Development and Test of a Model Linking Safety-Specific Transformational Leadership and Occupational Safety. *Journal of Applied Psychology*, 87(3), 488-496.
- Baron, M. (2012). Do we need smart cities for resilience? *Journal of Economics & Management*, 10, 32-46.
- Barrionuevo, J.M., Berrone, P. and Ricart, J.E. (2012). Smart Cities, Sustainable Progress, *IESE Insight*, 14(14) 50-57.
- Bartoli, A., Hernández-Serrano, J., Soriano, M. Dohler, M. Kountouris, A. and Barthel, D. (2011). Security and privacy in your smart city, in *Proceedings of the Barcelona Smart Cities Congress*. Available at: http://smartcitiescouncil.com/sites/default/files/public_resources/Smart%20city%20security.pdf
- Baruch, Y. (1999). Response rate in academic studies-A comparative analysis, *Human relations*, 52(4), pp. 421-438.
- 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*, 17(4), 159-82.
- Bătăgan, L. (2011). Smart cities and sustainability models. *Informatică Economică*, 15(3), 80-87.

- Battista, G., Evangelisti, L., Guattari, C., Basilicata, C. and de Lieto Vollaro, R. (2014). Buildings energy efficiency: Interventions analysis under a smart cities approach. *Sustainability*, 6(8), 4694-4705.
- Batty, M., Axhausen, K., Giannotti, F., Pozdnoukhov, A., Bazzani, A., Wachowicz, M., Ouzounis, G. and Portugali, Y. (2012). Smart cities of the future. *European Physical Journal Special Topics*, 214(1), 481-518.
- Baumeister, T. (2010). Literature Review on Smart Grid Cyber Security, Technical Report.
- Bekara, C. (2014). Security Issues and Challenges for the IoT-based Smart Grid. *Procedia Computer Science*, 34, 532-537. Available at: <http://www.sciencedirect.com/science/article/pii/S1877050914009193>
- Bélanger, F. and Crossler, R.E. (2011). Privacy in the Digital Age: A Review of Information Privacy Research in Information Systems. *MIS Quarterly*, 35(4), 1017–1041.
- Belissent, J. (2011). *The Core of a Smart City Must Be Smart Governance*. Cambridge, MA: Forrester Research, Inc.
- Berardi, U. (2013a). Clarifying the new interpretations of the concept of sustainable building. *Sustainable Cities and Society*, 8, 72-78.
- Berardi, U. (2013b). Sustainability assessment of urban communities through rating systems. *Environment, development and sustainability*, 15(6), 1573-1591.
- Berry, C.R. and Glaeser, E.L. (2005). The Divergence of Human Capital Levels across Cities. *Papers in Regional Science*, 84(3), 407-444.
- Bertelli, A. M. (2006). Determinants of bureaucratic turnover intention: Evidence from the Department of the Treasury. *Journal of Public Administration Research and Theory*, 17(2), 235-258.
- Bettini, C. and Riboni, D. (2015). Privacy protection in pervasive systems: State of the art and technical challenges. *Pervasive and Mobile Computing*, 17, 159-174. Available at: <http://www.sciencedirect.com/science/article/pii/S1574119214001631>

- Bharadwaj, A.S. (2000). A Resourced-Based Perspective on Information Technology Capability and Firm Performance: An Empirical Investigation. *MIS Quarterly*, 24(1), 169-196.
- Bhattacharjee, A. (2012). *Social science research: principles, methods, and practices*. CreateSpace Independent Publishing Platform; 2 edition.
- Bickman, L. and Rog, D.J. (Eds). (2008). *The Sage handbook of applied social research methods*. Sage publications.
- Blaxter, L. Hughes, C. and Tight, M. (2006). *How to research* (3rd edn). Poland: Open University Press.
- Blumberg B., Cooper D. & Schindler P. (2008) "Business Research Methods", (Vol. 2), *New York: McGraw-Hill Higher Education*.
- Bordonaba-Juste, V., Lucia-Palacios, L. and Polo-Redondo, Y. (2012). The influence of organizational factors on e-business use: analysis of firm size. *Marketing Intelligence & Planning*, 30(2), 212-229.
- Borgia, E. (2014). The Internet of Things vision: Key features, applications and open issues. *Computer Communications*, 54, 1-31. Available at: <http://dx.doi.org/10.1016/j.comcom.2014.09.008>.
- Borja, J. (2007). Counterpoint: Intelligent cities and innovative cities. *Universitat Oberta de Catalunya (UOC) Papers: E-Journal on the Knowledge Society*, 5. Available at <http://www.uoc.edu/uocpapers/5/dt/eng/mitchell.pdf>.
- Boss, S.R., Kirsch, L.J., Angermeier, I., Shingler, R.A. and Boss, R.W. (2009). If Someone Is Watching, I'll Do What I'm Asked: Mandatoriness, Control, and Information Security. *European Journal of Information Systems*, 18(2), 151-164.
- Bradley, R.V., Byrd, T.A., Pridmore, J.L., Thrasher, E., Pratt, R.M. and Mbarika, V.W. (2012). An Empirical Examination of Antecedents and Consequences of IT Governance in US Hospitals, *Journal of Information Technology*, 27(2), 156-177.
- Bresnahan, T.F. and Traitenberg, M. (1995). General purpose technologies 'Engines of Growth?'. *Journal of Econometrics*, 65(1), 83-108.

- Brink, D. (2001). A guide to determining return on investment for e-security. *RSA Security Inc.*
- Brown, C.V. (1997). Examining the Emergence of Hybrid Governance Solutions: Evidence from A Single Case Site. *Information Systems Research*, 8(1), 69-94.
- Bruque, S., & Moyano, J. (2007). Organisational determinants of information technology adoption and implementation in SMEs: The case of family and cooperative firms. *Technovation*, 27(5), 241-253.
- Bryman, A. and Bell, E. (2007). *Business research methods*. 2nd edn. Oxford University Press.
- Brynjolfsson, E. and Hitt, L.M. (1996). Paradox Lost? Firm-Level Evidence on the Returns to Information Systems. *Management Science*, 42(4), 541-558.
- Brynjolfsson, E. and Hitt, L.M. (2000). Beyond computation: Information technology, organizational transformation and business performance. *The Journal of Economic Perspectives*, 14(4), 23-48.
- Burrell G. & Morgan G. (1994) "Sociological paradigms & organisational analysis", *Heinemann*.
- Calzada, I. and Cobo, C. (2015). Unplugging: Deconstructing the smart city. *Journal of Urban Technology*, 22(1), 23-43.
- Cameron, K.S. (1986). Effectiveness as paradox: Consensus and conflict in conceptions of organizational effectiveness. *Management Science*, 32(5), 539–553.
- Cameron, K.S. and Whetten, D.A. (1981). Perceptions of organizational effectiveness over organizational life cycles. *Administrative Science Quarterly*, 26, 525–544.
- Campbell, T. (2009). Learning cities: Knowledge, capacity and competitiveness. *Habitat International*, 33(2), 195-201.
- Caragliu, A. and Del Bo, C. (2012). Smartness and European urban performance: assessing the local impacts of smart urban attributes. *Innovation: The European Journal of Social Science Research*, 25(2), 97-113.

- Caragliu, A., Del Bo, C. and Nijkamp, P. (2011). Smart cities in Europe. *Journal of Urban Technology*, 18(2), 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*, 51(6), 112-119.
- Carlson, K. and Hatfield, D. (2004). Strategic management research and the cumulative knowledge perspective. In: Ketchen, D.J. and Bergh, D.D. (Eds), *Research methodology in strategy and management* (pp. 273-301). San Diego, CA: Elsevier.
- Castells, M. (1996). *Rise of the Network Society: The Information Age*. Cambridge, MA: Blackwell
- 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*, 9(1), 70-104.
- Center on Governance (2003). *SmartCapital Evaluation Guidelines Report: Performance Measurement and Assessment of SmartCapital*. Ottawa, Canada: University of Ottawa. Available at http://www.christopherwilson.ca/papers/Guidelines_report_F_eb2003.pdf.
- Chadwick, B.A., Bahr, H.M. and Albrecht, S.L. (1984). *Social science research methods*. Prentice Hall.
- Chakravarthy, B.S. (1986). Measuring strategic performance. *Strategic Management Journal*, 7(5), 437-458.
- Chan, M., Woon, I. and Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior, *Journal of information privacy and security*, 1(3), 18-41.
- Chang, S.E. and Ho, C.B. (2006). Organizational Factors to the Effectiveness of Implementing Information Security Management, *Industrial Management & Data Systems*, 106(3), 345-361.

- Chang, S.E. and Lin, C.S. (2007). Exploring Organizational Culture for Information Security Management, *Industrial Management & Data Systems*, 107(3), 438-458.
- 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*, 54(2/3), 147-166.
- Chelliah, P.R. (2014). Elucidating the Cloud Enterprise Architecture for Smarter Enterprises. *IT Professional*, 16(6), 33-37.
- Chen, T. (2010). Smart grids, smart cities need better networks [Editor's Note]. *IEEE Network*, 24(2), 2-3.
- Choobineh, J., Dhillon, G., Grimaila, M.R. and Rees, J. (2007). Management of Information Security: Challenges and Research Directions, *Communications of the Association for Information Systems*, 20(1), 958-971.
- Chou, D.C., Yen, D.C., Lin, B. and Cheng, P.H-L. (1999). Cyberspace security management, *Industrial Management & Data Systems*, 99(8), 353-61.
- 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. In *System Science (HICSS), 2012 45th Hawaii International Conference*, 2289–2297.
- Churchill, G.A. (1979), “A Paradigm for Developing Better Measures of Marketing Constructs”, *Journal of Marketing Research*, Vol. 16, No. 1, pp. 64-73.
- Churchill, G.A. and Iacobucci, D. (2004). *Marketing research: Methodological foundations*. 9th edn. Ohio: Thomson South-Western.
- Cisco (2005). *Dubai: The Smart City*,
http://www.cisco.com/web/learning/1e21/1e34/downloads/689/nobel/2005/docs/Abdulhakim_Malik.pdf
- Clegg, C., Axtell, C., Damodaran, L., Farbey, B., Hull, R., Lloyd-Jones, R., Nicholls, J., Sell, R. and Tomlinson, C. (1997). Information technology: a study of performance and the role of human and organizational factors. *Ergonomics*, 40(9), 851-871.

- Coccoli, M., Guercio, A., Maresca, P. and Stanganelli, L. (2014). Smarter universities: A vision for the fast changing digital era. *Journal of Visual Languages & Computing*, 25(6), 1003-1011.
- Codagnone, C. and Wimmer, M.A. (Eds) (2007). *Roadmapping eGovernment Research – Visions and Measures towards Innovative Governments in 2020*. European Commission FP6 Project eGovRTD2020, Final Report, Brussels, Belgium, May 2007.
- Coe, A., Paquet, G. and Roy, J. (2001). E-governance and smart communities: A social learning challenge. *Social Science Computer Review*, 19(1), 80-93.
- Cohen, B., Stren, R., Montgomery, M.R. and Reed, H.E. (Eds) (2003). *Cities Transformed: Demographic Change and Its Implications in the Developing World* (Vol. 2). National Academies Press.
- Collins, B., Paquet, G., Roy, J. and Wilson, C. (2002). E-governance and smart communities: A social learning challenge. In *Proceedings of the SSHRC Knowledge Based Economy Workshop*, Newfoundland, Canada, May 10-11. Available at http://www.christopherwilson.ca/papers/Nfld_paper_2002.pdf.
- Collis, J. and Hussey, R. (2003). *Business Research: A Practical Guide for Undergraduates and Post-graduates Students*, 2nd Edition; Palgrave Macmillan, Basingstoke, Hampshire, England, UK.
- Comrey, A. and Lee, H. (1992). *A first course in factor analysis*. Hillsdale, NJ: Lawrence Erlbaum Associates
- Cooke-Davies, T. (2002). The 'Real' Success Factors on Projects, *International Journal of Project Management*, 20(3), 185-190.
- Correia, G. and Viegas, J.M. (2009). A conceptual model for carpooling systems simulation. *Journal of Simulation*, 3(1), 61-68. Available at: <http://www.palgravejournals.com/jos/journal/v3/n1/abs/jos20084a.html>.
- Correia, L.M. and Wünstel, K. (2011). *Smart Cities applications and requirements*. White Paper of the Experts Working Group, Net!Works European Technology Platform. Available at: http://www.networks-etp.eu/fileadmin/user_upload/Publications/Position_White_Papers/White_Paper_Smart_Cities_Applications.pdf

- Covenant of Mayors (2010). *Sustainable Energy Action Plan*. Available at: www.covenantofmayors.eu/IMG/pdf/seap_guidelines_en.pdf
- Creswell, J. W. (2002). *Educational research: Planning, conducting, and evaluating quantitative* (pp. 146-166). Upper Saddle River, NJ: Prentice Hall.
- Creswell, J.W., Plano Clark, V.L., Gutmann, M.L. and Hanson, W.E. (2003). Advanced mixed methods research designs. *Handbook of mixed methods in social and behavioral research*, 209, 240.
- Cretu, G.L. (2012). Smart Cities Design Using Event-driven Paradigm and Semantic Web. *Informatica Economica*, 16(4), 57-67.
- Cronbach, L.J. and Shavelson, R.J. (2004). My current thoughts on coefficient alpha and successor procedures. *Educational and psychological measurement*, 64(3), 391-418.
- Croteau, A.-M. and Raymond, L. (2004). Performance Outcomes of Strategic and IT Competencies Alignment, *Journal of Information Technology*, 19(3), 178-190.
- Culnan, M.J., Foxman, E.R. and Ray, A.W. (2008). Why IT Executives Should Help Employees Secure Their Home Computers, *MIS Quarterly Executive*, 7(1), 49-56.
- Dalvi, M.V. and Kant, R. (2015). Benefits, criteria and activities of supplier development: a categorical literature review. *Asia Pacific Journal of Marketing and Logistics*, 27(4), 653-675.
- Dameri, R.P. (2012). Defining an evaluation framework for digital cities implementation. In *International Conference on Information Society (i-Society)*, (pp. 466-470). IEEE Xplore.
- Dameri, R.P. (2013). Searching for smart city definition: a comprehensive proposal. *International Journal of Computers & Technology*, 11(5), 2544-2551 (Council for Innovative Research).
- Daniels, P.W. (2004). Urban challenges: The formal and informal economies in mega-cities. *Cities*, 21(6), 501–511.

- Dashti, A., Benbasat, I. and Burton-Jones, A. (2009). Developing trust reciprocity in electronic-government: The role of felt trust, In *Proc. Eur. Mediterranean Conference Information Systems*, Izmir, Turkey (pp. 1-13).
- David, J. (2002). Policy enforcement in the workplace, *Computers & Security*, 21(6), 506-13.
- Davis, A. (2005). Return on security investment—proving it's worth it. *Network Security*, 2005(11), 8-10.
- Dawes, S.S., Cresswell, A.M. and Pardo, T.A. (2009). From "need to know" to "need to share": Tangled problems, information boundaries, and the building of public sector knowledge networks. *Public Administration Review*, 69(3), 392-402.
- De Haes, S. and Van Grembergen, W. (2009). An exploratory study into IT governance implementations and its impact on business/IT alignment. *Information Systems Management*, 26(2), 123-137.
- De Wilde, R. (2000). *De Voorspellers. Een kritiek op de toekomstindustrie*. Amsterdam: De Balie.
- Deakin, M. (2012). Intelligent cities as smart providers: CoPs as organizations for developing integrated models of eGovernment Services. *Innovation: The European Journal of Social Science Research*, 25(2), 115-135.
- Deakin, M. and Al Waer, H. (2011). From intelligent to smart cities. *Intelligent Buildings International*, 3(3), 140-152.
- Debnath, A.K., Chin, H.C., Haque, M.M. and Yuen, B. (2014). A methodological framework for benchmarking smart transport cities. *Cities*, 37, 47-56. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0264275113001650> [Accessed 18 July 2014].
- Dehning, B. and Stratopoulos, T. (2003). Determinants of a Sustainable Competitive Advantage Due to an IT-Enabled Strategy, *The Journal of Strategic Information Systems*, 12(1), 7-28.
- Demirkan, H. (2013). A smart healthcare systems framework. *IT Professional*, 15(5), 38-45.

- Denton, D.W. (2012). Enhancing instruction through constructivism, cooperative learning, and cloud computing. *TechTrends*, 56(4), 34-41.
- Denzin, N.K. (1978). *The research act: A theoretical orientation to sociological methods*, 2nd edn). New York: McGraw-Hill.
- DeVaus D. (2002) "Surveys in Social Research", (5th ed.), *Routledge, London*.
- Dhillon, G. and Backhouse, J. (2000). Technical opinion: Information system security management in the new millennium. *Communications of the ACM*, 43(7), 125-128.
- Ding, D., Cooper, R.A., Pasquina, P.F. and Fici-Pasquina, L. (2011). Sensor technology for smart homes. *Maturitas*, 69(2), 131-136. Available at: <http://www.sciencedirect.com/science/article/pii/S0378512211000983>
- Dirks, S. and Keeling, M. (2009). *A Vision of Smarter Cities: How Cities Can Lead the Way into a Prosperous and Sustainable Future*. Somers, NY: IBM Global Business Services. Available at <ftp://public.dhe.ibm.com/common/ssi/ecm/en/gbe03227usen/GBE03227USEN.PDF>
- Dlamini, M.T., Eloff, J.H. and Eloff, M.M. (2009). Information security: The moving target. *Computers & Security*, 28(3-4), 189-198.
- Domingo, A., Bellalta, B., Palacin, M., Oliver, M. and Almirall, E. (2013). Public open sensor data: Revolutionizing smart cities. *IEEE Technology and Society Magazine*, 32(4), 50-56.
- Dommeier, C.J., Baum, P., Chapman, K.S. and Hanna, R.W. (2002). Attitudes of business faculty towards two methods of collecting teaching evaluations: Paper vs. online, *Assessment & Evaluation in Higher Education*, 27(5), 455-462.
- Dutta, A. and McCrohan, K. (2002). Management's role in information security in a cyber economy, *California Management Review*, 45(1), 67-87.
- Dutta, S. and Mia, I. (2010). The global information technology report 2009–2010. In *World Economic Forum and INSEAD*, SRO-Kundig Geneva, Switzerland.
- Dutton, W.H. (1987). *Wired Cities: Shaping the Future of Communications*. London: Macmillan.

- Earley, S. (2015). Analytics, Machine Learning, and the Internet of Things. *IT Professional*, 17(1), 10-13. Available at:
<http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7030173>.
- Easterby-Smith, M., Thorpe, R. and Lowe, A. (2002). *Management Research: An Introduction* (2nd edn). London: SAGE publications.
- Easterby-Smith M., Thorpe R., Jackson P. & Lowe A. (2008) "Management Research", (3rd edition), *Sage, London*.
- Easterby-Smith M., Thorpe R. & Jackson P. (2012) "Management research", *Sage Publications*.
- Ebrahim, Z. and Irani, Z. (2005). E-government adoption: architecture and barriers. *Business Process Management Journal*, 11(5), 589-611.
- Edvinsson, L. (2006). Aspects on the city as a knowledge tool. *Journal of Knowledge Management*, 10(5), 6-13. Available at
http://www.corporatelongitude.com/download/Aspects_on_city.pdf.
- Edvinsson, L., Dvir, R., Roth, N. and Pasher, E. (2004). Innovations: The new unit of analysis in the knowledge era: The quest and context for innovation efficiency and management of IC. *Journal of Intellectual Capital*, 5(1), 40-58.
- Eger, J.M. (2000, Feb 13). *Cities: Smart growth and the urban future*. The San Diego Union Tribune
- Eger, J.M. (2009). Smart growth, smart cities, and the crisis at the pump a worldwide phenomenon. *I-Ways – The Journal of E-Government Policy and Regulation*, 32(1), 47-53.
- Eger, J.M. and Maggipinto, A. (2010). Technology as a tool of transformation: e-Cities and the rule of law. In D'Atri, A. and Saccà, D. (Eds), *Information Systems: People, Organizations, Institutions, and Technologies* (pp. 23-30). Berlin/Heidelberg, Germany: Physica-Verlag.
- Ejiaku, S.A. (2014). Technology adoption: Issues and Challenges in information technology adoption in emerging economies. *Journal of International Technology and Information Management*, 23(2), 5.

- Elejoste, P., Angulo, I., Perallos, A., Chertudi, A., Zuazola, I.J.G., Moreno, A., Azpilicueta, L., Astrain, J.J., Falcone, F. and Villadangos, J. (2013). An easy to deploy street light control system based on wireless communication and LED technology. *Sensors*, 13(5), 6492-6523.
- Elmaghraby, A.S. and Losavio, M.M. (2014). Cyber security challenges in Smart Cities: Safety, security and privacy. *Journal of advanced research*, 5(4), 491-497.
- Eloff, J.H.P., and Eloff, M. (2003). Information Security Management: A New Paradigm. In Proceedings of the 2003 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on Enablement through Technology (SAICSIT 2003) (pp. 130-136), South African Institute for Computer Scientists and Information Technologists.
- Ernest Chang, S. and Ho, C.B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*, 106(3), 345-361.
- Ettredge, M., Richardson, V.J. and Scholz, S. (2001). The presentation of financial information at corporate Web sites. *International Journal of Accounting Information Systems*, 2(3), 149-168.
- Ezkowitz, H. (2008). *The triple helix: university, industry and government*. Routledge, London.
- Fabian, B. and Günther, O. (2009). Security challenges of the EPCglobal network. *Communications of the ACM*, 52(7), 121-125.
- FBI National Press Office (2014). Update on Sony Investigation. [online] Available at: <http://cyber-peace.org/wp-content/uploads/2015/01/FBI-%E2%80%94Update-on-Sony-Investigation.pdf> [Accessed 24 Mar. 2015].
- Fellows R. & Liu A. (2009) "Research methods for construction", *John Wiley & Sons*.
- Ferro, E., Caroleo, B., Leo, M., Osella, M. and Pautasso, E. (2013). The Role of ICT in Smart Cities Governance. In *Proceedings of 13th International Conference for E-Democracy and Open Government* (pp. 133-146). Krems: Edition Donau-Universität Krems. Available at: <http://www.enricoferro.com/paper/CEDEM13.pdf>
- Field, A. (2013). *Discovering statistics using IBM SPSS statistics*. Sage.

- Fliaster, A. (2004). Cross-hierarchical interconnectivity: forms, mechanisms and transformation of leadership culture, *Knowledge Management Research & Practice*, 2(1), 48-57.
- Florida, R. (2002). *The Rise of the Creative Class: And How It's Transforming Work, Leisure, Community and Everyday life*. New York: Basic Books. Available at <http://www.washingtonmonthly.com/features/2001/0205.florida.html>.
- Florida, R. (2002). Book Review: Class distinctions for the global economy.
- Fornell, C., and Larcker, D.F. (1981). Evaluating structural equation models with unobservable variables and measurement error, *Journal of Marketing Research*, 18(1), 39-50.
- Fowler, F.J. Jr. (2002). *Survey research methods*. Sage Publications Inc., London.
- Frankfort-Nachmias C. & Nachmias D. (2007) "Research methods in the social sciences", *Macmillan*.
- Fulford, H. and Doherty, N.F. (2003). The application of information security policies in large UK-based organizations: an exploratory investigation. *Information Management and Computer Security*, 11(3), 106-114.
- Gabrys, J. (2014). Programming environments: environmentality and citizen sensing in the smart city. *Environment and Planning D: Society and Space*, 32(1), 30-48.
- Gann, D.M., Dodgson, M. and Bhardwaj, D. (2011). Physical–digital integration in city infrastructure. *IBM Journal of Research and Development*, 55(1.2), 8:1-8:10.
- Garrity, J.T. (1963). Top Management and Computer Profits, *Harvard Business Review*, 41(4), 6-13.
- Gartner Inc (2013). Gartner says the Internet of Things Installed Base Will Grow to 26 Billion Units By 2020" Retrieved 24 March 2015, <http://www.gartner.com/newsroom/id/2636073>.
- Gergen, K., 1992, "Organization Theory in the Postmodern Era", in M. Reed and M. Hughes (eds), *Rethinking Organizations*, London: Sage.

- Germain, R., Dröge, C. and Christensen, W. (2001). The mediating role of operations knowledge in the relationship of context with performance, *Journal of Operations Management*, 19(4), 453-69.
- GhaffarianHoseini, A., Dahlan, N.D., Berardi, U., GhaffarianHoseini, A. and Makaremi, N. (2013). The essence of future smart houses: From embedding ICT to adapting to sustainability principles. *Renewable and Sustainable Energy Reviews*, 24, 593-607.
- Giffinger, R., Fertner, C., Kramar, H., Kalasek, R., Pichler-Milanovic, N., & Meijers, E. (2007). Smart Cities: Ranking of European medium-sized cities. Vienna, Austria: Centre of Regional Science (SRF), Vienna University of Technology. http://www.smart-cities.eu/download/smart_cities_final_report.pdf
- Giffinger, R. and Gudrun, H. (2010). Smart cities ranking: An effective instrument for the positioning of cities? *ACE: Architecture, City and Environment*, 4(12), 7-26
- Gil-Garcia, J.R. (2012). Enacting Electronic Government Success. An Integrative Study of Government-wide Websites, Organizational Capabilities, and Institutions (Vol. 31). New York: Springer.
- Gil-Garcia, J.R. (2013). Towards a smart State? Inter-agency collaboration, information integration, and beyond. ICT, Public Administration and Democracy in the Coming Decade, 20, 59-70.
- Gil-Garcia, J.R. and Aldama-Nalda, A. (2013). Making a city smarter through information integration: Angel network and the role of political leadership. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 1724-1733). IEEE.
- Gil-Garcia, J.R., Helbig, N. and Ojo, A. (2014). Being smart: Emerging technologies and innovation in the public sector. *Government Information Quarterly*, 31, 11-18.
- Gil-Garcia, J.R. and Pardo, T.A. (2005). E-government success factors: Mapping practical tools to theoretical foundations. *Government information quarterly*, 22(2), 187-216.
- Giuffrè, T., Siniscalchi, S.M. and Tesoriere, G. (2012). A Novel Architecture of Parking Management for Smart Cities. *Procedia - Social and Behavioral Sciences*,

53,16-28. Available at:

<http://www.sciencedirect.com/science/article/pii/S1877042812043182>.

Glaeser, E.L. and Berry, C.R. (2006). Why Are Smart Places Getting Smarter? *Policy Briefs* (617), pp.1-4. Available at:

http://www.hks.harvard.edu/var/ezp_site/storage/fckeditor/file/pdfs/centers-programs/centers/taubman/brief_divergence.pdf.

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

Goes, J.B. and Park, S.H. (1997). Interorganizational links and innovation: the case of hospital services, *Academy of Management Journal*, 40(3), 673-696.

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

Gope, P. and Hwang, T. (2015). Untraceable Sensor Movement in Distributed IoT Infrastructure.

Gordon, L.A., Loeb, M.P. and Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs? *Journal of Computer Security*, 19(1), 33-56.

Green, S.B. and Salkind, N.J. (2010). Using SPSS for Windows and Macintosh: Analyzing and understanding data. Prentice Hall Press.

Greener, S. (2008). *Business research methods*. BookBoon.

Grübler, A. and Fisk, D. (2013). Energizing Sustainable Cities: Assessing Urban Energy.

Guan, L. (2012). Smart steps to a battery city. *Government News*, 32(2), 24-27.

Gill J. & Johnson P. (2002) "Research methods for managers", Sage.

Guba E. & Lincoln Y. (1994) "Competing paradigms in qualitative research", *Handbook of qualitative research*, 2, pp. 163-194.

- 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*, 29(7), 1645-1660.
- Gurbaxani, V. and Whang, S. (1991). The impact of information systems on organizations and markets. *Communications of the ACM*, 34(1), 59-73.
- Hair Jr, J.F., Hult, G.T.M., Ringle, C. and Sarstedt, M. (2013). *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. SAGE Publications.
- Hair, J. F., Hult, G. T. M., Ringle, C. M., and Sarstedt, M. 2014. *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*. Thousand Oaks, CA: Sage.
- Hair, J.F., Ringle, C.M. and Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing Theory and Practice*, 19(2), 139-152.
- Hair, J. F., Sarstedt, M., Pieper, T. M., & Ringle, C. M. (2012). The use of partial least squares structural equation modeling in strategic management research: a review of past practices and recommendations for future applications. *Long range planning*, 45(5), 320-340.
- Hall, J.H., Sarkani, S. and Mazzuchi, T.A. (2011). Impacts of organizational capabilities in information security. *Information Management & Computer Security*, 19(3), 155-176.
- Hall, P. (2000). Creative cities and economic development. *Urban Studies*, 37(4), 633-649.
- Hall, R.E. (2000). The vision of a smart city. In *Proceedings of the 2nd International Life Extension Technology Workshop*, Paris, France, 28 September. Available at <http://www.osti.gov/bridge/servlets/purl/773961-oyxp82/webviewable/773961.pdf>
- Hameed, M.A., Counsell, S. and Swift, S. (2012). A meta-analysis of relationships between organizational characteristics and IT innovation adoption in organizations. *Information & management*, 49(5), 218-232.
- Hancke, G.P., de Carvalho e Silva, B. and Hancke Jr, G.P. (2012). The role of advanced sensing in smart cities. *Sensors*, 13(1), 393-425.

- Hanseth, O. and Braa, K. (2001). Hunting for the treasure at the end of the rainbow: standardizing corporate IT infrastructure. *Computer Supported Cooperative Work (CSCW)*, 10(3-4), 261-292.
- Harrison, C. and Donnelly, I.A. (2011). A theory of smart cities. In *Proceedings of the 55th Annual Meeting of the ISSS-2011*, Hull, UK (Vol. 55, No. 1).
- 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*, 54(4), 1-16. DOI: 10.1147/JRD.2010.2048257.
- Harwell, M. R. (2011). Research design in qualitative/quantitative/mixed methods. *The Sage handbook for research in education. 2nd ed. Los Angeles, CA: Sage*, 147.
- Hasan, M., Hossain, E. and Niyato, D. (2013). Random access for machine-to-machine communication in LTE-advanced networks: issues and approaches. *IEEE Communications Magazine*, 51(6), 86-93.
- Hawryszkiewicz, I.T. (2014). Cloud Requirements for Facilitating Business Collaboration: A Modeling Perspective. *Journal of Organizational Computing and Electronic Commerce*, 24(2-3), 174-185.
- Henderson, J.C. and Venkatraman, N. (1993). Strategic Alignment: A model for Organizational Transformation through Information Technology. *IBM Systems Journal*, 32(1), 4-16. Available at: <https://pdfs.semanticscholar.org/e840/2b65103442e2517982e5e3eb330f72886731.pdf>.
- Hannan, T. H., & McDowell, J. M. (1984). The determinants of technology adoption: The case of the banking firm. *The RAND Journal of Economics*, 328-335.
- Henseler, J., Ringle, C.M. and Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, 43(1), 115-135.
- Heracleous, L. (2001). What is the impact of corporate governance on organisational performance? *Corporate Governance: An International Review*, 9(3), 165-173.

- Herath, H., and Herath, T. (2008). Investments in Information Security: A Real Options Perspective with Bayesian Post-Audit, *Journal of Management Information Systems*, 25(3), 337-375.
- Herath, T., Herath, H. and Bremser, W.G. (2010). Balanced Scorecard Implementation of Security Strategies: A Framework for It Security Performance Management, *Information Systems Management*, 27(1), 72-81.
- Hernández-Espallardo, M., Rodríguez-Orejuela, A. and Sánchez-Pérez, M. (2010). Inter-organizational governance, learning and performance in supply chains. *Supply Chain Management: An International Journal*, 15(2), 101-114.
- 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*. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 6656, 447-462.
- Hoffer, J.A. and Straub Jr, D.W. (1989). The 9 to 5 underground: are you policing computer crimes? *Sloan Management Review*, 30(4), 35-43.
- Hollands, R.G. (2008). Will the real smart city please stand up? Intelligent, progressive or entrepreneurial? *City*, 12(3), 303-320.
- Hollands, R.G. (2015). Critical interventions into the corporate smart city. *Cambridge Journal of Regions, Economy and Society*, 8(1), 61-77.
- Hong, K-S., Chi, Y-P., Chao, L.R. and Tang, J-H. (2003). An integrated system theory of information security management. *Information Management & Computer Security*, 11(5), 243-248.
- Hovav, A. and D'Arcy, J. (2003). The impact of denial-of-service attack announcements on the market value of firms. *Risk Management and Insurance Review*, 6(2), 97-121.
- HP Fortify (2014). Lack of security in Internet of Things devices. *Network Security*, 2014(8). [online] Available at: <http://www.sciencedirect.com/science/article/pii/S1353485814700753> [Accessed 24 Mar. 2015].

Hrebiniak, L., Joyce, W. and Snow, C. (1989). Strategy, structure, and performance. In Snow, C.C. (Ed.), *Strategy, organization design, and human resource management*, Greenwich, CT: JAI Press, 3-54.

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

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*, 106(2), 242-255.

Hulland, J. (1999). Use of partial least squares (PLS) in strategic management research: a review of four recent studies, *Strategic Management Journal*, 20(2), 195-204.

IBM (2009). Smarter Cities: New York 2009, http://www.ibm.com/smarterplanet/us/en/smarter_cities/article/newyork2009.html.

IBM (2010). Smarter thinking for a smarter planet. Available at http://www.ibm.com/smarterplanet/global/files/us__en_us__loud__ibmlbn0041_trans_tasman_book.pdf.

IESE (2017). *IESE Cities in Motion Index 2017*. Madrid: IESE Business School. <https://www.iese.edu/research/pdfs/ST-0442-E.pdf>.

Info-Communications Development Authority (IDA) Singapore, "iN2015 Masterplan" (2012). <http://www.ida.gov.sg/~media/Files/Infocomm%20Landscape/iN2015/Reports/realisingthevisionin2015.pdf>.

lfinedo, P. (2011). An empirical analysis of factors influencing Internet/e-business technologies adoption by SMEs in Canada. *International Journal of Information Technology & Decision Making*, 10(04), 731-766.

llarri, S., Stojanovic, D. and Ray, C. (2015). Semantic management of moving objects: A vision towards smart mobility. *Expert Systems with Applications*, 42(3), pp.1418–1435. Available at: <http://linkinghub.elsevier.com/retrieve/pii/S0957417414005399>.

- Industry Canada (1998). *Report of the Panel on Smart Communities*. Ottawa, Canada: Government of Canada.
- Industry Canada (1999). *Smart Communities: Program Guide*. Ottawa, Canada: Government of Canada.
- Ishida, T. and Isbister, K. (Eds) (2000). *Digital Cities: Technologies, Experiences, and Future Perspectives* (Vol. 1765). Berlin, Germany: Springer.
- Ittner, C.D. and Larcker, D.F. (2003). Coming up Short on Nonfinancial Performance Measurement, *Harvard Business Review*, 81(11), 88-95.
- Jiwnani, K. and Zelkowitz, M. (2002). Maintaining software with a security perspective. In Proceedings of *Software Maintenance, 2002*, International Conference on (pp. 194-203). IEEE.
- Johnson, P., & Duberley, J. (2000). Understanding management research: An introduction to epistemology. Sage.
- Johnson, M.E. and Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*, 5(3).
- Johnston, A.C. and Hale, R. (2009). Improved Security through Information Security Governance. *Communications of the ACM*, 52(1), 126-129.
- Kahraman, E. (2005). *Evaluating IT Security Performance with Quantifiable Metrics*, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.4000&rep=rep1&type=pdf>.
- Kankanhalli, A., Teo, H.H., Tan, B.C. and Wei, K.K. (2003). An Integrative Study of Information Systems Security Effectiveness. *International Journal of Information Management*, 23(2), 139-154.
- Kaplan, R.S. and Norton, D.P. (1996). *The Balanced Scorecard: translating strategy into action*, Harvard Business School Press, Boston, MA.
- Kayworth, T. R., & Leidner, D. E. (2002). Leadership effectiveness in global virtual teams. *Journal of management information systems*, 18(3), 7-40.
- Kasperksy Lab (2015). Carbanak APT: The Great Bank Robbery. *Securelist*, available at: <http://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/>

- Kaye Nijaki, L. and Worrel, G. (2012). Procurement for sustainable local economic development. *International Journal of Public Sector Management*, 25(2), 133-153.
- Kayworth, T. and Whitten, D. (2010). Effective Information Security Requires a Balance of Social and Technology Factors. *MIS Quarterly Executive*, 9(3), 163-175.
- Kerlinger, F.N. (1979). *Behavioral research: A conceptual approach*. New York: Holt, Rinehart and Winston.
- Keung, C.C. (2009). Revitalizing teacher leadership via bureaucratic-professional practices: A structural equation model. *The Asia-Pacific Education Researcher*, 18(2), 283-295.
- Kitchin, R. (2014). The real-time city? Big data and smart urbanism. *GeoJournal*, 79(1), 1-14.
- Kline, R.B. (2011). *Principles and practice of structural equation modeling*. New York: Guilford Press.
- Knapp, K.J., Marshall, T.E., Rainer, R.K., and Ford, N.F. (2006). Information Security: Management's Effect on Culture and Policy, *Information Management and Computer Security*, 14(16), 24-36.
- Knapp, K.J., Morris Jr, R.F., Marshall, T.E. and Byrd, T.A. (2009). Information Security Policy: An Organizational-Level Process Model, *Computers & Security*, 28(7), 493-508.
- Komninos, N. (2002). *Intelligent Cities: Innovation, Knowledge Systems and Digital Spaces*, 1st edition. London: Routledge.
- Komninos, N. (2006). The architecture of intelligent cities. *Intelligent Environments*, 6, 53-61.
- Komninos, N. (2008). Intelligent cities: Towards interactive and global innovation environments. *International Journal of Innovation and Regional Development*, 1(4), 337-355.
- Kourtit, K. and Nijkamp, P. (2012). Smart cities in the innovation age. *Innovation: The European Journal of Social Science Research*, 25(2), 93-95.

- Kourtit, K., Nijkamp, P. and Arribas, D. (2012). Smart cities in perspective – a comparative European study by means of self-organizing maps. *Innovation: The European Journal of Social Science Research*, 25(2), 229-246.
- Kožuch, B. and Sienkiewicz-Małyjurek, K. (2016). Factors of effective inter-organizational collaboration: a framework for public management. *Transylvanian Review of Administrative Sciences*, 12(47), 97-115.
- KPMG (2015). *Dubai - a new paradigm for smart cities*. Available at: <https://www.kpmg.com/AE/en/Documents/Dubai%20A%20new%20paradigm%20for%20smart%20cities.pdf>
- Kramers, A., Höjer, M., Lövehagen, N. and Wangel, J. (2014). Smart sustainable cities—Exploring ICT solutions for reduced energy use in cities. *Environmental Modelling & Software*, 56, 52-62.
- Kuk, G. and Janssen, M. (2011). The business models and information architectures of smart cities. *Journal of Urban Technology*, 18(2), 39-52.
- Kulatunga K., Amaratunga R. & Haigh R. (2007) “Researching construction client & innovation: methodological perspective”, *USIR, Salford*.
- Lam, W. (2005). Barriers to e-government integration. *Journal of Enterprise Information Management*, 18(5), 511-530.
- Landry, C. (2000). *The Creative City: A Toolkit for Urban Innovation*. London: Earthscan.
- Lanza, J., Sánchez, L., Muñoz, L., Galache, J.A., Sotres, P., Santana, J.R. and Gutiérrez, V. (2015). Large-Scale Mobile Sensing Enabled Internet-of-Things Testbed for Smart City Services. *International Journal of Distributed Sensor Networks*, 11(8), 785061.
- Laryea, E.T. (1999). The technological challenges facing developing countries in the move to paperless international trade, *Bond Law Review*, 11(2), 10.
- Lazaroiu, G.C. and Roscia, M. (2012). Definition methodology for the smart cities model. *Energy*, 47(1), 326-332.

- Lee, C.P., Lee, G.G. and Lin, H.F. (2007). The role of organizational capabilities in successful e-business implementation. *Business Process Management Journal*, 13(5), 677-693.
- Lee, S.H., Han, J.H., Leem, Y.T. and Yigitcanlar, T. (2008). Towards ubiquitous city: Concept, planning, and experiences in the Republic of Korea. In Yigitcanlar, T., Velibeyoglu, K. and Baum, S. (Eds), *Knowledge-Based Urban Development : Planning and Applications in the Information Era* (pp. 148- 169). Hershey, PA: IGI Global.
- Lee, S.W., Sarp, S., Jeon, D.J. and Kim, J.H. (2014). Smart water grid: the future water management platform. *Desalination and Water Treatment*, 55(2), 339-346.
- Lee, Y.C., Chu, P.Y. and Tseng, H.L. (2011). Corporate performance of ICT-enabled business process re-engineering. *Industrial Management & Data Systems*, 111(5), 735-754.
- Lewin, A. and Minton, J. (1986). Determining organizational effectiveness: Another look, and an agenda for research. *Management Science*, 32(5), 514-538.
- Leydesdorff, L. and Deakin, M. (2011). The Triple-Helix Model of Smart Cities: A Neo-Evolutionary Perspective. *Journal of Urban Technology*, 18(2), 53-63.
- 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, in *Multimedia Information Networking and Security (MINES)*, 4th International Conference, pp. 91-94. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=6407394.
- Lindskog, H. (2004). Smart communities initiatives. In *Proceedings of the 3rd ISOneWorld Conference* (Las Vegas, NV, Apr 14-16). Available at <http://www.heldag.com/articles/Smart%20communities%20a%20pril%202004.pdf>
- Lindup, K. (1996). The role of information security in corporate governance. *Computers & Security*, 6(15), 477-485.
- Loh, L. and Venkatraman, N. (1992). Diffusion of Information Technology Outsourcing: Influence Sources and the Kodak Effect. *Information Systems Research*, 3(4), 334-358.

- Lombardi, P., Giordano, S., Farouh, H. and Yousef, W. (2012). Modelling the smart city performance. *Innovation: The European Journal of Social Science Research*, 25(2), 137-149.
- Longworth, N. and Osborne, M. (2010). Six Ages towards a Learning Region—A Retrospective. *European Journal of Education*, 45(3), 368-401.
- Lynggaard, P. and Skouby, K.E. (2015). Deploying 5G-Technologies in Smart City and Smart Home Wireless Sensor Networks with Interferences. *Wireless Personal Communications*, 81(4), 1399-1413.
- Ma, Q., Schmidt, M.B. and Pearson, J.M. (2009). An Integrated Framework for Information Security Management, *Review of Business*, 30(1), 58-69.
- Mahizhnan, A. (1999). Smart cities. *Cities*, 16(1), 13-18.
- Malecki, E.J. (2009). Hard and soft networks for urban competitiveness. *Urban Studies*, 39(5-6), 929-945.
- Malek, J.A. (2009). Informative global community development index of informative smart city. In *Proceedings of the 8th WSEAS International Conference on Education and Educational Technology*, Genova, Italy, 17-19 October.
- Maltz, A.C., Shenhar, A.J. and Reilly, R.R. (2003). Beyond the balanced scorecard: Refining the search for organizational success measures. *Long Range Planning*, 36(2), 187-204.
- Marceau, J. (2008). Introduction: Innovation in the city and innovative cities. *Innovation: Management, Policy & Practice*, 10(2-3), 136-145.
- 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 Communication Networks*, 5(9), 987-1005. Available at: <http://onlinelibrary.wiley.com/doi/10.1002/sec.384/abstract>.
- Mark, R. (1996). *Research made simple: A handbook for social workers*. Sage.
- Markovic, D.S., Zivkovic, D., Cvetkovic, D. and Popovic, R. (2012). Impact of nanotechnology advances in ICT on sustainability and energy efficiency. *Renewable*

and *Sustainable Energy Reviews*, 16(5), 2966-2972. Available at:

<http://dx.doi.org/10.1016/j.rser.2012.02.018>.

Markus, M.L. (2004). Technochange management: using IT to drive organizational change, *Journal of Information Technology*, 19(1), 4-20.

Marsa-Maestre, I., Lopez-Carmona, M.A., Velasco, J.R. and Navarro, A. (2008). Mobile agents for service personalization in smart environments. *Journal of Networks*, 3(5), 30-41.

Marsal-Llacuna, M.L., Colomer-Llinàs, J., & Meléndez-Frigola, J. (2014). Lessons in urban monitoring taken from sustainable and livable cities to better address the Smart Cities initiative. *Technological Forecasting and Social Change*, 90, 611-622.

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*, 51(6), 136-141.

Martins, A. and Eloff, J. (2002). Assessing Information Security Culture, *Information Security South Africa (ISSA)*, Johannesburg, South Africa, 1-14.

Martinsons, M., Davison, R. and Tse, D. (1999). The Balanced Scorecard: A Foundation for the Strategic Management of Information Systems, *Decision Support Systems*, 25(1), 71-88.

McAfee, A., Brynjolfsson, E., Davenport, T.H., Patil, D.J. and Barton, D. (2012). Big data. The management revolution. *Harvard Business Review*, 90(10), 60-68.

McDaniel, P. and McLaughlin, S. (2009). Security and privacy challenges in the smart grid. *IEEE Security & Privacy*, (3), 75-77.

McGahan, A.M. and Porter, M.E. (1997). How much does industry matter, really? *Strategic Management Journal*, 18(S1), 15-30.

Wasko, M.M. and Faraj, S. (2005). Why should I share? Examining social capital and knowledge contribution in electronic networks of practice. *MIS Quarterly*, 29(1), 35-57.

- Melville, N., Kraemer, K. and Gurbaxani, V. (2004). Review: Information technology and organizational performance: An integrative model of IT business value. *MIS quarterly*, 28(2), 283-322.
- Menzies, R. (1993). Information systems security. IT strategy for business. London: Pitman Publishing.
- Mercuri, R.T. (2003). Analyzing Security Costs, *Communications of the ACM*, 46(6), 15-18.
- Mohr, J. and Spekman, R. (1994). Characteristics of Partnership Success: Partnership Attributes, Communication Behavior, and Conflict Resolution Techniques. *Strategic Management Journal*, (15:2), pp 135-152.
- Metke, A.R. and Ekl, R.L. (2010). Security Technology for Smart Grid Networks. *IEEE Transactions on Smart Grid*, 1(1), 99-107. Available at: http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=5460903.
- Meyer, A.D. (1991). What is strategy's distinctive competence? *Journal of Management*, 17(4), 821-833.
- Melville S. & Goddard W. (1996) "Research Methodology: An introduction for science & engineering students", *Juta & Co Ltd, Cape Town, South Africa*.
- Moreno, M.V., Zamora, M.A. and Skarmeta, A.F. (2014). User-centric smart buildings for energy sustainable smart cities. *Transactions on Emerging Telecommunications Technologies*, 25(1), 41-55.
- Morgan, R.E. and Strong, C.A. (2003). Business Performance and Dimensions of Strategic Orientation, *Journal of Business Research*, 56(3), 163-176.
- Moser, M.A. (2001). What is smart about the smart communities movement? *EJournal*, 10/11(1), 1-11. Available at <http://www.ucalgary.ca/ejournal/archive/v10-11/v10-11n1Moser-print.html>.
- Moss Kanter, R. and Litow, S.S. (2009). Informed and interconnected: A manifesto for smarter cities. Harvard Business School General Management Unit Working Paper, 09-141. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1420236.

- Moulton, R. and Coles, R. (2003). Applying information security governance. *Computers & Security*, 22(7), 580-584. Available at: <http://www.sciencedirect.com/science/article/pii/S0167404803007053>.
- Mulligan, C.E. and Olsson, M. (2013). Architectural implications of smart city business models: an evolutionary perspective. *IEEE Communications Magazine*, 51(6), 80-85.
- Muriithi, B. W., Mburu, J., & Ngigi, M. (2011). Constraints and determinants of compliance with EurepGap standards: a case of smallholder french bean exporters in Kirinyaga district, Kenya. *Agribusiness*, 27(2), 193-204.
- Murphy, G.B., Trailer, J.W. and Hill, R.C. (1996). Measuring performance in entrepreneurship research. *Journal of Business Research*, 36(1), 15-23.
- Muthen, L.K. and Muthen, B.O. (2002). How to use a Monte Carlo study to decide on sample size and determine power, *Structural Equation Modelling*, 9(4), pp.599-620.
- Nam, T. (2012). Modelling municipal service integration: a comparative case study of New York and Philadelphia 311 systems. Dissertation. University at Albany, State University of New York.
- Nam, T. and Pardo, T.A. (2011a). Conceptualizing smart city with dimensions of technology, people, and institutions. In Proceedings of the 12th Annual International Digital Government Research Conference on Digital Government Innovation in Challenging Times - dg.o '11, p.282. Available at: <http://dl.acm.org/citation.cfm?id=2037556.2037602>
<http://dl.acm.org/citation.cfm?id=2072069.2072100>
<http://dl.acm.org/citation.cfm?doid=2037556.2037602>.
- Nam, T. and Pardo, T. A. (2011b). Smart city as urban innovation: Focusing on management, policy, and context. In *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance* (pp. 185-194). ACM.
- Nam, T. and Pardo, T.A. (2013). Building Understanding of Municipal Service Integration: A Comparative Case Study of NYC311 and Philly311. In *System Sciences (HICSS), 2013 46th Hawaii International Conference on* (pp. 1953-1962). IEEE.

- Nam, T. and Pardo, T.A. (2014). The changing face of a city government: A case study of Philly311. *Government Information Quarterly*, 31, S1-S9.
- Nam, T. and Sayogo, D.S. (2011). Who uses e-government?: examining the digital divide in e-government use, In *Proceedings of the 5th International Conference on Theory and Practice of Electronic Governance* (pp. 27-36), ACM.
- Naphade, M., Banavar, G., Harrison, C., Paraszczak, J. and Morris, R. (2011). Smarter cities and their innovation challenges. *Computer*, 44(6), 32-39.
- Narain Singh, A., Gupta, M.P. and Ojha, A. (2014). Identifying factors of “organizational information security management”. *Journal of Enterprise Information Management*, 27(5), 644-667.
- Neirotti, P., De Marco, A., Cagliano, A.C., Mangano, G. and Scorrano, F. (2014). Current trends in Smart City initiatives: Some stylised facts. *Cities*, 38, 25-36.
- Neuman W. (2005) “Social research methods”,(6th edition). *Pearson, London*.
- Nickerson, J.A. and Silverman, B.S. (2003). Why firms want to organize efficiently and what keeps them from doing so: Inappropriate governance, performance, and adaptation in a deregulated industry. *Administrative science quarterly*, 48(3), 433-465.
- Nijkamp, P. (2008). “*E pluribus unum*”, Research Memorandum, Faculty of Economics, VU University Amsterdam.
- Northstream (2010). *White paper on revenue opportunities*, from <http://northstream.se/white-paper/archive>.
- Nunnally, J.C. and Bernstein, I.H. (1994). *Psychometric theory* (3rd edn). New York: McGraw-Hill.
- Odendaal, N. (2003). Information and communication technology and local governance: Understanding the difference between cities in developed and emerging economies. *Computers, Environment and Urban Systems*, 27(6), 585-607.
- OECD (1996). *The Knowledge-based Economy*. Organisation for Economic Co-operation and development: Paris. Available at: <http://www.oecd.org/sti/sci-tech/1913021.pdf>.

- OECD (2002). OECD Guidelines for the Security of Information Systems and Networks. Towards a Culture of Security. Available at: <http://www.oecd.org/internet/ieconomy/15582260.pdf>.
- OECD (2004). *Definition of ICT*. Available at: <http://stats.oecd.org/glossary/detail.asp?ID=6274>.
- OECD (2005). Oslo manual. Guidelines for collecting and interpreting innovation data.
- OECD (2009). *Smart Sensor Networks: Technologies and Applications for Green Growth*. Available at: <http://www.oecd.org/dataoecd/39/62/44379113.pdf>.
- OECD (2011). M-Government. Mobile technologies for responsive government and connected societies. Technical report, OECD Publishing.
- Ogier, J. (2005). *The response rates for online surveys—a hit and miss affair, 2005* Australasian Evaluations Forum: University Learning and Teaching: Evaluating and Enhancing the Experience, UNSW, Sydney, 28-29 November.
- O'Neill, M. (2014). The Internet of Things: do more devices mean more risks? *Computer Fraud & Security*, 2014(1), 16-17.
- Orlikowski, W.J. and Baroudi, J.J. (1991). Studying information technology in organizations: Research approaches and assumptions, *Information systems research*, 2(1), 1-28.
- Page Hocevar, S., Fann Thomas, G., & Jansen, E. (2006). Building collaborative capacity: An innovative strategy for homeland security preparedness. In *Innovation through collaboration* (pp. 255-274). Emerald Group Publishing Limited.
- Pallant, J. (2013). *SPSS survival manual*. McGraw-Hill Education (UK).
- Pardo, T.A. and Nam, T. (2016). A Comprehensive View of the 21st Century City: Smartness as Technologies and Innovation in Urban Contexts. In *Smarter as the New Urban Agenda* (pp. 1-19). Springer International Publishing.
- Parthiban, P., Zubar, H.A. and Katarar, P. (2013). Vendor selection problem: a multi-criteria approach based on strategic decisions. *International Journal of Production Research*, 51(5), 1535-1548.

- Patel, H., Pettitt, M. and Wilson, J.R. (2012). Factors of Collaborative Working: A Framework for a Collaboration Model, *Applied Ergonomics*, 43(1), 1-26.
- Peltier, T.R. (2002). Information Security Policies, Procedures and Standards, Guidelines for Effective Information Security Management, Auerbach Publications, 1-3.
- Pérez López, S., Manuel Montes Peón, J. and José Vázquez Ordás, C. (2004). Managing knowledge: the link between culture and organizational learning. *Journal of knowledge management*, 8(6), 93-104.
- Pipkin, D.L. (2000). *Information Security: Protecting the Global Enterprise*, 1st edn. Prentice Hall, Upper Saddle River, NJ, USA.
- Piro, G., Cianci, I., Grieco, L.A., Boggia, G. and Camarda, P. (2014). Information centric services in Smart Cities. *Journal of Systems and Software*, 88(1), 169-188. Available at: <http://dx.doi.org/10.1016/j.jss.2013.10.029>.
- Plumb, D., Leverman, A. and McGray, R. (2007). The learning city in a 'planet of slums'. *Studies in Continuing Education*, 29(1), 37-50.
- Posthumus, S. and von Solms, R. (2004). A Framework for the Governance of Information Security, *Computers & Security*, 23(8), 638-646.
- Puhakainen, P. and Siponen, M. (2010). Improving employees' compliance through information systems security training: an action research study. *MIS Quarterly*, 757-778.
- Raymond, L. (1990). Organizational context and information systems success: a contingency approach, *Journal of Management Information Systems*, 6(4), 5-20.
- Reinen, I.J. and Plomp, T. (1997). Information technology and gender equality: a contradiction in terminis? *Computers & Education*, 28(2), 65-78.
- Reverte, C., Gómez-Melero, E. and Cegarra-Navarro, J.G. (2016). The influence of corporate social responsibility practices on organizational performance: evidence from Eco-Responsible Spanish firms. *Journal of Cleaner Production*, 112, 2870-2884.

- Rexwhite Enakrire, T. and Onyenania, O.G. (2007). Factors affecting the development of information infrastructure in Africa. *Library Hi Tech News*, 24(2), 15-20.
- Rios, P. (2012). *Creating "the smart city"*, Doctoral dissertation. Available at http://archive.udmercy.edu:8080/bitstream/handle/10429/393/2008_rios_smart.pdf.
- Ritz, A. (2009). Public service motivation and organizational performance in Swiss federal government. *International review of administrative sciences*, 75(1), 53-78.
- Robson, C. (2002). *Real world research* (2nd edn). Oxford: Blackwell.
- Roman, R., Najera, P. and Lopez, J. (2011). Securing the internet of things. *Computer*, 44(9), 51-58.
- Roscoe, J.T. (1975). *Fundamental research statistics for the behavioral sciences* [by] John T. Roscoe.
- Ross, J.W., Beath, C.M. and Goodhue, D.L. (1996). Develop Long-Term Competitiveness through IT Assets, *Sloan Management Review*, 38(1), 31-42. Available at: <https://sloanreview.mit.edu/article/develop-longterm-competitiveness-through-it-assets/>.
- Rowe, W.G. and Morrow Jr, J.L. (1999). A note on the dimensionality of firm financial performance using accounting, market, and subjective measures. *Canadian Journal of Administrative Sciences*, 16(1), 58-71.
- 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*, 38, 223-234. Available at: <http://www.sciencedirect.com/science/article/pii/S136403211400416X>.
- Rumelt, R.P. (1991). How much does industry matter? *Strategic Management Journal*, 12(3), 167-185.
- Rumelt, R., Schendel, D. and Teece, D. (1994). *Fundamental issues in strategy*. Boston, MA: Harvard

- Sairamesh, J., Lee, A. and Anania, L. (2004). Information cities. *Communications of the ACM*, 47(2), 28-31
- Sambamurthy, V. and Zmud, R.W. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies, *MIS Quarterly*, 23(2), 261-291.
- Sanchez, L., Muñoz, L., Galache, J. A., Sotres, P., Santana, J. R., Gutierrez, V., Ramdhany, R., Gluhak, A., Krco, S., Theodoridis, E. and Pfisterer, D. (2014). SmartSantander: IoT experimentation over a smart city testbed. *Computer Networks*, 61, 217-238.
- Santhanam, R. and Hartono, E. (2003). Issues in Linking Information Technology Capability to Firm Performance, *MIS Quarterly*, 27(1), 125-153.
- Saunders M., Lewis P. & Thornhill A. (2009) "Research methods for business students", (5th edition). *Prentice Hall, Harlow*.
- Saunders, M.N., Saunders, M., Lewis, P. and Thornhill, A. (2011). *Research methods for business students*. 5th edn. Pearson Education India.
- Schaffers, H., Komninos, N., Pallot, M., Trousse, B., Nilsson, M. and Oliveira, A. (2011). Smart Cities and the Future Internet: Towards Cooperation Frameworks for Open Innovation. In Domingue, J., Galis, A., Gavras, A., Zahariadis, T., Lambert, D., Cleary, F., Daras, P., Krco, S., Muller, H., Li, M.S. and Schaffers, H. (Eds): *The Future Internet: Future Internet Assembly*, LNCS 6656, pp. 431–446.
- Schuurman, D., Baccarne, B., De Marez, L. and Mechant, P. (2012). Smart Ideas for Smart Cities: Investigating Crowdsourcing for Generating and Selecting Ideas for ICT Innovation in a City Context. *Journal of Theoretical and Applied Electronic Commerce Research*, 7(3), 49-62.
- Sayogo, D. S., & Gil-Garcia, J. R. (2014, June). Understanding the determinants of success in inter-organizational information sharing initiatives: results from a national survey. In *Proceedings of the 15th Annual International Conference on Digital Government Research*(pp. 100-109). ACM.
- Shapiro, J.M. (2006). Smart cities: quality of life, productivity, and the growth effects of human capital. *The review of economics and statistics*, 88(2), 324-335. Available at: <http://www.mitpressjournals.org/doi/abs/10.1162/rest.88.2.324>.

- Scott, P. G. (1997). Assessing determinants of bureaucratic discretion: An experiment in street-level decision making. *Journal of Public Administration Research and Theory*, 7(1), 35-58.
- Seetharaman, A., Sreenivasan, J., and Boon, L.P. (2006). Critical Success Factors of Total Quality Management, *Quality and Quantity*, 40(5), 675-695.
- Sekaran, U. (2000). *Research Methods for Business: A Skill-building Approach*. USA: John Willey & Sons.
- Sekaran, U. (2003). *Research methods for business*. Hoboken.
- Setis-EU (2012). setis.ec.europa.eu/implementation/technology-roadmap/European-initiative-on-smart-cities.
- Shuaib, K., Khalil, I. and Abdel-Hafez, M. (2013). Communications in smart grid: A review with performance, reliability and security consideration. *Journal of Networks*, 8(6), 1229-1240.
- Sicari, S., Rizzardi, A., Grieco, L. and Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, 76, 146-164. Available at: <http://www.sciencedirect.com/science/article/pii/S1389128614003971>.
- Siemens, (2004). *Stadt der Zukunft*, http://www.siemens.com/innovation/de/publikationen/zeitschriften_pictures_of_the_future/PoF_Fruhjahr_2004/SmartCity.htm.
- Sila, I. (2010). Do organisational and environmental factors moderate the effects of Internet-based interorganisational systems on firm performance? *European Journal of Information Systems*, 19(5), 581-600.
- Sila, I. (2013). Factors affecting the adoption of B2B e-commerce technologies. *Electronic commerce research*, 13(2), 199-236.
- Simonsson, M., Johnson, P. and Ekstedt, M. (2010). The effect of IT governance maturity on IT governance performance. *Information systems management*, 27(1), 10-24.

- Siponen, M.T. and Oinas-Kukkonen, H. (2007). A Review of Information Security Issues and Respective Research Contributions, *ACM SIGMIS Database: The DATABASE for Advances in Information Systems*, 38(1), 60-80.
- Siponen, M., Mahmood, M.A. and Pahlila, S. (2009). Are Employees Putting Your Company at Risk by Not Following Information Security Policies? *Communications of the ACM*, 52(12), 145-147.
- 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*, 19(3), 313-339. DOI: 10.1111/j.1365-2575.2007.00274.x.
- Smith, S. and Jamieson, R. (2006). Determining Key Factors in E-Government Information System Security. *Information systems management*, 23(2), 23-32.
- So, M.W. and Sculli, D. (2002). The role of trust, quality, value and risk in conducting e-business. *Industrial Management & Data Systems*, 102(9), 503-12.
- Söderström, O., Paasche, T. and Klauser, F. (2014). Smart cities as corporate storytelling. *City*, 18(3), 307-320.
- Solanas, A., Patsakis, C., Conti, M., Vlachos, I., Ramos, V., Falcone, F., Postolache, O., Pérez-Martínez, P.A., Di Pietro, R., Perrea, D.N. and Martínez-Ballesté, A. (2014). Smart health: a context-aware health paradigm within smart cities. *IEEE Communications Magazine*, 52(8), 74-81.
- Sonnenreich, W., Albanese, J. and Stout, B. (2006). Return on security investment (ROSI)-a practical quantitative model. *Journal of Research and Practice in Information Technology*, 38(1), 45-56.
- Spears, J.L. and Barki, H. (2010). User Participation in Information Systems Security Risk Management. *MIS quarterly*, 34(3), 503-522.
- Sproull, L. and Patterson, J.F. (2004). Making information cities livable. *Communications of the ACM*, 47(2), 33-37.
- Stanton, J.M., Stam, K.R., Mastrangelo, P. and Jolton, J. (2005). Analysis of end user security behaviors, *Computers & Security*, 24(2), 124-33.

- Steers, R. (1975). Problems in measurement of organizational effectiveness. *Administrative Science Quarterly*, 20, 546-558.
- Stewart, A. (2005). Information Security Technologies as a Commodity Input, *Information Management & Computer Security*, 13(1), 5-15.
- Straub, D.W. (1988). Organizational Structuring of the Computer Security Function, *Computers & Security*, 7(2), 185-195.
- Straub Jr, D.W. (1990). Effective IS Security: An Empirical Study, *Information Systems Research*, 1(3), 255-276.
- Straub Jr, D.W. and Collins, R.W. (1990). Key Information Liability Issues Facing Managers: Software Piracy, Proprietary Databases, and Individual Rights to Privacy, *MIS Quarterly*, 14(2), 143-156.
- Straub, D.W. and Welke, R.J. (1998). Coping with Systems Risk: Security Planning Models for Management Decision Making, *MIS Quarterly*, 22, 441-470.
- Streitz, N. (2009). Ambient intelligence landscapes for realizing the cities of the future: Introduction and overview. In *Proceedings of the 3rd European Conference on Ambient Intelligence*, Salzburg, Austria, 18-21 November. Available at <http://www.smart-future.net/14.html>.
- Su, K., Li, J. and Fu, H. (2011). Smart city and the applications. In *IEEE International Conference on Electronics, Communications and Control (ICECC)*, 1028-1031, IEEE Xplore.
- Suciu, G., Vulpe, A., Halunga, S., Fratu, O., Todoran, G. and Suciu, V. (2013). Smart cities built on resilient cloud computing and secure internet of things. In *Control Systems and Computer Science (CSCS), 2013 19th International Conference on* (pp. 513-518). IEEE.
- Švob-Đokiæ, N. (Ed.) (2007). *The Creative City: Crossing Visions and New Realities in the Region*. Zagreb, Croatia: Institute for International Relations, Available at <http://www.culturelink.org/p>
- Tabachnick, B.G., Fidell, L.S. and Osterlind, S.J. (2001). *Using multivariate statistics*. New York: Pearson.

- Tapscott, D. and Agnew, D. (1999). Governance in the digital economy. *Finance and Development*, 36(4), 34.
- Tavakol, M. and Dennick, R. (2011). Making Sense of Cronbach's Alpha. *International Journal of Medical Education*, 2, 53-55.
- Teo, T.S.H., Srivastava, S.C. and Jiang, L. (2008). Trust and electronic government success: an empirical study. *Journal of Management Information Systems*, 25(3), 99-132.
- Thite, M. (2011). Smart cities: implications of urban planning for human resource development. *Human Resource Development International*, 14(5), 623-631.
- Thomas, R.C., Antkiewicz, M., Florer, P., Widup, S. and Woodyard, M. (2013). How Bad Is It?—A Branching Activity Model to Estimate the Impact of Information Security Breaches. *A Branching Activity Model to Estimate the Impact of Information Security Breaches* (11 March 2013).
- Thuzar, M. (2011). Urbanization in SouthEast Asia: Developing Smart Cities for the Future? *Regional Outlook*, 96.
- Toppeta, D. (2010). The smart city vision: how innovation and ICT can build smart, "livable", sustainable cities. *The Innovation Knowledge Foundation*, 5, 1-9. Available from: http://www.inta-aivn.org/images/cc/Urbanism/background%20documents/Toppeta_Report_005_2010.pdf.
- Tosi, H.L., Werner, S., Katz, J.P. and Gomez-Mejia, L.R. (2000). How much does performance matter? A meta-analysis of CEO pay studies. *Journal of Management*, 26(2), 301-339.
- Tsiakis, T. and Stephanides, G. (2005). The economic approach of information security. *Computers & security*, 24(2), 105-108.
- Tu, Z. and Yuan, Y. (2014). Critical Success Factors Analysis on Effective Information Security Management: A Literature Review.
- Udo, G.J. and Edoho, F.M. (2000). Information Technology Transfer to African Nations: An Economic Development Mandate. *Journal of Technology Transfer*, 25(3), 329-342.

- UNESCAP (2007). *Good Governance*. UNESCAP. Available at:
<http://www.unescap.org/pdd/prs/ProjectActivities/Ongoing/gg/governance.asp>.
- United Nations (2014). *World urbanization prospects*. Available at:
<http://esa.un.org/unpd/wup/FinalReport/WUP2014-Report.pdf>
- Van Bastelaer, B. (1998). Digital Cities and transferability of results. In the *Proceedings of the 4th EDC Conference on Digital Cities*, Salzburg (pp. 61-70).
- Van Niekerk, J.F. and Von Solms, R. (2010). Information Security Culture: A Management Perspective, *Computers & Security*, 29(4), 476-486.
- Van Teijlingen, E.R. and Hundley, V. (2001). The importance of pilot studies. *Social Research Update*, 35.
- Vassileva, I., Dahlquist, E., Wallin, F. and Campillo, J. (2013). Energy consumption feedback devices' impact evaluation on domestic energy use. *Applied Energy*, 106, 314-320.
- Venkatraman, N. and Ramanujam, V. (1986). Measurement of business performance in strategy research: A comparison of approaches. *Academy of Management Review*, 11(4), 801-814.
- Vermeulen, C. and von Solms, R. (2002). The information security management toolbox – taking the pain out of security management, *Information Management & Computer Security*, 10(2/3), 119-125.
- 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*, 51(6), 128-134.
- Von Solms, B. (2001). Corporate governance and information security. *Computers & Security*, 20(3), 215-218.
- von Solms, B. (2005). Information Security governance: COBIT or ISO 17799 or both? *Computers & Security*, 24(2), 99-104.
<http://www.sciencedirect.com/science/article/pii/S0167404805000210>.

von Solms, B. and von Solms, R. (2004). The 10 deadly sins of information security management. *Computers & Security*, 23(5), 371-376. Available at: <http://www.sciencedirect.com/science/article/pii/S0167404804001221>.

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

Von Solms, R. (1999). Information Security Management: Why Standards Are Important, *Information Management & Computer Security*, 7(1), 50-58.

Walravens, N. (2012). Mobile business and the smart city: developing a business model framework to include public design parameters for mobile city services. *Journal of Theoretical and Applied Electronic Commerce Research*, 7(3), 121-135.

Waltz, C.F. and Bausell, B.R. (1981). Nursing research: design statistics and computer analysis. Davis FA.

Wand Y. & Weber R. (1993) "On the ontological expressiveness of information systems analysis & design grammars", *Information Systems Journal*, 3(4), pp. 217-237.

Wang, W. and Lu, Z. (2013). Cyber security in the Smart Grid: Survey and challenges. *Computer Networks*, 57(5), 1344-1371. Available at: <http://www.sciencedirect.com/science/article/pii/S1389128613000042>.

Want, R., Schilit, B.N. and Jenson, S. (2015). Enabling the Internet of Things. *Computer*, 48(1), 28-35.

Washburn, D., Sindhu, U., Balaouras, S., Dines, R.A., Hayes, N.M. and Nelson, L.E. (2010). Helping CIOs Understand "Smart City" Initiatives: Defining the Smart City, Its Drivers, and the Role of the CIO. Cambridge, MA: Forrester Research, Inc. Available at http://public.dhe.ibm.com/partnerworld/pub/smb/smarterplanet/forr_help_cios_und_smart_city_initiatives.pdf.

Weber, C.A., Current, J.R. and Benton, W.C. (1991). Vendor selection criteria and methods. *European Journal of Operational Research*, 50(1), 2-18.

- Weber, R. (2010). Internet of Things – New security and privacy challenges. *Computer Law & Security Review*, 26(1), 23-30.
- Weerakkody, V., El-Haddadeh, R., Al-Sobhi, F., Shareef, M.A. and Dwivedi, Y.K. (2013). Examining the influence of intermediaries in facilitating e-government adoption: An empirical investigation. *International Journal of Information Management*, 33(5), 716-725.
- Weill, P. (2004). Don't just lead, govern: how top-performing firms govern IT, *MIS Quarterly Executive*, 3(1), 1-17.
- Weill, P. and Ross, J. (2004). IT governance: how top managers manage IT decision rights for superior results, Harvard Business School Press, Boston.
- Werlinger, R., Hawkey, K. and Beznosov, K. (2009). An integrated view of human, organizational, and technological challenges of IT security management. *Information Management & Computer Security*, 17(1), 4-19.
- Westerlind, K. (2004). *Evaluating return on information technology investment*. Masters' Thesis, School of Economics and Commercial Law, Gothenburg University.
- Whitmore, A., Agarwal, A. and Da Xu, L. (2014). The Internet of Things-A survey of topics and trends. *Information Systems Frontiers*, 17(2), 1-14.
- Wiengarten, F., Humphreys, P., Cao, G. and McHugh, M. (2013). Exploring the important role of organizational factors in IT business value: Taking a contingency perspective on the resource-based view. *International Journal of Management Reviews*, 15(1), 30-46.
- Williams, P. (2001). Information security governance. *Information Security Technical Report*, 6(3), 60-70. Available at: <http://www.sciencedirect.com/science/article/pii/S1363412701003090>.
- Willke, H. (2007). *Smart Governance. Governing the Global Knowledge Society*. Frankfurt am Main and New York: Campus.
- Wind, Y., & Robinson, P. J. (1968). The determinants of vendor selection: the evaluation function approach. *Journal of Purchasing and Materials Management*, 4(3), 29-41.

- Winters, J.V. (2011). Why are smart cities growing? Who moves and who stays. *Journal of Regional Science*, 51(2), 253-270.
- Woo, C.Y. and Willard, G. (1983). *Performance representation in business policy research: Discussion and recommendation*. Paper presented at Academy of Management meetings, Dallas, TX.
- Yang, S-M., Yang, M-H. and Wu, J-T.B. (2005). The impacts of establishing enterprise information portals on e-business performance, *Industrial Management & Data Systems*, 105(3), 349-68.
- Yang, T.M. and Maxwell, T.A. (2011). Information-sharing in public organizations: A literature review of interpersonal, intra-organizational and inter-organizational success factors. *Government Information Quarterly*, 28(2), 164-175.
- Yigitcanlar, T. and McCartney, R. (2010). Strategising knowledge-based urban development: Knowledge city transformations of Brisbane, Australia. In *Proceedings of the 14th International Planning History Society (IPHS) Conference*, Istanbul, Turkey, 12-15 July.
- Yigitcanlar, T. and Velibeyoglu, K. (2008). Knowledge-based urban development: The local economic development path of Brisbane, Australia. *Local Economy*, 23(3), 195-207.
- Yigitcanlar, T., O'Connor, K. and Westerman, C. (2008a). The making of knowledge cities: Melbourne's knowledge-based urban development experience. *Cities*, 25(2), 63-72.
- Yigitcanlar, T., Velibeyoglu, K. and Martinez-Fernandez, C. (2008b). Rising knowledge cities: The role of urban knowledge precincts. *Journal of Knowledge Management*, 12(5), 8-20.
- Yildirim, E.Y., Akalp, G., Aytac, S., and Bayram, N. (2011). Factors influencing information security management in small-and medium-sized enterprises: A case study from Turkey, *International Journal of Information Management*, 31(4), 360-365.
- Yoshikawa, Y. (2012). Hitachi's Vision of the Smart City. *Hitachi Review*, 61(3), 111-118.

- Yovanof, G.S. and Hazapis, G.N. (2009). An architectural framework and enabling wireless technologies for digital cities & intelligent urban environments. *Wireless Personal Communications*, 49(3), 445-463. Available at <http://www.springerlink.com/content/g1v63025217mt8x0/>.
- Zafar, H. and Clark, J.G. (2009). Current state of information security research in IS. *Communications of the Association for Information Systems*, 24, 557-596. Available at: <http://aisel.aisnet.org/cais/vol24/iss1/34>.
- Zammuto, R.F. (1984). A comparison of multiple constituency models of organizational effectiveness. *Academy of Management Review*, 9(4), 606-616.
- Zanella, A., Bui, N., Castellani, A., Vangelista, L. and Zorzi, M. (2014). Internet of things for smart cities. *IEEE Internet of Things Journal*, 1(1), 22-32.
- Zhang, J., Dawes, S.S. and Sarkis, J. (2005). Exploring stakeholders' expectations of the benefits and barriers of e-Government knowledge sharing. *The Journal of Enterprise Information Management*, 18(5), 548-567.
- Zygiaris, S. (2013). Smart city reference model: Assisting planners to conceptualize the building of smart city innovation ecosystems. *Journal of the Knowledge Economy*, 4(2), 217-231.

APPENDICES

Appendix I Smart city table of definitions

Source	Definition
Marsal-Llacuna et al. (2014)	“Smart Cities initiatives try to improve urban performance by using data, information and information technologies (IT) to provide more efficient services to citizens, to monitor and optimize existing infrastructure, to increase collaboration among different economic actors, and to encourage innovative business models in both the private and public sectors.”
Zygiaris (2013)	“A smart city is understood as a certain intellectual ability that addresses several innovative socio-technical and socio-economic aspects of growth. These aspects lead to smart city conceptions as “green” referring to urban infrastructure for environment protection and reduction of CO ₂ emission, “interconnected” related to revolution of broadband economy, “intelligent” declaring the capacity to produce added value information from the processing of city’s real-time data from sensors and activators, whereas the terms “innovating”, “knowledge” cities interchangeably refer to the city’s ability to

	raise innovation based on knowledgeable and creative human capital.”
Bakıcı et al. (2013)	“Smart city is a high-tech intensive and advanced city that connects people, information and city elements using new technologies in order to create a sustainable, greener city, competitive and innovative commerce, and an increased life quality.”
Barrionuevo et al. (2012)	“Being a smart city means using all available technology and resources in an intelligent and coordinated manner to develop urban centers that are at once integrated, habitable, and sustainable.”
Guan (2012)	“A smart city, according to ICLEI, is a city that is prepared to provide conditions for a healthy and happy community under the challenging conditions that global, environmental, economic and social trends may bring.”
Kourtiti and Nijkamp (2012)	“Smart cities are the result of knowledge-intensive and creative strategies aiming at enhancing the socio-economic, ecological, logistic and competitive performance of cities. Such smart cities are based on a promising mix of human capital (e.g. skilled labor force), infrastructural capital (e.g. high-tech communication facilities), social capital (e.g. intense and open network linkages) and entrepreneurial capital (e.g. creative and risk-taking business activities).”
Kourtiti et al. (2012)	“Smart cities have high productivity as they have a relatively high share of highly educated people, knowledge-intensive jobs, output-oriented planning systems, creative activities and sustainability-oriented initiatives.”

Cretu (2012)	“Two main streams of research ideas: 1) smart cities should do everything related to governance and economy using new thinking paradigms and 2) smart cities are all about networks of sensors, smart devices, real-time data, and ICT integration in every aspect of human life.”
IDA (2012)	“Smart city [refers to] a local entity - a district, city, region or small country -which takes a holistic approach to employ[ing] information technologies with real-time analysis that encourages sustainable economic development.”
Lazaroiu and Roscia (2012)	“A community of average technology size, interconnected and sustainable, comfortable, attractive and secure.”
Lombardi et al. (2012)	“The application of information and communications technology (ICT) with their effects on human capital/education, social and relational capital, and environmental issues is often indicated by the notion of smart city.”
Komninos (2006)	“(Smart) cities as territories with high capacity for learning and innovation, which is built-in the creativity of their population, their institutions of knowledge creation, and their digital infrastructure for communication and knowledge management.”
Caragliu et al. (2011)	“A city is smart when investments in human and social capital and traditional (transport) and modern (ICT) communication infrastructure fuel sustainable economic growth and a high quality of life, with a wise management of natural resources, through participatory governance.”
Gartner Inc. (2011)	“A smart city is based on intelligent exchanges of information that flow between its many different subsystems. This flow of information is analyzed and translated into citizen and

	commercial services. The city will act on this information flow to make its wider ecosystem more resource- efficient and sustainable. The information exchange is based on a smart governance operating framework designed to make cities sustainable.”
Nam and Pardo (2011a)	“A smart city infuses information into its physical infrastructure to improve conveniences, facilitate mobility, add efficiencies, conserve energy, improve the quality of air and water, identify problems and fix them quickly, recover rapidly from disasters, collect data to make better decisions, deploy resources effectively, and share data to enable collaboration across entities and domains.”
Thite (2011)	“Creative or smart city experiments [, etc.] aimed at nurturing a creative economy through investment in quality of life which in turn attracts knowledge workers to live and work in smart cities. The nexus of competitive advantage has [, etc.] shifted to those regions that can generate, retain, and attract the best talent.”
Thuzar (2011)	<p>“Smart cities of the future will need sustainable urban development policies where all residents, including the poor, can live well and the attraction of the towns and cities is preserved.”</p> <p>“Smart cities are cities that have a high quality of life; those that pursue sustainable economic development through investments in human and social capital, and traditional and modern communications infrastructure (transport and information communication technology); and manage natural resources through participatory policies. Smart cities should also be sustainable, converging economic, social, and environmental goals.”</p>

Harrison et al. (2010)	“A city connecting the physical infrastructure, the IT infrastructure, the social infrastructure, and the business infrastructure to leverage the collective intelligence of the city.”
Chen (2010)	“Smart cities will take advantage of communications and sensor capabilities sewn into the cities’ infrastructures to optimize electrical, transportation, and other logistical operations supporting daily life, thereby improving the quality of life for everyone.”
Washburn et al. (2010)	“The use of Smart Computing technologies to make the critical infrastructure components and services of a city—which include city administration, education, healthcare, public safety, real estate, transportation, and utilities—more intelligent, interconnected, and efficient.”
Toppeta, 2010	“A city combining ICT and Web 2.0 technology with other organizational, design and planning efforts to de-materialize and speed up bureaucratic processes and help to identify new, innovative solutions to city management complexity, in order to improve sustainability and livability.”
Eger (2009)	“Smart community – a community which makes a conscious decision to aggressively deploy technology as a catalyst to solving its social and business needs – will undoubtedly focus on building its high-speed broadband infrastructures, but the real opportunity is in rebuilding and renewing a sense of place, and in the process a sense of civic pride. [, etc.] Smart communities are not, at their core, exercises in the deployment and use of technology, but in the promotion of economic development, job growth, and an increased quality of life. In other words, technological propagation of smart communities isn’t an end in itself, but only a means to reinventing cities for a

	new economy and society with clear and compelling community benefit.”
Giffinger et al. (2007)	“A city well performing in a forward-looking way in economy, people, governance, mobility, environment, and living, built on the smart combination of endowments and activities of self-decisive, independent and aware citizens. Smart city generally refers to the search and identification of intelligent solutions which allow modern cities to enhance the quality of the services provided to citizens.”
Hall (2000)	“A city that monitors all its critical infrastructures, including roads, bridges, tunnels, rails, subways, airports, seaports, communications, water, power, even major buildings, and integrates conditions and actions in order to optimize its resources, plan its preventive maintenance activities, and monitor security aspects. All these with respect to maximizing the efficiency of services provided to its citizens.”

Source: Devised by author

Appendix II LinkedIn message

-----LinkedIn Message-----

Hi Mr/Ms/Dr/Prof X,

Hope you're well, I am doing an organisational survey part of a PHD research on “smart cities information security management” and hope for your participation as a fellow information security professional. The questionnaire requires 8-10 minutes to complete, fully anonymous and approved by Brunel University London:

<https://goo.gl/forms/1nFRXsrFhYBIPjgC2>

Hope to hear from you,

Best regards,

Mohamad Amin Hasbini

-PHD candidate, Brunel University London

-Senior Security Researcher, Kaspersky Lab

-Board member, SecuringSmartCities

-DNS security review team, ICANN

-----Linkedin Message-----

Appendix III Research survey/questionnaire

-----Research Questionnaire-----

You are invited to participate in this survey, I am a PhD scholar of Management Sciences, conducting a survey on “***Investigating The Organisational Factors Influencing Information Security Management In The Context of Smart City Organisations***” to complete my Ph.D. dissertation. Your responses are of high importance and this effort is part of a PhD research study. The survey comprises different kinds of questions, there is no right or wrong answer to the questions, I am only interested in your personal opinions. This survey will require 8-10minutes of your time.

Why have I been selected? - You have been selected as you possess information security skills and a current related role in your organisation.

Will my information be protected? - No personal identifying information will be collected in this survey. Responses data will not be published in raw and will be treated with confidentiality (encryption and complex passwords). Responses data will be destroyed in a non-recoverable manner once the research purpose of the study is attained.

What are the possible benefits of taking part in this survey? - we cannot promise that participating in this survey will provide you with any direct benefits, we hope to identify the organisational factors that most influence Information Security Management in smart city organisations, to help organisations better prepare for smart cities. If desired, you can request a summary of the results when the study is complete.

What are the possible disadvantages and risks of taking part in this survey? -

Taking part in this survey or not, will not pose risks, impact or disadvantage on you anyhow. The study will take up some of your time, which might be an inconvenience (8min to 10min estimated).

What if something goes wrong? How can I complain? - If you wish to complain

about the experience of this survey or anything else, please contact Professor Thomas Betteridge: Thomas.Betteridge@brunel.ac.uk, Chair of the College of Business, Arts and Social Sciences Research Ethics Committee, Brunel University London.

Who is organising and funding this research? - This research is primarily conducted by Mohamad Amin Hasbini (PHD candidate, College of Business, Arts and Social Sciences, Brunel University), supervised by Dr Tillal Eldabi (College of Business, Arts and Social Sciences, Brunel University)) in conjunction with the Business School, Brunel University London. This research is not funded.

Who has reviewed the study? - This study has been reviewed and approved by the Research Ethics Committee at the Brunel University London.

Passage on the University's commitment to the UK Concordat on Research

Integrity: Brunel University is committed to compliance with the Universities UK Research Integrity Concordat. You are entitled to expect the highest level of integrity from our researchers during the course of their research.

For further information, you can contact:

- Mr Mohamad Amin Hasbini, mohamad.hasbini@brunel.ac.uk
- Dr Tillal Eldabi, Tillal.eldabi@brunel.ac.uk

Your involvement in this study is voluntary, and the decision to take part is yours. By clicking on "Next" you are consenting to participate and have the right to withdraw at any time.

Introduction

As cities become smarter, they employ the ICT infrastructure to the development of citizens living quality and growth. Information Security management is one of the most important challenges for smart cities organisational performance. This

research is attempting to identify the organisational factors that most influence Information Security Management in some of the smartest world cities. The goal is to help organisations have a sense of priorities towards better preparing and developing their strategies for smart city presence.

Section A: General Information

Age group: Less than 25 25 to 35 More than 35

Gender: Male Female

My Information Security Role inside my organisation is:

Security management, Risk, Audit, Policy

Technical, Specialist, Architect

Chief, Executive, Director

Size of my organisation: (number of employees)

<50

50 to 250

250+

My organisation belongs to the:

Public sector

Financial services

Integrator services

Telecommunications

Industrial/manufacturing

International or Multinational

Other

I am based in _____ city

My organisation is based in _____ city

I am reporting to my organisation's office in _____ city

Sections B to M: Please rate each statement in terms of the degree of agreement with each statement; encircle appropriate response based on the following scale

SCALE:

[1= Disagree] [2=Somewhat Disagree] [3=Neither Agree nor Disagree]

[4=Somewhat Agree] [5=Agree]

#	Section B: Organisational Performance	1	2	3	4	5
1	My organisation is experiencing an integral improvement in the finance and performance (e.g. sales, profits, etc.)					
2	My organisation is experiencing an integral improvement in its relationship with its customers (e.g. market share, customer satisfaction, etc.)					
3	My organisation is experiencing an integral improvement in human resources development (e.g. employee skills, personnel development, etc.)					
4	My organisation is experiencing an integral improvement in preparing for the future (e.g. quality/depth of strategic planning, indicators of partnerships, preparing for changes in the environment, products and services, etc.)					
	Section C: Information Security Management	1	2	3	4	5
5	My organisation has a continuously well-documented and continuously updated information security policy, disaster recovery and business continuity plan documents.					
6	My organisation routinely conducts internal and external (third party) information security audits					

7	My organisation has a continuously updated inventory record of all the information assets (hardware and software)					
8	My organisation has an access control policy that clearly details which users have access to what data					
9	My organisation takes disciplinary action against employees violating the information security rules/policy					
10	My organisation cannot survive a disaster that may result in the loss of systems, premises, etc.					
	Section D: Leadership Attitude	1	2	3	4	5
11	Senior executives regard the significance of information security					
12	Senior executives attend information security meetings, are involved in decisions, and are open to the needed changes					
13	Senior executives praise good performance and provide regular feedback on job performance and behaviour					
	Section E: Legislative Influence	1	2	3	4	5
14	My organisation complies with information security legislations					
15	Senior Leadership regard the significance of complying with information security legislations					
16	Employees in my organisation could be legally liable in case of information security failure					
17	There is a team/committee in my organisation for monitoring compliance with data protection laws/legislations					

	Section F: Adaptation to Rapid Technology Development	1	2	3	4	5
18	The rapid adoption of smart/e-business technologies helps in increasing our revenues/profits and reducing costs					
19	Management recognizes the need and supports the use of the latest smart/e-business technologies in our operations					
20	Our customers and partners are demanding the use of the latest smart/e-business technologies in doing business with them.					
21	We know our suppliers and partners are ready to do business over using the latest smart/e-business technologies.					
	Section G: Vendor Selection	1	2	3	4	5
22	My organisation emphasises the vendor solutions quality rather than the cost of purchase or friendships with the vendor					
23	My organisation combines solutions from different vendors in the implementation of products, services and their security					
24	My organisation selects technology vendor based on its potential to support a competitive advantage and position					
25	My organisation evaluates different vendors to find best matching and most secure offerings for the organisation					
	Section H: Skilful Workforce	1	2	3	4	5
26	My organisation conducts regular information security trainings for general and technical employees					

27	My organisation makes sure all employees are vigilant toward information security					
28	My organisation employs the personnel with the right skills in the right role/position					
29	My organisation does not face a shortage of information security skilled labour					
	Section I: Better utilization of the ICT (Information and Communication Technologies) infrastructure	1	2	3	4	5
30	My organisation acknowledges the need to best utilize the ICT infrastructure provided by the Telco					
31	My organisation analyses the quality of service received from the ICT infrastructure provider (Internet/Data/Voice...)					
32	My organisation has a team/committee to evaluate ICT service provider service quality					
	Section J: Type of Organisation	1	2	3	4	5
33	The type of industry my organisation belongs to, influences the measures needed to protect services and clients/partners data					
34	The type of industry my organisation belongs to, influences the speed with which cybersecurity incidents need to be handled					
35	The type of industry my organisation belongs to, influences the information security legislations it needs to comply with					
36	The type of industry my organisation belongs to, influences the information security skills level needed to defend it					
	Section K: Bureaucracy	1	2	3	4	5

37	My organisation speed of change is at par with leading organisations					
38	My organisation exerts tight control and standardized administrative practices in controlling, monitoring and delivering its core products/services					
39	My organisation is adopting innovative solutions to reduce internal processes complexity (e-documents, automated workflow, business intelligence)					
	Section L: Employees compliance to organisational policies	1	2	3	4	5
40	Employees inside my organisation, are required to comply with the information security policies and legislations					
41	Employees inside my organisation, believe the information security policies are well developed to help in the protection of assets					
42	Employees inside my organisation, will comply with the information security policy, even if faced with urgent or critical issues.					
	Section M: Intra-organisational collaboration	1	2	3	4	5
43	The respect and preservation of different points of view internally is encouraged in my organisation.					
44	The collaboration and co-operation among the different duties and departments is encouraged.					
45	My organisation has a team/committee for conducting regular meetings in between the different departments to consolidate efforts against cyber threats					
	Section N: Inter-organisational collaboration	1	2	3	4	5

46	My organisation considers individuals as an asset and tries to appreciate them continuously.					
47	Collaboration and co-operation with other organisations is encouraged and monitored					
48	My organisation has a team/committee for conducting regular meetings with other organisations towards better threat information sharing and collaboration.					

Appendix IV: Research ethics approval



College of Business, Arts and Social Sciences Research Ethics Committee
Brunel University London
Kingston Lane
Uxbridge
UB8 3PH
United Kingdom
www.brunel.ac.uk

3 August 2017

LETTER OF APPROVAL

Applicant: Mr Mohamad Amin Hasbini
Project Title: Information Security Management in Smart City Organizations³
Reference: 7296-LR-Aug/2017 - 8023-1

Dear Mr Mohamad Amin Hasbini

The Research Ethics Committee has considered the above application recently submitted by you.

The Chair, acting under delegated authority has agreed that there is no objection on ethical grounds to the proposed study. Approval is given on the understanding that the conditions of approval set out below are followed:

- The agreed protocol must be followed. Any changes to the protocol will require prior approval from the Committee by way of an application for an amendment.

Please note that:

- Research Participant Information Sheets and (where relevant) flyers, posters, and consent forms should include a clear statement that research ethics approval has been obtained from the relevant Research Ethics Committee.
- The Research Participant Information Sheets should include a clear statement that queries should be directed, in the first instance, to the Supervisor (where relevant), or the researcher. Complaints, on the other hand, should be directed, in the first instance, to the Chair of the relevant Research Ethics Committee.
- Approval to proceed with the study is granted subject to receipt by the Committee of satisfactory responses to any conditions that may appear above, in addition to any subsequent changes to the protocol.
- The Research Ethics Committee reserves the right to sample and review documentation, including raw data, relevant to the study.
- You may not undertake any research activity if you are not a registered student of Brunel University or if you cease to become registered, including abeyance or temporary withdrawal. As a deregistered student you would not be insured to undertake research activity. Research activity includes the recruitment of participants, undertaking consent procedures and collection of data. Breach of this requirement constitutes research misconduct and is a disciplinary offence.

A handwritten signature in black ink, appearing to read 'Tom Betteridge'.

Professor Thomas Betteridge

Chair

College of Business, Arts and Social Sciences Research Ethics Committee
Brunel University London