Association for Information Systems
AIS Electronic Library (AISeL)

Research-in-Progress Papers | ECIS 2016 Proceedings

Summer 6-15-2016

COMPETENCE-BASED MODEL FOR SECURING THE IN-TERNET OF THINGS IN ORGANIZATIONS

Rui Silva
Lisbon School of Economics & Management, rui.silva@aln.iseg.ulisboa.pt

Gurpreet Dhillon
Virginia Commonwealth University, gdhillon@vcu.edu

Winnie Picoto
Lisbon School of Economics & Management, w.picoto@iseg.ulisboa.pt

COMPETENCE-BASED MODEL FOR SECURING THE INTERNET OF THINGS IN ORGANIZATIONS

Research in Progress

Silva, Rui, Lisbon School of Economics & Management, Portugal, rui.silva@aln.iseg.ulisboa.pt

Dhillon, Gurpreet, Virginia Commonwealth University, Richmond, VA, USA, gdhillon@vcu.edu

Picoto, Winnie, Lisbon School of Economics & Management, Portugal, w.picoto@iseg.ulisboa.pt

Abstract

The next generation in computing transcends the paradigm of traditional desktop and client-server architectures. IT products and solutions of the third platform, specifically in the scope of the Internet of Things (IoT) raise new security threats and vulnerabilities, suggesting that a set of competences is needed for any IoT product or service, regarding information security. The knowledge of that set of skills allows top managers to properly assess current organizational competences against future requirements, allowing proper business realignment.

The paper at hand aims to contribute to the topic state of the art both at academic and practical level by developing a Competence-based Model for Securing the Internet of Things. The construction of the Model aims to define and develop organizational competence, specifically in the context of organizations that are IoT service providers.

The model, to be developed and empirically tested using the Design Science Paradigm, will be based on an existing model that defines competence from a strategic management perspective using Resource Based View theory, strategic management theory and the concept of collective mind as heedful interrelating.

Keywords: Information Security, Internet of Things, Organizational Competence, Competence-based Model.

1 Introduction

The next generation in computing transcends the paradigm of traditional desktop and client-server architectures (Gubbi et al., 2013). The IT industry has been directing most of its products to key areas that have transformed the sector radically. IT companies and consultants designate this new paradigm by *the third platform*, which is a new business model approach grounded on a cluster of products and services based on 4 pillars: (1) Cloud Computing, (2) Mobility, (3) Big Data and (4) Social Media (Gens, 2013).

Internet usage has been growing in a very solid manner. In fact, in the end of 2011, internet users exceeded 2.2 billion. The number of devices connected to the internet overcame 6.8 billion (the world population in 2010) between 2003 and 2010. It is expected that in 2020 the number of devices connected to the internet reaches the value of 50 billion (Mukhopadhyay, 2014). These impressive figures support the hypothesis that the IoT will have an inevitable development in the near future, having a major impact on people's lives and global economy. The IoT paradigm still has many unexplored potentialities (Mukhopadhyay, 2014; Bassi & Biswas, 2012) and Sensors and Radio Frequency Identification (RFID) technologies will suffer a very large development (Gubbi et al., 2013). Just like in the beginning of the internet, the IoT has been defined in its own development process (Bassi & Biswas, 2012) and it is being

influenced by computational ubiquity and by the development of the next internet generation – *the ubiquitous computing web* (Gubbi et al., 2013; Mukhopadhyay, 2014).

The motivation for this topic is actually directly connected to a new paradigm that rises with an exponential growth of internet usage, number of *things* connected to the internet, the enormous amount of data generated by those *things*, and the new vulnerabilities and threats linked to those kinds of devices (Mukhopadhyay, 2014). News headlines alert us to security breaches and new information security issues that occur over compromised point-of-sale terminals, botnet armies that include refrigerators (Higginbotham, 2014), which send 750,000 spam emails, or even a Linux worm that can infect security cameras (Symantec, 2013). This kind of daily news suggest inadequacy of the current security practices in this particular context. Moreover, when we think about the information generated by *Critical Information Systems* (military IS, terrorism information, crime investigation, satellite communications, astronautical IS, nuclear power plants, financial accounts, bank transactions, health care IS,...) that can be controlled and destroyed using an IoT infrastructure, it is very easy to understand that we are talking about sensitive information whose integrity, availability and confidentiality must be protected at all cost (Kaushik, Puri & Gupta, 2012).

When it comes to securing the Internet of Things (IoT), maybe the current methodologies have to change (Leusse, Periorellis & Dimitrakos, 2009) and it is not possible to directly transpose the existing models of securing general IT to the IoT context. More importantly, this new security threats posts new challenges for the top management of IoT Service Providers concerning the set of Organizational Competence skills necessary to face new technological trend, different customer needs and market demands.

Many literature exists in the area arguing that organizational competence is needed for competitive advantage and to develop IT effectiveness (Andreu & Ciborra, 1996; Cragg, Caldeira & Ward, 2011; Dhillon, 2008; McGrath, MacMillan & Venkataraman, 1995; Sanchez & Heene, 1997; Sanchez, 2004). However, there is no conceptual model defining and measuring the generation of organizational competence in the specific area of information security in the scope of the IoT. This gap suggests that some research should be done in this particular area that can contribute to a better understanding and a new approach for the definition and development of organizational competence as a strategic process paradigm.

In order to address this gap in the literature, this research proposes to answer the following research questions: *What are the required set of organizational competences for an IoT product/service, regarding information security?* and, *how can organizational competence in the scope of IoT Security be a valid management tool to achieve competitive advantage?*

The following main objectives were establish for the current work: (1) Understand the state of the art in terms of relevant literature related with Organizational Competence in relation to Information Security in the Scope of IoT; (2) Develop the significant constructs that will define the specific conceptual model; (3) Design a Competence-based Model for Securing the Internet of Things, using the Design Science Paradigm; (4) Validate and test the designed research Model using a survey instrument to several companies in the market and a panel of experts in the field.

The study proposed by this research shall contribute also to the development of business cases and the conception of more reliable and robust management tools capable of a dynamic assessment of organizational competence. Such tools could be a small contribution for organizations to perceive and achieve competitive advantage for their business.

The remainder of the paper starts the theoretical background, introducing the scope of the IoT and information security in IoT field. Then, the paper portrays key considerations about Organizational Competence in order to define the Research Model. Subsequently, the methodological approach is presented. The paper closes with the concluding remarks.

2 Background

2.1 The Internet of Things

In the last years, many different approaches have arisen for the implementation of technological agnostic solutions, related to the research area of IoT and *machine-to-machine* (M2M). This effort has originated a great deal of investment in the area of hardware and software interoperability (Mukhopadhyay, 2014). Many companies working on IoT or M2M services are members of *IPSO Alliance*, created in 2008 as a non-profit organization, currently with 50 companies. This organization aims to coordinate an initiative to establish IP as the standard network protocol for the connection of *smart things* (IPSOAlliance, 2015). Commercial products like *ThingWorx* (ThingWorx, 2015) and *SmartThing* (SmartTHING, 2015) follow the *IPSO Alliance* standards and recommendations. Recently, some web-based initiatives contributed for the creation of IoT-based networks integration mechanisms on the internet, using cloud services.

Part of the research on IoT has also been developed through project funding by the European Commission. Those projects are coordinated by *IERC – European Research Cluster on the Internet of Things* that aims to address the large potential for IoT-based capabilities in Europe and to coordinate the convergence of ongoing activities, sharing knowledge globally (Mukhopadhyay, 2014). In the strategic document *Guidelines and Priorities for the IoT-I Initiative* (Bassi & Biswas, 2012), *IERC* identifies as research priorities: (1) Enhancement of Frameworks and Mechanisms for Trust Relationships; (2) Security against Breaches on the Infrastructure and (3) Privacy Protection Mechanisms.

In the scientific community, the concept of IoT was first advanced by Auto-ID Center at MIT (Mukhopadhyay, 2014) and its definition assumed different perspectives (Bandyopadhyay & Sen, 2011; Atzori, Iera & Morabito, 2010) that have evolved over time (Roman, Zhou & Lopez, 2013). This fact explains the numerous definitions available in the literature on the topic. Thus, the IoT expression is syntactically built on the terms Internet and Things. The first term is related to a network-oriented vision, while the second term is related to generic objects integration on a common framework (Bandyopadhyay & Sen, 2011). Although the IoT definition has been initially proposed by Kevin Ashton in 1999 (Mukhopadhyay, 2014; Gubbi et al., 2013; Bandyopadhyay & Sen, 2011), the concept, when introduced (Gubbi et al., 2013) by Auto-ID Center from MIT, was directly related to RFID and Electronic Product Code (EPC) technologies (Mukhopadhyay, 2014). Gubbi et al. (2013, p.1647) define IoT as '*the interconnection of devices (sensors and actuators) capable of information sharing between different platforms, through a unified framework, forming a common basis for innovative applications*".

The applicability areas of the IoT are very diverse and range from health to logistics, through environmental monitoring and home automation, and there is no single strategy for its implementation. Solutions may involve services under a centralized or distributed approach (Roman, Zhou & Lopez, 2013; Han et al., 2013). For the implementation of IoT-based solutions, many technologies in several areas are being used. Some of them are: (1) identification; (2) architecture; (3) communications; (4) networking; (5) discovery mechanisms and object detection engines; (6) software and special algorithms; (7) hardware; (8) data processing; (9) relationship network management; (10) power and energy storage; (11) security and privacy and (12) standardization (Bandyopadhyay & Sen, 2011). The most common solutions are very much oriented in 3 major areas; (1) internet (middleware); (2) things (sensors, actuators and other devices) and (3) semantics (knowledge) (Gubbi et al. 2013).

2.2 Security Models and IoT Security

Architectures based on the IoT paradigm have to deal with the generation of huge amounts of data. These data volumes must be stored, processed and available in an efficient and easy to interpret manner (Gubbi et al., 2013). For this reason, information security research is a central issue. Information security research covers a very broad spectrum of information technologies, using technical, behavioural, administrative, philosophical and organizational approaches to deal with information assets security (Crossler *et al.*, 2013).

Literature on information security identifies five theories regarding information security management (Tassabehji, 2005; Hong & Chi, 2003): (1) Security Policy; (2) Risk Management; (3) Control and Audit; (4) Management System and (5) Contingency. Security policies and Security Management Systems are incorporated in IS using formal methods and models (Dhillon, 2007). Sometimes, those formal methods form complex and large models. There are some models for security specification (Dhillon, 2007), some examples are: (1) Bell-La Padula Model (concerned with mandatory access control); (2) Biba Model (concerned with preventing data from low integrity environments polluting high integrity data); (3) Clark-Wilson Integrity Model (concerned with integrity, introduces the concept of a program arbitrating an object access); (4) Brewer Nash Model (also known as the Chinese Wall model, provides access controls that change dynamically depending on the previous actions of a user) and (5) Graham-Denning Model (concerned with information flow).

The design of security parameters can aggregate information from different security models. One good example of this is the Comprehensive Security Model NSTISS (National Security Telecommunications and Information Systems Security) 4011 Standard Model. In this Model, three different dimensions are considered: (1) Critical Information Characteristics; (2) Information States and (3) Security Measures (Wang, 2005, p.183). Jirasek (2012) proposed the GRC Information Security Model, which introduces the topic of information security to business managers and CIOs. This model considers the areas of security drivers, stakeholders and security management (Jirasek, 2012, p.2).

Many information security models, constructed under a functionalist paradigm, are based on a trust structure with well determined roles and responsibilities, being valid and complete only in the environments that they were designed for. With new information security challenges, information security management cannot be done using only conventional approaches (Dhillon & Backhouse, 2001; Leusse et al., 2009). Crossler *et al.* (2013), argue that to answer research questions on information security issues, researchers have to use specific tools and sometimes multiple research methodologies that go beyond the traditional positivist paradigm, considering new approaches.

The IS security is a very important function for the protection of key information assets of an organization, through the identification of threats, providing suitable countermeasures and maintaining some security requirements: (1) confidentiality; (2) integrity; (3) availability (Dhillon, 2007; Wang, 2005); (4) authentication and (5) nonrepudiation (Dhillon, 2007). The information security management is an essential process assured by the conformity of standards and regulations for organizations to ensure business protection (Siponen & Willison, 2009). Information Security in the scope of the IoT is closely related to the concept of cybersecurity. In fact, Solms & Niekerk (2013) argue that, although cybersecurity is often used as a synonym for information security, it is not actually an equivalent term. Information security is the protection of information assets regarding threats and vulnerabilities, while cyber security refers to the protection of: (1) cyberspace; (2) cyberspace users and (3) all of their assets (including information).

3 Research Model for IoT Security Organizational Competence

To sustain organizational competitiveness it is fundamental to develop and manage intellectual capital, intangible assets and '*technical fitness*' (Teece, 2007). Enterprises must develop a long-term vision in terms of performance in order to attain '*effective capability development*' (Wang & Ahmed, 2007).

A dynamic view of competitive advantage implies that its life is limited in time. This means that top management should adopt the strategy of being always in pursuit of new competitive advantages. The main mechanisms to discover such advantages are new initiatives (new products, services, technologies and markets) (McGrath, MacMillan & Venkataraman, 1995), new reconfigured sets of resources (Eisenhardt & Martin, 2000) and new business models (Teece, 2007).

As Caldeira and Ward (2001) noticed, a significant number of researchers used, at a conceptual level, the resource-based view theory to conclude that the success of a long term IS initiative lies on Organizational Competence.

Existing literature in the strategy field explain Organizational Competence using two paradigms (McGrath, MacMillan & Venkataraman, 1995; Dhillon, 2008). The first relies on industrial organization economics concepts, where barriers to competition are emphasized in order to build obstacles to competitive forces and thus sustain competitive advantage. The second is based on the fact that firms are essentially idiosyncratic, developing over time unique combinations of resources and particular organizational competencies.

On the literature review process, the work of McGrath, MacMillan & Venkataraman (1995) caught our attention because they focus on the requirements to develop competences, defining and developing organizational competence in operational terms.

The authors consider two main assumptions in their study: (1) competitive advantage in a business initiative is only achievable if the necessary set of competences is properly developed and (2) competences are perceived as an enterprise resource combination that deliberately facilitate the execution of necessary tasks and processes.

Figure 1 shows the conceptual model for organizational competence, adapted from the work of McGrath, MacMillan & Venkataraman (1995).

In the model, the authors consider that '*the degree of competence in an initiative can be assessed by the extent to which ex ante objectives are being realized in ex post results*' and define competence of an organizational subunit as '*its ability to reliably and consistently meet or exceed its objectives*' (McGrath, MacMillan & Venkataraman, 1995, p.254).

The model rational is that a necessary precursor to competitive advantage is competence emergence. In turn, organizational competence cannot be developed without the emergence of *Comprehension* and *Deftness*. Comprehension is defined as '*the outcome of a process by which elements of individual know-how and skill become linked*' and deftness as '*a quality in a group which permits heedful interactions to be conducted at minimal cost*' (McGrath, MacMillan & Venkataraman, 1995, pp. 255 and 256 respectively).

For the measurement and operationalization of the three constructs, the model authors considered the 10 items comprising the construct *competence*, the 16 items comprising the construct *comprehension* and the 15 items comprising the construct *deftness* (McGrath, MacMillan & Venkataraman, 1995, pp.270-275) as showed in Figure 1.

McGrath, MacMillan & Venkataraman (1995, p.267) concluded that: (1) the developed measures are parsimonious and easy to attain and analyze; (2) the research execution on measures developed by this perspective of organizational competence is practical; and (3) this study enables the use of this approach of competence measurement in other contexts, measured differently.

We argue that a specific set of competences is needed for any IoT product/service regarding information security. The concrete knowledge of what kind of skills are required, allows top management to properly assess current organizational competences against future business requirements.

This comparative assessment allows managers to realign the organizational approach of IoT products, regarding the security of their customers' information.

This line of argument embodies the same perspective of organizational competence as the one use in McGrath, MacMillan & Venkataraman (1995) work, being therefore a good starting point for de development of the Competence-based Model for securing the Internet of Things on an organizational environment.

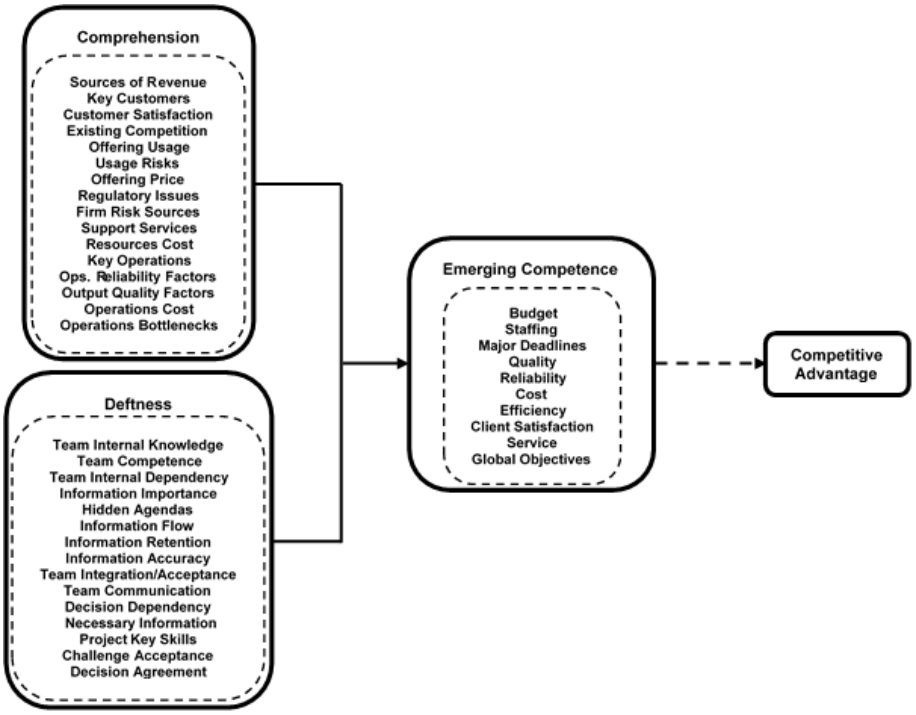

Figure 1. *Conceptual Model for Organizational Competence adapted from* (McGrath, MacMillan & Venkataraman, 1995, p.255).

4 Research Methods

Given the paradigmatic nature of IS (Vaishnavi & Kuechler, 2004), the main objective in IS Research is to achieve the necessary knowledge for the development and implementation of technological solutions, capable of addressing unsolved business problems (Hevner *et al.*, 2004). The methods and technics to be used on a IS research are the set of activities considered appropriate, by the scientific community, for knowledge creation (Vaishnavi & Kuechler, 2004).

Arguing that the best answer to the stated research questions is the development of a Competence-based Model, the Design Science paradigm appears to be a valid methodological approach with academic merit. The Design Science Research (DSR) allows knowledge creation by the development of the Model (the *artefact*), satisfying a set of functional requirements using design, analysis, reflection and abstraction (Vaishnavi & Kuechler, 2004).

In the project at hand the DRS applies given that the Competence-based Model: (1) is an artefact with construction objectively limited in IoT security context (epistemological posture); (2) is able to represent multiple realities of the world, including different socio-technological alternatives (ontological posture); (3) is development-oriented, measuring the artefact impact according to its constructs and variables (methodological posture); and (4) is oriented to the control and creation of a solution, thereby achieving an improvement process for the actual practice (axiological posture).

According to the Knowledge Contribution Framework proposed by Gregor & Hevner (2013), the Competence-based Model can provide a valid contribution to knowledge, in that it can support a new solution for a known problem (*Improvement*).

The research proposed in the paper at hand adopts the DSR Process Model proposed by Peffers *et al.* (2007), given that it synthesizes the previous work on DSR. This process model proposes a design process including six sequential steps, comprising successive design iterations, driven by evaluation cycles. The number of design cycles will be determined on the course of the investigation itself, taking into account the results achieved on each iteration and also the time available for research execution.

In the Appendix, Figure 2 presents the research process phases and Table 2 summarises the main tasks related to each step of the research process.

In the development and evaluation of the artifact to be developed will be used the set of guidelines proposed by Hevner *et al.* (2004, p.83) and the IS Research Framework (Hevner *et al.*, 2004, p.80) that encompasses three different cycles of activities: (1) *The Relevance Cycle* where necessary requirements of the problem context are applied to the research project and the artifact is presented to field testing; (2) *The Rigor Cycle* where grounded theories, methods and expertise of the knowledge base are provided to the research and new knowledge acquired by the research is added to the knowledge base; and (3) *The Design Cycle* where a loop of research process is conducted for the creation and evaluation of design artifacts (Hevner, 2007).

Applying the focus groups theory for artifact refinement and evaluation (Tremblay, Hevner & Berndt, 2010), this study will also use a Panel of Experts as an exploratory focus group (EFG) in the design phase and a confirmatory focus group (CFG) in the Demonstration and Evaluation phases of the study.

5 Concluding Remarks

The next generation in computing transcends the paradigm of traditional desktop (Gubbi *et al.*, 2013) and client-server architectures. This new reality based on Cloud Computing, Mobility, Big Data and Social Media (Gens, 2013) is called the third platform. New security threats and vulnerabilities (Higginbotham, 2014; Symantec, 2013) suggest that new research is needed, resorting to specific tools and multiple research methodologies (Crossler *et al.*, 2013). IoT is a paradigm that involves IS and communication technologies capable of enabling and disabling human activity.

We argue that a specific set of competences is needed for any IoT product/service regarding information security. The concrete knowledge of what kind of skills are required, allows top management to properly assess current organizational competences against future business requirements.

The present research project aims to develop a Competence-based Model for securing the IoT in organizations that will be based on an existing model that defines competence from a strategic management perspective using Resource Based View theory, strategic management theory and the concept of collective mind as heedful interrelating.

This study aims to contribute to the research topic state of the art both at academic and practical level. To the academy, the overview, throughout time, of the Competence-based Model for Securing the IoT in Organizations may provide the development of aspects of Organizational Competence definition and measurement that were not previously considered or fully differentiated in the literature on the topic, being a valid contribution for the knowledge on the subject. To practitioners, this study contributes with the development of business cases and the conception of more reliable and robust management tools capable of a dynamic assessment of the organizational competence required for the continuous evolution of an IoT product or service. The design of such tool could be a small contribution so that IoT service providers can perceive and achieve relevant competitive advantages for their business.

References

Andreu, R. & Ciborra, C. (1996) Organisational learning and core capabilities development: the role of IT. *The Journal of Strategic Information Systems*. [Online] 5 (2), 111–127. Available from: doi:10.1016/S0963-8687(96)80039-4.

Atzori, L., Iera, A. & Morabito, G. (2010) The Internet of Things: A survey. *Computer Networks*. [Online] 54 (15), 2787–2805. Available from: doi:10.1016/j.comnet.2010.05.010.

Bandyopadhyay, D. & Sen, J. (2011) Internet of Things: Applications and Challenges in Technology and Standardization. *Wireless Personal Communications*. [Online] 58 (1), 49–69. Available from: doi:10.1007/s11277-011-0288-5.

Bassi, A. & Biswas, A. (2012) IOT – I Final Analysis of existing IoT Strategic Research Directions and Priorities. *IERC-EU*. (257565), 1–159.

Caldeira, M.M. & Ward, J.M. (2001) Using Resource-Based Theory To Interpret the Successful Adoption and Use of Information Systems & Technology in Manufacturing Small and Medium Sized Enterprises. In: *9th European Conference on Information Systems - Global Co-Operation in the New Millennium*. [Online]. 2001 Bled, Slovenia. pp. 1159–1169. Available from: http://www.sigmod.org/publications/dblp/db/conf/ecis/ecis2001.html.

Cragg, P., Caldeira, M. & Ward, J. (2011) Organizational information systems competences in small and medium-sized enterprises. *Information & Management*. [Online] 48 (8), 353–363. Available from: doi:10.1016/j.im.2011.08.003.

Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q. (2013) Future directions for behavioral information security research. *Computers & Security*. [Online] 3290–101. Available from: doi:10.1016/j.cose.2012.09.010.

Dhillon, G. (2008) Organizational competence for harnessing IT: A case study. *Information & Management*. [Online] 45 (5), 297–303. Available from: doi:10.1016/j.im.2008.01.008.

Dhillon, G. (2007) *Principles of Information Systems Security: Text and Cases*. Hoboken, NJ, John Wiley & Sons, Inc.

Dhillon, G. & Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives. *Information Systems Journal*. [Online] 11127–153. Available from: http://onlinelibrary.wiley.com/doi/10.1046/j.1365-2575.2001.00099.x/full [Accessed: 22 November 2015].

Eisenhardt, K.M. & Martin, J. a (2000) Dynamic Capabilities : What are they? *Strategic Management*. 21 (10/11), 1105–1121.

Gens, F. (2013) *IDC Predictions 2013 : Competing on the 3rd Platform*.

Gregor, S. & Hevner, A. (2013) Positioning and Presenting Design Science Research for Maximum Impact. *MIS Quarterly*. 37 (2), 337–355.

Gubbi, J., Buyya, R., Marusic, S. & Palaniswami, M. (2013) Internet of Things (IoT): A vision, architectural elements, and future directions. *Future Generation Computer Systems*. [Online] 29 (7), 1645–1660. Available from: doi:10.1016/j.future.2013.01.010 [Accessed: 22 November 2015].

Han, C., Jornet, J.M., Fadel, E. & Akyildiz, I.F. (2013) A cross-layer communication module for the Internet of Things. *Computer Networks*. [Online] 57 (3), 622–633. Available from: doi:10.1016/j.comnet.2012.10.003.

Hevner, A., March, S., Park, J. & Ram, S. (2004) Design Science in Information Systems Research. *Journal of Management Information Systems*. 28 (1), 75–105.

Hevner, A.R. (2007) A Three Cycle View of Design Science Research. *Scandinavian Journal of Information Systems*. 19 (2), 87–92.

Higginbotham, S. (2014) *The internet of things needs a new security model. Which one will win?* [Online]. 2014. GIGAOM. Available from: http://gigaom.com/2014/01/22/the-internet-of-things-needs-a-new-security-model-which-one-will-win/ [Accessed: 22 November 2015].

Hong, K. & Chi, Y. (2003) An integrated system theory of information security management. *Information Management and Computer Security*. 11 (5), 243–248.

IPSOAlliance (2015) *IPSO Alliance*. [Online]. 2015. Enabling the Internet of Things. Available from: http://www.ipso-alliance.org/ [Accessed: 12 May 2015].

Jirasek, V. (2012) Practical application of information security models. *Information Security Technical Report*. [Online] 17 (1-2), 1–8. Available from: doi:10.1016/j.istr.2011.12.004.

Kaushik, S., Puri, S. & Gupta, P. (2012) Design and Implementation of Sensitive Information Security

Model based on Term Clustering. *International Journal of Computer Applications*. [Online] 43 (7), 1–6. Available from: doi:10.5120/6112-8200.

Leusse, P. de, Periorellis, P., Dimitrakos, T. & Nair, S.K. (2009) Self Managed Security Cell, a Security Model for the Internet of Things and Services. In: *2009 First International Conference on Advances in Future Internet*. [Online]. June 2009 IEEE. pp. 47–52. Available from: doi:10.1109/AFIN.2009.15.

McGrath, R.G., MacMillan, I.A.N.C. & Venkataraman, S. (1995) Defining and developing competence: a strategic process paradigm. *Long Range Planning*. [Online] 28 (4), 123. Available from: doi:10.1016/0024-6301(95)94265-Z.

Mukhopadhyay, S.C. (2014) *Internet of Things*. Smart Sensors, Measurement and Instrumentation. Subhas Chandra Mukhopadhyay (ed.). [Online]. Cham, Springer International Publishing. Available from: doi:10.1007/978-3-319-04223-7.

Peffers, K., Tuunanen, T., Rothenberger, M. a. & Chatterjee, S. (2007) A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*. [Online] 24 (3), 45–77. Available from: doi:10.2753/MIS0742-1222240302 [Accessed: 19 November 2015].

Roman, R., Zhou, J. & Lopez, J. (2013) On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*. [Online] 57 (10), 2266–2279. Available from: doi:10.1016/j.comnet.2012.12.018.

Sanchez, R. (2004) Understanding competence-based management - Identifying and managing five modes of competence. *Journal of Business Research*. [Online] 57 (5), 518–532. Available from: doi:10.1016/S0148-2963(02)00318-1.

Sanchez, R. & Heene, A. (1997) Reinventing strategic management: New theory and practice for competence-based competition. *European Management Journal*. [Online] 15 (3), 303–317. Available from: doi:10.1016/S0263-2373(97)00010-8.

Siponen, M. & Willison, R. (2009) Information security management standards: Problems and solutions. *Information & Management*. [Online] 46 (5), 267–270. Available from: doi:10.1016/j.im.2008.12.007.

SmartTHING (2015) *The SmartTHING Limited*. [Online]. 2015. SmartTHING. Available from: http://www.smartthing.org/#products [Accessed: 22 November 2015].

von Solms, R. & van Niekerk, J. (2013) From information security to cyber security. *Computers & Security*. [Online] 3897–102. Available from: doi:10.1016/j.cose.2013.04.004.

Symantec (2013) *Linux Worm Targeting Hidden Devices*. [Online]. 2013. Symantec Connect Community. Available from: http://www.symantec.com/connect/blogs/linux-worm-targeting-hidden-devices [Accessed: 11 November 2015].

Tassabehji, R. (2005) Principles for Managing Information Security. *University of Bradford, UK*. 842–844.

Teece, D.J. (2007) Explicating dynamic capabilities: the nature and microfoundations of (sustainable) enterprise performance. *Strategic Management Journal*. [Online] 28 (13), 1319–1350. Available from: doi:10.1002/smj.640.

ThingWorx (2015) *ThingWorx*. [Online]. 2015. Available from: http://www.thingworx.com/ [Accessed: 12 November 2015].

Tremblay, M.C., Hevner, A.R. & Berndt, D.J. (2010) Focus Groups for Artifact Refinement and Evaluation in Design Research. *Communications of the Association for Information Systems*. [Online] 26 (27), 599–618. Available from: doi:10.1007/978-1-4419-5653-8_10.

Vaishnavi, V. & Kuechler, B. (2004) Design science research in information systems. *Association for Information Systems*. [Online] (last updated: Outubro 23, 2013). Available from:

http://www.desrist.org/design-research-in-information-systems/ [Accessed: 17 November 2015].

Wang, A.J.A. (2005) Information security models and metrics. In: *Proceedings of the 43rd annual southeast regional conference on - ACM-SE 43*. [Online]. 2005 New York, New York, USA, ACM Press. p. 178. Available from: doi:10.1145/1167253.1167295.

Wang, C.L. & Ahmed, P.K. (2007) Dynamic capabilities: A review and research agenda. *International Journal of Management Reviews*. [Online] 9 (1), 31–51. Available from: doi:10.1111/j.1468-2370.2007.00201.x.

APPENDIX - Research Process Overview

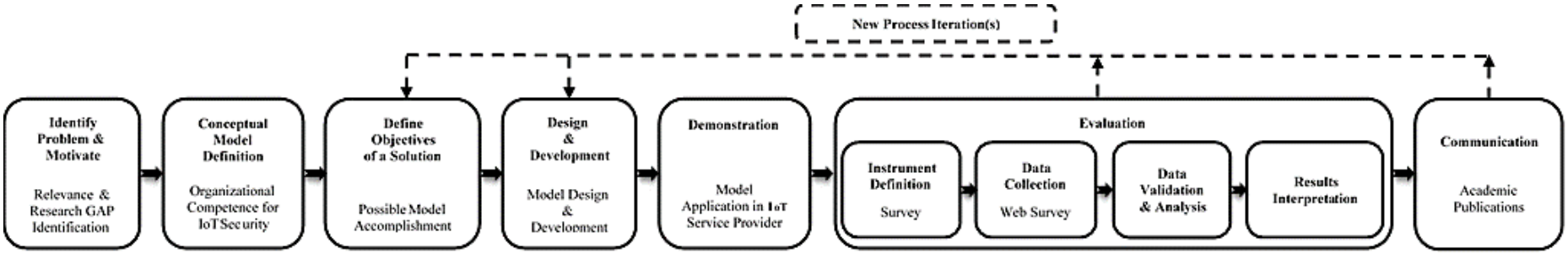

Figure 2. Research process outline based on the Design Science Process Model (Peffers *et al.*, 2007, p.54).

STEP	DESCRIPTION	TASKS
Identify Problem & Motivate	In this step, the problem is defined and the value of a solution for the investigation topic is justified. The motivation for the study aims, not only captivate the researcher and the stakeholders for the solution and accept the results, as well as understanding the scope and researcher knowledge on the subject.	• Relevant literature review; • Practitioner (industry) documentation analysis; • Case study Analysis; • Consultation of concluded or ongoing Research Projects.
Conceptual Model Definition	In this step, it will be defined the key constructs that can be identified in the organizational competence literature related with the topic of information security in the scope of IoT. The defined constructs will be integrated on a beta model based on the competence model proposed by (McGrath, MacMillan & Venkataraman, 1995).	• Relevant literature review; • Relevant constructs definition; • Initial Model development (starting point for the design step).
Define Objectives of a Solution	In this stage, objectives are established for a possible solution for the problem under investigation and the knowledge of what is doable in the research process.	• Relevant literature review; • Modeling Techniques Analysis; • Decision of the methodology for the design template.
Design & Development	In this step, the artifact is created. This activity involves the discovery of the functionality for the design artifact in the research process.	• Relevant organizational competence literature review; • Problem Instances Analysis; • Work with an Exploratory Focus Group (EFG).
Demonstration	At this stage, the idea is to prove that the concept of the artifact design works effectively. The use of the artifact in several instances of the problem must be demonstrated.	• Case Study in an IoT Service Provider; • Applicability tests defined during the case study.
Evaluation	Must be observed and measured if the designed artifact supports a solution for the problem to be addressed. At this methodology stage, the results of the Demonstration activity will be analyzed. The methodology adopted in this step can only be appropriately decided after the completion of the Design & Development step.	• Work with a Confirmatory Focus Group (CFG); • Evaluation instrument (survey) construction and application; • Model conformity tests with the statistical study, the set of guidelines and the IS Research Framework proposed by Hevner *et al.* (2004).
Communication	This phase involves the communication of the research question, the proposed solution for the research problem, the effectiveness of the solution and the research work main results/conclusions.	• PhD thesis report; • Paper(s) submission(s) to scientific publications.

Table 2. The Design Science Process Steps.