Volume 5, No. 6, July-August 2014

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

CUSE AND STUDY REPORT

Available Online at www.ijarcs.info

A Maturity Model for Information Security Management in Small and Medium-Sized Moroccan Enterprises: An Empirical Investigation

Ossama Matrane[1], Prof. Mohamed Talea[2]
Laboratory of Electronics & Information Processing
University Hassan II Mohammedia Casablanca, Morocco

Abstract: Today, security concerns are at the heart of information systems, both at technological and organizational levels. So, Information Security has become an essential support for the business strategy of organization. Therefore, many studies on information security have been carried out. Some refer specifically to maturity models of information security management (ISM). Starting from an analysis of existing literature, Matrane and al. have developed a new maturity model for information security management. In this paper, we aim to validate this maturity model, which leads to determine the level of maturity in security information management. This model will be validated by two approaches. The first is a pilot test of the new maturity model of (ISM) in a Moroccan medium-sized enterprise (SMEs), in order to demonstrate its capacity of assessing the maturity of ISM and whether it can develop an improvement roadmap. The second is an empirical investigation in Moroccan SMEs by using a survey to depict whether it can evaluate the maturity of (ISM) in different industries.

Keywords: Maturity Models, Information Security, Management, Roadmap, Pilot test, empirical investigation.

I. INTRODUCTION

The frequent changes in the organization nowadays, need an alignment of business processes on business strategies, which, at the same time, require a set of methods, tools, management practices and the adaptation of information and communication technologies [1]. Besides, the development of information and communication technology and the spread of the Internet are not only remarkably changing individual lifestyles and business conduct but also explosively creating new businesses [2].

A business's information is one of its most important assets, making the protection of information a strategic issue [3]. Besides, according to role of information as valuable goods in business, it seems necessary to protect its [4]. Nowadays, Information security is a critical issue that many firms face [5]. It is identified as the protection of integrity, confidentiality and availability with the respect to information assets of any organization [6] [7]. It involves identifying unique threats and challenges which need to be addressed by implementing the appropriate countermeasures [8].

Information security in enterprises comprises of complicated processes affected by many factors such as the human factor, education and technology which are obligatorily to be managed under one framework. With the aim of managing these processes, structuring security systems following international standards and providing high level information security, standardization studies have progressed rapidly throughout the worldwide management of enterprise information security all around the world [9].

In fact, organisations require guidance in establishing an information security-aware or implementing an acceptable information security culture. They need to measure and report on the state of information security culture in the organisation. Organisations, therefore, have need of a comprehensive framework to cultivate a security-aware culture [10].

Since information security has a very important role in supporting the activities of the organization, we need a standard or benchmark which regulates governance over information security. Therefore, several standards Governance has been created, which leads to information security such as PRINCE2, OPM3, CMMI, P-CMM, PMMM, ISO27001, BS7799, PCIDSS, COSO, SOA, ITIL and COBIT. However, some of these standards are not well adopted by the organizations, with a variety of reasons [11]. So, after a literature review, Matrane and al. propose a new maturity model for information security management. It is built upon the following three dimensions: Maturity level dimensions, Life cycle stages of standard model in information security management and the critical success factors (CSFs) of RSA Framework.

In this paper, we will try to evaluate the level maturity and the capability of the model of information security management [11] in different Moroccan SMEs and al. For that, we will conduct, first of all, a pilot test and secondly, empirical investigation in Moroccan SMEs.

II. INFORMATION SECURITY MANAGEMENT SYSTEM

Defining security management is difficult, precisely because of the entanglement of the social and the material within information security [12]. ISO 17799 defines information security management as: "an approach and framework to implementing, maintaining, monitoring, and improving information security that is consistent with organisational culture" [13].

A security management system starts as a set of policies that dictate the way in which computer resources can be used. The policies are then implemented by the organization's technical departments and enforced. This can be easy for smaller organizations but can require a team for larger international organizations that have thousands of business processes [14].

Information security management guidelines play a key role in managing and certifying organizational Information System (IS) [15]. So, Information Security Management System is considered as part of a comprehensive management system that is based on estimates and risk

analysis, to design, implement, administer, monitor, reviewing, maintain and improve information security and its implementation have derived from Organization objectives and requirements, security requirements, procedures used and the size and structure of its organization [4]. Besides, it provides a standard, formal and continuous approach to security management for information, enabling secure technology and business processes that are aligned with business requirements and enterprise security management [16]. Also, it includes a series processes for systematically establishing, documenting and continuous managing procedures to improve the safety and reliability of the assets of an enterprise, and for realizing information confidentiality, integrity and availability which are the goals of information security, and includes the continuous enhancement of information security [17]. So, Information security management, defined as 'the protection of information from a wide range of threats in order to ensure business continuity, minimize business risk, and maximize return on investments and business opportunities',[1] is becoming a critical corporate discipline, alongside marketing, sales, HR and financial management [18]. Also, Information technology security management can be defined as processes that supported enabling organizational structure and technology to protect an organization's IT operations and assets against internal and external threats, intentional or otherwise [19].

III. INFORMATION SECURITY MANAGEMENT IN SMES

SMEs play a pivotal role and can be considered as a back bone of national economy [20]. They contribute to the employment rate in their respective countries and they are a good indicator of a healthy economy [21]. From the review it emerged that, SMEs are socially and economically important and need tools and solutions to preserve their competitiveness in challenging environments [22], particularly because they operate in highly competitive, turbulent and uncertain markets [23]. Therefore, it is necessary to ensure information security so that it becomes a natural phase in the daily activities of an organization. So, organizations must define the threats and vulnerabilities to their information resources to ensure the confidentiality, integrity and availability [24][25][26]. In fact, it is essential for an enterprise to define security requirements [9], because the key part of establishing the enterprise information system in an organization is the development of security related protocol to administer processes [27].

Enterprises too often view information security in isolation: the perception is that security is someone else's responsibility and there is no collaborative effort to link the security program to business goals [28]. However, Information Security continues to mature as an organisational function and it is apparent that the management of Information Security depends on technology, processes and people [29]. Fundamentally, Information security management is a part of the risk management process and business continuity strategy in an organization [30].

IV. MODEL VALIDATION

Matrane and al. suggest a new maturity model for information security management in order to identify and explore the strength and weaknesses of particular organization's security. It is intended as a tool to evaluate the ability of organizations to meet the objectives of security [11].

In this article, we aim to validate this model by two approaches. The first is a pilot test of the model in a Moroccan medium-sized enterprise to demonstrate whether it can assess the maturity of Information security management system and develop an improvement roadmap. The second is a survey to verify practical values of the maturity model in Moroccan SMEs and to assess the capability of the model in different industries.

A. PILOT test:

To evaluate the model in an actual industry setting, we conducted a pilot test with Moroccan medium-sized enterprise that gives a great importance for information security and has already implemented an information security management system. For confidential reasons, we will call this company INFORMATICS.

INFORMATICS is a company specialized in IT services, consulting, Outsourcing and professional services. It belongs to a Moroccan group. It has more than 100 employees.

The maturity level of INFORMATICS 'maturity model information security management can be summarized in table 2 as it was assessed by INFORMATICS 'security responsible.

After the assessment of maturity level, based on the proposed model, we developed an improvement roadmap for INFORMATICS 'security responsible as it is shown in table 3.

Table I: The maturity level of INFORMATICS' ISMS

Maturity Level Of Information Security Management	CSFs of Information Security Management	Maturity Level of INFORMATICS' CSFs of Information Security Management	Maturity Level of INFORMATICS' stages of ISM
Business Management	Definition of business objectives	LEVEL 3	LEVEL 1
	Objectives of risk level	LEVEL 1	
	Definition of critical business resources	LEVEL 2	
Risk Management	Understanding of internal and external threats	LEVEL 3	LEVEL 2
	Identifying vulnerabilities	LEVEL 2	
	Classification of resources with high value	LEVEL 2	

Operations Management	Prioritization of work based on risk	LEVEL 1	LEVEL 1
	Adding security checks required	LEVEL 2	
	Improving supervision and visibility	LEVEL 2	
Incidents Management	Identification of security events	LEVEL 3	LEVEL 1
	Prioritization by business impact	LEVEL 1	
	Report to business managers	LEVEL 1	
Problems Management	Avoiding Repeated Incidents	LEVEL 1	LEVEL 1
	Minimizing Impact Of Problems	LEVEL 2	
	Initiating actions to prevent recurrence of incidents	LEVEL 2	

Table: 2 The Improvement roadmap for INFORMATICS' ISMS

Maturity Level Of Information Security Management	**CSFs of Information Security Management**	**Improvement roadmap for INFORMATICS 'security responsible**
Business Management	Definition of business objectives	Maintain a global study of definition of business objectives.
	Objectives of risk level	The risk level must be defined and cleared.
	Definition of critical business resources	The definition of critical business resources must be cleared (Definition of all business resources).
Risk Management	Understanding of internal and external threats	Maintain the level of understanding internal and external threats (be closer to your security team).
	Identifying vulnerabilities	Vulnerabilities must clearly identified (Use some tools to identify all vulnerabilities).
	Classification of resources with high value	Resources with high value must be clearly classified.
Operations Management	Prioritization of work based on risk	Responsible of security must adopt a prioritization of work based on risk.
	Adding security checks required	Provide a good awareness to security checks. You must add all that are required.
	Improving supervision and visibility	The supervision and visibility must be entirely improved (Use some tools of control).
Incidents Management	Identification of security events	Maintain the identification of security events.
	Prioritization by business impact	The prioritizations must be adopted by business impact.
	Report to business managers	A clear report must be delivered to business managers.
Problems Management	Avoiding Repeated Incidents	The metrics of repeated incidents must be established.
	Minimizing Impact Of Problems	The metrics of problems must be properly defined.
	Initiating actions to prevent recurrence of incidents	All actions of prevent recurrence incidents must be initiated.

B. The empirical investigation:

To verify practical values and validity of the proposed model, we applied it to Moroccan SMEs. The study included 70 Moroccan SMEs which adopt a system of information security's management with a workforce of less than 250, a turnover of less than 10 millions USD.

We will try in this section to give an answer, with reference to the context investigated, to the following research question: What are the maturity levels that characterize Management of Information Security in Moroccan SMEs? The research question will be answered through hypotheses testing. For this question we propose one hypothesis: A company could be very advanced regarding one level of Information Security's Management life cycle, while being rather antiquated regarding another.

In order to examine the above research question, a survey method was selected.

The sample is composed of SMEs from different economic sectors. This includes manufacturing, information technology, insurance, sales and distribution industries.

The maturity model of Information Security Management presented in this paper was used in developing a survey in order to evaluate the level of maturity of ISM in Moroccans SMEs. The instrument used is a structured questionnaire with 15 questions. Each one of this questions, cover a process of model maturity of ISM. It allows the researchers to collect data pertaining to maturity model of ISM at each stage Level. Also, we make sure that the form and the questions would be unequivocal and easy to answer, in order to avoid possible ambiguity for the reader [31].

The survey is sent to sample of 70 Moroccan SMEs by email attachment. Within each company, the survey was addressed to one person at Technical level (Security manager, IT manger, SI Manager, Engineer in Computer, Administrator System).

The survey covered a sample of 70 SMEs whose only 17 have completed responses to the questionnaire, a response rate of approximately 26%, which meets Malhotra and Grover's 20% response rate hurdle [32].

As exposed in table 3, it was found that every stage of each maturity level ISM was independent from each other

and that a particular company could be very advanced regarding one level stage, while being rather antiquated regarding another.

The results show that the average of maturity level of different stages of ISM is "Initial" and near to level 2 of Maturity Model of ISM.

From the analysis of the global level stage results, it emerged that only 12, 8 % have a stage 3 (Managed) of maturity level. But, 61,4 % of SMEs Moroccan have a stage 1 (Initial) of maturity level. We can conclude that the majority of Moroccan SMEs don't pay attention to this stage. So, most of Moroccan SMEs don't implement a clear process for Information Security Management. Also, it didn't give more importance to documentation of processes related to information security.

In this study, we found that the Moroccan SMEs are between level 1 and level 2 of Maturity Model of Information Security Management, suggested by Matrane and al. This demonstrates that the Moroccan SMEs focus their efforts in definition of objectives, the risk level, identifying and understanding internal and external threats, classification and definition the critical resources.

The survey's results reflect an initial stage of maturity level and near to level 2 of Maturity Model ISM. It represents opportunities for Moroccan Small and Medium-Sized enterprises' improvement. Also, the empirical analysis demonstrates the capacity of the proposed model to assess the maturity of information security management in SMEs in different industries.

Table 3. Maturity level for each stage of ISM

	Maturity Level of Information Security Management					
Stage of Maturity Level	**Business Management**	**Risks Management**	**Operations Management**	**Incidents Management**	**Problems Management**	
Initial	49 %	34 %	69 %	72 %	83 %	61,4 %
Defined	31 %	45 %	21 %	18 %	14 %	25,8 %
Managed	20 %	21 %	10 %	10 %	3 %	12,8 %
Total	100 %	100 %	100 %	100 %	100 %	100 %

V. CONCLUSION

Matrane and al. have contributed in creating a new concept of maturity model in information security management. It helps organisations by proceeding through the five levels of Maturity Management, to have a better understanding of where they are and how to proceed. It facilitates the detection and providing solutions to problems of information security in enterprises.

Just as with the pilot test and the empirical investigation carried out to validate and to demonstrate the effectiveness of the proposed model of information security management, these results seem to be more interesting in assessing maturity level and developing roadmap. There are, also, some evidences from the results which that the level maturity stage for ISM is at round "Initial" and the level maturity for ISM is near to the second level Maturity Model.

It was found that the Moroccan SMEs take into consideration only the process that is linked to the objective and strategy of enterprise. As a result, they overlook technical aspects (tools of control and security, checking you level security, reports events, statistics and metrics of different events, training on security's tools). Thus, the Moroccan small and medium-sized enterprises have to launch a new project to improve their Information Security Management.

VI. REFERENCES

[1]. P. B. Nassar, Y. Badr, F. Biennier, K. Barbar *"Securing Collaborative Business Processes: A Methodology for Security Management in Service-Based Infrastructure*", IFIP International Federation for Information Processing, Ifip Aict 384, 2012, pp. 480–487.

[2]. D. Botta, K. Muldner, K. Hawkey, K. Beznosov, "*Toward understanding distributed cognition in IT security management: the role of cues and norms*", Cognition, Technology & Work, Volume 13, Issue 2, June 2011, pp 121-134

[3]. K. Hedström, E. Kolkowska, F. Karlsson, "Value conflicts for information security management", The Journal of Strategic Information Systems, Volume 20, Issue 4, December 2011, Pages 373–384.

[4]. S. Gilaninia, S. J. Mousavian, O. Taheri, H. Nikzad, H. Mousavi, F. Z. Seighalani, "Information Security Management on performance of Information Systems Management", Journal of Basic and Applied Scientific Research, J. Basic. Appl. Sci. Res., 2(3)2582-2588, 2012.

[5]. R. Hyeun-Suk, Y. U. Ryub, K. Cheong-Tag, "Unrealistic optimism on information security management", computers & security 31 (2012) 221-232.

[6]. ISO/IEC 27001:2005 – *Information technology – Security techniques – Information security management systems – Requirements*. Institute of Innovative Technologies EMAG, Poland, 2012.

[7]. ISO/IEC 27002:2005 – *Information technology - Security techniques - Code of practice for information security management* (formerly ISO/IEC 17799). Institute of Innovative Technologies EMAG. Poland, 2012.

[8]. D. Zissis, D. Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems, Volume 28, Issue 3, March 2012, p: 583–592.

[9]. E. Y. Yildirim, G. Akalp, S. Aytac, N. Bayram "Factors influencing information security management in small- and medium-sized enterprises A case study from Turkey", International Journal of Information Management - INT J INFORM MANAGE 01/2011.

[10]. A. Da Veiga, J.H.P. Eloff, "A framework and assessment instrument for information security culture", Computers &

Security, Volume 29, Issue 2, March 2010, Pages 196–207.

[11]. O. Matrane, M. Talea, C. Okar, « Towards A New Maturity Model for Information Security Management», International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 6, June 2014.

[12]. Lizzie Coles-Kemp "Human Factors in Information Security", Journal of Information Security and Applications, Volume 14, Issue 4, Pages 175-230 (November 2009).

[13]. http://www.iso.org/iso/fr/iso_catalogue/catalogue_ics/catalogue_detail_ics.htm?csnumber=39612

[14]. John R. Vacca, Book, "Computer and Information Security Handbook", (Second Edition) 2013, Pages 409–414.

[15]. Siponen ,Mikko ; Willison ,Robert .(2009). Information security management standards: Problems and solutions,journal of Information & Management 46 ,pp267–270.

[16]. D. Milicevic, M. Goeken, "Social Factors in Policy Compliance – Evidence found in Literature to Assist the Development of Policies in Information Security Management", 46th Hawaii International Conference on System Sciences, 2013.

[17]. C. S. Park, S. S. Jang, Y. T. Park, "Study of Effect of Information Security Management System [ISMS] Certification on Organization Performance", IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.3, March 2010.

[18]. A. Calder, S. G. Watkins, "Information Security Risk Management for ISO27001/ISO27002", April 2010, Pages: 187.

[19]. John R. Vacca, Book, "Computer and Information Security Handbook", (Second Edition) 2013, Pages 449–458.

[20]. Hidayanto, A. N., Karnida, Y. Y., and Moerita, G. (2012). "Analysis Of Software As A Service (SaaS) For Software Service Provision Alternative: A Case Study of E-Office", On-Demand Service of PT Telkom Indonesia. International Journal of Innovation and Learning (In press).

[21]. T. R. Phihlela, S. A. Odunaike, "A Measurement Framework to assess SME performance", 2012 Proceedings of the Information Systems Educators Conference New Orleans Louisiana, USA ISSN: 2167-1435 v29 n1982.

[22]. Cocca, Paola and Alberti, Marco. "PMS maturity level and driving forces: an empirical investigation in Italian SMEs". In: 15th International Annual EurOMA Conference "Tradition and Innovation in Operations Management. 2008. p. 15-18.

[23]. Zaidi, Lubina. "Problems affecting the growth of small and Medium Enterprises (SMEs) in India", International Conference on Technology and Business Management, March. 2013. p. 20.

[24]. Gollmann, D. 1999. Computer Security. New York. John Wiley & Sons Ltd.

[25]. Pfleeger, C. P. 1997. Security in Computing. Prentice Hall PTR.2nd Edition.

[26]. Sebastiaan, H. Van. Solms & Jan HP Eloff. 2003. Information Security. B & D Printers.

[27]. Eggy E. Chaudhry, Sohail S. Chaudhry and R. Reese, "Developing a model for enterprise information systems security", Journal of Academic Research in Economics, 2011, vol. 3, issue 3 (November), pages 243-252.

[28]. Isaca 2009, "An Introduction to the Business Model for Information Security".

[29]. D. Ashenden, "Information Security mXanagement: A human challenge ?", Information Security Technical Report Volume 13, Issue 4, November 2008, Pages 195–201.

[30]. John R. Vacca, Book, "Managing Information Security", 2014, Pages 1–45.

[31]. C. Forza, "Survey research in operations management: a process-based perspective", International Journal of Operations & Production Management, Vol. 22, No 2, 2002, pp. 152-194.

[32]. M. K. Malhotra, and V. Grover, "An assessment of survey research in POM from construct to theory", Journal of Operations Management, Vol. 16, 1998, pp. 407-42.