THE EFFECT OF INFORMATION TECHNOLOGY CAPABILITIES IN IMPLEMENTING, INFORMATION SECURITY MANAGEMENT SYSTEMS

Mr.Anas Ali alkasasbeh
Muta'h University, Faculty of science-Department of Computer

Abstract

This study aimed to measure The Effect of Information Technology Capabilities in Implementing Information Security Management Systems; Study of Commercial banks in Jordanian capital, Amman. The study sample included 14 Commercial banks in Amman Jordanian capital city that adopted IT. The study results show that there is direct relationship between effect of Information Technology Capabilities and Implementation of Security Information Management Systems in Jordanian banks. Based on the results of the study, the research proposed several recommendations to commercial banks, most importantly on how to take care of its IT capabilities In order to Increase their operations in Implementing Information Security Management Systems.

Keywords: IT-Infrastructure**, IT**-Human Resources, **IT**-related Intangible, **IT** Coordination, **IT** Governance. Security policies, Internal System Security Audits, External System Security Audits

Theoretical Background

(IT) is the general term that describes any technology that helps to produce, manipulate, process, store, communicate, and/or disseminate ‘’information.” William Sawyar, (2005) stated that IT includes hardware, software, databases, networks and other related components which are used to build information systems. At the enterprise level, many researchers have defined capabilities as broadly referring to the entire gamut of skills, entrepreneurial, managerial, and technicalities required establish and operate firms internally. Bone & Saxon, (2000) defined capability as “the combination of the right people with the right skills, using the correct plant and equipment through effective business processes, and thereby delivering the company’s ‘’strategic intent." A capability is a lower-order functional,

operational, or technical capacity that may be further subdivided into specific (individual) skills or specialized capabilities. A capability has several attributes, namely, speed; process consistency, agility, cross- functionality, and complements core competencies. Although there is no one formula for developing capabilities, Feeny & Willcocks (1998) suggested that nine capabilities form the foundation of a firm. These included: leadership, business-systems-thinking, relationship building, architecture planning, contract facilitation, making information technology work, contact monitoring, informed buying, and vendor development.

Capabilities involve the know-how of all the processes, meaning, and the minimal necessary routine to make work a productive process (Byrd, 2000). This routine is constantly improved through the learning process. The permanent exchanges between the organization and its external environment bring new types of know-how, innovation of the product, the process, or the organizational management. This ability to make things work in a different way can be understood as the internal company's capability of innovation, that is, the technological capability of the organization. These internal capabilities are unique to each company. Therefore, they change according to the organization (Devaraj, 2003).

Managerial IT skills or knowledge represent the fusion of IT-related and business-related knowledge possessed by and exchanged among IT managers and business unit or line managers (Mata et al., 1995). IT capabilities (hardware, software, executive systems, proprietary software, shared services, IT human skills, and processes) are integrated and interrelated capabilities of internally consistent elements that are focused toward the fulfillment of an IT or business objective. Without such focus on an IT capability, the firm may make expenditures in a fragmented manner. Kalakota R, (2001), research results have demonstrated that the primary mechanisms through which IT capabilities impact overall business performance are through internal business process efficiency and streamlining.

The continued emphasis on business processes as real targets for IT investment and IT capability innovation should incorporate the notion of real options. That is, the idea that in making an IT investment today, the immediate benefit may not be realized until the future. The focus on IT capabilities and the influence they exert through business processes leads to management realizing a need for focused IT capabilities investment. These IT capabilities can be extended and manifested as an IT competency to a customer. For example, using Enterprise Application Software, IT can integrate major systems internally and then this capability can be used to integrate customers (with a firms order management system). The phrase "IT capability" describes different aspects of an organization's base of IT

resources. These resources influence and determine the organization's ability to convert IT assets and services into strategic applications (Bharadwaj 2000), and to mobilize and deploy IT based resources with other resources and capabilities. There are five dimensions of IT capability:

IT Infrastructure: This includes physical IT assets in terms of hardware, software and networks (Byrd, & Turner, 2000).

IT Human Resources: These include technical and managerial skills such as programming, systems analysis, network administration, database management, project management, co-ordination and leadership, interaction with user community and effective management of IT functions (Copeland & McKenny, 1988).

IT-related Intangible Resources: Sustained use of IT can lead to the creation of various intangible benefits, which can serve as the basis for additional capabilities (Bharadwaj, 2000).

IT Coordination: IT coordination is recognized as an independent construct in the measurement of IT capability. Coordination runs the continuum from a low level, in which transaction processing systems within different functions are independent, to a second level, in which data flows across functions, to a third level described by processing interdependence, work flow, and the use of IT for integrated activities (Mulligan, 2002).

IT Governance: Governance describes the authority, control, and audit in the allocation and delivery of IT resources and services. The existence of IT governance systems has been shown to affect firm profitability and strongly influences the value that an organization generates from IT (Weill & Ross, 2004).

ISO/IEC 27000 (2009) defined Information Security Management System (ISMS) as:

"Part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security". Management System is "a framework of policies, procedures, guidelines, and associated resources to achieve the objectives of the organization", and Information security is "preservation of confidentiality, integrity, and availability of information". Tipton & Krause, (2008) also defined Information Security Management System (ISMS) as: "Coordinated activities to direct and control the preservation of confidentiality, integrity, and availability of information".

Information Security Management System (ISMS) family of standards consist of the following International Standards, under general title of "Information Technology Security Techniques": (ISO/IEC 27000, 2009)

ISMS certification criteria: ISO/ IEC 27000:2009, Information security management system – Overview and Vocabulary. ISO/IEC27001:2005, Information security management system – Requirements. ISO/IEC 27002:2005, Code of practice for Information security management. ISO/IEC27003,Information security management system implementation guidance. ISO/IEC27004:2007 Information security management—Measurement. ISO/IEC27005:2008 Information security risk management ISO/IEC 27006:2009, Requirements for bodies providing audit and certification of information security management system. ISO/IEC 27007, Guidelines for information security management systems auditing. ISO/IEC 27011, Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 Code of practice for information security management.

In 2001 e-Banking architecture was hosted internally within the bank and is fully supported by various teams of technical support personnel. It consists of a trained network infrastructure with various security controls in place to provide protection against insider and external attacks. The e-Banking application is written by an internal development team within the development environment. It is then migrated to the (QA) environment under-going both usability and stress testing dedicated team of experts. It will also be exposed to rigorous security testing by representatives of the Security Team. Once all necessary sign-off has been given the code is migrated to the production environment by the Webmaster.

Security policies: Those policies which are available, to improve security process and "to address issues pertaining to system access controls, data confidentiality/privacy, and data integrity" (Locke & Harley, 2001).

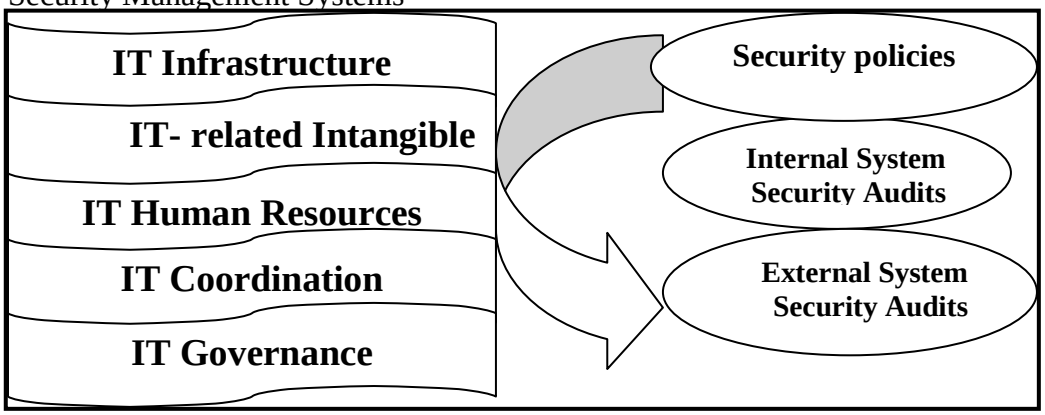
Internal systems security audits: provide firms with internal sense of security in that they may feel that their systems are more successful at detecting intrusions.

External systems security audits: audits aimed at detecting intrusions and violations practiced by T.P. (Cushing, 2001).

Internal attacks vulnerability: These individuals may believe that firms with corporate security policies are less vulnerable to attacks by internal and external parties (Nevins, 2003).

External attacks vulnerability: Organizations with more frequent external systems security audit were perceived to be more successful at detecting intrusions, and are likely to have more secured systems or less vulnerable to attacks by external parties.

Five dimensions of IT capability in Implementing Information Security Management Systems



Design and Methodology

The researcher uses a deductive approach which is more likely to work with quantitative data in order to answer the questions about relationships among measured variables with the purpose of explaining, predicting & controlling phenomena. Thus, the aim of a deductive approach is to generalize from a sample to a population (Leedy & Ormrod, 2001).

The design was quantitative because the data took a numerical form. That is, by employing a deductive approach with a quantitative research method, the researcher has been able to measure & analyze the relationship between influencing factors. This approach also allows for testing the research hypotheses & generalizing the research findings to the population (Zikmund, 2003).

The methodological approach in this research is a descriptive one, because the researcher attempts to identify, explain variables of this research & to describe the relationships between these variables in order to provide a picture of a particular phenomenon, but not to ferret out cause-effect relationships (Churchill & Iacobucci, 2002).

Study Population and Sample

The population of the study is the whole of the Commercial banks that apply IT And number (14). On the other hand, the researcher chooses a random sample consisting of (120) IT Department employees in the Jordanian banks. To analyze Multi-collinearity, two types of measurements can be used: Variation Inflation Factor (VIF) & Tolerance. The VIF,

measures the extent the variance of the estimated regression coefficients are inflated as a result of being related to the other independent variables, & Tolerance is the amount of variability of the selected independent variables not explained by other independent variables.

Results in Table below (1) shows that VIF for all independent variables ranged between (1.109 - 2.063), which are less than the limited valued (10) & Tolerance for all independent variables ranged between (.485 - .901), which are greater than (0.10). This indicates that there was no high correlation among the independent variables (Multi-collinearity).

Table (1): The Multicollinearity Test

Variables	Tolerance	VIF
IT Infrastructure	**.901**	**1.109**
IT Human Resources	**.787**	**1.271**
IT- related Intangible	**.701**	**1.427**
IT Coordination	**.663**	**1.508**
IT Governance	**.580**	**1.723**

The ratio of Skewness to its standard error can be used as a test of normality (that is, you can reject normality if the ratio is less than -2 or greater than +2). A large positive value for Skewness indicates a long right tail; an extreme negative value indicates a long left tail" Table (5) presents the Skewness normality distribution test:

Table (2): Skewness Coefficients

Variable	Skewness
IT Infrastructure	**-.122**
IT Human Resources	**-.423**
IT- related Intangible	**-1.353**
IT Coordination	**-.530**
IT Governance	**-.689**

The reading of the *Skewness* test findings, all variables are normally distributed, ranging from **(-1.353 to -.122)** falling within the interval of **(2,-2).** Fitness of the Model: of the original model reveals model that 0.352. This means that the model explains 35.2% of the Information Security Management Systems Table (3). The model is statistically significant, as the p-value for the model is 0.000 which is less than the limit for statistical significance limit in same Table, which is 0.10 for weak significance & 0.05 for significance. This level is good.

Table (3): Model Summary [b]

Mode	R	R Square	Adjusted R Square	S.D Error of the Estimate	Durbin-Watson	F	Sig.
1	.593[a]	.352	.322	.35148	2.037	11.877	**.000**

a. Information Technology (IT) Capabilities
b. Information Security Management Systems

Table (4): T-Value & Significance

Model	Unstandardized Coefficients		Standardized Coefficients	t	Sig
	B	**S.D Error**	**Beta**		
(Constant)	1.854	.308		6.011	**.000**
IT Infrastructure	.041	.039	.072	1.049	**.296**
IT Human Resources	.224	.060	.272	3.709	**.000**
IT- related Intangible	.300	.060	.392	5.039	**.000**
IT Coordination	.010	.069	.011	.143	**.886**
IT Governance	-.016	.040	-.035	-.411	**.682**

Dependent Variable**: Information Security Management Systems**

From the results showed in Table (4), IT Infrastructure has a non-significant direct effect on successful adoption of : Information Security Management Systems in Jordanian banks (t = 1.049; sig = .296). While IT Human Resources has a significant direct impact on the Jordanian banks (t = 3.709; sig = .000). Furthermore, IT- related Intangible Van has a significant direct impact on the successful Jordanian banks (t = 5.039; sig = 0.000).

IT Coordination has no significant direct impact on Information Security Management Systems of Jordanian banks (t = .143; sig = .886). IT Governance has a non-significant direct effect on Information Security Management Systems in Jordanian banks (t = -.411; sig = .682).

Conclusion

Below are some of the positive effects within the studied variables: The main results are:

1. The results from the study showed, that IT Infrastructure has a non-significant direct effect on successful adoption of: Information Security Management Systems in Jordanian banks.

2. While the IT Human Resources has a significant direct impact on the Information Security Management Systems Jordanian banks.

3. The results also showed that IT- related Intangible Van has a significant direct impact on the successful Information Security Management Systems in Jordanian banks.

4. The results similarly showed that IT Coordination has no significant direct impact on Information Security Management Systems in Jordanian banks.

5. The results finally showed that IT Governance has a non-significant direct effect on Information Security Management Systems in Jordanian banks.

Recommendation

Due to the results, the research presents some useful recommendations:

1. The commercial banks should that take care of its IT capabilities In order to Increase their in Implementing Information Security Management Systems.

2. Most Jordanian Banks interest in IT Coordination has no significant direct impact on Information Security Management Systems.

3. Most Jordanian Banks interest in IT Governance has a non-significant direct effect on Information Security Management Systems in Jordanian banks.

4. More so Commercial Jordanian banks especially those located in Amman have to train their employees and in IT because it's the key factor in Implementing Information Security Management Systems in Jordanian banks.

References:

Bone, S., Saxon, T., 2000. Developing effective technology strategies. Research Technology Management Washington 4, 50–58.

Byrd, Terry Anthony & Turner, Doyglas E, (2000), "Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct", Journal of Management Information Systerns, Vol. 17, No. 1: 167-208.

Bharadwaj, A. (2000) A Resource Based Perspective on Information Technology and Firm Performance:An Empirical Investigation, MIS Quarterly,24,1,169-196.

Byrd, Terry Anthony & Turner, Doyglas E, (2000), "Measuring the Flexibility of Information Technology Infrastructure: Exploratory Analysis of a Construct", Journal of Management Information Systerns, Vol. 17, No. 1: 167-208.

Copeland, D.G. and McKinney, J.L. (1988) Airline Reservation Systems: Lessons from History, MIS Quarterly, 12,3,353-370.

Cushing, K. (2001). “Would you turn to the dark side?” Computer Weekly.
Churchill, G., & Iacobucci, D. (2002). “Marketing research: Methodological foundations”. 8th Ed, Orl&o: Harcourt College Publishers.
Devaraj, S., Kohli, R. (2003) performance impacts of information technology: is actual usage the missing link? , management science, 49(3), 273-289.
Foss, Nicolai J & Christensen, Jens Frøslev (1996). “Dynamic Corporate Coherence and Competence-Based Competition: Theoretical Foundations and Strategic Implications”, forthcoming in Aimée Heene & Ron Sanchez (eds.) (1996). Competence-Based Strategic Management, Oxford: Elsevier.
Feeny, D. and Willcocks, L. (1998). Core IS Capabilities for Exploiting Information Technology. Sloan Management Review, 39(3), 9–2.
H. F., Krause, M., (2008), “Information Security Management Handbook”, (6th ed) 2, Auerbach Publucations.
ISO/IEC 27000, (2009), “Information technology - Security techniques - Information security management systems - Overview and vocabulary”, ISO / *IEC.*
ISO/IEC 27002:2005, Code of practice for Information security management.
Kalakota R. & Robinson M. (2001), M-business: The race to mobility, McGraw-Hill, New York.
Leedy, P., & Ormrod, J. (2001). “Practical Research: Planning & design”. 7th Ed, Pearson Educational International & Prentice Hall: New Jersey.
Locke, A. D., & Hartley, B. V. (2001, May). “Security as a process”. DM Review.
Mulligan, P (2002) Specification of a capability-based IT classification framework, Information and Management 39, 8, pp. 647 - 658.
Mata, F. J., Fuerst, W. L. & Barney, J. B. (1995): Information Technology and Sustained Competitive Advantage: A Resource-Based Analysis, in: MIS Quarterly, December : 487- 505 May 2001.
William, B.K and S.C Sawyar. (2005). “using information technology “.edition, McGraHill Publishing Co. U.S.A: 3,4,147William B.K and S.C. Sawyar. (2005). ‘Using Information Technology’, 6th .
Weill, P and Ross, IT Governance (2004) How top managers manage IT decision rights.
Zikmund, W. (2003). “Business Research Methods”. Harcourt Brace Jovanovich: Fort Worth..