The current issue and full text archive of this journal is available at
www.emeraldinsight.com/2042-5961.htm

Evaluating the impact of information security on enhancing the business decision-making process

Akram Jalal-Karim
Management Information System Department, College of Business and Finance, Ahlia University, Manama, Kingdom of Bahrain

Abstract

Purpose – In today's digital economy, information secrecy is one of the essential apprehensions for businesses. Because of the uncertainty and multiple interpretations, most of the reviewed literature regarding business decision-making revealed that decisions tend to be more fluid, inaccurate, and informal. Recently, the number of organizations that have disclosed their information has been raised. The aim of this research is to theorize and empirically measure the effects of information disclosure on the accuracy of business decision-making.

Design/methodology/approach – This study presents a proposed conceptual framework, which assists businesses in evaluating the extent to which information secrecy has a substantial effect on decision-making accuracy. The primary research purpose is explanatory and the conceptual framework was empirically tested to measure the effects of the proposed five independent variables: information security rules and regulations, secured internal and external business communication, security consciousness management support, business security culture, and superior deterrent efforts on efficient information security, the consequences of which on accurate decision-making processes are considered a dependent variable.

Findings – The results of this study, which are based on the use of the proposed conceptual framework, indicate that information security has a substantial effect on generating accurate, effective and efficient business decisions. Information security could undermine decision accuracy when information collected has little effect on the purpose and time of decisions.

Originality/value – The findings of this study present some insights into the strategic choices of any organizations and, to improve the efficiency of the decisions taken, they must improve the level and efficiency of information secrecy.

Keywords Information security, Decision-making process, Decision making, Information management

Paper type Research paper

1. Introduction

Despite a global recession, businesses have thrived over the last decade, growing year after year; they have enhanced output, improved efficiency and produced new alliances, mainly by relying on the internet.

Today, the digital innovation concerning the internet and worldwide use of web sites has set the platform for e-commerce and, because of the rising frequency and cost of security incidents, the significance of valuable information security is fast becoming one of the most important ethical issues of our information age and one of the most precious assets for various types of organizations (Gordon *et al.*, 2005). These assets are susceptible to theft, modification and even rejection of timely access. Disabling an information security system has a significant harmful consequence on the value of a business (Cavusoglu *et al.*, 2004; Ishiguro *et al.*, 2006).

World Journal of Entrepreneurship, Management and Sustainable Development
Vol. 9 No. 1, 2013
pp. 55-64

2042-5961
DOI 10.1108/20425961311315719

The internet is unlimited, providing the capability for worldwide communication; in contrast, it may provide an interconnected path for damages, attacks and other malicious actions. These attacks can have destructive consequences on business operations and assets by exploiting vulnerabilities to disclose the secrecy, integrity, reliability or accessibility of the information being managed by those systems.

Whitten *et al.* (2004, p. 12) stated: "information is an arrangement of people, data, process, and information technology that interact to collect, process, store and provide as output the information needed to support an organization," which indicates that an information system is an arrangement of groups, data, processes and technology that act together to accumulate, process, store and provide information output needed to enhance and increase the speed of the process of decision making.

Information security has evolved to be an alarm for modern organizations (Park *et al.*, 2006; Pavlou *et al.*, 2007). Senior leaders/executives have the same objective: to decrease or remove vulnerabilities to guarantee unremitting delivery of critical decision making based on opportunity and security of information. Thus, any attacks or threats to information can result in inadequate decisions, which consequently affect the entire structure of the organization.

To make knowledgeable decisions, senior management must have vital information presented in a way that will allow them to recognize the significant concerns and most important queries and inquire further.

Today, firms are expending large amounts of money on information security systems to avoid, detect, and fix information security breaches (Berinato, 2007; Latimer-Livingston and Tracy, 2008; Tam and Lawton, 2007).

Business decision making is a highly complicated process that most business organizations need to survive in the competitive environment, which becomes progressively restraining. This type of competition shows that there is an increasing need for informational assistance to facilitate decision makers to produce fast and accurate timely decisions. Hundreds of organizations have spent large amounts of money on the revitalization and enhancing of business processes and the augmentation of information systems' abilities to achieve competitive advantage over competitors effectively. Accurate and adequately early business decision-making processes are essential for organizations. With the aim of making accurate decisions, consistent, perfect and on time, information must be supplied (Akram, 2011).

The impact of earlier access to related and extensive information on business decision making is demanding, especially when it evaluates and measures this impact on business results as a consequence.

The developments of information technology in addition to the raising of the values of information to decision makers are the reasons for the increasing concern about information security management systems.

This concern continues to grow; an organization's facility to utilize their information may be vulnerable, and decision makers need to find a balance between the efficient, effective operation of businesses and the protection of information security (Smith, 1994).

Research literature in information security suggests that the effective communication between senior management and IS security can show the true picture of the availability, reliability, credibility and efficiency of information and how it affects the process of drafting resolutions and reaching successful decisions. Belsis and Kokolakis (2005) argued that most business decision makers require knowledge of IS security issues to play a significant role in a successful decision-making process.

Academic surveys in information security systems have observed organizational intranet and extranet privacy issues concerning the sharing of high-privacy information in several different ways: for instance, online confidential communications with other organizations (Dinev and Hart, 2006; Malhotra *et al.*, 2004), e-commerce, e-banking and e-government (Wang *et al.*, 2003; Van Slyke *et al.*, 2006). The overall impression from this set of literature is that secure online communication maybe one of the most important factors which could cause the disclosure of vital information, or it may be safe if it was used the right way.

Due to the desire to follow the appropriate emphasis of information security research, we claim that different factors under different conditions should be examined in order to gain an advance comprehension of a manager's decision making.

This empirical study aimed to explore the extent of the impact of: information security rules and regulations, security consciousness management support, business security culture, superior deterrent efforts and secured internal and external business communication in organizations on efficient information security which consequently impacts on accurate decision-making processes in an organization.

Eloff and Eloff (2005) and McCarthy and Campbell (2001) indicated that rules and regulations are a top priority for effective business information security.

The evaluations of efficient information security will typically increase the confidentiality, integrity and availability of decisions made by top managers.

This paper is structured as follows: the Section 2 lists research questions used for this study and presents the proposed conceptual framework, followed by testing of the hypothesis and results analysis of the current challenge in Section 3. Finally, the conclusion reached in this research paper will be discussed in Section 4.

2. Research questions and hypotheses

To achieve the purpose of the current study, the following research questions have been formulated:

(1) To what extent do the selected independent variables influence improvement in efficient information security?

(2) To what extent is efficient information security being utilized to support the accuracy of the decision-making process?

To answer these questions, and based on the previous research literature in business information security, we propose the following conceptual framework and hypothesize the relationships between the dependent and independent variables (Figure 1).

The framework assumes that having information security rules and regulations, secured internal and external business communication, security consciousness management support, business security culture, and superior deterrent efforts in organizations will have a positive impact on enhancing efficient information security, which consequently has a positive impact on generating an accurate business decision-making process.

The research questions posited require empirical clarification if this study is to produce a superior theoretical perception of efficient information security and accuracy of the decision-making process. The literature research that has been discussed in the last section revealed that there has been an increase in the number of empirical studies

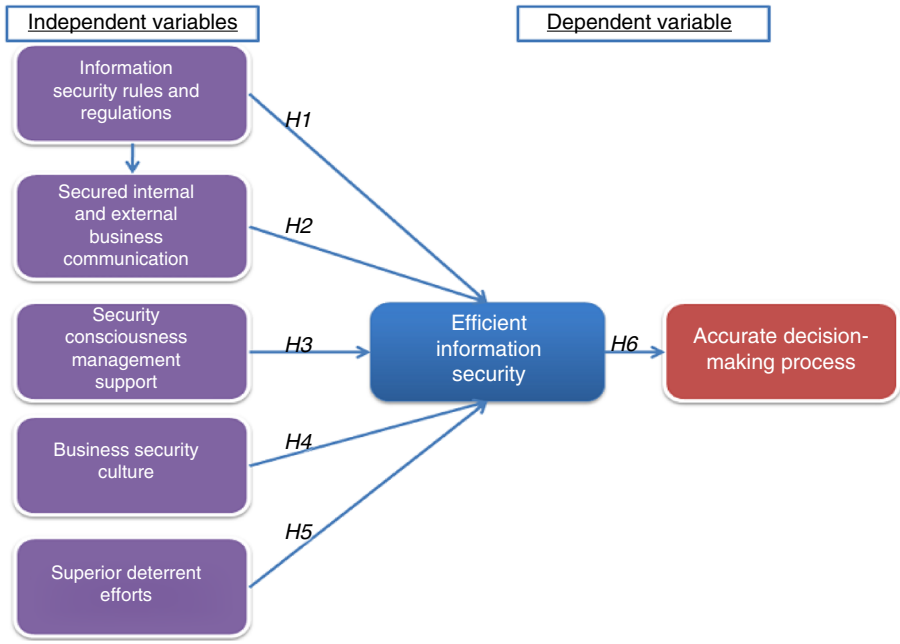

Figure 1.
Conceptual framework

of information security; however, more is still required. To answer the two research questions, the current study focusses on the following six hypotheses developed from previous studies:

H1. There is a significant relationship between information security rules and regulations and enhancing efficient information security.

H2. There is a significant relationship between secured internal and external business communication and enhancing efficient information security.

H3. There is a significant relationship between security consciousness management support and enhancing efficient information security.

H4. There is a significant relationship between business security culture and enhancing efficient information security.

H5. There is a significant relationship between superior deterrent efforts and enhancing efficient information security.

H6. There is a significant relationship between efficient information security and an accurate business decision-making process.

By developing the above hypotheses, the study thus adapts the quantitative research design to better test those hypotheses. Quantitative research uses a survey as the main instrument to collect data.

2.1 Survey instrument

The questionnaire developed for this study was divided into two sections. The first section concentrates on the general profile of the respondent, including his/her age group, education level and profession and income group. The second section was designed to identify the factors affecting efficient information security and the accuracy of the decision-making process. The respondents were provided with a list of 14 questions – two questions on each of the seven variables. Participants were asked to indicate their perception regarding each question, using a Likert scale (1-5), with responses ranging from "strongly disagree" to "strongly agree." The collected data were analyzed based on correlation and regression analyses using the Statistical Package for Social Sciences (SPSS) version 17 computer program.

2.2 Sample and data collection

The primary data collection method was used in the survey was conducted during the last quarter of year 2011 by primary data collection method which was designed and distributed to 171 employees in different age groups and of different education levels working at different organizations. The chosen participants all work with information systems as part of their jobs.

The survey was printed in the English language. Prior to distribution, the questionnaire was pre-tested on ten individuals working in different sectors to ensure consistency, clarity and relevance to the case. Minor changes requested by the test group relating to question content, wording or sequence were incorporated into the questionnaire before the final copy was produced. The instrument was then tested to determine how long it would take a respondent to complete the form. It was found that it would take from 6 to 9 minutes.

A digital online form was created using "Google Documents" in the same questionnaire style; then, the link was shared and publicized through e-mail and was posted on discussion forums. Once a participant had completed the questionnaire, the raw data were logged on a spreadsheet that could be accessed and downloaded only by the researcher.

Of the 171 questionnaires distributed, only 101 were usable. Of those, 49.1 percent were completed by females, and 79.1 percent were completed by respondents between the ages of 20 and 45 years.

2.3 Reliability

To find out whether the questionnaire was reliable we measured its internal reliability, which is the most popular method of determining reliability. Cronbach's α-test was used (Nunnally and Bernstein, 1994). A minimum α of 0.6 is said to suffice for the early stage of research.

As shown in Table I, the Cronbach's αs in this study were all much > 0.6. It is 0.853, which indicates a high level of internal consistency for our scale. The constructs were therefore deemed to have adequate reliability.

Reliability statistics

Cronbach's α	Cronbach's α based on standardized items	Number of items
0.853	0.874	7

Table I.
Cronbach's α estimation

3. Analytical results and discussion

3.1 Correlation test

Correlation analysis was incorporated to describe the strength and direction of linear relationship between the dependent and independent variables (Pallant, 2001).

The results of the correlation analysis reveal that information security rules and regulations ($r = 0.778$, $p < 0.01$), secured internal and external business communication ($r = 0.940$, $p < 0.01$), security consciousness management support ($r = 0.958$, $p < 0.01$), business security culture ($r = 0.970$, $p < 0.01$) and superior deterrent efforts ($r = 0.853$, $p < 0.01$) were found to be strongly and positively correlated with the efficient information security which consequently has a positive impact on generating an accurate business decision-making process ($r = 0.912$, $p < 0.01$) (Table II).

3.2 Regression test

For further analysis, a linear regression analysis was conducted to examine the extent to which the independent variables (information security rules and regulations, secured internal and external business communication, security consciousness management support, business security culture and superior deterrent efforts) influence the successful effectiveness of the efficient information security (dependent variable).

Table III shows the results of the regression which revealed that information security rules and regulations ($t = 2.143$, significance $= 0.035$), secured internal and external business communication ($t = 3.881$, significance $= 0.000$), security consciousness management support ($t = 6.516$, significance $= 0.000$), business security culture ($t = 9.015$, significance $= 0.000$) and superior deterrent efforts ($t = 3.093$, significance $= 0.003$) were found to significantly affect the process of enhancing efficient information security.

In Table IV, the results of the regression show that the efficient information security ($t = 22.192$, significance $= 0.000$) was found to significantly affect the generation of an accurate business decision-making process.

4. Conclusion

Business information security is an essential theme in today's business environment. The intimidation intended for this vital business asset is sometimes uncontrollable by management.

The primary objective of this paper, which was presented in the proposed conceptual framework, has been to identify, quantifiably analyze and validate the factors that firms can apply to their security improvement projects in order to enhance their business information security outcomes.

The proposed conceptual framework hypothesized that information security rules and regulations, secured internal and external business communication, security consciousness management support, business security culture and superior deterrent efforts have a positive impact on enhancing efficient information security, which consequently has a positive impact on generating accurate business decision-making processes.

The analysis results also indicated that each of the above independent factors has a significant relationship with business information security. These findings are consistent with our research literature in information systems security.

Within this scope, and based on an empirical study, we showed an interesting finding in our results that there is positive and significant association between

Table II. Results of correlation analysis

		Information security rules and regulations	Secured internal and external business communication	Security consciousness management support	Business security culture	Superior deterrent efforts	Efficient information security	Accurate business decision-making process
Information security rules and regulations	Pearson's correlation	1	0.705	0.730	0.775	0.634	0.778	0.703
	Significance (two-tailed)		0.000	0.000	0.000	0.000	0.000	0.000
	n	101	101	101	101	101	101	101
Secured internal and external business communication	Pearson's correlation	0.705	1	0.914	0.908	0.809	0.940	0.858
	Significance (two-tailed)	0.000		0.000	0.000	0.000	0.000	0.000
	n	101	101	101	101	101	101	101
Security consciousness management support	Pearson's correlation	0.730	0.914	1	0.920	0.816	0.958	0.879
	Significance (two-tailed)	0.000	0.000		0.000	0.000	0.000	0.000
	n	101	101	101	101	101	101	101
Business security culture	Pearson's correlation	0.775	0.908	0.920	1	0.819	0.970	0.884
	Significance (two-tailed)	0.000	0.000	0.000		0.000	0.000	0.000
	n	101	101	101	101	101	101	101
Superior deterrent efforts	Pearson's correlation	0.634	0.809	0.816	0.819	1	0.853	0.821
	Significance (two-tailed)	0.000	0.000	0.000	0.000		0.000	0.000
	n	101	101	101	101	101	101	101
Efficient information security	Pearson's correlation	0.778	0.940	0.958	0.970	0.853	1	0.912
	Significance (two-tailed)	0.000	0.000	0.000	0.000	0.000		0.000
	n	101	101	101	101	101	101	101
Accurate business decision-making process	Pearson's correlation	0.703	0.858	0.879	0.884	0.821	0.912	1
	Significance (two-tailed)	0.000	0.000	0.000	0.000	0.000	0.000	
	n	101	101	101	101	101	101	101

Note: **Correlation significant at 0.01 level (two-tailed)

Table III.
Regression (coefficients) for testing *H1-H5*

Model		Coefficients[a] Unstandardized coefficients *B*	SE	Standardized coefficients *β*	*t*	Significance
1	Constant	−0.128	0.064		−2.011	0.047
	Information security rules and regulations	0.046	0.022	0.053	2.143	0.035
	Secured internal and external business communication	0.172	0.044	0.166	3.881	0.000
	Security consciousness management support	0.299	0.046	0.299	6.516	0.000
	Business security culture	0.426	0.047	0.431	9.015	0.000
	Superior deterrent efforts	0.088	0.028	0.088	3.093	0.003

Note: [a]Dependent variable: efficient information security

Table IV.
Regression (coefficients) for testing *H6*

Model		Coefficients[a] Unstandardized coefficients *B*	SE	Standardized coefficients *β*	*t*	Significance
1	(Constant)	0.293	0.158		1.849	0.067
	Accurate business decision-making process	0.925	0.042	0.912	22.192	0.000

Note: [a]Dependent variable: efficient information security

efficient information security and business decision-making processes. The analysis results ring true and are supported by various extant research literatures in this field. Although the proposed conceptual model may seem to be somewhat inaccurate to some readers, we propose that the components in the framework all do have a positive significant impact on improving the value of information security effects.

References

Akram, J.-K. (2011), "The value of competitive business intelligence system (CBIS) to stimulate competitiveness in global market", *International Journal of Business and Social Science*, Vol 2 No. 19.

Belsis, P. and Kokolakis, S. (2005), "Information systems security from a knowledge management perspective", *Information Management and Computer Security*, Vol. 13 No. 3, pp. 189-202.

Berinato, S. (2007), "The 5th Annual Global State Of Information Security: the end of innocence", *CIO Magazine* (a Joint Research Project of CIO and CSO in partnership with PriceWaterhouseCoopers), available at: www.pwc.com/en_BE/be/publications/state-of-infsecurity-pwc-07.pdf; (accessed June 23, 2008).

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2004), "The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers", *International Journal of Electronic Commerce*, Vol. 9 No. 1, pp. 69-104.

Dinev, T. and Hart, P. (2006), "An extended privacy calculus model for e-commerce transactions", *Information Systems Research*, Vol. 17 No. 1, pp. 61-80.

Eloff, J. and Eloff, M. (2005), "Integrated information security architecture", *Computer Fraud and Security*, No. 11, pp. 10-6.

Gordon, L.A., Loeb, M.P., Lucyshyn, W. and Richardson, R. (2005), *2005 CSI/FBI Computer Crime and Security Survey*, Computer Security Institute, San Francisco, CA.

Ishiguro, M., Tanaka, H., Matsuura, K. and Murase, I. (2006), "The effect of information security incidents on corporate values in the Japanese stock market", paper presented at the Workshop on the Economics of Securing the Information Infrastructure, Washington, DC, October 23-24.

Latimer-Livingston, N.S. and Tracy, L. (2008), "2008 update: what organizations are spending on IT security", Gartner Research.

McCarthy, M. and Campbell, S. (2001), *Security Transformation*, McGraw-Hill, New York, NY.

Malhotra, N.K., Kim, S.S. and Agarwal, J. (2004), "Internet users' information privacy concerns (IUIPC): the construct, the scale, and a causal model", *Information Systems Research*, Vol. 15 No. 4, pp. 336-55.

Nunnally, J.C. and Bernstein, I.H. (1994), *Psychometric Theory*, 3rd ed., McGraw-Hill, New York, NY.

Pallant, J. (2001), *SPSS Survival Manual*, Open University Press, Milton Keynes.

Park, I., Lee, J., Rao, H.R. and Upadhyaya, S. (2006), "Guest editorial part 2: emerging issues for secure knowledge management – results of a Delphi study", *IEEE Transactions on Systems, Man, and Cybernetics, Part A: Systems and Humans*, Vol. 36 No. 3, pp. 421-8.

Pavlou, P.A., Liang, H. and Xue, Y. (2007), "Understanding and mitigating uncertainty in online exchange relationships: a principal – agent perspective", *MIS Quarterly*, Vol. 31 No. 1, pp. 105-36.

Smith, H.J. (1994), *Managing Privacy: Information Technology and Corporate America*, University of North Carolina Press, Chapel Hill, NC.

Tam, P.-W. and Lawton, C. (2007), "For IT, 'dull' sounds pretty good", *The Wall Street Journal*, May 29, p. B3.

Van Slyke, C., Shim, J.T., Johnson, R. and Jiang, J. (2006), "Concern for information privacy and online consumer purchasing", *Journal of the Association for Information Systems*, Vol. 7 No. 6, pp. 415-44.

Wang, Y.-S., Wang, Y.-M., Lin, H.-H. and Tang, T.-I. (2003), "Determinants of user acceptance of internet banking: an empirical study", *Journal: International Journal of Service Industry Management*, Vol. 14 No. 5, pp. 501-19.

Whitten, J.L., Bentley, L.D. and Dittman, K.C. (2004), *System Analysis and Design Methods*, 6th ed., McGraw-Hill, New York, NY.

Further reading

Ezingeard, J., McFadzean, E. and Birchall, D. (2005), "A model of information assurance benefits", *Information Systems Management*, Vol. 22 No. 2, pp. 20-9.

McFadzean, E., Ezingeard, J.N. and Birchall, D. (2003), "Boards of directors engagement with information security", Henley Working Paper No. HWP0309, available at: www.henleymc.ac.uk

About the author

Akram Jalal-Karim is currently the Chairman of the Management Information System Department at Ahlia University, Manama, Kingdom of Bahrain. He is currently teaching

research methodology for business and finance, managing enterprise systems, management information system, project management, knowledge management, database management system, enterprise resource planning, and fundamental of management at Ahlia University. He holds a PhD in Information Management from Brunel University, UK. His Master's in Computer Science is from Metropolitan University, UK and his Bachelor in Information System Engineering from Westminster University, UK. His research and publication activities include enterprise resource planning, supply chain management, project management, business intelligence system, healthcare management system, knowledge management, e-governments, global business management, early warning systems (EWS), risk management, and data mining and data warehousing. He has a large number of publications and the first book in nearing completion. He has supervised a large number of Master's and is currently supervising four PhD students. He has been participating in several international and national projects and conferences as an organizer, reviewer and advisor. Akram Jalal-Karim can be contacted at: akarim@ahlia.edu.bh