Information Security: Cost and Individuals' Habit

Lubna Sulaiman

College of Commerce and Business Administration, Dhofar University

Abstract — *The aim of this research is to identify the availability levels of cost, habit, and Information Security (IS) and determining the impacts of cost, and habit on IS. The primary data of the study collected using manual distributed questionnaire. By using appropriate statistical test, the collected data has been analyzed. The reliability and hypotheses tested using several statistical methods such as multiple and linear regression test. While validity tested using Cronbach's alpha. The findings of the study proved that cost and habits has an effect on information security as they explained (18.5%) of the variation in IS. However, implications have discussed.*

Keywords — *cost, habit, Information Security(IS).*

I. INTRODUCTION

Information security is a program that protects all confidential data, whether physical or electronic, dating back to the use of the information protection order to antiquity. It also protects information and data from tampering and spoiling it. It works to balance the management of data confidentiality and maintain loss in any circumstance[1]. This is done more in managing the various operational risks, the steps that define the assets, their sources, the risks resulting from them, the expected effects and the expected rules during these operations, followed by the recommendation of the risk management plan. This achieves or results in the greatest degree of discipline and accuracy[2]. The adoption of information technology has been investigated by few research, providing e-government services from citizens as well as employees perspectives [3]–[6], accepting E-Mail System University Students[7], Clients acceptance of Internet Banking[8], [9], adopting ICT by SMEs employees [10], and customers attitudes to adopt e-shopping [11], [12]. Moreover, from the teaching assessment perspective also few studies has been done in the context of the study[13], [14].

Academics and professionals share the development of instructions and policies, and to adjust industrial standards on private passwords, anti-virus programs, protection of encryption programs, legal literacy and training standards for users. This confusion may be greater through large sets of laws, rules and regulations that change, affect, access, process, store, transport, and maintain risk[15]. The protection of information is continuous, that is, it necessarily needs continuity in keeping up with all the updated and advanced safety levels and methods in protecting this information. With the development of means of communication and communication, the world today relied on sending some data through networks, Leakage and theft, access to rival people and misinformation attack, direct access to connection cables, and is considered the biggest threat to safe information. Viruses are known as small subversive programs, designed for destructive purposes, and attack files stored on the computer by professional programmers who aim to harm another user's computer for some reason, and the most dangerous malicious programs are routine, and the viruses have the ability to replicate and spread significantly[16]. Therefore, the world today maintains the security of information in terms of who will receive this data. There are ways to secure the information, the most important of which is: A firewall: a device or application that is placed at the network filters, data monitoring: is a set of applications that monitors internal and external data to the network. Also use effective virus programs to continue to respond to viruses and the provision of an electrical provider to avoid the problem of power outages and the use of HTTP Everywhere for users of the browser Google Chrome and keep up-to-date updates of antivirus programs and rely on the SFTP technology when I send data over the Internet and expand Scope of security awareness and awareness of users and the policy of backing up information. To determine their compatibility with the International Standard for Information Security (ISO / IEC 27002), and to stand on the downside in the safe practice of information and make decisions to improve them. The study focused on three dimensions of safe human resources: physical, environmental and technical security. This study was based on field visits and personal interviews. The results showed that the percentage of human resources compatibility was 100%, physical and environmental security 90.5% and finally 90.5%. The study resulted in many recommendations, including: Continuing training and educating students in libraries to use information resources and services, and work in the development of secure

information, and provide an alternative source of energy to operate the computer and backup systems and software [17], [18].

II. LITERATURE REVIEW

Some research leaks for the International Space Station have raised habits for behavior to secure information. With the exception of Vance et al in 2012. It was looking for future research on different types of behavior of the International Space Station. Human habits can be considered to bind securely to complex information. This needs future research to study the process that makes the employee interested and not negligent and has the ability to change negative habits and behavior of non-compliance[19].

From the research of safe behavioral information security research has offered many different theoretical models derived from the disciplines to describe or predict the political negatives of the safe information of employees and related objects. This has led to the application of many theories to different disciplines to various political violations of various forms of information security behavior. There are negative aspects: many of them are similar. Such as deterrence theory [20], [21], costs under the rational choice theory [19], and constraints on suppression. This has given rise to theories of complementary explanations that can be combined into one model to supplement the expected limitations of individual models. [19], [20], [22].

For the research and theory of the International Space Station, a study that compares existing models and experimented with them will be valuable, given the many information security System approaches [23]. UMISPC takes a first step towards this goal by examining the suitability of experimental models as well as the extent to which different theories are complementary. In terms of future research and theory, UMISPC aims to inspire future research in four ways. First, UMISPC can be tested in different contexts to determine its limits and identify situations in which its components fail to explain the phenomenon. Second, future research could further expand the UMISPC by adding additional structures and observers in different contexts or by seeking to strengthen the boundary conditions of the theory. Thirdly, future research may find that some UMISPC structures may be irrelevant in some information security System contexts. Fourth, future research can test our results at different scales. Finally, we hope that monotheistic research will inspire future information security research to develop more theories and empirically demonstrate important differences between competing theories in the information security System context that have not been achieved through current procedures. Information security System practitioners may be interested in understanding why employees have or are not committed to information security System policies [21]. This understanding can provide a basis for information security education or for intervention campaigns in organizations. With different information security System models / theories, practitioners face the question of which one to apply. This raises the question: should they choose from deterrence, rational choice, habit, preventive stimulation, or else, or should they all apply at the same time, which can be impractical? Similarly, the extent to which existing models complement each other empirically may be unclear. UMISPC, although currently tentative, proposes one answer to these questions that future research may be able to refine or further support. Practitioners can use UMISPC not only to diagnose why some employees fail to comply with information security System policies in the organization, but why others are committed to doing so. Finally, our article also presents a list of current models by listing all the previously identified structures on the behavior of the International Space Station in a single sheet.

The rewards and costs of an intent behavior were also included as extensions to the original theory[24]. These extensions were built upon the PMT model and extant research on PMT, which has consistently shown the importance of rewards as motivators to engage in a behavior, and the importance of costs as motivators to disengage from a behavior. Effectively, PMT synthesizes with HBM to explain why individuals protect themselves from perceived threats[24].

RESEARCH MODEL

Based on the literature the suggested model is presented in figure (1). More, the research suggests the following hypotheses:

Figure (1): suggested Model

H1: Cost has an effect on information security within the organization.

H2: habit has an effect on information security within the organization.

III. RESEARCH METHODOLOGY

A questionnaire-based survey has been distributed manually to collect the primary data from the targeted sample. However, the study instrument has been prepared based on previously validated models [25]. Valid questionnaires for analysis were 84 questionnaires. Also, reliability test (Cronbach's Alpha) was used to check the validity of the gathered data which obtained by questionnaire[26]. The results of this test, as appears in table (1), confirmed the internal consistency of construct and measures validity. As well as, simple and multiple regression were used for hypotheses test[27], [28].

IV. DATA ANALYSIS

Table 1 shows the coefficient of alpha Cronbach's which are ranging from (0.705) for habit, (0.724) for the IS, and (0.840) for cost.

Table 1. Descriptive and Reliability Statistics

	N	Mean	Std. Deviation	Cronbach's Alpha
Cost	84	4.1667	.89995	.840
Habit	84	3.5040	1.04963	.705
IS	84	3.4702	.97050	.724

Multiple linear regression analysis was conducted with the cost, and habit as predictor variables, and IS as a dependent variable.

Table 2. Results of regression analysis ^a

Adjusted R ²	F	Sig.
.185	10.393	.000 ^b

a. Dependent Variable: IS

b. Predictors: (Constant), cost, habit

Table 3. the results of hypotheses test ^a

Suggested Hypotheses	B	Std. Error	Beta	t	Sig
H1	.425	.095	.460	4.496	.000
H2	-.204	.110	-.189	-1.848	.068

a. Dependent Variable: IS

A number of 84 responses have been analyzed. The statistical results presented in Table 2 shows that the entire model was significant { $F = 10.393$, $P < 0.001$ } with adjusted R^2 being (0.18) which explains only (18 %) of the changes in the IS. Both constructs cost ($\beta = 0.460$; $t = 4.496$), and habit ($\beta = -0.189$; $t = -1.848$) were significant.

V. DISCUSSION

The main objective of this study is to identify the effects of cost and habit on IS. The availability level of cost is high since the mean is (4.16). More, the availability level of habit is high because the mean is (3.5). In addition, IS availability level is high as the mean is (3.47).

The study found that cost and habits have a significant statistical impact on IS and explains (18%) of the variation in the independent variable.

According to the results, the organizations should increase restrictive procedures of information security and make sure that all employees will understand the sequences of violating them and enhancing the background of people about the importance of Information security to avoid any problems.

REFERENCES

- [1] M. Siponen, M. Adam Mahmood, and S. Pahlila, "Employees' adherence to information security policies: An exploratory field study," *Inf. Manag.*, vol. 51, no. 2, pp. 217–224, Mar. 2014, doi: 10.1016/j.im.2013.08.006.
- [2] J. D'Arcy and T. Herath, "A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings," *European Journal of Information Systems*, vol. 20, no. 6, Palgrave Macmillan Ltd., pp. 643–658, 14-Jun-2011, doi: 10.1057/ejis.2011.23.
- [3] M. N. Alraja, S. Hammami, and T. Alhousary, "Factors affecting e-government services adoption: Field study," *J. Theor. Appl. Inf. Technol.*, vol. 78, no. 1, 2015.
- [4] M. N. Alraja, S. Hammami, B. Chikhi, and S. Fekir, "The influence of effort and performance expectancy on employees to adopt E-government: Evidence from Oman," *Int. Rev. Manag. Mark.*, vol. 6, no. 4, 2016.
- [5] M. N. Alraja, "The effect of social influence and facilitating conditions on e-government acceptance from the individual employees' perspective | Efekt Wpływu Społecznego Oraz Warunków Ułatwiających Akceptację E-Administracji Z Punktu Widzenia Indywidualnych Pracowników," *Polish J. Manag. Stud.*, vol. 14, no. 2, 2016, doi: 10.17512/pjms.2016.14.2.02.
- [6] R. Mourta, F. Salem, and S. Alshaer, "Citizen Engagement and Public Services in the Arab World: The Potential of Social Media," Jun. 2014.
- [7] M. N. Alraja, "User Acceptance of Information Technology: A Field Study of an E-Mail System Adoption from the Individual Students' Perspective," *Mediterr. J. Soc. Sci.*, vol. 6, no. 6 s1, pp. 19–25, Nov. 2015, doi: 10.5901/mjss.2015.v6n6s1p19.
- [8] M. N. Alraja, B. F. Salim, M. A. Uddin, and M. Yousoof, "The adoption of internet banking: Clients' perspective in Oman," *Int. Rev. Manag. Mark.*, vol. 6, no. 4, 2016.
- [9] A. Shatat, "FACTORS AFFECTING THE ADOPTION AND USAGE OF ONLINE SERVICES IN OMAN," *J. Internet Bank. Commer.*, vol. 22, no. S7, 2017, Accessed: 23-Dec-2018. [Online]. Available: <http://www.icommercecentral.com>.
- [10] M. A. Hussein, H. Ahmed, and M. N. Alraja, "The adoption of information and communication technology by small and medium enterprises in Oman: Case of Dhofar region," *J. Bus. Retail Manag. Res.* *www.jbrmr.com A J. Acad. Bus. Retail Manag.*, vol. 11, no. 3, pp. 64–71, 2017, Accessed: 02-May-2017. [Online]. Available: http://www.jbrmr.com/admin/content/pdf/content_65013_17-04-22-11-45-45.pdf.
- [11] M. N. Alraja and B. Chikhi, "Perceived Factors affecting Customers Attitudes toward Electronic Shopping: an Empirical Study," *Int. J. Econ. Res.*, vol. 12, no. 3, pp. 815–823, 2015, Accessed: 17-May-2019. [Online]. Available: http://serialsjournals.com/abstract/51627_17.pdf.

-
- [12] K. Hassanein and M. Head, "The Impact of Infusing Social Presence in the Web Interface: An Investigation Across Product Types," *Int. J. Electron. Commer.*, vol. 10, no. 2, pp. 31–55, Dec. 2005, doi: 10.2753/JEC1086-4415100202.
- [13] M. A. Uddin, F. Ahmar, and M. N. Alraja, "E-examinations for management students in Oman," *Int. J. Appl. Bus. Econ. Res.*, vol. 14, no. 1, 2016.
- [14] J. C. Sánchez-Prieto, S. Olmos-Migueláñez, and F. J. García-Peñalvo, "Informal tools in formal contexts: Development of a model to assess the acceptance of mobile technologies among teachers," *Comput. Human Behav.*, vol. 55, pp. 519–528, Feb. 2016, doi: 10.1016/j.chb.2015.07.002.
- [15] J. D'Arcy, T. Herath, and M. K. Shoss, "Understanding Employee Responses to Stressful Information Security Requirements: A Coping Perspective," *J. Manag. Inf. Syst.*, vol. 31, no. 2, pp. 285–318, Oct. 2014, doi: 10.2753/MIS0742-1222310210.
- [16] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Inf. Syst. Res.*, vol. 20, no. 1, pp. 79–98, 2009, doi: 10.1287/isre.1070.0160.
- [17] M. A. hamdan, "The reality of safe practices in the main library of SQU, and its compatibility with the International Information Security Standard," *Qscience Proc.*, p. 1, 2007, Accessed: 02-Aug-2020. [Online]. Available: https://www.google.com/search?ei=xOUmX8jMEcHbgwfdn464Dw&q=The+reality+of+safe+practices+in+the+main+library+of+SQU%2C+and+its+compatibility+with+the+International+Information+Security+Standard.&oq=The+reality+of+safe+practices+in+the+main+library+of+SQU%2C+and+its+compatibility+with+the+International+Information+Security+Standard.&gs_lcp=CgZwc3ktYW IQDFCJDliJDmD-FWgBcAB4AIABAIAgBAJIBAJgBAKABAAABAqoBB2d3cy13aXQwAQDAAQE&scient=psy-ab&ved=0ahUKEwjIvtm79PzqAhXB7eAKHd2PA_cQ4dUDCAw.
- [18] F. M. Alkhalidi, S. M. Hammami, S. Kasem, A. Rashed, and M. N. Alraja, "Enterprise System as Business Intelligence and Knowledge Capabilities for Enhancing Applications and Practices of IT Governance," *Int. J. Organ. Collect. Intell.*, vol. 7, no. 2, pp. 63–77, 2017, doi: 10.4018/IJOCL.2017040105.
- [19] A. Vance, M. Siponen, and S. Pahlila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," 2012, doi: 10.1016/j.im.2012.04.002.
- [20] J. D'Arcy and A. Hovav, "Deterring internal information systems misuse," *Commun. ACM*, vol. 50, no. 10, pp. 113–117, Oct. 2007, doi: 10.1145/1290958.1290971.
- [21] M. Siponen and A. Vance, "Neutralization: New Insights into the Problem of Employee Information Systems Security Policy Violations," *MIS Q.*, vol. 34, no. 3, p. 487, 2010, doi: 10.2307/25750688.
- [22] M. Siponen, M. Karjalainen, and uprateek Sarker, "Unearthing Social Mechanisms that Lead Employees to Violate IS Security Procedures: An Inductive Study," in *IFIP TC 8 International Workshop on Information Systems Security Research*, 2010, Accessed: 02-Aug-2020. [Online]. Available: <https://ifip.byu.edu/ifip2010.html>.
- [23] M. T. Siponen, "Analysis of modern IS security development approaches: towards the next generation of social and adaptable ISS methods," *Inf. Organ.*, vol. 15, no. 4, pp. 339–375, Oct. 2005, doi: 10.1016/J.INFOANDORG.2004.11.001.
- [24] J. E. Maddux and R. W. Rogers, "Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change," *J. Exp. Soc. Psychol.*, vol. 19, no. 5, pp. 469–479, Sep. 1983, doi: 10.1016/0022-1031(83)90023-9.
- [25] G. D. Moody, M. Siponen, and S. Pahlila, "Toward a Unified Model of Information Security Policy Compliance," *MIS Q.*, vol. 42, no. 1, pp. 285–311, Jan. 2018, doi: 10.25300/MISQ/2018/13853.
- [26] M. N. Alraja and N. R. Alomian, "THE EFFECT OF INFORMATION TECHNOLOGY IN EMPOWERMENT PUBLIC SECTOR EMPLOYEES: A FIELD STUDY," *Interdiscip. J. Contemp. Res. Bus.*, vol. 5, no. 1, pp. 805–815, 2013, Accessed: 17-May-2019. [Online]. Available: <https://journal-archievers32.webs.com/805-815.pdf>.
- [27] M. N. Alraja and N. M. M. Malkawi, "E-Business Adoption in Banking Sector: Empirical Study," *Indian J. Sci. Technol.*, vol. 8, no. 27, Oct. 2015, doi: 10.17485/ijst/2015/v8i27/70739.
- [28] S. Hammami, H. Al Samman, and M. Alraja, "The role of CRM systems in consolidating the strategic position of the organization," *Int. J. Appl. Bus. Econ. Res.*, vol. 13, no. 4, 2015.