International Journal of Recent Advances in Multidisciplinary Topics
Volume 4, Issue 5, May 2023
https://www.ijramt.com | ISSN (Online): 2582-7839

The Impact of Information Security Management System (ISMS) on e-Government Adoption

Ramesh Kumar Moona Haji Mohamed[1*], Dilashenyi Selvarajah[2], Sarala Silvaraju[3], K. Raja Kumar K. Kathiravelu[4], Prem Kumar Nadarajan[5], Nor Azim Ahmad Radzi[6]
[1,4,5,6]*Faculty of Business & Finance, Universiti Tunku Abdul Rahman, Jalan Universiti, Malaysia*
[2]*Segi University, Selangor, Malaysia*
[3]*Faculty of Economics & Management, Universiti Kebangsaan Malaysia, Selangor, Malaysia*

***Abstract*: Data breaches often affect an organization's reputation and can actually lead to customer churn, loss of revenue, loss of operational continuity, and more. This current study investigated the extent to which Information Security Management System (ISMS) has a positive impact on technology adoption (e-government) of public services in government sector. About 112 data been collected from senior managers, strategists and technicians with management experience) of public services in government department using stratified random sampling. Further data have been analyzed using SPSS and SMART PLS - SEM. Based on results there were, several solutions have been suggested to overcome all the challenges facing the organization with future study suggestion and limitation of the study.**

***Keywords*: e-government, confidentiality, integrity, availability, accountability, technology adaption.**

1. Introduction

The government recognizes the importance of the flexibility factor in today's technology and it is beginning to exploit its features in maintaining control and communication with the people. The transition from electronic government (e-government) to m-government requires a study on the process of integration between e-government and m-government other than studies of constraints or pressures that may affect the transition process, notably the security of government's data. Therefore, System (ISMS) been created.

Information Security Management System (ISMS) is a systematic and structured approach to information management. Implementation of ISMS includes policies, processes, procedures, organizational structure, software and even the functionality of a hardware.

MAMPU has obtained the ISMS Certification (Information Security Management System) Certification under ISO/IEC 27001: 2013 Information Security Management Systems for a period of 3 years from 13 August 2016 to 12 August 2019 with certificate number: 027-ISO49 by Cyber Security Malaysia [1].

ISMS dates back to the early 1990s when the UK's Department of Trade Industry called for the British Institution Standard to develop standards that could raise awareness of security issues and propose controls to protect information.

Not to mention, Cyber threats are now becoming increasingly difficult to predict and challenging. Once an intruder took a long time to hack into ICT assets, but now, with the help of hacking tools available on the internet, these activities can be done easily and quickly. Therefore, every agency should be aware of this situation. The statistics of security incidents will continue to increase if each agency does not take seriously or fail to take enforcement action. Accordingly, on Feb 24, 2010, the Cabinet decided that all Critical National Information Infrastructure (CNII) agencies implement information security system management in accordance with MS ISO/IEC 27001 and obtain ISMS Certification within 3 years. [1]

The objective of ISMS is to manage and protect the security of information in accordance with the requirements and expectations of the bearer. It emphasizes on the concept or principle of information security, namely, the preservation of confidentiality, integrity and availability.

Therefore, this study is to investigate the extent to which security management or Information Security Management System (ISMS) has a positive impact on technology adoption (e-government) of public services in government sector.

2. Literature Review

Data security, privacy and compliance have always been key factors in Information Security Management, but as business processes change, it is increasingly difficult to do so. Therefore, compared to data security, what the company needs to do today is not important [2].

According to the [3] the definition of information security is the group of technologies, standards, policies, and management practices that applied to information to ensure its security. Data security, on the other hand, refers to the process of protecting data from unauthorized access to computers, databases, and websites. In addition, data security protects and prevents data from destroying. For example, data security technologies

*Corresponding author: rameshk@utar.edu.my

include backup, data masking, and data erasure. The main data security technical measures are encryption, such as digital data, software or hardware, and the hard drive encrypted and so unauthorized users and hackers are unreadable to the data [4].

However, security issues are beyond the system. On the other hand, security breaches often caused by human error or malicious insider behavior. According to a recent report, 63% of confirmed data breaches are due to the use of weak passwords, default passwords or stolen passwords and other common errors send sensitive data to the wrong person, not properly handling company data, IT system configuration errors, and loss and Stolen laptops and mobile devices [5].

Data is important for any business to protect the private data of employees and customers, which are a top priority for all organizations, whether large or small [5]. Data protection is legally important, so if a data breach occurs, it can lead to legal proceedings, fines, and even criminal proceedings. As regulations vary from region to region, it is also important to understand the compliance requirements of each jurisdiction. [6]. Below are the dimension of Information Security Management

A. Confidentiality

The definition of the confidentiality is which the secret data must be kept secret. This means that if someone wants someone to use some data, the operating system should make the data available to those specific people, and nobody can view the data. It avoids the unauthorized disclosure of security information (Khan, 2017; Tchernykh, Schwiegelsohn, Talbi, & Babenko, 2019).

H1: Confidentiality has positive impact on e-government adoption

B. Integrity

The definition of integrity is limiting unauthorized modifications to secure information. Unauthorized users should not be allowed to modify data without the owner's permission. Data modification includes not only changing or deleting data, but also deleting data or adding erroneous data to change its behaviour [7], [8].

H2: Integrity has positive impact on e-government adoption

C. Availability

The definition of the availability is which no one can bother the system to make it unusable. It ensures that the system runs in a timely manner and does not deny the services of authorized users. This is to limit unauthorized users by hiding information, resulting in the denial of authorized users' services. [7], [8].

H3: Availability has positive impact on e-government adoption

D. Accountability

Accountability in dealing with employees is responsible for their behaviour in information security. Organizations can fulfil their responsibilities by informing employees of their information security policies and by establishing discipline practices and procedures. Accountability is an employee's responsibility for tasks assigned by an employer in an organization [9]. A sense of responsibility for the job provided is important because through a sense of responsibility, an employee will make more informed decisions to avoid making any mistakes. This can help improve the productivity level of the work and achieve the main objectives of an organization.

H4: Accountability has positive impact on e-government adoption

Research on the level of technology adoption among government officials is increasing. Some theoretical models that attempt to explain the relationship between consumer attitudes and beliefs in the use of technology already exist such as Theory of Reasoned Action (TRA), Theory of Planned Behavior (TPB), and Technology Acceptance Model (TAM).

Among them, TAM is the most widely accepted model for its extensive empirical support, but there are still shortcomings in addressing several factors in the process of adopting E-government and m-government [10], [11]. TAM confirms the Perceived usefulness (PU) factor while Perceived ease of use (PEOU) is a key determinant of the use of information technology (TM). The complex nature of technology adaptation has led to the need to study additional factors such as security management [12], [13].

3. Methodology

This study aims to assess the extent to which security management or the Information Security Management System (ISMS) has a positive impact on the e-government adoption of public service jobs in the government sector. The key informants are senior managers or their partners (such as senior managers, strategists and technicians with management experience). In addition, these Respondents should have experience and/or knowledge in the IT field. The questionnaire was adapted from [14] where it produced through previous literature reviews. In addition to questionnaire items for collecting demographic information, the questionnaire consisted of two sections: one to evaluate ISM practices and the other to evaluate e-government adoption. Questionnaires related to demographic statistics related to gender, education, business age, and age, number of employees, department, and occupation level. The questionnaire was distributed throughout the government departments in Malaysia by stratified random sampling [15].

4. Analysis and Result

About 127 respondents answered the questionnaire and 15 of them excluded due to incomplete data. Data from 112 respondents were analyze using SPSS and SMART PLS -SEM. The sample size for the acceptance study depends on the type of research in case in an exploratory study, the size of this sample is sufficient to represent people's perspective and base on G power.

A. Measurement model

1) Convergent Validity

The first phase validity test is used to identify that unobserved variables can be measured by using each observed variable construct through Confirmatory Factor Analysis

(CFA) or commonly referred to as factor analysis. According to [16], an indicator is considered to have a high degree of validity when it has a loading factor value greater than 0.70. However, indicators with loading factor of 0.50 to 0.60 are still acceptable. From the first test results, there are two indicators with a loading factor of less than 0.5 (λ <0.5). This indicates that there are invalid indicators or that have not met the convergent validity test and therefore require model validation. By looking at the loading factor, an indicator with a value below 0.5 will be redefined. Therefore, the researchers eliminated these indicators and then re-speculated the research model. Here is the result of respiration in table 1.

Table 1
Convergent validity

Items	Loadings	CR	AVE	VIF
AC1	0.687	0.903	0.609	1.338
AC2	0.711			1.534
AC3	0.827			2.565
AC4	0.86			3.333
AC5	0.806			2.203
AC6	0.778			2.265
AV1	0.898	0.923	0.799	2.562
AV2	0.922			2.864
AV3	0.861			2.028
C1	0.897	0.916	0.687	3.329
C2	0.857			2.484
C3	0.813			2.267
C4	0.768			1.745
C5	0.805			2.099
INT1	0.829	0.918	0.692	2.015
INT2	0.884			2.645
INT3	0.851			2.588
INT4	0.825			2.211
INT5	0.767			1.883
IT1	0.822	0.889	0.668	1.995
IT2	0.833			2.135
IT3	0.819			1.905
IT4	0.794			1.872

The second phase validity test is the discriminant validity test. This test is based on the value of cross loading measurements with the construct and Average Variance Extracted (AVE) values. AVE is good, required to be greater than 0.50. The following are the values from the AVE table 1. The table above shows the AVE values of the research model. It can be seen from the table that the AVE Value for all of the research variables is above 0.5, so the AVE value for discriminant validity testing is met for further testing.

Table 2
HTMT

	Acc	Av	Con	Gov	Int
Acc	HTMT				
Av	0.629	HTMT			
Con	0.829	0.619	HTMT		
Gov	0.784	0.455	0.691	HTMT	
Int	0.691	0.576	0.474	0.472	HTMT

The Heterotait Monotrait Ratio (HTMT) ratios (Table 2) also indicate that the validity of the discrimination is achieved based on a correlation value of less than 0.90 (HTMT.90 <0.90). Table 2, the validity value of differentiation based on the Heterotrait Monotrait ratio (HTMT) is less than the threshold value of 0.85. Then there is the validity of the differentiation between the constructs. Therefore, it's achieved.

B. Structural Model

The evaluation of the inner model done by looking at the Determination Coefficient. The Determination coefficient aims to measure the extent to which the model's ability to explain the variance of the dependent variable. The value of the coefficient of determination is between zero and one. If the value of the coefficient of determination is small or is less than or equal to 0.500 ($R^2 \leq 0.500$), then the ability of the independent variables to explain the variation of the dependent variable is very limited. Whereas if the value of a large coefficient of 0.500 ($R^2 > 0.500$) means the ability of the independent variables to provide almost all the information needed to predict the variance of the dependent variable. Based on Table R Square (R^2) it can be conclude that Confidentiality, Integrity, Availability, Accountability can explain the behavioral intention variance of 0.497 or 49.7% through linear relationships. While the remaining 0.503 or 50.3% were, affect by other variables outside of this study. The effect Size (f square) also to determine how well is the model. Uphold that effect sizes of 0.35, 0.15, and 0.02 indicate a large, medium, and small effect, respectively. Highlighted that R^2 values of 0.75, 0.50, and 0.25 reflect substantial, moderate, and weak values respectively. The results shows moderate R square and confidential has highest effect size followed by Integrity, availability and accountability. While the PLS prediction ($Q2^)$ also shows 42.8%.

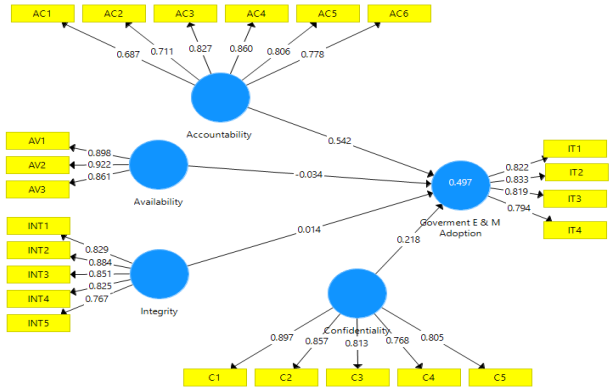

Fig. 1.

C. Hypothesis Results

The table above shows that the relationship between Confidentiality, Integrity, Availability, and behavioral intention is significant with a T-statistic of 3.496.2.198, 3.022 while Accountability (T Statistic< 0.837) not significant. The value of the original sample estimate is positive at 0.31804 indicating that the direction the relationship between Confidentiality, Integrity, Availability, Accountability and behavioral intention is positive. Thus, the hypothesis in this study states, "Information Security Management System in public services in government sector has a direct and significant positive impact on behavioral intention.

Table 3
Hypothesis results

Hypothesis	Beta value	Std Error	T Value	P Values
H1	0.449	0.128	3.496	0
H2	0.159	0.072	2.198	0.014
H3	0.322	0.107	3.022	0.001
H4	0.1	0.12	0.837	0.201

LL	UL	R2	F2	Q2	Decision
0.232	**0.654**	**0.207**			**Supported**
0.053	**0.291**	**0.041**			**Supported**
0.156	**0.508**	**0.001**			**Supported**
-0.095	0.294	0.497	0.000	0.428	Not supported

5. Discussion and Managerial Implication

Data security of human resource management has brought several positive impacts, but it also has some negative impacts toward the company. First of the negative impact for the data encryption is high cost. Government should not need to hire any unnecessary third parties to handle the encryption process. For example, the IT department of Government should develop a group of IT specialists to overcome the encryption process. This is because developing its own IT specialist group can reduce the cost of the encryption process. If Government hire a third party like IT company to handle the encryption process, it will be another unnecessary cost for Government and this unnecessary cost will be very expensive. Besides, Government should also develop a new IoT encryption chip to replace encryption process. This is because the new IoT encryption chips can reduce the cost of the encryption process. For example, MIT had created a new IoT encryption chip, which can replace the encryption process in order to decrease the power requirements for future internet-connected devices.

Furthermore, Government should implement the Employee security awareness training. This training is a great strategy for reducing the chances of a data breach. This is because if the employees are aware of corporate security policies and basic security principles and the consequences of breaking the rules will reduce the insider taking part either wailing or accidently in a breach. This training also can greatly lower down the success rate of attacks commonly associated with data breaches such as phishing. Besides that, Government can weed out the old and ineffective training methods and establish a new method. This will increase the interest of employees on the security awareness training. Government should consider how to make employees feel a sense of belonging to the company's security, which requires more creativity and personalization through the security training. In addition, Government also can establish a strong compliance-training program to encourage employees to improve security awareness. For example, send a regular email that reminds employees to update security software, passwords or require them to acknowledge security policies. Although the actual impact is small but this effort is better than nothing is.

Moreover, when updating the program, it might get some new bugs. So, in order to avoid and fix the software bug, Government can adopt the bug tracking tools. Due to the advances in technology, there are several types of bug tracking tools. When Air Asia using bug-tracking tools will reduce the chance of errors and helps to fix the bugs. Therefore, Government can implement the test automation. It is a software to control the execution of tests and compare the actual test results against predicted results. Besides that, Government should check the application from time to time. This is because keeping a check on the application from time to time will help to indicate an error early in the process. However, updating the system is very important. Government should update the system because upgrade the system allows computer to get the additional protections and ensure that system has the latest defensive solutions helps and prevents the unauthorized access by malware or crackers. Nowadays, the hacker is continually designing a new way of attacking the user's system. Therefore, Government should keep its software up to date in order to get benefit from latest security tools.

In addition, updating software will frequently provide some features and speed enhancements that will improve the existing one. The software program may gain a new stability and no more crashing. Updating the software might boost the program performance of Government.

6. Futures Study Suggestion, Limitation and Conclusion

This study is focus on e government only; in the future, it can study M government as well as add moderator and mediator variables as well as the extent of the research model. This study focuses only on senior managers, strategists and technicians with management experience) of public services in government, department and future studies can study other respondents. We also encountered many problems during this study where the data we needed was sensitive and confidential so it was difficult to collect it, which took 6 months. We also cannot cover all government departments due to privacy issues.

Government is concerned about the privacy of its customers. Therefore, Government is committed to collecting personal information from customers and protecting their privacy in all possible ways. Government uses the encryption process to improve data security, so it is difficult for hackers to steal customer information. In order to improve data security, Government should replace the new encryption process with new IoT encryption. The chip's data transfer speed is faster, storage requirements are lower, and higher security provided. In addition, Government is constantly improving its data security skills, knowledge and policies. Therefore, if a data breach occurs, the organization's employees have more ability and knowledge to handle and resolve. Finally, yet importantly, Government regularly updates its own system because it protects Government from known security breaches.

For recommendations, Government should use an error-tracking tool, which reduces the chance of errors and helps fix errors. In short, it has had some impact on Government's strong customer data security. This is because strong data security will ultimately build customer confidence and increase customer loyalty to Government.

References

[1] MAMPU, MyGOV - The Government of Malaysia's Official Portal. (2019). https://www.malaysia.gov.my/portal/content/30089?language=my

[2] Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. computers & security, 56, 70-82.

[3] Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: guidelines for effective information security management. Auerbach Publications.

[4] Gerhart, D. E., Lappi, C., Lipps, D. R., & Walker, W. J. (2018). U.S. Patent No. 9,959,218. Washington, DC: U.S. Patent and Trademark Office.

[5] Biro, M. M. (2017, December 07). Data Security Must Be a Top Priority for HR. Retrieved from https://www.huffingtonpost.com/meghan-m-biro-/data-security-must-be-a-t_b_10932396.html

[6] Park, S., Akatyev, N., Jang, Y., Hwang, J., Kim, D., Yu, W., & Kim, J. (2018). A comparative study on data protection legislations and government standards to implement Digital Forensic Readiness as mandatory requirement. Digital Investigation, 24, S93-S100.

[7] Khan, W. (2017, March 23). Basic Concepts of Security. https://www.prolifics.com/blog/basic-concepts-security

[8] Tchernykh, A., Schwiegelsohn, U., Talbi, E. G., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. Journal of Computational Science, 36, 100581.

[9] Azadi, M., Zare, H., & Zare, M. J. (2018). Confidentiality, Integrity and Availability in Electronic Health Records: An Integrative Review. In Information Technology-New Generations (pp. 745-748). Springer, Cham.

[10] Lai, P. C. (2017). The literature review of technology adoption models and theories for the novelty technology. JISTEM-Journal of Information Systems and Technology Management, 14(1), 21-38.

[11] Taherdoost, H. (2019). Importance of Technology Acceptance Assessment for Successful Implementation and Development of New Technologies. Global Journal of Engineering Sciences, 1(3).

[12] Davis, F. D., & Venkatesh, V. (1996). A critical assessment of potential measurement biases in the technology acceptance model: three experiments. International journal of human-computer studies, 45(1), 19-45.

[13] Davis, F. D., Davis, G. B., Morris, M. G., & Venkatesh, V. (1989). Technology acceptance model. Journal of Management Science, 982-1003.

[14] Chang, S. E., & Lin, C. S. (2007). Exploring organizational culture for information security management. Industrial management & data systems.

[15] Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. John Wiley & Sons.

[16] Hair Jr, J. F., Hult, G. T. M., Ringle, C., & Sarstedt, M. (2016). A primer on partial least squares structural equation modeling (PLS-SEM). Sage publications.