INTERNATIONAL JOURNAL OF RESEARCH IN SOCIAL SCIENCES & HUMANITIES

An International Open-Access Peer Reviewed Referred Journal

Impact Factor: 8.909 E-ISSN : 2249 – 4642 P-ISSN: 2454 - 4671

Evaluation of Cyber Security Management in Light of the Technology Acceptance Model

Rafid Abdulwahid Mhawi, Prof. Dr. Ali Hasson Fandi

College of Administration and Economics, University of Baghdad, Iraq

DOI: http://doi.org/10.37648/ijrssh.v11i03.029

Paper Received:

14th August, 2021

Paper Accepted:

09th September, 2021

Paper Received After Correction:

10th September, 2021

Paper Published:

12th September, 2021

How to cite the article: Rafid Abdulwahid Mhawi, Prof. Dr. Ali Hasson Fandi, Evaluation of Cyber Security Management in Light of the Technology Acceptance Model, July-September 2021 Vol 11, Issue 3; 492-507 DOI: http://doi.org/10.37648/ijrssh.v11i03.029

ABSTRACT

The main objective of the research is to investigate the correlation and influence between cyber security management and the technology acceptance model in the Iraqi Ministry of Interior. The data was collected from (150) respondents represented by an intentional sample of the Directorate of Systems and Informatics and the Information Technology Department in the General Directorate of Human Resources Management and for data analysis, statistical programs (AMOS, SPSS) were employed. By adopting appropriate statistical methods, the results of the research showed that the Ministry of Interior, whenever it tries to pay attention to cyber security management, the more it is reflected in the level of technology acceptance. In other words, cyber security management has a fundamental and influential role in the extent of acceptance of the technology that will be adopted within the ministry.

Keywords: *cyber security management, technology acceptance model*

INTRODUCTION

Despite advances in technology and countermeasures and situational awareness, electronic violations continue to increase in number, complexity, and risk (Ablon, 2014: 11). Therefore, the interest in cyber security increases with the increase in technological progress and the increase in the interest in cyber issues. As environmental changes occur very frequently, making it difficult, if not impossible, to maintain this security (Tisdale, 2016: 229). Cyber security has generally been associated with three aspects of IT "people, process, and technology" (Goodyear et. al., 2010:7). As organizations and individuals rely on the built-in security features of IT products and services, even with sophisticated intrusion detection systems, Organizations remain at risk because workers make mistakes because of the disguised nature of social engineering incidents (such as phishing attacks) A worker, even with good intentions, may operate in an unsafe manner or under pressure and pose a threat (Carlton, 2016: 1). The senior management must be aware that comprehensive cyber security is a difficult goal to achieve because cyber security, as is the case with security in general, is a continuum of administrative procedures and processes and not an end state (Gleason & Clinton, 2017: 24).

(Chen et al, 2017: 94) adds that the technology acceptance model predicted that behavioral beliefs about usefulness and ease of use are the main determinants of individuals' attitudes towards using a particular technology or system. That in turn affects their intent to use or engage in the actual behaviors provided by the technology. Cyber security simply expresses security measures that are applied to information technology to provide the required level of protection (Goodyear et. al., 2010:7).

LITERATURE REVIEW

Cyber Security Management

Cyber security consists of two keywords: Internet and security. Talking about the Internet means talking about information, communications (telecommunications, networks), gateways (computers, devices, and users), rooms, or spaces, and it is about the involvement, use, or association of computers, networks, and the Internet. At the same time, security is usually associated with the protection of assets. As security are the protection of assets and the protection of computers, networks, programs, and data from unintended or unauthorized access, alteration, or destruction, and the protection of information and systems from major cyber threats (Rizal & Yani, 2016:66). Integrating a cyber security management

model in an organization is also a very difficult process as it requires a great deal of understanding, and the biggest problem an organization faces is linking technologies and management together because technical and management specialists often speak different languages. Organizations must begin to understand cyber security not as a technical discipline but as a challenge facing organizations (Limba et. al., 2017: 569). And based on that it should not be cyber security is linked to information technology alone should not be considered as the field of information technology only (Chmielecki et. al., 2014: 863). Perhaps it is time to take a step towards integrating technology and management to go hand in hand to ensure effective cyber security. Cyber security requires an organized management approach consisting of a set of organizational, procedural, and technological elements (Everdij et. al., 2016:34). This requires a cyber security management system that is the overarching structure that brings together all the processes related to cyber security (Schmittner et. al., 2020: 1635).

Cyber security management can be defined as "the administration that is concerned with taking the necessary security measures to protect individuals, organizations and society from cyber threats, defining policies and permits for safe access to information, and implementing training programs to educate and sensitize its employees and stakeholders on cyber risks, with the participation of all employees in the department at their different levels." As for the dimensions of cyber security management, they are as follows:

Security Policy: It requires the development of a policy to reflect internal and external contexts that serve as a beginning for the management of cyber security. Policymaking requires management attention and support for cyber security. The policy must be formulated first, and then employees' awareness of the importance of adhering to the policy (Jung, 2018: 41). That is, it is to provide a practical guide to the specific areas of cyber security regulation that policymakers focus on and that align with the country's comprehensive national or international cyber security strategy (Kaja et al: 5).

Senior Management Responsibility and Support: The commitment of senior management usually translates into providing moral and financial support for the implementation of information security, as organizations with stronger support from top management are more involved in preventive efforts than organizations with weaker support from

top management (Masrek et. al., 2019: 984). It is "the extent of the conviction and belief of the senior management in the organization of the importance and benefits of cyber security management, as it gives an obligation to all employees to implement it and provide the appropriate material and financial support for that".

Employee Training and Awareness Program: Cyber security management education—which provides a combination of cyber security technology fundamentals and core management skill sets, and is made available through various modalities—is of vital importance to the organization (Trilling, 2018: 78). Training is primarily defined as "the process of providing people with the tools, knowledge, and opportunities they need to develop and increase their effectiveness" (Burrell, 2018: 110). While awareness is not training, the purpose of awareness shows is simply to focus attention on security, awareness shows are meant to allow individuals to recognize cyber security concerns and respond accordingly (Bada & Sasse, 2014: 10).

Risk Management Tools: is a platform for effective decision-making and results from communication within organizations, proactively identifying potential managerial and technical problems so that appropriate actions can be taken to reduce or eliminate the possibility and/or impact of these problems (Kure et. al., 2018:2).

Cyber Insurance: It can be defined as a way to hedge against potential risks through the dependence of organizations that rely on the Internet and electronic networks in their work on other organizations specialized in the field of cyber insurance through a fee paid by the insured organization to the insurance company to bear losses from this aspect instead.

Technology Acceptance Model

The theory of logical action provided the theoretical framework used by (Davis, 1989) to study the behavior of technology adoption, and through which his model was developed in line with the recommendations of this theory (Fayad & Paper, 2015:1002). TAM addresses the issue of how users accept and use technology (Teo et al, 2009:1001). In this context, Davis (1989) proposed a technology acceptance model by focusing on why users accept or reject information technology and how to improve acceptance. He surveyed a group of 112 users in Canada to validate his model. The model is designed to understand the causal relationship between the external variables of the user's acceptance of the computer, and any attempt to understand the behavior of this user through knowledge of utility

and ease of use. As this model is based on a set of elements represented in the perceived benefit and ease of use that is affected by external variables, It is also reflected on attitudes and attitudes and thus on the behavioral intention to use and accept technology (Silva & Dias, 2007: 78). Confirms both (Dishaw & Strong, 1999: 10) that in the light of this model perceived interest through ease of use Perceived affected, and that behavior is determined by the intention of behavioral and behavior and intent behavior are closely linked and are determined by the attitude toward behavior. Thus, the model is achieved in the factors of user behavior towards the use of information technology or when adopting new technology by studying the perceived ease of use and the perceived benefits that affect the effectiveness of users' use of technology systems (Chin & Lin, 2015:33). The technology acceptance model also refers to a series of mental and behavioral states that a person experiences that lead to the adoption or rejection of an innovation and acceptance of technology (Sepasgozaar et. al., 2017: 1238). As for the dimensions of the technology acceptance model, we summarize them as follows:

Perceived Benefit: Benefit is perceived as "the degree to which the individual believes that the use of a particular system would enhance job performance" (Beglaryan et al, 2017: 8).

Ease of Use: It is the degree to which users realize that technology is easy to use, and the more users believe that technology is easy to use, the more positive their attitudes towards technology adoption, which can enhance the effectiveness and efficiency of technology information systems (Cheng et al, 2015:4).

Behavioral Intentions: The user or individual intends to enter into an interactive exchange relationship to accept the technology (AlGahtani, 2011:56).

2-3 the relationship of cyber security management and technology acceptance model Information technology is becoming increasingly important to the competitive position of the organization; managers are becoming more sensitive to IT risk management. With major cyber-attacks occurring with great frequency, and mounting evidence that all organizations are under constant threat from cyber attacks, ensuring the adequacy of cyber security measures for the organization has become a key area of the Governing Council. To address this problem, by appointing personnel with great security experience one of the best protection mechanisms in an increasingly risky business environment, both from the perspective of sound corporate governance

and in terms of sensitive IT governance (Islam & Stafford, 2017: 1). As the organizations were also focusing on technological factors to play the primary role in finding effective solutions to secure information and prevent security breaches (Zaini et. al., 2020: 668). Because "the speed with which cyber-attacks change is much higher than the ability to find appropriate solutions for Events" (Trilling, 2018: 81). As insurance is a means of accepting a hedge against potential risks (Jung, 2018: 45). An insurance policy cannot reduce risk but it can serve as a valuable risk transfer mechanism that protects the balance sheet from serious financial losses. Most insurance companies also provide additional services such as access to a forensic IT specialist who can assist before and after information loss and advice on appropriate policies and procedures to ensure the best security of information (Bara et. al., 2015: 6).

RESEARCH METHODOLOGY

The review of the cyber security management literature and the technology acceptance model resulted in the crystallization of a hypothetical scheme for research as in Figure (1), which was prepared in light of the research problem and its objectives, and the main hypotheses were formulated as follows:

The first main hypothesis (H1): *There is a significant correlation between cyber security management with the technology acceptance model.*

The second main hypothesis (H2): *There is a significant effect of cyber security management with the technology acceptance model.*

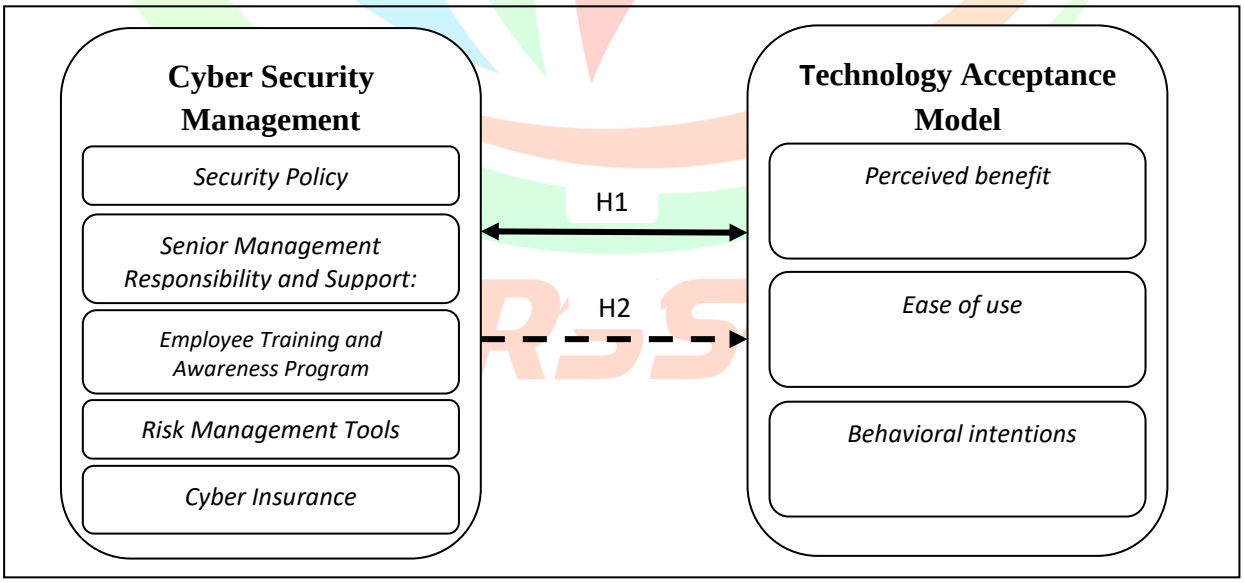

Figure (1) the proposed research model

Cyber Security Management Scale: The independent variable is Cyber Security Management, which consists of (34) paragraphs distributed into (5) dimensions (security policy, responsibility, and support of senior management, employee training and awareness program, risk management tools, cyber insurance) based on (Jung, 2018).

Technology Acceptance Model Scale: The responsive variable, technology acceptance model, included (12) items, divided into (3) dimensions (perceived benefit, ease of use, and behavioral intentions). Relying on (Al-Sabawi & Muhammad, 2018) and (Venkatesh & Davis, 1996).

Research sample: The total number of the research community reached (169). As (169) questionnaires were distributed directly by the researcher to the sample. (11) Were not answered, and (8) were not returned. The final sample was 150.

DISCUSS THE PRACTICAL RESULTS

Reliability Test

It means to what degree the scale gives close readings when it is applied each time. A volatile tool that gives varying results when applied more than once is a cause for concern and lack of confidence in its results, and thus is a waste of effort, money, and time. The value of Cronbach's alpha ranges between zero (an unstable instrument), and equal to one (a fully stable instrument), as the value of Cronbach's alpha ranges between zero and one, and the scale is considered to have low stability. And it has high stability if the value of Cronbach's alpha coefficient is (0.70) or higher. But if the stability is low, then this means that there is at least one of the paragraphs or expressions of the scale not fixed and the internal consistency is considered weak. The stability test of the measuring instrument (resolution) can be clarified as is shown in Table (1).

The scale	Dimensions coefficient (Cronbach's alpha)
Security Policy	0.799
Senior Management Responsibility and Support	0.752
Employee Training and Awareness Program	0.849
Risk Management Tools	0.911
Cyber Insurance	0.880
Cyber Security Management	***0.957***
Perceived benefit	0.900
Ease of use	0.794
Behavioral intentions	0.743
Technology Acceptance Model	***0.866***
The Total Questionnaire	**0.908**

Table (1) results of consistency between (components of the scale)

Discusses the Results

To test the hypothesis (H1): which states (there is a statistically significant correlation between the dimensions of cyber security management and the technology acceptance model), the correlation coefficient between the cyber security management and the technology acceptance model was achieved (0.623**) at the significance level (0.000) It is less than the significance level (0.05). This means rejecting the null hypothesis and accepting the alternative hypothesis which states (there is a statistically significant correlation between the cyber security management and the technology acceptance model), which indicates the existence of a correlation between the cyber security management and the technology acceptance model. That is, the more the ministry seeks to apply cyber security correctly and effectively, the more this helps to ease the use of technology and increase the support and confidence of the senior management in the technology acceptance model, as a result of the great advantages that the higher leaders will feel and thus work to accept the technology model within the ministry in question. As shown in Table (2):

Cyber Security Management Dimensions	Correlation value and significance level	Technology Acceptance Model Dimensions		
		Perceived benefit	Ease of use	Behavioral intentions
Security Policy	*R*	0.324**	0.428**	0.578**
	Sig.	0.000	0.000	0.000
Senior Management Responsibility and Support	*R*	0.436**	0.452**	0.626**
	Sig.	0.000	0.000	0.000
Employee Training and Awareness Program	*R*	0.188*	0.410**	0.582**
	Sig.	0.022	0.000	0.000
Risk Management Tools	*R*	0.200*	0.420**	0.551**
	Sig.	0.014	0.000	0.000
Cyber Insurance	*R*	0.335**	0.491**	0.580**
	Sig.	0.000	0.000	0.000
Cyber Security Management	*R*	0.329**	0.498**	0.658**
	Sig.	0.000	0.000	0.000
Number of hypotheses		***6***	***6***	***6***
accepted percentage		***100%***	***100%***	***100%***
** Correlation at a significance level of 0.01 * Correlation at a significance level of 0.05				
Sample size = 150				

Table (2) Correlation values between cyber security management and the technology acceptance model dimensions

To test the hypothesis (H2): which states (there is a statistically significant effect between the cyber security management in the technology acceptance model), the value of (F) calculated among the cyber security management in the technology acceptance model was (93,744). It is greater than the tabular value (F) of (3.89) at the level of significance (0.05), and accordingly, we will reject the null hypothesis and accept the alternative hypothesis, which states (there is a statistically significant effect between the cyber security management in the technology acceptance model) at the level of significance (5%).) i.e. with a confidence level (95%), That is, the management of cyber security has an effective and clear impact on the technology acceptance model, which indicates that the more the ministry can implement and manage cyber security successfully and effectively, this will work on that the ministry will have the technology acceptance model.

As shown in Table (3) Through the value of the corrected coefficient of determination (R^2) of (0.384), it is clear that the Cyber Security management explains 38% of the variables that occur in the technology acceptance model, while the remaining percentage (62%) is due to other variables that are not included in the research model The value of (t) calculated for the marginal slope coefficient was (9.682). It is greater than the tabular value (t) of (1.660) at the level of significance (0.05), and this indicates the significance of the marginal slope coefficient of the cyber security management variable. One unit of cyber security will increase the technology acceptance model by (55%), and the value of the constant (α) was recorded in the equation (1.924), meaning when the cyber security management is equal to zero, the technology acceptance model will not be less than this value.

Dependent Variable	Dimensions of the variable cyber security management			(R^2)	Adjusted R^2	(F)	(t)	Sig.	decision
Technology Acceptance Model	*Security Policy*	(α)	1.990	.3120	.3070	66.972	8.184	0.000	significance
		(β)	.5260						
	Senior Management Responsibility and Support	(α)	1.923	.4040	.4000	100.381	10.019	0.000	significance
		(β)	.5410						
	Employee Training and Awareness Program	(α)	2.608	.2440	.2390	47.817	6.915	0.000	significance
		(β)	.3720						
	Risk Management Tools	(α)	2.747	.2400	.2350	46.851	6.845	0.000	significance
		(β)	.3410						
	Cyber Insurance	(α)	2.380	.3480	.3430	78.924	8.884	0.000	significance
		(β)	.4310						
	cyber security management	(α)	1.924	.3880	.3840	93.744	9.682	0.000	significance
		(β)	.5530						
Tabular value (F) = 3.89 Tabular value (t) = 1.660 Sample size = 150									

Table (3) Analysis of cyber security management dimensions in the technology acceptance model

CONCLUSIONS

The results of the research showed that the more the Ministry of Interior tries to pay attention to cyber security management, the more it is reflected in the level of technology acceptance. This means that the cyber security department has a fundamental and influential role in the extent of acceptance of the technology that will be adopted within the ministry. Especially since most employees have good knowledge of what is a security management system. The results also showed that the application of the technology model will reflect positively on achieving ease of work and use by employees, as well as the upper and middle management within the ministry and that the behavioral intention of the employer is an intention to accept and not reject technology, and therefore the presence of these factors will help in achieving of technology acceptance model Within the researched ministry.

REFERENCES

1. Ablon , L., Libicki, M., & Golay, A. (2014). Markets for cybercrime tools and stolen data. Santa Monica: RAND Corporation.
2. AlGahtani, Said S. (2011) "Modeling the electronic transaction's acceptance using an extended technology acceptance model." Applied computing and informatics 9.1, pp. 47-77.
3. Al-Sabawi, Dr. Ahmed Younis and Muhammad, Syed Salem Ali (2018), *Using the TAM model to measure the acceptance of the electronic distribution system for petroleum products in the northern region*, Proceedings of the Fourth Specialized Scientific Conference of the Administrative Technical College / Baghdad, Volume One / Deposit No. (641).
4. Bada, Dr. Maria & Sasse, Professor Angela (2014). Global Cyber Security Capacity Centre: Draft Working Paper Cyber Security Awareness Campaigns Why do they fail to change behavior?.
5. Bara ,Danijel ,Ćorić ,Sanja & Jurišić ,Goran (2015). The Role of Cyber Insurance in Managing and Mitigating Cyber Security Risk with Special Emphasis on the Potential of Croatia and Serbia Cyber Insurance Market.
6. Beglaryan, Mher&Varduhi Petrosyan, & Edward Bunker. (2017)"Development of a tripolar model of technology acceptance: Hospital-based physicians' perspective on EHR." International journal of medical informatics 102, pp. 50-61.
7. BURRELL, Darrell Norman (2018). Exploring leadership coaching as a tool to improve the people management skills of information technology and cyber security project managers. The Florida Institute of Technology, Melbourne, Australia. HOLISTIC Vol 9, Issue 2, 2018, pp. 107-126 DOI: 10.
8. Carlton, Melissa (2016).Development of a Cyber security Skills Index: A Scenarios-Based, Hands-On Measure of Non-IT Professionals' Cyber security Skills. A dissertation submitted in partial fulfilment of the requirements for the degree of Doctor of Philosophy in Information Systems College of Engineering and Computing Nova South-eastern University.
9. Cheng, Shih-I. & Shih-Chih Chen& David C. Yen. (2015)"Continuance intention of E-portfolio system: A confirmatory and multigroup invariance analysis of technology acceptance model." Computer Standards & Interfaces 42, pp. 17-23.

10. Chin, Jacky & Lin, Shu-Chiang. (2015)"Investigating users' perspectives in building energy management system with an extension of technology acceptance model: A case study in Indonesia manufacturing companies." Procedia Computer Science 72, pp. 31-39.
11. Chmielecki,Tomasz , Chołda, Piotr ,Pacyna,Piotr , Potrawka,Paweł , Rapacz, Norbert ,Stankiewicz,Rafał &Wydrych Piotr (2014).Enterprise-oriented Cyber security Management .AGH University of Science and Technology, Kraków, Poland ,Proceedings of the 2014 Federated Conference on Computer Science and Information Systems pp. 863–870.
12. Djamasbi, Soussan& Diane M. Strong& Mark Dishaw. (2010) "Affect and acceptance: Examining the effects of positive mood on the technology acceptance model." Decision Support Systems 48.2, pp.383-394.
13. Everdij,Mariken , Gijsen , Bart , Smulders ,André ,Verhoogt ,Theo & Wiegers ,René (2016).Cyber-Security Management Of Atm Services: Are We Ready For The Future?.
14. Farahat, Taher. (2012) "Applying the technology acceptance model to online learning in the Egyptian universities." Procedia-Social and Behavioral Sciences 64, pp.95-104.
15. Fayad, Rima, & Paper,David . (2015) "The technology acceptance model e-commerce extension: a conceptual framework." Procedia Economics and Finance 26, pp. 1000-1006.
16. Gleason, Peter & Clinton, Larry (2017). Managing Cyber Risk: A Handbook for UK Boards of Directors. Director's Series Handbook—UK Edition.
17. Goodyear, Marilu, Portillo, Shannon, Goerdel, Holly T. & Williams, Linda (2010)Cybersecurity Management in the States: The Emerging Role of Chief Information Security Officers. IBM Center The Business of Government.
18. Islam, Md. Shariful & Stafford, Thomas (2017). Information Technology (IT) Integration and Cybersecurity/Security: The Security Savviness of Board of Directors.Twenty-third Americas Conference on Information Systems, Boston.
19. JUNG, JEYONG (2018).A Study of Cyber Security Management within South Korean Businesses – An examination of risk and cybercrime involving industrial security. The thesis is submitted in partial fulfillment of the requirements for the award of the degree of Doctor of Philosophy of the University of Portsmouth.
20. Kaja, Ciglic. McKay, Angela.Hering, John & Moore, Theo, Cybersecurity Policy Framework, A practical guide to the development of national cybersecurity policy.
21. Kure , Halima Ibrahim , Islam ,Shareeful & Razzaque ,Mohammad Abdur (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System.

22. Limba, Tadas , Plėta,Tomas , Agafonov,Konstantin & Damkus ,Martynas (2017).Cyber Security Management Model For Critical Infrastructure.The International Journal Entrepreneurship And Sustainability Issues.Volume 4 Number 4 (June).
23. Masrek ,Mohamad Noorman , Harun ,Qamarul Nazrin , Ramli ,Ishak & Prasety ,Helmy (2019). The Role Of Top Management In Information Security Practices. Proceedings of SOCIOINT 2019- 6th International Conference on Education, Social Sciences and Humanities 24-26 June 2019- Istanbul, Turkey.
24. Rizal, Muhamad & Yani, Yanyan M.(2016) Cybersecurity Policy and Its Implementation in Indonesia.Journal of ASEAN Studies, Vol. 4, No. 1 (2016), pp. 61-78.
25. Schmittner , Christoph ,Dobaj, Jrgen ,Macher, Georg ,& Brenner, Eugen (2020). A Preliminary View on Automotive Cyber Security Management Systems.
26. Sepasgozaar, Samad ME&Sara, Shirowzhan, &Cynthia, Changxin Wang. (2017) "A scanner technology acceptance model for construction projects." Procedia Engineering 180: 1237-1246.
27. Silva, Patricia Maria& Dias, Guilherme Ataíde (2007)" Theories About Technology Acceptance: Why The Users Accept Or Reject The Information Technology?", Bjis, V.1, N.2, P.69-86.
28. Teo, T., Lee, C. B., Chai, C. S., & Wong, S. L. (2009)." Assessing the intention to use technology among pre-service teachers in Singapore and Malaysia: A multigroup invariance analysis of the Technology Acceptance Model (TAM)". Computers & Education, 53(3), pp. 1000-1009.
29. Tisdale, Susan M. (2016). Architecting A Cybersecurity Management Framework. Issues in Information Systems Volume 17, Issue IV, pp. 227-236.
30. Trilling, Rick (2018). Creating a New Academic Disciplineiscipline: Cybersecurity Management Education. Session 3A: Papers Applied SIGITE'18, October 3-6, 2018, Fort Lauderdale, FL, USA.
31. Viswanath, Venkatesh, & Davis, Fred D. (1996) "A model of the antecedents of perceived ease of use: Development and test." Decision Sciences 27.3, pp.451-481.
32. Zaini,Muhamad Khairulnizam ,Masrek ,Mohamad Noorman & Sani,Mad Khir Johari Abdullah (2020). The impact of information security management practices on organizational agility. Information & Computer Security Vol. 28 No. 5, 2020 pp. 681-700.