The Influence of Security Control Management and Social Factors in Deterring Security Misbehaviour

H.A.Hamid, M.M.Yusof, N.R.S.Mohd Dali

ABSTRACT: ***Complying with the security rules and standard is important to safeguard valuable information in the organisation. Failure to prevent security breaches costs the organisation huge losses and bad reputation. Technical solutions are abundant but nonetheless still unsuccessful to deter information security incidents. The root cause of incompliance is humans as they are the weakest link of security chain. Based on the integration of social cognitive theory and extended deterrence theory, this paper examines the information security control management particularly on information security awareness, training and education, risk analysis and management, policies and procedures as well as physical security monitoring, and cognitive factors which give impact towards the employees' information security compliant behaviour in the organisation. Utilising purposive sampling, a survey was conducted to employees of public and private sectors in Malaysia who are identified as Software- as-a- Service cloud users. Data collected was analysed using PLS-SEM. Result shows that information security control management and social factors have significant impact in deterring information security misbehaviour in the context of cloud users.***

KEYWORDS:Security, Compliance, Behaviour, Model.

1. INTRODUCTION

The emerging of cloud computing has uplifted the information technology to the more advanced level. In the Software as a Service (SaaS) environment for instance, everything is served in and around the cloud to which people are not required to bring their own storage devices, since data can be saved in the clouds. Nevertheless, study shows that security is a major hindrance of cloud adoption [1], [2]. Scientists have come up with an abundant of technical solutions to solve information security problems, yet security incidents still happen because humans have been the weakest link of security chain [3], [4]. Security incompliance, either accidentally or intentionally, causes substantial costs to the organisation, both tangibly and intangibly.

Hence this study will approach the information security compliance behaviour (ISCB) from the socio-organisational perspective. Previous studies discussed the factors inculcating security culture in the organisation [5][6][7] but there is no first-hand evidence that could prove the claim. The aim of this paper is to empirically examine the driving factors of security compliant behaviour in the organisation. Specifically, this paper, as part of the whole ISCB research, will seek to answer this question: How significant are the social and information security control management factors in deterring security misbehaviour?

Adapting Social Cognitive Theory (SCT), as well as extended deterrent theory (DT) as our framework, this study will examine the impact of security control management (SCM), personal values (PV), environment (ENV) and employees' behaviour (BHV) towards information security compliance behaviour (ISCB). SCT is a three dimensional complementary model that is used to determine human behaviour which consists of cognitive or personal factors, environmental factors and behavioural factors [8]. The theory founder [8] further accentuates that "expectations, beliefs, self- perceptions, goals and intentions give shape and direction to behaviour. What people think, believe, and feel, affects how they behave [8], [9]. He nevertheless argued that behaviour cannot easily change the environment much like it is influenced by the environment unless the behaviour first change itself. The

Revised Manuscript Received on June 01, 2019.

H.A.Hamid, M.M.Yusof, Faculty of Information and Communication Technology, niversiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76100 Durian Tunggal, Melaka, Malaysia.

H.A.Hamid, Facultyof Science and Technology, Universiti Sains Islam Malaysia, 71800 Nilai, Negeri Sembilan, Malaysia.

Mohd Dali, Islamic Finance and Wealth Management Institute/Faculty of Economics and Muamalat, Universiti Sains Islam Malaysia, 71800 Nilai,
Negeri Sembilan, Malaysia.

Retrieval Number: A00270681S519/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering &
Sciences Publication

DT of punishment can be traced to the early works of classical philosophers such as Thomas Hobbes (1588–1678), Cesare Beccaria (1738–1794), and Jeremy Bentham (1748–1832) [10]. Rooted from school of criminology, DT advocates that individual choose to commit crime when the benefits of the action outweigh the costs [11]. Deterrence has been indicated significant in decreasing negative practices and has likewise been observed to be a viable instrument in administration [12]. In Information System (IS) research, DT has been extended by integrating some security control as a measure to deter security breaches [13].

2. METHODOLOGY

2.1 Hypotheses Development

To ensure successful information security in the organisation, the SCM is vital. Past scholars have highlighted on the important roles of SCM in making sure that employees act according to the standards and procedure, and rules and regulations [14], [15]. Security awareness [16]–[18], as well as security training and education [16], [17], [19], [20] are among the most basic factor needed in inculcating information security culture in the organization which must be given much attention by the top management. Employees must be aware that their behaviour must always in accordance to the rules and regulations to avoid security breaches that may occur accidently or intentionally. However, in today's technology advancement where threats are rising almost from any angle, security awareness is still lagged behind [21]. The lack of security awareness causes security incompliance in the cloud environment, which makes outsourcing arrangement of IT services becomes more complex [22]. Without proper security education, training and awareness (SETA) programmes, people do not know if they have committed security breaches. It was found out that SETA programmes has positive influence on managing and deterring security behaviour [15].

In addition, the organisations that have proper information security policies and procedures (SPP) are better at guiding employees to good security behaviour. Research shows that complying with organisation security policy can shape and mitigate the risk of employees misbehaviour [23]. However, employees must be aware of the information security policies in place in order to have an effective deterrence factor[15]. It is also a critical factor to consider setting up ethical conduct policy [24] in building up security culture in the organisation. It is argued that previous research in ISCB did not give attention on ethical conduct due to different organisations have different kinds of values and culture[17].

Another security control is risk analysis assessment and management (RAM). The organization will be able to identify areas that are highly critical for information security and to improve the security effectiveness. Information is secured with the three triads of information system – confidentiality, integrity and availability. However, in nowadays computing, cloud computing for instance, has exposed information to more security risks and challenges issues. Information is at risks of the existence of vulnerability and threats. It is claimed that organizations which have security RAM in place are being more aware of their losses due to security breaches [17].

The fourth factor for SCM is physical security monitoring (PSM) which is essential to control the security behaviour of employees in the organisation [13]. While technical threats are easier to detect and rectify, the human threats are proven to be difficult to identify. Thus, the uses of PSM activities are said to be effective in controlling the behaviour of the employees with regards to the safety of information.Past research examined how PV have been a significant driving factor in complying with security regulations. This includes their attitude [25], [26], security knowledge [18], [27], [28], religious and ethical beliefs [29], [30] as well as level of trust [29], [31]. Humans act according to their habitual conducts. When human do things repeatedly , these actions become a habit and are stored in the subconscious minds.

Depending on the individual preference towards an object (person, event, thing, time, activity), attitude can be expressed positively or negatively. Attitude has been proven to have a positive effect on employee security compliance behaviour [25] and self-efficiency in attitude help cultivates ISCB [16]. The ENV plays an important role is shaping a positive behaviour of a person. This can be either internal or external environment that influence from within and outside organisation. As an individual, people tend to adapt themselves to the particular situation for the fact that they are unable to change the environment alone. In this situation, the government plays an important role to ensure the information security is at the highest priority.

The Personnel Data Protection Act 2010 was enacted by the Malaysian Government for these reasons. It was suggested that the enforcement of the act will help shaping the behaviour of the people with regards to information security [32]. The influence of regulation with regards to information security culture should be empirically tested [5]. Another ENV element is social norms.

Individuals' behaviours are

Retrieval Number: A00270681S519/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering &
Sciences Publication

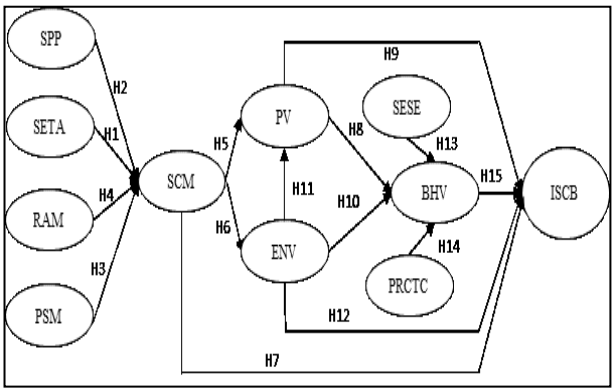
very much shaped by their ENV such as peer influence. The colleagues and immediate supervisor, other departments' behaviour, the mechanism for rewarding good behaviour and punishing bad behaviour are constructing factors which influence the security behaviour of the employees in the organisation [12], [16]. It is argued that among others, ENV factors that influence the security behaviour of people are still yet to be explored [33], [34],[3].

BHV is the conduct of a person towards a particular situation which is based upon the ENV as well as the personality traits one owns. The BHV elements which includes skills, practice and self-efficacy (SESE) of employees are formed gradually in such a long span of time and cannot be obtained overnight. ISCB research found out that security conscious behaviour has a significant impact towards the safety of information in the organisation [14], [28], [34]. Good security behaviour will result in security compliance thus reduce security breaches. In long term this good behaviour will become norms which exhibit security culture of the organisation. The skills to measure risks and recognise threats are crucial for information safekeeping. Those who possess lower skills in recognizing and detecting threats are more vulnerable to the attacks.

Good security practice will likely reduce security incidents as users take all the precaution steps to comply with security policies and procedures. Experience in information security context means one's familiarity with the skills or knowledge in the field of information security, which were acquired over a period of time through actual exercise and apparently has enhanced better ability or grasp in behaving according to the security rules and regulations [35]. Using social bond theory [36], [23] found out in their study that the experience and involvement of employees have significant effect on their attitude towards complying with security policy. Self-efficacy is a person's certainty of his or her ability to perform required behaviours to achieve certain accomplishments [37].

Self-efficacy is a form of self-evaluation that can be the most influential apparatus of human agents in motivating and regulating human behaviour. Many studies in information technology and information systems adoption in various domains claimed that self-efficacy is an influencing factor for users to adopt such technology and systems. Self-efficacy has been found to have a significant relationship towards information security behaviour of the employees [12], [25], [38], [39]. Hence, we posit the following hypotheses as shown in the following diagram:

H1: SETA programme has a positive impact towards SCM.
H2: The SPP has positive impact towards SCM.
H3: The PSM has a positive impact towards SCM.
H4: The RAM has a positive impact SCM.
H5: SCM has positive impact towards PV.
H6: SCM has positive impact towards the ENV.
H7: SCM has a positive impact towards ISCB.
H8: PV have positive impact towards BHV.
H9: PV have positive impact towards ISCB.
H10: ENV has positive impact towards BHV.
H11: ENV has a positive impact towards PV.
H12: ENV has positive impact towards ISCB.
H13: SESE have positive impact towards BHV.
H14: PRCTC has positive impact towards BHV.
H15: BHV has positive impact towards ISCB.



2.1 Method

The survey instruments were adapted from the work of [18], [27], [40], [41] for cognitive factors using reflective measurement. The security control management instruments were adapted from [15] using formative measurement. All items were measured on a 5-point Likert-scale from 1-strongly disagree to 5- strongly agree. The survey was conducted online to professionals in the organisations in Malaysia from October to December 2016 to 1000 potential respondents at various organisations from public and private sectors. Google doc was used as the platform of the survey.

Potential respondents were contacted through Facebook, and email messages to which the link of the survey was attached to the messages. Convenience sampling was used as the sampling method. Respondents were informed about the purpose of the study and given option to quit answering at any time. Screening questions were asked to identify the correct respondents. Respondents were asked about the usage of mobile devices such as laptops or smartphones for their job-related tasks. Respondents were also questioned about their exposure to cloud applications such as cloud storage, social media networks as well as email applications.

Retrieval Number: A00270681S519/19©BEIESP
Published By:
Blue Eyes Intelligence Engineering &
Sciences Publication

Altogether, there were 410 people responded to the questions. Screening the missing data, 396 data was useful for empirical analysis. Partial Least Square (PLS) was used to analyse the ICSB model.

3. RESULTS AND DISCUSSION

Descriptive analysis was conducted to identify the background of the respondents. Female respondents outnumbered male respondents by 26% where 251 female respondents participated in this study compared to male (145). There were two big majority age groups, each at the range of 31-40 (39.4%) and 41-50 (33.6%), followed by 21-30 (23.5%), 61-70 (2.5%), 20 and below (0.8%) and 51-60 (0.5%). With regards to education background, two majority groups are from degree (41%) and master's degree holder (35.4%), followed by PhD (11.9%), diploma (8.4%) as well as high school level (3.3%). Their working experiences vary, from below 5 and years (33.7%), 5 to 7 years of experience (23%), 11 to 15 years (16.9%), 16 to 20 years (16.9%) and only 15% have experience more than 25 years. Around 46.2% of the respondents are from the public sector, 43.7% from the private sector and the rests are from NGO. Table 1 summarizes their profiles.

Items		**n**	**%**
Gender	Male	145	36.6
	Female	251	63.4
Age	20 and below	3	0.8
	21-30	93	23.5
	31-40	156	39.4
	41-50	132	33.3
	51-60	2	0.5
	61-70	10	2.5
Education	High school	13	3.3
	Diploma	33	8.4
	Degree	162	41.0
	Master	140	35.4
	PhD	47	11.9
Working Experience	<= 5 years	94	23.7
	6-10 years	91	23.0
	11-15 years	67	16.9
	16-20 years	76	19.2
	21-25 years	56	14.1
	>= 26 years	12	3.0
Organisation	Public	182	46.2
	Private	172	43.7
	NGO	40	10.1

Respondents were also asked with regards to their exposure to the SaaS applications as part of screening valid respondents. Majority of the respondents were exposed to the usage of SaaS applications such as email and social media. Result shows that 48.5% of the respondents have an extensive experience utilizing email and 54.5% users have an extensive exposure to social media service. Only 17.4% of the users have an extensive usage on cloud storage while 31.6% of them have some exposure to cloud storage and 12.4% of them have no cloud storage at all. With regards to single sign on portal, 30.8% of the users have quite a lot experience using it while 9.8% of them have none experience at all. The result of their SaaS exposure is summarized as below:

Exposure		Frequency	Percent
Email	None	6	1.5
	Very limited	17	4.3
	Some experience	45	11.4
	Quite a lot	136	34.3
	Extensive	192	48.5
Cloud Storage	None	49	12.4
	Very limited	77	19.4
	Some experience	125	31.6
	Quite a lot	76	19.2
	Extensive	69	17.4
Mobile Apps	None	20	50.1
	Very limited	47	11.9
	Some experience	81	20.5
	Quite a lot	126	31.8
	Extensive	122	30.8
SSO Portal	None	39	9.8
	Very limited	68	17.2
	Some experience	94	23.7
	Quite a lot	122	30.8
	Extensive	73	18.4
Social Media	None	9	2.3
	Very limited	16	4.0
	Some experience	50	12.6
	Quite a lot	105	26.5
	Extensive	216	54.5
E-Services	None	36	9.1
	Very limited	67	16.9
	Some experience	122	30.8
	Quite a lot	117	29.5
	Extensive	54	13.6

Table 2: Users SaaS Exposure

The PLS evaluation of measurement model analysis of formative exogenous latent variables takes 3 steps as suggested by [42] such as examining the convergent validity, the presence of collinearity among indicators, and the significance and relevance of outer weights. Prior to that, the content validity has been achieved by referring the scales to the subject-matter experts and industrial

Retrieval Number: A00270681S519/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering &
Sciences Publication

professionals through a pilot study, as well as through conducting an EFA analysis.

The convergent validity can be examined by looking at the value of path coefficient which must be above 0.80 or at least 0.64 [42]. The analysis shows the value of path coefficient for each exogenous construct is above 0.80, which indicates that the formative scales exhibits a sufficient convergent validity of the scales. To examine collinearity issues, the variance inflation factor (VIF) values was referred. Analysis shows that some of the indicators have VIF values above the threshold 5.0 hence, the bootstrapping procedure was further conducted to examine the significance and relevance of the indicators. For this analysis, the outer weight and outer loading values must be significant respectively.

The result of formative measurement assessment shows that PSM 35, PSM 36 and PSM 37, RAM26, SETA24, SPP15, SPP16, SPP17 and SPP18 were dismissed from the scale because the VIF are above the threshold value of 5.0. The outer weight and outer loading were further examined to all indicators and those items were found to be insignificant and hence resulting items dismissal. The final formative constructs (PSM, RAM, SETA, SPP) were having convergent validity.

Next is the measurement of reflective scales for exogenous latent variable of SESE and PRCTC as well as endogenous latent variables of BHV, ENV, SCM and ISCB. The reflective measurement specifically analyses for the reliability and validity, convergent validity as well as discriminant validity. The composite reliability values for reflective endogenous latent variable are above 0.70 demonstrate that all reflective constructs have high levels of internal consistency reliability according to [43]. Convergent validity assessment builds on the AVE value as the evaluation criterion. The AVE values of BHV (0.823), ENV (0.55), PV (0.702), ISCB (0.806) and SCM (0.887) are well above the minimum requirement level of 0.5, as suggested by [42]. Thus, the measure of the reflective constructs has high levels of convergent validity.

Finally, the discriminant validity assessment was conducted using the Fornell-Larcker criterion and the result revealed there were no discriminant validity problem. The PLS structural model analysis involves five steps of assessment as suggested by [42] which includes assessment for collinearity, significance and relevance, level of R^2, the effect size f^2, as well as predictive relevance Q^2 and effect size q^2. The result of structural collinearity assessment shows that VIF tolerance value for all sets of predictors are below the threshold 5.0 which indicates no collinearity problem in the structural model. The bootstrapping procedure was conducted to assess the significant of path coefficients. Table 3 exhibits the results of path coefficients of ISCB model.

Hypotheses	Path	Path Coefficient	T Values	Sig. Level	P Values	Remarks
H1	SETA -> SCM	-0.009	0.112	NS	0.911	Rejected
H2	SPP-> SCM	0.405	4.174	***	0.000	Supported
H3	PSM -> SCM	0.345	4.892	***	0.000	Supported
H4	RAM -> SCM	0.183	2.285	**	0.023	Supported
H5	SCM -> PV	0.048	0.93	NS	0.353	Rejected
H6	SCM -> ENV	0.349	5.464	***	0.000	Supported
H7	SCM-> ISCB	0.257	4.084	***	0.000	Supported
H8	PV -> BHV	0.185	3.472	***	0.001	Supported
H9	PV -> ISCB	0.206	3.518	***	0.000	Supported
H10	ENV -> BHV	0.106	2.385	**	0.017	Supported
H11	ENV -> PV	0.449	7.277	***	0.000	Supported
H12	ENV-> ISCB	0.075	1.109	NS	0.268	Rejected
H13	SESE -> BHV	0.608	12.951	***	0.000	Supported
H14	PRCTC ->BHV	0.047	1.433	NS	0.152	Rejected
H15	BHV -> ISCB	0.348	6.123	***	0.000	Supported

The result clearly shows that all paths except for H1, H5, H12 and H14, are significant at least at 5%, hence hypotheses H2, H3, H4, H6, H7, H8, H9, H10, H11, H13 AND H15 are supported.

4. CONCLUSIONS

Driving by the aim of the study, we examined the influencing factors of information security compliant behaviour of SaaS cloud users. All results for information security control management factors are consistent with [15] and [44] except for SETA programmes. Contradict to SETA programmes, the security policy and procedure (SPP), the risk analysis and management (RAM), together with physical security monitoring (PSM) have significant impact to the security control management of information security. A clear information security policy and procedures is vital for it becomes a guidance of what can or cannot be done legally and ethically.

In addition, the results also suggest that the management should emphasize on the PSM more intensively for the fact that this is an effective deterrent factor to prevent information security breaches, which is consistent with [13] result. This perhaps includes the access management system as well as constant monitoring through computer surveillance to inculcate good information security behaviour. Furthermore, the RAM is a proactive solution, which is crucial not only for correcting information security incidents but also for preventing potential security issues. Organisations which have RAM in place are taking advance step ahead in deterring security

Retrieval Number: A00270681S519/19©BEIESP
Published By:
Blue Eyes Intelligence Engineering &
Sciences Publication

breaches to ensure that information is safely protected as well as to avoid substantial losses due to security compromise. Nevertheless, it is quite a surprise that SETA programme is found to be insignificant towards driving good information security behaviour of the users, which is contradict to [13] and [14]. SETA programme has been found to be a salient factor to shape good security behaviour of the users. The contradicting result is most probably due to insufficient security awareness training and education being conducted at the public and private sectors in Malaysia.

Despite SETA is being insignificant to SCM, SCM has significant impact towards the security environment but not to the personal values of employees. Nevertheless, the environment significantly influences the personal values of employees, indicating that the environment is the mediator of the SCM and personal values. The skills, experience and self-efficacy have significant impact to the behaviour of the employees and this is consistent with the results of [25], [39]. Self-efficacy has been proven to be a substantial factor in many security behaviour research to which users believe that their abilities in complying with security regulations as well as utilizing security measures are important in keeping good security behaviour [45]. Without these, employees are unable to distinguish between the good and bad security conduct. Overall, the security control management, the personal values and the behaviour of the employees play a significant role in establishing ISCB.

This study contributes to the knowledge [46] of ISCB through the extension of the SCT and extended DT theories in the context of SaaS cloud users, as well as the development of integrated of an ISCB model. The findings from this study could be enhanced from a different perspective by using a case study method to provide an in-depth explanation of the phenomenon. A case study is suggested to be conducted at the public organisation to assess the security [47] compliance behaviour using this model both for external validation as well as for understanding the actual phenomena [48] of information security.

ACKNOWLEDGMENTS

We would like to thank Ministry of Higher of Education Malaysia, Universiti Teknikal Malaysia Melaka and Universiti Sains Islam Malaysia for their sponsor, supports and assistance.

REFERENCES

[1] H. Abdul Hamid and M. Mohd Yusof, "State-of-the-Art of Cloud Computing Adoption in Malaysia: A Review," *J. Teknol. (Sciences Eng.*, vol. 77, no. 18, pp. 1–6, 2015.

[2] H. Abdul Hamid and M. M. Yusof, "Conceptualizing global cloud landscape: A review of adoption issues and challenges," *Res. J. Appl. Sci.*, vol. 11, no. 6, pp. 333–339, 2016.

[3] A. AlHogail, "Design and validation of information security culture framework," *Computer. Human Behaviour*, vol. 49, pp. 567–575, 2015.

[4] L. Connolly, M. Lang, and D. Tygar, "Managing Employee Security Behaviour in Organisations: The Role of Cultural Factors and Individual Values," *ICT Syst. Secur. Priv. Prot.*, vol. 428, pp. 417–430, 2014.

[5] Shakeel, P.M., Tolba, A., Al-Makhadmeh, Zafer Al-Makhadmeh, Mustafa Musa Jaber, "Automatic detection of lung cancer from biomedical data set using discrete AdaBoost optimized ensemble learning generalized neural networks", Neural Computing and Applications,2019,pp1-14.https://doi.org/10.1007/s00521-018-03972-2

[6] A. Bandura, *Social foundations of thought and action: A social cognitive theory*. Englewood Cliffs, NJ, US: Prentice-Hall series in social learning theory, 1986.

[7] P. E. Lieberman, "Deterrence Theory," *Billboard*, vol. 1, no. 45, pp. 8–8, 2010.

[8] T. Herath and H. R. Rao, "Protection motivation and deterrence: a framework for security policy compliance in organisations," *European Journal of Information Systems*, vol. 18, no. 2. pp. 106–125, 2009.

[9] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness," *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, 2009.

[10] J. D'Arcy and A. Hovav, "Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures," *J. Bus. Ethics*, vol. 89, pp. 59–71, 2009.

[11] G. Bozic, "The role of a stress model in the development of information security culture," *Proc. 35th Int. Conv. MIPRO, May 2012*, pp. 1555–1559, 2012.

[12] M. A. Alnatheer, "Information Security Culture Critical Success Factors," *2015 12th Int. Conf. Inf. Technol. - New Gener.*, pp. 731–735, 2015.

[13] K. Parsons, A. McCormac, M. Butavicius, M. Pattinson, and C. Jerram, "Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q)," *Comput. Secur.*, vol. 42, pp. 165–176, 2014.

[14] S. Furnell and L. Moore, "Security literacy: The missing link in today's online society?" *Comput. Fraud Secur.*, vol. 2014, no. 5, pp. 12–18, 2014.

[15] D. Bachlechner, S. Thalmann, and R. Maier, "Security and compliance challenges in complex IT outsourcing arrangements: A multi-stakeholder perspective," *Comput. Secur.*, vol. 40, pp. 38–59, Feb. 2014.

[16] Gomathi, P., Baskar, S., Shakeel, M. P., & Dhulipala, S. V. (2019). Numerical Function Optimization in Brain Tumor Regions Using Reconfigured Multi-Objective Bat Optimization Algorithm. Journal of Medical Imaging and Health Informatics, 9(3), 482-489.

[17] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management needs more holistic approach: A literature review," *Int. J. Inf. Manage.*, vol. 36, no.

Retrieval Number: A00270681S519/19©BEIESP

Published By:
Blue Eyes Intelligence Engineering &
Sciences Publication

2, pp. 215–225, 2016.

[18] M. R. Fazlida and J. Said, "Information Security: Risk, Governance and Implementation Setback," *Procedia Econ. Financ.*, vol. 28, no. April, pp. 243–248, 2015.

[19] 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.

[20] N. Sohrabi Safa, R. Von Solms, and S. Furnell, "Information security policy compliance model in organizations," *Comput. Secur.*, vol. 56, pp. 70–82, 2016.

[21] PricewaterhouseCoopers International Limited, "Managing Cyber risks in an interconnected world: Key findings from the global state of information security survey 2015," 2014.

[22] A. Da Veiga and J. H. P. Eloff, "A framework and assessment instrument for information security culture," *Computers & Security*, vol. 29, no. 2. pp. 196–207, 2010.

[23] J. F. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, 2010.

[24] L. Connolly, M. Lang, and J. D. Tygar, "Investigation of Employee Security Behaviour: A Grounded Theory Approach," *IFIP Adv. Inf. Commun. Technol.*, vol. 455, pp. 283–296, 2015.

[25] S. Alfawaz, K. Nelson, and K. Mahannak, "QUT Digital Repository: Information Security Culture: A Behaviour Compliance Conceptual Framework," in *Security, Information Aisc, Conference*, 2010.

[26] M. Al-Hamar, R. Dawson, and L. Guan, "A culture of trust threatens security and privacy in Qatar," *Proc. - 10th IEEE Int. Conf. Comput. Inf. Technol. CIT-2010, 7th IEEE Int. Conf. Embed. Softw. Syst. ICESS-2010, ScalCom-2010*, no. Cit, pp. 991–995, 2010.

[27] J. Leiwo and S. Heikkuri, "An analysis of ethics as foundation of information security in distributed systems," *Proc. Thirty-First Hawaii Int. Conf. Syst. Sci.*, vol. 6, no. c, 1998.

[28] A. Colella, A. Castiglione, and A. De Santis, "The Role of Trust and Co-partnership in the Societal Digital Security Culture Approach," *2014 Int. Conf. Intell. Netw. Collab. Syst.*, pp. 350–355, 2014.

[29] N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N. A. Ghani, and T. Herawan, "Information security conscious care behaviour formation in organizations," *Comput. Secur.*, vol. 53, pp. 65–78, 2015.

[30] M. A. Alnatheer, "Information Security Culture Critical Success Factors," *2015 12th Int. Conf. Inf. Technol. - New Gener.*, pp. 731–735, 2015.

[31] S. Alfawaz, K. Nelson, and K. Mohannak, "Information security culture: A behaviour compliance conceptual framework," *Conf. Res. Pract. Inf. Technol. Ser.*, vol. 105, pp. 47–55, 2010.

[32] R. B. Cialdini and N. J. Goldstein, "Social influence: compliance and conformity.," *Annu. Rev. Psychol.*, vol. 55, pp. 591–621, 2004.

[33] R. Cialdini and M. Trost, *Social influence: Social norms, conformity and compliance.*, vol. 1 & 2, no. 24th ed. New York, NY, US: McGraw-Hill, 1998.

[34] I. Topa and M. Karyda, "Identifying Factors that Influence Employees' Security Behavior for Enhancing ISP Compliance," in *Trust, Privacy and Security in Digital Business*, 2015.

[35] A.-B. Munteanu and D. Fotache, "Enablers of Information Security Culture," *Procedia Econ. Financ.*, vol. 20, no. 15, pp. 414–422, 2015.

[36] T. Hirschi, "On the compatibility of rational choice and social control theories of crime," *Reason. Crim. Ration. choice Perspect. offending*, pp. 105–118, 1986.

[37] A. Bandura, "Self-efficacy: toward a unifying theory of behavioural change.," *Psychol. Rev.*, vol. 84, no. 2, pp. 191–215, 1977.

[38] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Inf. Manag.*, vol. 49, no. 3–4, pp. 190–198, 2012.

[39] Shakeel PM, Baskar S, Dhulipala VS, Jaber MM., "Cloud based framework for diagnosis of diabetes mellitus using K-means clustering", Health information science and systems, 2018 Dec 1;6(1):16.https://doi.org/10.1007/s13755-018-0054-0

[40] M. Siponen, M. Adam Mahmood, and S. Pahnila, "Employees' adherence to information security policies: An exploratory field study," *Inf. Manag.*, vol. 51, no. 2, pp. 217–224, 2014.

[41] K.-L. Thomson, R. von Solms, and L. Louw, "Cultivating an organizational information security culture," *Comput. Fraud Secur.*, vol. 2006, no. 10, pp. 7–11, 2006.

[42] J. F. Van Niekerk and R. Von Solms, "Information security culture: A management perspective," *Comput. Secur.*, vol. 29, no. 4, pp. 476–486, 2010.

[43] J. F. J. Hair, G. T. M. Hult, C. Ringle, and M. Sarstedt, *A Primer on Partial Least Squares Structural Equation Modeling (PLS-SEM)*, vol. 46, no. 1–2. 2014.

[44] J. C. Nunnally Jr., *Introduction to psychological measurement.* New York, NY, US: McGraw-Hill, 1970.

[45] W. He, X. Yuan, and X. Tian, "The self-efficacy variable in behavioral information security research," *Proc. - 2nd Int. Conf. Enterp. Syst. ES 2014*, pp. 28–32, 2014.

[46] A. Bandura, "Social cognitive theory," *Ann. child Dev.*, vol. 6, no. Six theories of child development, pp. 1–60, 1989.

[47] B. Y. Ng, A. Kankanhalli, and Y. (Calvin) Xu, "Studying users' computer security behavior: A health belief perspective," *Decis. Support Syst.*, vol. 46, no. 4, pp. 815–825, 2009.

[48] M. Alnatheer and K. Nelson, "Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context," no. December 2009.