UTHM
Universiti Tun Hussein Onn Malaysia

UNIVERSITI TUN HUSSEIN ONN MALAYSIA

FINAL EXAMINATION
(ONLINE)
SEMESTER II
SESSION 2019/2020

COURSE NAME	:	SPECIAL TOPICS IN INFORMATION SECURITY
COURSE CODE	:	BIS 33403
PROGRAMME CODE	:	BIS
EXAMINATION DATE	:	JULY 2020
DURATION	:	3 HOURS
INSTRUCTION	:	1. ANSWER **ALL** QUESTIONS 2. PLEASE MAKE SURE TO CLICK 'SAVE ANSWER" BUTTON FOR SUBJECTIVE QUESTIONS. OBJECTIVE QUESTIONS ARE SAVED AUTOMATICALLY.

THIS QUESTION PAPER CONSISTS OF **THREE (3)** PAGES

Q1 Referring to paper provided in the APPENDIX A:

(a) Identify a sentence that indicates a research problem in the **ABSTRACT** section

(2 marks)

(b) Formulate the research problem using your own word based on information in **INTRODUCTION** section

(5 marks)

(c) List **FIVE (5)** previous work by others that have been discussed as the foundation knowledge to the proposed solution

(5 marks)

(d) Extract main ideas from the **METHODOLOGY** section to discuss proposed solution using your own words.

(5 marks)

(e) Write a suitable summary for the **CONCLUSION** section.

(8 marks)

Q2 (a) An organization requires a strong authentication system to protect it from unauthorized person.

(i) Propose **THREE (3)** options available to authenticate a person.

(6 marks)

(ii) Propose a scenario where a *strong authentication* is more suitable than simple ones Explain the detail of such strong authentication

(6 marks)

(b) No password is strong enough to protect users in an organization. Write a "perfect" **TWELVE (12)** points password policy to secure an organization's password security. You should think of all the possibilities of breaking the password.

(12 marks)

(c) Granting access rights to subject should be based on the level of trust a company has in a subject and the subject's need to know.

(i) Provide **ONE (1)** example to demonstrate the importance of the above concept.

(4 marks)

(ii) Propose **FIVE (5)** effective ways of assigning access control rights.

(5 marks)

(d) Using multiple social engineering techniques, propose a "perfect" plan on how to change your blood type in the PKU's Student Medical Records. Make assumptions that several good security layers were already implemented at the PKU, and you are required to show exactly how you can break them

(12 marks)

-END OF QUESTIONS-

A policy-driven, human-oriented information security model: a case study in UAE banking sector

Khalid Eisa Haidar Abdalla Alhosani
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia
Batu Pahat Malaysia
gi180042@siswa uthm edu my

Shamsul Kamal Ahmad Khalid
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia
Batu Pahat Malaysia
shamsulk@uthm edu my

Noor Azah Samsudin
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia
Batu Pahat Malaysia
azah@uthm edu.my

Sapiee Jamel
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia
Batu Pahat, Malaysia
sapiee@uthm edu my

Kamaruddin Malik bin Mohamad
Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia
Batu Pahat, Malaysia
malik@uthm edu my

Abstract*— As companies continue to invest in information security, human weaknesses continue to remain a root cause of data breaches in organisations. Several security models have been proposed in the literature but largely remain ineffective at addressing this human vulnerability. In this paper, a policy-driven, human-oriented information security model is proposed. By adopting an information security policy, organizations set strong foundations on which sound security practices can be disseminated and enforced within the organisation. Instead of viewing human as the source of problem, it is a model that put human as the primary source of effectiveness to implement security policy. In this model, staffs in an organization will collectively secure an organisation from attacks. From existing literature and interviews conducted with selected banks in UAE, three primary factors, namely information security policy awareness, security training, and computer & security technology proficiency have been identified and incorporated into the new security model.

Keywords*—Information security policy, security model, awareness, compliance, banking information security, security performance.*

I. INTRODUCTION

When organizations lack a policy framework to guide information systems security, they fundamentally suffer an increase in cost as they try to manage information security in unstructured and unorganised ways [1] Ultimately an information security policy is the foundation on which sound security practices are disseminated and enforced within the organisation. This consensus exists among practitioners as information security policy becomes a prerequisite of organizational security management). Security experts have realized that in the absence of security policy, security practices would be developed with no clear establishment of objectives and allocation of responsibilities. This especially applies to financial institutions [2]. Financial institutions often deal with sensitive customer and transaction information, and this poses a significant challenge as such information is continuously increasing, and the organisations have the need to manage them securely and confidentially [2].

The UAE Banking sector has been of interest to cybercriminals and other financial criminals in both recent and distant times [3]. Ref [4] reports that the UAE lost about 2.8 billion US dollars in 2014 as a result of data loss and downtime. In 2017, the AE lost over US$ 1.1 billion to cybercrime mainly in the banking sector [5]. In 2018, over 14 million records were compromised with over 7/4 cyber-attacks at different entities across the country [6]. The level of protection against these crimes is very low (43%) whilst these criminals have advanced hacking methods and become more sophisticated. The Middle East region has reported costliest of data breaches over the years; 56% of breaches lead to loses above $500,000 compared to 33% globally [3]. The overall security outlook has raised concerns for banks in the UAE and resulted in changes in IT security policies and systems that these banks use [7].

According to Ref [8], legislation in the UAE requires that banks take the necessary measures to prevent the unauthorised access and use of customer data and ensure a robust security performance. Among such measures is the need for a firm security policy installation in every financial institution. Despite these commitments, the need for improved awareness of information security systems in the UAE and surrounding regions have been emphasised as being of serious concern [9] The lack of awareness in the region heightens the risk of security breaches and makes the entire installed security system vulnerable due to poor compliance [10]. Training programs require assessment within the real banking situation in order to practice and comprehend the risks and associated competencies to avoid security breaches In this paper a policy-driven, human-oriented information security model is proposed. It is a model that put humans as the main centre of implementing a policy document. Policy awareness, training and efficacy become instrumental to overall security performance in the sector, instead of a source of the problem.

The rest of this paper is organised as follows. In section 2, related work will be discussed. Interviews with selected banks conducted to gain important perspective with regard to awareness, training and efficacy are discussed in section 3.The outcome model is elaborated in section 4. Finally, section 5 concludes the finding and suggest further research in the area.

II. Literature Review

A. Theoretical Frameworks of Information Security Policy

Several theoretical conceptualisation attempts have been undertaken by various scholars to theorise information security policy. The information Security Process Model [11], the culture and information security practices model [17], information security governance framework [13] and the information security compliance model [14] are some of the few sampled theoretical frameworks presented in Table 1. Other models have associated information security models with unique functional or regional contexts of observation; these include Ref [12] on Saudi Arabia and Ref [14] on e-government information security policy framework (Table 1).

Table 1 Comparison of Information Policy Models

Model or Framework	Strengths	Weaknesses	Source
Information Security Process/ Integration Model	Process based and can permits integration into other business processes	The activity based process does not capture functional aspects of info. security	Savola et al. [11]
Information Security Culture and Practices Model	Country context-based by considering unique factors	Cannot be applied to other countries or regions	Alnatheer and Nelson [12]
Information Systems Policy Development Life Cycle	Information security policy development perspective	Sensemaking model but cannot be measured	Flowerday and Tuyikeze [15]
Meta policy model of Information Security Policy for emerging organizations	Trio perspective of management users and designers of information security policy	Does not address the dynamism in organizations over time	Baskerville and Siponen [16]
Governance of Information Security / Information Security Governance Framework	All-encompassing and most common framework or model of Info security policy	Multiple perspectives and inconsistencies across sources	Ula et al. [13]
Information Security Policy Compliance Framework	Diverse focus on technology, organisational culture, process and environment	Established based on interpretivist techniques	Al Kalbani et al [14]; Herath and Rao [18]
A behavioural compliance conceptual framework	Knowledge, values, skills framework of compliance	Analytical framework - complex	Alfawaz et al., [19]
Information security culture Model	Empirically supported and validated the research model	Behavioural info. security governance variables	De Veiga and Eloff [17]
Information Security Policy Framework for E-Commerce	Technology context-based by considering special factors of smart government	Cannot be applied to other contexts aside from e-government	Palmer et al., [20]
The framework of Human Factors in Information Security	Builds on attitude, intention and other belief factors	Cannot apply holistically to other non-human contexts	Gonzalez and Sawicka [21]

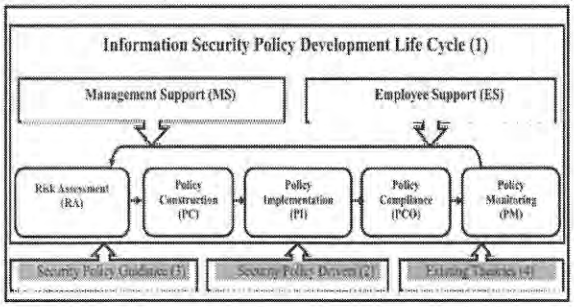

Fig. 1. Information Security Policy Development Model.

Among these models, the information security policy development life cycle observed that employees and management must together efforts to ensure compliance, monitoring and implementation of security policies in the development process [15] (see Fig 1). It shows security policy guidance as emanating from management whilst compliance, monitoring and feedback for continuous improvement are supplied through employee support.

This theory, and many of those presented in Table 1 predominantly built on behavioural and attitudinal theories to conceptualization. Two popular theories with the highest presence in this area includes the Theory of Planned Behaviour (TPB) and the Theory of Reasoned Action (TRA) [19] [22]. Ref [22] builds on the TPB and the InfoSec literature whilst Ref [19] combined the TPB and TRA in the bid to support information security compliance. The core of information security policy and compliance can be traced to behavioural theories.

B Information Security Policy Awareness and Attitude towards Information System Usage

The relationship between information system policy awareness and intention to take action in the right direction that is safe and secure has been established by Ref [10]. Awareness, whether perceived or assessed, have a fundamental effect on the intention to comply with security policy [10]. The same may be observed regarding the need to ensure that training programs are in place if installed security measures will prove to be effective in ensuring a safe and secure information environment [23].

Ultimately, adequate training and development of employees and stakeholders on the information security policy of any organization are critical to creating necessary awareness towards reduced vulnerability and improved safety [10] [23]. Finally, self-efficacy for security monitoring to comply [10] [18] [24].

According to Ref [25] and more recently [26] and [27] information security policy remains an integral measure of the performance of information security performance in any organization. Nonetheless, the human element in the form of attitudinal and behavioural intentions, whether international or non-intentional, play a fundamental role in overall security performance of the organisation as a whole [26] [27] The level of perceived risk and knowledge about probable causes of risk is critical to the overall success of any information security system [26] [27]. The proposed study considers the three main antecedents in the areas of awareness of information security policy, security training & education awareness (SETA), and Computer and Security Efficacy (COSE). These three antecedents support attitude and intention to comply with information security policy

III. Methodology

Three semi-structured interviews were conducted with security experts in three local UAE Banks; Al Hilal Bank, Arab Bank, and Sharjah Bank. The semi-structured interview guide was employed with four leading questions on security policy awareness, security training, computer self-efficacy, and overall compliance by bank employees. The interviews lasted approximately 30-35 minutes each, and none of them was recorded. Important notes were directly written, and follow-up questions were asked to draw deeper insight.

A. Findings from the interviews

The banking employees are considered central to the successful security posture of the bank. Employees are the most vulnerable security link in the bank, and awareness of information security policies ensure that the workers know their dos and don'ts. Employees would not rush to open emails from unknown senders but would first validate the sender to prevent opening up the organisation's security network to outside sabotage. Been able to identify a threat ensures that the security specialised are able to do proper threat hunting instead of handling a breach incident. According to the second expert: *"Part of the PCI [Payment Card Industry] and DSS [Data Security Standard] requirement awareness of Security must be in place in any critical or financial institution establishing and maintaining information security awareness through a security awareness program is vital to an organisation's progress and success"*.

All three experts agreed that by providing awareness of security policies, staff will understand the policy requirements and follow the same in the bank, security incidents will be reduced, and security performance effectiveness will be improved. Security quiz, privileged access (physical and/or logical access), phishing campaign, social engineering assessment are some of the central strategies that can help banks to increase the security performance through awareness and compliance posture assessment.

Security performance in the Bank is measured by the KPIs that are related to employees and organisation. A continuous learning and education culture will lead to minimisation incidents as employee remain abreast with security trends and landscapes. Training makes employees immune to information security threats in support of the advanced security team. A robust and properly implemented security awareness program assists the organisation with the education, monitoring and ongoing maintenance of security awareness. The minimum benchmark for theses security training programs include to meet PCI DSS requirement, demonstrate the ability to address and quickly adapt to the ever-changing data security threat environment, and demonstrate an ability to reinforce the organisation's business security culture. Different sets of audiences are trained depending on their nature of work and job responsibilities and needed security controls by which security performance effectiveness will be improved. Training usually entails a combination of classroom sessions, cognitive behavioural therapy (CBT), videos, real cyber threat cases among others.

In ideal scenario user and advanced computer skills are instrumental in helping the team to stay away from cyber harm, especially if there are clear policy guidelines that would help the users address any suspicious actives encountered. Even in the event of a high technology inclination, increased usage and scope of employee's activities can spur threat incidents. *"Usually from experience, the more users and computer the more trouble and issues for the security team "*

To boost one's information security self-efficacy, they must first ensure full knowledge of organisational security program, training content and communication channels. They must also ensure full awareness of security content usually offered during training and be aware of the security incident checklist. General and unrelated computer and security self-efficacy will assist the staff to understand the nature of security controls and follows the same in the bank, by which security performance will be improved.

A variety of security extensions are adopted in the banking sector: *"The most effective systems would be the AV, APT, DLP, proxy services, DNS security and email gateways along with network admission control. With the enforcement of security control, it is a must to access corporate resources,without enforcement it will not exceed 40% as a very optimistic number."*

The bank must have 95%+ compliance with security policies to relegate breach incidents to an issue of minimal chance

IV. Results and Discussion

Human strengths or weaknesses have been the focal point of a security system. From a positive angle, aligning strengths toward compliance of a security policy document will effectively prepare the organization against attacks. Compliance to information security policy has been considered critical to banking security performance. Findings support the argument that the source of information securitypolicy compliance and banking security performance stem from a behavioural and attitudinal orientation of the employees [26] [27] [28]. Likewise, perceived risk and awareness, training, and overall technology proficiency are key to reduce threat incidents, ensure compliance and improve performance [29].

From these findings, we now present the conceptual model and formal model of a policy-driven, human-oriented information security model. It ends with an example of the model implementation for a simple bank.

A. A Conceptual Model

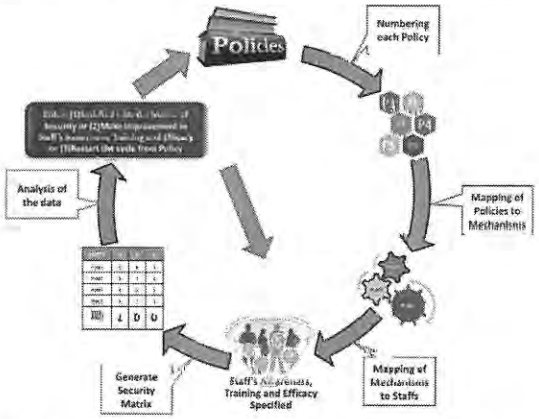

Fig 2. The Policy Driven, IIuman Oriented Information Security Conceptual Model

In Figure 2, the policy-driven, human-oriented information security model starts with a policy document. From the policy document, each policy stated in the document is assigned a unique number. For each policy, suitable mechanism will be generated to ensure the achievement of the policy. It is common practice for an organisation to employ multiple mechanisms to implement a policy. A mechanism is then assigned to all or some staffs to implement it. In order to carry out a policy satisfactorily, a staff must have appropriate awareness, training and efficacy. Finally, the state of information security of the bank is given by a security matrix combining all state of staff's awareness, training and efficacy.

B. The Formal Model

Definition 1:

P is a security policy document of a bank. Each policy stated in the document can be assigned a unique number such as P_1, P_2, ... , P_α, where α is the total number of policy in the document.

Definition 2:

M is a security mechanism used to address a security policy. In line with the principle of "Defense in Depth", there can be more than one mechanism to effectively address a policy. Therefore, a P_1 can be addressed by a list of mechanisms M_1, M_2, ... , M) , where β is the maximum number of mechanisms supported for a policy.

Definition 3:

S is a staff responsible for addressing a mechanism M of a policy P. A staff can be categorized into at least two types:

a. **Security team**, labelled as S^{sec}, are staffs specialized in information security of the bank.

b. **All** staffs working in the bank, labelled as S^{all}, including the security team.

As a note, $S^{\text{sec}} = S^{\text{id1}}, S^{\text{id1}}, \ldots, ^{\text{idmax}}$ indicates all the staffs in the information security department of a bank. The staff-id number is used to identify specific staff

The capacity of a staff to address a security mechanism primary depends on 3 aspects, as pointed out in previous section The three aspects are:

a. Security *awareness* (SA), labelled as a

b. Security *training* and education (SETA), labelled as t

c. Computer and security *efficacy* (COSE), labelled as e

Efficacy is the capability to implement a policy in normal and problematic situation A staff with efficacy is actually living the policy in his/her daily life.

Definition 4.

The state of awareness, a of a security staff, S can be represented by:

$$S_a^{sec}$$

Therefore, the mapping of Policy P_1 and Mechanism M_1 to the above staff's awareness of the policy is given by:

$$\langle P_1, M_1 \rangle \rightarrow S^{sec}_{a_{\langle P_1, M_1 \rangle}}$$

It represents the policy and mechanism to be addressed by a security staff's awareness of $\langle P_1, M_1 \rangle$.

Definition 5:

The state of awareness, training and efficacy, (a, t, e) of a security staff, S can be represented by:

$$S^{sec}_{(a,t,e)}$$

Therefore, the mapping of Policy P_1 and Mechanism M_1 to the above staff's awareness, training and efficacy of the policy is given by:

$$\langle P_1, M_1 \rangle \rightarrow S^{sec}_{(a,t,e)_{\langle P_1, M_1 \rangle}}$$

It represents the policy and mechanism to be addressed by a security staff's awareness, training and efficacy of $\langle P_1, M_1 \rangle$. The value of

$$\langle P_1, M_1 \rangle \rightarrow S^{sec}_{(a,t,e)_{\langle P_1 M_1 \rangle}} \equiv \langle a, t, e \rangle$$

Definition 6:

Let us assume α as the maximum number of policy and $\beta = (\theta_1, \theta_2, \ldots, \theta_\varepsilon)$ stores all maximum numbers of mechanisms supported for a policy. The state of information security for the bank is the combination of each staff's awareness, training and efficacy addressing all mechanisms required by every policy stated in the policy document. Thus, the state of information security of the bank is represented as:

$$[\alpha, \beta = (\theta_1, \theta_2, \ldots, \theta_\varepsilon)] \vdash \sum_{i=1}^{\alpha} \sum_{j=1}^{\beta_j} \langle P_i, M_j \rangle \rightarrow S^{\text{sec }|all}_{(a,t,e)_{\langle P_i, M_j \rangle}}$$

For example, if $\beta = (3, 5, \ldots, 7)$ and $j = 2$, then $\beta_2 = 5$. This supports varied number of mechanisms for a given policy.

In the following section, we present an example of the state of information security of a bank with several assumptions to help the reader understand the model.

C. An Example

Let us assume a bank has only 2 policies.

P_1: All corporate email account must have 15-characters length password

P_2: Our corporate firewall must block all outbound and inbound ports not required by corporate applications.

From P_1, we generate 3 mechanisms:

M_1: Every staffs entered 15 characters length password for their corporate email account.

M_2: Security staff configure the email server or LDAP server to accept only 15-characters length password.

M_3 : Every 6 months, the security staff will do a password audit for all corporate email accounts

From P_2, we generate 2 mechanisms:

M_1: Security staff configure the firewall to block all ports, inbound and outbound, except the ones required by corporate applications.

M_2: Security staff will run a randomly scheduled weekly basic penetration testing to detect unauthorized open ports.

Furthermore, let us assume the bank has only 4 staffs:

S^1, the Manager

S^2, an accounting officer, working in the Accounting Department

S^3, a sales assistant, working in the Sales Department

S^4, a firewall administrator, working in the Information Security Department

Based on the above information,

$S^{sec} = S^4$

$S^{all} - S^1, S^2, S^3, S^4$

The Policy-Mechanism mapping to appropriate staff:

$$\langle P_1, M_1 \rangle \rightarrow S^{all}_{(a,t,e)_{\langle P_1, M_1 \rangle}}$$

$$\langle P_1, M_2 \rangle \rightarrow S^{sec}_{(a,t,e)_{\langle P_1, M_2 \rangle}}$$

$$\langle P_1, M_3 \rangle \rightarrow S^{sec}_{(a,t,e)_{\langle P_1, M_3 \rangle}}$$

$$\langle P_2, M_1 \rangle \rightarrow S^{sec}_{(a,t,e)_{\langle P_2, M_1 \rangle}}$$

$$\langle P_2, M_2 \rangle \rightarrow S^{sec}_{(a,t,e)_{\langle P_2, M_2 \rangle}}$$

Assuming the number of level provided for each a, t and e is only 2 (yes or no/1 or 0), the state of each staff with regard to a, t, e is provided below:

$\langle P_1, M_1 \rangle$	Every staff entered 15 characters length password for their corporate email account.			
Staff Id	Awareness of $\langle P_1, M_1 \rangle$	Attended Training of $<\langle P_1, M_1 \rangle$	Efficacy of $\langle P_1, M_1 \rangle$	$\langle P_1, M_1 \rangle \rightarrow S^{sec\ \mid all}_{a_{\langle P_1, M_1 \rangle}}$
S^1	Yes	Yes	Yes	<1,1,1>
S^2	No	No	No	<0,0,0>
S^3	Yes	Yes	No	<1,1,0>
S^4	Yes	Yes	Yes	<1,1,1>
S^{all}	No	No	No	<0,0,0>

S^{all} for awareness will receive a value of 0 if any single staff is not aware of the policy. Similarly, for training and efficacy. This is due to security compromise caused by the staff with no awareness, training or efficacy S^2 is possibly the weakest link in the bank.

$\langle P_1, M_2 \rangle$	Security staff configure the email server or LDAP server to accept only 15 characters length password			
Staff Id	Staff Awareness of $\langle P_1, M_2 \rangle$	Staff Attended Training of $\langle P_1, M_2 \rangle$	Staff Efficacy of $\langle P_1, M_2 \rangle$	$\langle P_1, M_2 \rangle \rightarrow S^{sec\ \mid all}_{a_{\langle P_1, M_2 \rangle}}$
S^1	Yes	Yes	No	<1,1,0>
S^{sec}	Yes	Yes	No	<1,1,0>

$\langle P_1, M_3 \rangle$	Every 6 months, the security staff will do a password audit for all corporate email accounts.			
Staff Id	Staff Awareness of $\langle P_1, M_3 \rangle$	Staff Attended Training of $\langle P_1, M_3 \rangle$	Staff Efficacy of $\langle P_1, M_3 \rangle$	$\langle P_1, M_3 \rangle \rightarrow S^{sec\ \mid all}_{a_{\langle P_1, M_3 \rangle}}$
S^4	Yes	Yes	Yes	<1,1,1>
S^{sec}	Yes	Yes	Yes	<1,1,1>

$\langle P_2, M_1 \rangle$	Security staff configure the firewall to block all ports, inbound and outbound, except the ones required by corporate applications.			
Staff Id	Staff Awareness of $\langle P_2, M_1 \rangle$	Staff Attended Training of $\langle P_2, M_1 \rangle$	Staff Efficacy of $\langle P_2, M_1 \rangle$	$\langle P_1, M_3 \rangle \rightarrow S^{sec\ \mid all}_{a_{\langle P_2, M_1 \rangle}}$
S^4	Yes	Yes	Yes	<1,1,1>
S^{sec}	Yes	Yes	Yes	<1,1,1>

$\langle P_2, M_2 \rangle$	Security staff will run a randomly scheduled weekly basic penetration testing to detect unauthorised open ports.			
Staff Id	Staff Awareness of $\langle P_2, M_2 \rangle$	Staff Attended Training of $\langle P_2, M_2 \rangle$	Staff Efficacy of $\langle P_2, M_2 \rangle$	$\langle P_1, M_3 \rangle \rightarrow S^{sec\ \mid all}_{a_{\langle P_2, M_2 \rangle}}$
S^4	Yes	No	No	<1,0,0>
S^{sec}	Yes	No	No	<1,0,0>

The current information security state of the bank is a matrix:

0	0	0
1	1	0
1	1	1
1	1	1
1	0	0

We can generate other indicators from the matrix. For example. the state of awareness is (4/5) = 80%. While the efficacy of staff at handling computer and security efficacy is (2/5) = 40%. Training Needs and Analysis can also be made based on the matrix

V Conclusion

As companies continue to invest in information security human errors continue to remain a root cause of data breaches in organisations. In this paper two contributions have been made to the body of knowledge. Firstly, from previous published works and interviews, three key human factors have been identified that greatly influence the effectiveness of a company security implementation. Secondly, a new policy driven, human oriented security model has been proposed, which puts human as the centre stage for implementing security policy stated in a company's information security policy document. Further works need to be investigated on how this basic model can help an organization achieve better security posture. A comprehensive survey will be conducted in UAE banking industry to confirm the role of the three factors as well as adding new factors and improve the model with larger scope that can take into account daily dynamic attacks on the banking industry.

References

[1] D. Zhang, Big data security and privacy protection. In 8th International Conference on Management and Computer Science (ICMCS 2018). Atlantis Press, October 2018.

[2] K. Pilarczyk. Importance of Management Information System in Banking Sector. Annales Universitatis Mariae Curie-Skłodowska. Sectio H. Oeconomia, Vol. 50(2), pp. 69-80, 2016

[3] M. Roseberg. UAE banks need to plug all holes against cyber threats. Retrieved from: https://gulfnews.com/business/analysis/uae-banks-need-to-plug-all-holes-against-cyber-threats-1.2288760 October 2018.

[4] EMC. Global Data Protection Index (2014). Retrieved from http://www.datamanager.it/wp-content/uploads/2014/12/EMC-Data-Protection-Index-Key-Findings-Italy-FINAL.pdf 2014.

[5] A. Sharma. Cybercrime to remain an expensive foe with more waging battle over email in 2019. https://www.thenational.ae/business/technology/cybercrime-to-remain-an-expensive-foe-with-more-waging-battle-over-email-in-2019-1.807760, December 2018.

[6] N. K. Cherrayil. UAE had two major industry data breaches in first half of 2018. Gulf News. Retrieved from: https://gulfnews.com/technology/uae-had-two-major-industry-data-breaches-in-first-half-of-2018-1.2288816 June 2018

[7] V. Ambhire, and P. Teltumde. "Information Security in Banking and Financial Industry", International Journal of Computational Engineering and Management, Vol. 14, pp. 101 105, 2011.

[8] DLA Piper. Data Protection Laws of The World. Retrieved from https://www.dlapiperdataprotection.com, 2013

[9] Basamh, S. S., Qudaih, H. A., & Ibrahim, J. (2014). An overview on cybersecurity awareness in Muslim countries. *International Journal of Information and Communication Technology Research*, 4(1), 21-24.

[10] P. Zhang, and X. Li. Determinants of Information Security Awareness: An Empirical Investigation in Higher Education. Information Security Awareness, Thirty Sixth International Conference on Information Systems, Fort Worth , 2015

[11] R. Savola, J. Anttila, A. Sademies, J. Kajava, J., and J. Holappa. Measurement of information security in processes and products. In: Security Management, Integrity, and Internal Control in Information Systems, Springer, Boston, MA, pp. 249-265, 2005Alnatheer & Nelson (2009)

[12] M Alnatheer and K I Nelson *A Proposed Framework for Understanding Information Security Culture and Practices in the Saudi Context*. In: 7th Australian Information Security Management Conference, 1-3 December 2009, Perth. 2009. (In Press)

[13] M. Ula, Z. Ismail, and Z. M. Sidek. "A Framework for the governance of information security in banking system", Journal of Information Assurance and Cyber Security pp 1-12 2011

[14] A. Al Kalbani, H. Deng, and B. A. Kam. Conceptual framework for information security in public organizations for e-government development ACIS 2014

[15] S. V. Flowerday, and T. Tuyikeze. "Information security policy development and implementation: The what, how and who", Computers and security, Vol. 61, pp. 169-183. 2016

[16] R Baskerville and M Siponen "An information security meta-policy for emergent organizations", Logistics Information Management, Vol. 15(5/6), pp. 337-346, 2002.

[17] A. Da Veiga, and J. H. Eloff. "A framework and assessment instrument for information security culture", *Computers and Security*, Vol. 29(2), pp. 196-207, 2010.

[18] T. Herath, T., and H. R. Rao. "Protection motivation and deterrence: a framework for security policy compliance in organisations", European Journal of Information Systems, 18(2), 106-125, 2009b

[19] S. Alfawaz, K. Nelson, and K. Mohannak. Information security culture: a behaviour compliance conceptual framework. In: Proceedings of the Eighth Australasian Conference on Information Security-Volume 105. Australian Computer Society, Inc. pp. 47-55, January 2010.

[20] M. E. Palmer, C. Robinson, J. C. Patilla, and E. P. Moser. "Information security policy framework: best practices for security policy in the e-commerce age", Information Systems Security, Vol. 10(2), pp. 1-15, 2001.

[21] J. J. Gonzalez, and A. Sawicka. A framework for human factors in information security. In Wseas international conference on information security, Rio de Janeiro, pp. 448-187, October 2002.

[22] F. Bélanger, S. Collignon, K. Enget, and E. Negangard. Determinants of early conformance with information security policies. Information and Management, Vol. 54(7), pp. 887 901, 2017

[23] A. Tsohou, S. Kokolakis, M. Karyda, and E. Kiountouzis. Investigating Information Security Awareness: Research and Practice Gaps. Information Security Journal: A Global Perspective Vol. 17, pp. 207-227, 2008

[24] B. Bulgurcu, H. Cavusoglu, and I. Benbasat. "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness". MIS Quarterly, Vol. 34(3), pp. 523-548, 2010

[25] S. E. Schimkowitsch. Key Components of an Information Security Metrics Program Plan. Master Thesis Presented to the Interdisciplinary Studies Program: Applied Information Management and the Graduate School of the University of Oregon, 2009

[26] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos. The human factor of information security: Unintentional damage perspective. Procedia Social and Behavioral Sciences, Vol. 147, pp. 424-428, 2014a.

[27] E. Metalidou, C. Marinagi, P. Trivellas, N. Eberhagen, C. Skourlas, and G. Giannakopoulos. Human factor and information security in higher education. Journal of Systems and Information Technology, Vol. 16(3), pp. 210-221, , 2014b.

[28] H. A. Kruger, and W. D. Kearney. A prototype for assessing information security awareness computers and security, Vol. 25(4), pp. 289-296, 2006

[29] I. Bernik, and K. Prislan. "Measuring information security performance with 10 by 10 model for holistic state evaluation", PloS one, Vol. 11(9), pp. e0163050, 2016