The Role of Culture in the Design of Effective Cybersecurity Training and Awareness Programmes. A Case Study of the United Arab Emirates (UAE)

Abdulla Al Neaimi(✉) and Philip Lutaaya

SecureTech, LLC, Abu Dhabi, UAE
alneaimi@gmail.com, lutaphilo@gmail.com

Abstract. The question whether culture of a society needs to be considered when designing cybersecurity training and awareness programs has recently risen in literature. While some programs may be effective in the west, they may not apply in the Middle East or Africa. Since cybersecurity has overtaken terrorism as the leading security concern globally, criticality of user training and awareness programmes cannot be overemphasized. This paper demonstrates that a cybersecurity training or awareness program that considers cultures of the people is more effective than generic one. Staff in a midsized organization were randomly divided into two groups. Group one consisting of Indians was treated to a culturally sensitive training programme in Hindi while group two consisting of Ugandans, Nepalese, Pakistanis and the Philippines undertook a generic one in English. A survey was conducted subsequent to the treatments. Results revealed that group one demonstrated better understanding of cybersecurity issues after one month.

Keywords: Training and awareness · Culture · Cybersecurity
United Arab Emirates (UAE)
Information and Communication Technology (ICT) · Internet of Things (IoT)

1 Introduction

The worldwide increase in ICT security threats has primarily been due to recent rapid increase in volumes of electronic data, increased number of mobile terminals and other digital electronic devices like digital watches and Smart TVs among others interconnected via the internet as IoT devices.

Well organized attacking groups with sophisticated profiles and meagre cybersecurity awareness amongst employees has deepened the gap in most organization's cybersecurity systems [1]. Many countries globally including the United States, Africa and the Middle East have introduced cyber laws with strict punishment against cybercrime. Unfortunately, cyber threats still succeed because people lack appropriate training and awareness. More still, authors in [1] argue that while organizations continue to train their professionals in technology very little effort has been put into

V. Odumuyiwa et al. (Eds.): AFRICOMM 2017, LNICST 250, pp. 131–139, 2018.
https://doi.org/10.1007/978-3-319-98827-6_11

cybersecurity awareness and training programmes which possess a major risk to the employees in case of cyber-attacks.

Employees are the weakest link to information security of any organization, those who undergo awareness sessions and comply with rules and procedures for information security assist in strengthening the organization's overall security and attitude to prevent cyberattacks [2]. It is revealed that information security awareness and education is very important in improving organization's overall security [3]. Additionally, cybersecurity training is looked at as a key influence to behavior of users on security issues by reducing the knowing-doing gap amongst organization's employees [4]. Cybersecurity can be defined as the protection of systems, networks and data in cyberspace from any form of unauthorized access or attacks. Among these attacks include viruses erasing an entire system, someone breaking into network system and altering files, someone using computers to attack others on the same or different networks, or someone stealing credit card information and making unauthorized purchases. Unfortunately, there's no 100% guarantee that even with the best technological precautions in place these attacks won't happen.

Organizations need to establish cultural sensitive cybersecurity training and awareness programs to disseminate information regarding the identification, protection, detection, response and recovery from cybercrime [5]. Available empirical evidence reveals that the human factor has become the major ambiguity in the implementation of information security programmes in different organizations since employees are usually careless and unaware of most information security practices, policies and procedures [6]. Our hope is that the findings of this paper bring out the role of designing cultural sensitive cyber and information security training and awareness programs in different entities across the UAE, Africa and Globally. The rest of the paper is divided into five sections, Sect. 2 provides a critical review of related literature and the research strategy, Sect. 3 presents results from the pre and post awareness training assessment given to two distinct groups and describes the case study used, Sect. 4 provides a brief discussion from the survey, and finally Sect. 5 concludes the study.

2 Study Background

Information security training and awareness programmes explain the role of employees towards information security of their organizations by showing what they need or can do to protect their organization's critical data in case of cyber-attacks [7]. User behaviors and attitudes need to change if cyber and information security incidents are to be reduced in any organization. In addition, cultural aspects of the people also need to be considered to ensure quick information dissemination and understanding. This notion has been discussed by several authors in literature, for instance Garett [8] looks at culture as the totality of socially transmitted behavior patterns, arts, beliefs and all other products of human work.

It represents a shared set of traditions and behaviors shaped by history, religion, ethnic identity, language and nationality that provides a lens through which people can see and understand the world. Governments and employers need to play a leadership

role towards instituting a cyber-security culture amongst nationals through multi-disciplinary and multi-stakeholder approaches that includes training and awareness, cultural sensitive cybersecurity policies and Education [8].

Awareness programs explain an employee's role in information security by showing the users what they can do to protect their organization's critical data and instilling a sense of responsibility and purpose into the employees who manage critical information. Additionally, people's mistakes cannot be solved by mere addition of technology but through a joint effort and partnerships between the IT community of interest, the business community, the nationals through training and awareness along with critical government and top management support [9].

In [10] Seibert et al., looks at culture as an organized group of learned responses with readily made solutions to problems faced by people through interactions with others in the society. It is revealed that culture shapes responses to illness and treatment of people in society. Further, over 85% of the UAE population is from foreign labour which implies that several cultures, cultural norms and religious practices have been imported in the region from different continents like Asia, Africa, Europe, and the Gulf Cooperation Council (GCC) among others. This has created a multi-cultural society speaking different languages.

In this paper, we believe that cultural sensitive cybersecurity training and awareness programmes would close the communication gap and improve employee awareness and knowledge of cyber threats. Meanwhile, different cultures of people have different training and awareness needs implying the need to design appropriate training and awareness programmes and requires planning with clearly defined roles and responsibilities. Furthermore, awareness programs need to teach people information security issues like confidentiality, integrity and availability of information with emphasis on what needs to be protected, against who, when and how [11]. Business success depends upon continuity of operations and information provided to the business processes by information systems. Awareness programs help in sensitizing users on how to behave and benefit from information without jeopardizing its confidentiality, integrity and availability. Lack of awareness and mishandling of information could expose it to competitors or attackers. Therefore, the only thing which can change the behavior and thinking of the staff is awareness and training, since people join organizations with different beliefs, values, culture and principles in line with the aim of this paper [12].

It is patent that solely technological solutions are unlikely to prevent security cracks within organizations [2, 13]. Therefore, security functions need to organize employee training and awareness programmes in addition to the existing technological defenses by acknowledging the influence of individual cultural differences, personality traits and cognitive abilities. Meanwhile, an online survey about information security threats was conducted for a period of one month on a group of two hundred (200) users who volunteered to answer the survey questions. Survey results showed that users who had ever attended information security training programmes before demonstrated more knowledge in the understanding of information security issues. However, this survey did not consider the cultural context of the people online [14].

Authors in [15] argue that cultural factors impact the security knowledge and behavior of different people. The authors used an information security vocabulary test to assess the level of awareness, knowledge and behaviors amongst students in two selected Universities in South Africa. Their main objective was to identify whether cultural differences would affect students' understanding of security issues. The findings revealed that cultural factors such as a person's mother tongue and place of origin showed a significant impact on awareness levels of security issues among selected students. Therefore, the issue of culture cannot be under estimated when designing cyber and information security training and awareness programmes.

Meanwhile, Kruger and Dhillon [16, 17], claims that informal behavior forms a fundamental role in describing characteristics of people and acts of communication that form information. It is stated that the process of communication forms a central hub in information systems and that patterns of learning, culture as well as norms are form constituent elements of informal behavior. Therefore, complete management of information security can only be ensured if the behavioral aspects of individuals and groups have been well understood. This necessitates a study to prove validity of these findings especially in a multi-cultural environment like the United Arab Emirates. In this study a randomly selected group of 50 employees from a mid-sized organization were divided into two groups based on country of origin, culture and common language examining them before and after a cybersecurity training and awareness programme as detailed in the next section;

3 Case Study

A total of fifty (50) employees were randomly selected from a midsized organization in Abu Dhabi and divided into two groups. Group one, involving employees from a similar cultural background and language (Indians only) while Group two considered members from different cultural backgrounds (Ugandans, Nepalese and Philippines). A survey consisting questionnaire items concerning cyber and information security issues pertaining their organization was administered to members before a cybersecurity awareness training programme, the aim was to assess if they understood cyber and information security vulnerabilities affecting their organizations. Pre training assessment results from the two groups were kept and an information security awareness training programme was organized.

Group one went through a *culturally sensitive* cybersecurity awareness programme conducted in HINDI while Group two was given a generic one conducted in English. The survey involved provision of a post training assessment after a period of one month with help of scored questionnaires tailored towards cybersecurity awareness and information security administered to the two groups. The responses from the respondents in the two cases were later coded into IBM SPSS 21, a statistical application for analysis of data and generation of results. The results of the survey following the above treatments were as seen in Tables 1 and 2 below;

Table 1. Pre training assessment results for group one and group two

Variable (questionnaire item)	Available Options	(Group one) (100%) Hindi session	(Group two) (100%) English session
I know What to do If a security breach occurs	Yes (1)	15.4	51
	No (5)	84.6	49
Valuable Information is stored in	Private Email (3)	57.7	27.3
	Company Email (5)	38.5	0
	Different Location (1)	3.8	72.7
Information in email won't be changed by virus	Yes (5)	73.1	63.6
	No (1)	3.8	18.2
	I don't know (3)	23.1	18.2
I have Undergone Cybersecurity Training before	Yes (1)	11.1	16
	No (5)	88.5	84
I understand Cybersecurity Concept	Yes (5)	26.9	37
	No (1)	73.1	73
My organization has a cyber-Security Plan	Yes	53.8	45.5
	No	3.8	45.5
	Not Sure	42.3	9.1
I understand different forms of Cyber attacks	Yes (1)	23.1	59.2
	No (5)	73.1	90.9
I know Email Scam	Yes	50	40.8
	No	42.3	90.9
I know my responsibility in Cybersecurity	Yes (1)	11.5	45.5
	No (5)	38.5	15
	Not Sure (4)	42.3	39.5
I Share documents with staff	Yes	54.5	15.4
	No	45.5	84.6
My company has a Cybersecurity Team	Yes	19.2	0
	No	0	9.1
	I don't know	76.9	90.1
I have ever found a Computer Virus	Yes	34.6	100
	No	3.8	0
	I don't know	53.8	0
Password Sharing is good	Yes	0	0
	No	100	100
Security of my Computer	Very secure	0	7.7
	Not secure	18.2	15.4
	Am not sure	81.8	76.9
Firewall is enabled on my Computer	Yes	0	15.4
	No	0	23.1
	I don't know	100	50
I know Phishing attack	Yes (1)	0	3.85
	No (5)	100	92.31
Download and Install software	Yes (5)	38.5	0
	No (1)	61.5	100
Use same Password for different accounts	Yes	0	18.2
	No	100	81.8

Table 2. Post training assessment results for group one and group two

Variable (questionnaire item)	Available Options	(Group one) (100%) Hindi session	(Group two) (100%) English session
I know who to contact if a security threat occurs	Yes	95.5	83.3
	No	4.5	16.7
I know phishing attack	Yes	75	68.2
	No	25	31.8
The Best Place for storage of critical data	Private Email	33.3	40.9
	Company Email	9.1	31.3
	Personal Computer	18.2	32.2
	External Location	48.5	27.8
Undergone Cybersecurity Training before	Yes	100	100
	No	0	0
I understand my Role in Cybersecurity	Yes	86.4	91.7
	No	9.1	8.3
Not a sign of cyber Attack	Persistent popups	0	27.3
	Missing Data	0	27.7
	System behavior change	8.7	27.3
	Computer makes Noise	91.3	13.6
I understand different forms of Cyber attacks	Yes	72.7	50
	No	18.2	50
I understand Email Scam	Yes	81.8	85
	No	13.6	15
I know my responsibility in Cybersecurity	Yes	91.3	69
	No	3	27
	Not Sure	5.7	2
I open email attachment only when….	I know the person or company it comes from	54.5	50
	As long as it's a person	36.4	41.7
	There is nothing wrong	0	-
I share Passwords with others	Yes	0	0
	No	100	100
Why people fail to Understand security issues	Nothing important	59.1	41.7
	Technology working	13.6	25.0
	All the above	18.2	33.3
Why do we need security?	Privacy concerns	91.7	27.3
	To kill attackers	0	0
	Protect managers	8.3	63.6
I know signs when my PC is Hacked	Yes	63.6	66.7
	No	31.8	16.7
I use personal device to transfer data	Yes	8.3	36.4
	No	87	45.5
My computer has no value to hackers	I don't know	4.7	16.7
	Yes	18.2	0
	No	72.7	100

4 Discussions

Figure 1 below extracts results concerning the respondent's understanding of "*Phishing attacks*" as detailed in Tables 1 and 2 above before and after the culturally sensitive cybersecurity awareness training session;

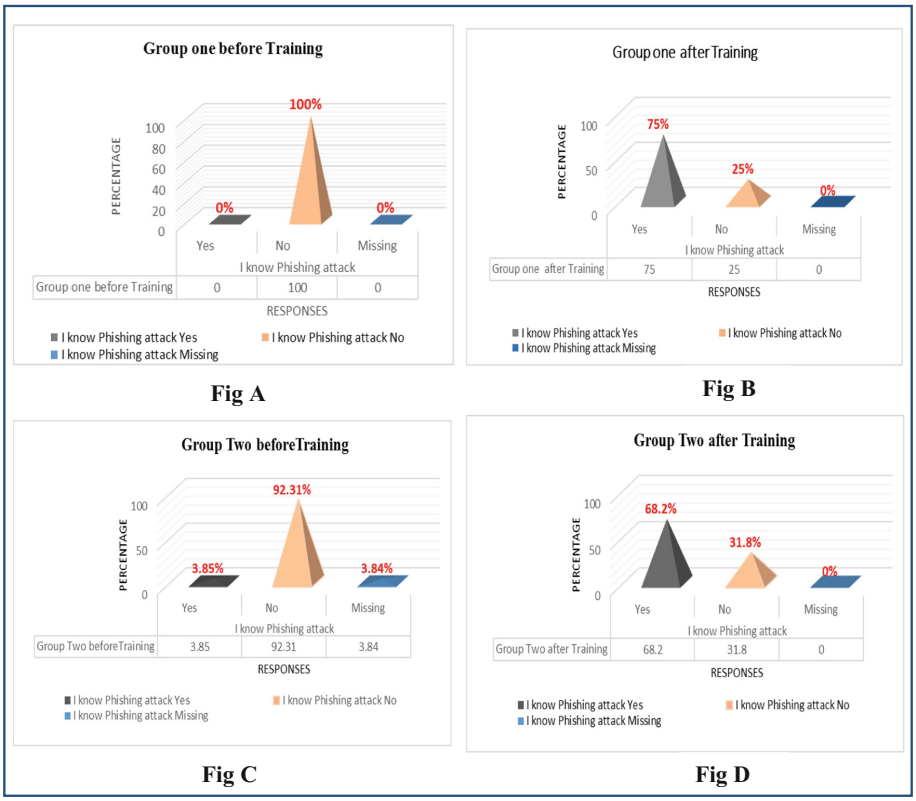

Fig. 1. Results from phishing attacks assessment before and after cybersecurity awareness training sessions

Generally, after comparing employee responses to information security questionnaire items in Tables 1 and 2, we observe a considerable improvement in the understanding of cyber and information security issues by the two groups (group one and group two) after the cybersecurity awareness training session. The post awareness training assessment conducted a month later showed that participants who undertook a culturally sensitive awareness training programme exhibited better understanding of the Cyber and information security issues including phishing attacks as compared to the generic group. For instance, results in Fig. 1A shows that participants from the culturally sensitive group (group one) had no idea of phishing attacks before the awareness session, while 3.85% from the generic group (group two, Fig. 1C) understood phishing attacks before the awareness session.

After the awareness session, post training assessment results show that 75% of the participants from the culturally sensitive group one understood Phishing attacks as indicated by the post assessment results (Fig. 1B). This was higher than the 68.2% from the generic group two (Fig. 1D). This trend clearly confirms that when people are trained cybersecurity concepts in their local languages considering their cultural

background and languages, they understand the concepts better than generic training programs conducted in secondary languages. This approach is very critical for developing countries and the UAE where most of the expatriates come from different countries with different cultural beliefs and languages.

5 Conclusion

In this paper, the question of whether the culture of a society needs to be taken into account when designing cybersecurity training and awareness programs has been clearly discussed and critically evaluated by using the survey results. Culturally sensitive cybersecurity training programs will provide a good avenue for the local and international people to fully participate and embrace security issues of critical importance to their organizations and the government at large. Our results can be used as a stepping stone in the design of appropriate training and awareness programs for combating the cybersecurity problem that emerged recently as one of the key security issue in the United Arab Emirates and other multi-cultural regions like Africa.

References

1. Aloul, F.A.: The need for effective information security awareness. J. Adv. Inf. Technol. **3** (3), 176–183 (2012). Academy Publisher, https://doi.org/10.4304/jait.3.3.176-183
2. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. In: Management Information Systems Research Centre, University of Minnesota, USA, vol. 34, no. 3 (2010)
3. Siponen, M.T.: A conceptual foundation for organizational information security awareness. Inf. Manag. Comput. Secur. **8**(1), 31–41 (2000)
4. Horcher, A.-M., Tejay, G.P.: Building a better password: the role of cognitive load in information security training. In: IEEE, Richardson, TX, USA (2009)
5. Wunderle, W.D.: Through the Lens of Cultural Awareness: A Primer for US Armed Forces Deploying to Arab and Middle Eastern Countries, Combat Studies Institute Press Fort Leavenworth, KS 66027 (2006)
6. Lim, J.S., Ahmad, A., Chang, S., Maynard, S.B.: Embedding information security culture emerging concerns and challenges. In: PACIS 2010 Proceedings, Brisbane, Australia, pp. 463–474 (2010)
7. McCrohan, K., et al.: Influence of awareness and training on cyber-security. J. Internet Commer. **9**, 23–41 (2010). Method Approaches, pp. 3–23. Sage/Media, Inc., London/Hingham
8. Garret, C.: Developing a Security-Awareness Culture - Improving Security Decision Making. SANs Institute (2005)
9. Hight, S.D.: The importance of a security, education, training and awareness program (2005). http://www.infosecwriters.com/Papers/SHight_SETA.pdf. Accessed 25 Oct 2017
10. Seibert, P.S., Stridh-lgo, P., Zimmerman, C.G.: A checklist to facilitate cultural awareness and sensitivity. J. Med. Ethics **28**, 143–146 (2002)

11. Whitmer, M.G.: IT security awareness and training, changing the culture of state government (2007). https://www.nascio.org/Portals/0/Publications/Documents/NASCIO-ITSecurityAwarenessAndTraining.pdf. Accessed 15 Oct 2017
12. Ashraf, S.: Organization Need and Everyone's Responsibility Information Security Awareness. SANS Institute (2005)
13. Kritzinger, E., Von Solms, S.H.: Cyber-security for home users: a new way of protection through awareness enforcement. Comput. Secur. **29**(8), 840–847 (2010)
14. Parsons, K., McCormac, A., Butavicius, M., Ferguson, L.: Human factors and information security: individual, culture and security environment. Australian Government, Department of Defence (2010)
15. Al Shehri, Y.: Information security awareness and culture. Br. J. Arts Soc. Sci. (2012). ISSN: 2046-9578. British Journal Publishing
16. Kruger, H.A., Flowerday, S., Drevin, L., Steyn, T.: An assessment of the role of cultural factors in Information Security awareness. ISSA, IEEE Xplore Digital Library (2011). www.researchgate.net
17. Dhillon, G.: Principles of Information Systems Security, Text and Cases. Wiley, New Jersey (2007)