Journal for Re Attach Therapy and Developmental Diversities
eISSN: 2589-7799
2023 August; 6 (10s2): 912-916

The Impact of Digital Threat Awareness on Performance Against Cybercrime among Police Officers in Dubai

[1]Tayeb Alharmoodi, [2]Zaim Ahmad
[1]College of Law, Government and International Studies, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah
tayeb276@hotmail.com
[2]College of Law, Government and International Studies, Universiti Utara Malaysia, 06010 UUM Sintok, Kedah
zaim@uum.edu.my

Received: 11- June -2023
Revised: 13- July -2023
Accepted: 19- August -2023

ABSTRACT

Cyber security awareness combines knowledge and taking the necessary measures to protect organizations' information assets. Moreover, when security personnel is aware of electronic security, they understand electronic threats, the potential impact of a cyberattack on society, and the steps required to mitigate the risks and prevent cybercrime from infiltrating their online workspace. Awareness comes from digital threat research, where the authors provide basic guidelines that, if respected and applied, can reduce security risks in the electronic world. These guidelines can help increase awareness of electronic threats and also provide information on how to interact safely in the electronic world. Users who know how to deal with the risks in cyberspace are less afraid of becoming victims of cybercrime. The insights gained in this study are helpful for all cyberspace users and have practical value as they can use for further cybercrime research. This paper explores the theoretical review of the impact of digital threat awareness on performance against cybercrime among police officers in Dubai. A cross-sectional poll was performed with more than 376 police officers in Dubai who were chosen using judgmental sampling. Findings from this review shed some light on the potential of digital threat awareness and its impact on performance against cybercrime among police officers in Dubai.

Keyword: Digital Threat Awareness, Performance Against Cybercrime

Introduction

The population of the United Arab Emirates is increasing rapidly annually. Between 2018 and the beginning of 2021, the population increased from 9.5 million to 9.8 million. Most of the population is tech-savvy millennials; about 70-80% of the population carries smartphones, which puts the state in a position and higher position in the world in terms of development and technological progress. Moreover, this growing trend has prompted the UAE government to take innovative initiatives to effectively manage the ever-increasing population, including using IoT technologies embedded in the 'smart cities in the UAE. It aims to provide its people with the best facilities and to build a country with happy people. The United Nations World Happiness Report 2019 ranks the UAE 21st among other countries worldwide (Khan et al., 2017; Chandra, Sharma, and Liaqat, 2019).

The United Arab Emirates is also among the ten most positive countries globally. It includes two of the most intelligent cities in the world, Abu Dhabi and Dubai. The UAE Vision 2021 emphasizes innovation and the transition towards a knowledge-based economy by tripling research and development by 2021. According to the Global Innovation Index 2018, the UAE ranks 38, but it shows high commitment through its national agenda to become one of the ten most innovative countries by 2021 (Efthymiopoulos, 2016). Nevertheless, wherever technology is found, risks and threats accompany it; as the city undergoes a digital transformation, more significant threats to the country must be identified and mitigated. Furthermore, according to malware reports from Schwab and Poujol, the UAE was one of the top ten countries where 1.9% of users were attacked by malware in the third quarter of 2018. Dark Matter reported that it is a UAE cyber security company, and the country is subject to 5% of global cyber-attacks. Such attacks increased by almost 55% over the past five years. Many such statistics depict the weaknesses in cyber security in the UAE. However, the country is determined to enhance cyber security through collaboration between various key stakeholders - government, national and international industry players, academics, and society. Accordingly, this research aims to understand the importance of these

players and the extent of their contributions to the UAE in building an innovative and secure country (Efthymiopoulos, 2016; Chandra, Sharma, and Liaqat, 2019).

Cyber security awareness combines knowledge and taking the necessary measures to protect organizations' information assets. Moreover, when security personnel is aware of electronic security, they understand electronic threats, the potential impact of a cyberattack on society, and the steps required to mitigate the risks and prevent cybercrime from infiltrating their online workspace (Zwilling et al., 2022). High awareness of digital threats related to information security and cybercrime issues among users at home and in government and educational institutions, especially youth, would reduce the incidence of cybercrime (Sawaneh, 2020). The effectiveness of combating cybercrime among users, especially young people, will be successful if they are familiar with and interested in using the Internet. Thus, factors such as gender, age, knowledge, and skills (experience) may help increase awareness of digital threats among young people (Wood, 2019). According to Bossler and Berenblum (2019), only a few studies were conducted to examine employees' awareness of digital threats, their perception of risks against cybercrime, and the actual level of attention and perception regarding the rise of cybercrime. Most government agencies in the region's countries look at digital security exclusively from one dimension (political, technical, industry-specific) and not a multidimensional perspective (Schneier, 2015).

LITERATURE REVIEW

To continuously improve efficiency, Dubai Police has shifted the identification process from the traditional method to technology (Elnaghi et al., 2019). The Dubai Internet Department focuses on applying new information and communication technologies to conventional or contemporary government practices and identifying opportunities and limitations for publishing with government authority (Alketbi, 2018). Internet governance was presented at the World Summit on collecting information and developing principles, rules, and programs that constitute the evolution of Internet use (Shackelford & Craig, 2014). Moreover, the complexity of implementing the Internet governance system in Dubai includes five dimensions of internet issues: infrastructure, legal, economic, developmental, social, and cultural. Furthermore, many actors play a role in all these dimensions in the private and public sectors and the industry, including civil society activities (Ben Moussa & Benmessaoud, 2020).

However, cybercrime covers any criminal act that deals with computers, networks, and the Internet. Most cybercrimes regularly involve using a specific malware system that controls computer networks in the area (Bossler & Berenblum, 2019). Younies and Al-Tawil (2020) indicated that most of the perpetrators of cybercrime are from outside the UAE and that to reduce cybercrime, we must cooperate with other international agencies worldwide. Most internet users in the UAE were victims of cyber-crimes that targeted citizens' privacy and property; governments also suffer from a reputation problem. It is tough to prove these online crimes; usually, criminals target UAE nationals due to the global economic situation and the high rate of mobile phone use (Younies & Na, 2020).

Early discussions about the effectiveness of cybercrime theory centered on theoretical reflections on the similarities and differences between virtual and natural environments and online and offline behavior patterns (Leukfeldt & Yar, 2016). However, recent academic discussions have been complemented by studies on cybercrime that apply cybercrime theory to various online crimes, thereby assessing its ability to explain apparent patterns in crime and victimization data. While such studies provide important insights into cybercrime theory, These include reliance on a limited sample set, limited sample size, cyberbullying, malware infection (computer-focused crime), identity fraud, and consumer fraud (financial crime). Moreover, stalking and threats in communications (personal offense) enable comparison of crime theory. Electronic is related to applying different types of cybercrime (Obeng-Adjei, 2017). Researchers debate the suitability of cybercrime theory for analyzing and interpreting cybercrime (Younies & Na, 2020). The discussion on the ability of 'traditional' criminology to accommodate cybercrime is resolved by drawing on its well-established theoretical, conceptual, and analytical resources (Leukfeldt & Yar, 2016). In this debate, cybercrime theory is often mobilized to demonstrate that cybercrime can be understood and explained by resorting to resources received from criminology (Obeng-Adjei, 2017). Moreover, a structured theoretical reflection on cybercrime theory's ability to describe cybercrime

patterns, taking into account each of the essential elements of the cybercrime scheme theory of the criminal situation that it tests in terms of its applicability in the online environment (Bossler & Berenblum, 2019).

Awareness comes from digital threat research, where the authors provide basic guidelines that, if respected and applied, can reduce security risks in the electronic world. These guidelines can help increase awareness of electronic threats and are also a source of information on how to interact safely in the electronic world (Alqahtani & Kavakli-Thorne, 2020). Users who are aware of the risks in cyberspace and know how to deal with them are less afraid of becoming victims of cybercrime. The insights gained in this study are helpful for all cyberspace users and have practical value as they can use for further cybercrime research (Leukfeldt & Yar, 2016). Therefore, awareness and fear of digital cybercrime threats are linked to the user's knowledge of the electronic dangers lurking in the electronic world (Choi, Martins, Bernik, 2018).

Humans are usually the first line of defence for securing information assets, no matter how advanced and powerful technological security solutions are. Furthermore, security breaches such as virus infection, identity theft, and hacking are the direct cause of negligence and lack of knowledge and action on the part of users (Younies & Na, 2020). High awareness of digital threats related to information security and cybercrime issues among users at home and in government and educational institutions, especially youth, would reduce the incidence of cybercrime (Sawaneh, 2020). The effectiveness of combating cybercrime among users, especially young people, will be successful if they are familiar with and interested in using the Internet. Thus human factors such as gender, age, knowledge, and skills (experience) may help increase awareness of digital threats among young people (Alqahtani & Kavakli-Thorne, 2020).

RESEARCH METHODOLOGY

Quantitative research generates numerical information or perhaps data interpreted as numbers by which the study seeks to know the problem through numerical evidence. On the other hand, qualitative research produces non-numerical and primarily descriptive data with which the study aims to explain more precisely the cause of this particular phenomenon. Many trials use qualitative and quantitative analysis (Creswell, 2013; Shuttleworth, 2008). Quantitative methods are commonly used for scientific research, starting with establishing a hypothesis to be examined. Mathematical and statistical measures must prove this hypothesis and will be the focus of the entire study. A quantitative research design may be the most effective way to draw conclusions or prove the required null hypothesis (Creswell, 2013; Hair et al., 2014; Bell & Bryman, 2011).

In this study, only a specific target population, the officers who deal with crimes, will be selected. Thus, probability sampling was not possible because not all sectors of society had equal chances of being included in the sample. Judgmental sampling, also called purposive sampling or authoritative sampling, is a non-probability sampling technique in which the sample members are chosen only based on the researcher’s knowledge and judgment. As the researcher’s knowledge is instrumental in creating a sample in this sampling technique, there are chances that the results obtained will be highly accurate with a minimum margin of error. The selection process using judgmental sampling involves the researchers carefully picking and choosing each individual to be a part of the sample. (Sekaran & Bougie, 2016). Unlike probability sampling, there are no rules regarding the sample size for non-probability sampling techniques (except for quota sampling). The sample size depends on the research question(s) and its objectives (Saunders et al., 2009). In addition, investigative research is generally known for its low response rates. (Bhattacherjee, 2012). Typically, a 70% or higher response rate is typical and reasonable (Saunders et al., 2009). Because of these reasons and to reach an acceptable response rate, the survey population is 17,500 officers, and the appropriate sample size based on the Krejcie & Morgan (1970) formula is 376.

Conclusion

This research has analysed and produced a preliminary conceptual model for the characteristics to provide insight into performance against cybercrime literature when digital threat awareness is high. Future academic research may find this conceptual framework interesting. Future studies may examine the link between these components to comprehend them better. Nevertheless, wherever technology is found, risks and threats accompany it; as the city undergoes a digital transformation, more significant threats to the country must be identified and mitigated. Cyber security awareness combines knowledge and taking the necessary measures to protect organizations' information assets. Moreover, when security personnel is aware of electronic security, they understand electronic

threats, the potential impact of a cyberattack on society, and the steps required to mitigate the risks and prevent cybercrime from infiltrating their online workspace (Zwilling et al., 2022). High awareness of digital threats related to information security and cybercrime issues among users at home and in government and educational institutions, especially youth, would reduce the incidence of cybercrime (Sawaneh, 2020).

References

1. Alketbi, A., Nasir, Q., & Talib, M. A. (2018, February). Blockchain for government services—Use cases, security benefits and challenges. In 2018 15th Learning and Technology Conference (L&T) (pp. 112-119). IEEE.
2. Alqahtani, H., & Kavakli-Thorne, M. (2020). Design and evaluation of an augmented reality game for cybersecurity awareness (CybAR). Information, 11(2), 121.
3. Bhattacherjee, A. (2012). Social science research: Principles, methods, and practices. USA.
4. Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. Journal of Crime and Justice, 42(5), 495-499.
5. Bossler, A. M., & Berenblum, T. (2019). Introduction: new directions in cybercrime research. Journal of Crime and Justice, 42(5), 495-499.
6. Bryman, A., & Bell, E. (2011). Reliability and validity in qualitative research. Business Research Methods, 2, 215-243.
7. Chandra, G. R., Sharma, B. K., & Liaqat, I. A. (2019). UAE's strategy towards most cyber resilient nation. International Journal of Innovative Technology and Exploring Engineering (IJITEE), 8(12), 2803-2809.
8. Choi, S., Martins, J. T., & Bernik, I. (2018). Information security: Listening to the perspective of organisational insiders. Journal of information science, 44(6), 752-767.
9. Creswell, J. W. (2013). Steps in conducting a scholarly mixed methods study.
10. Efthymiopoulos, M. P. (2016). Cyber-security in smart cities: the case of Dubai. Journal of Innovation and Entrepreneurship, 5, 1-16.
11. Elnaghi, M., Alshawi, S. N., Kamal, M. M., Weerakkody, V., & Irani, Z. (2019). Exploring the role of a government authority in managing transformation in service re-engineering–Experiences from Dubai police. Government Information Quarterly, 36(2), 196-207.
12. Hair Jr, J. F., Sarstedt, M., Hopkins, L., & Kuppelwieser, V. G. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. European business review, 26(2), 106-121.
13. Krejcie, R. V., & Morgan, D. W. (1970). Determining sample size for research activities. Educational and psychological measurement, 30(3), 607-610.
14. Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263-280.
15. Moussa, M. B., Benmessaoud, S., & Douai, A. (2020). Internet memes as "tactical" social action: A multimodal critical discourse analysis approach. International Journal of Communication, 14, 21.
16. Obeng-Adjei, A. (2017). Analysis of Cybercrime Activity: Perceptions from a South African Financial Bank (Doctoral dissertation, University of the Witwatersrand, Faculty of Commerce, Law and Management, School of Economic and Business Sciences).
17. Saunders, M., Lewis, P., & Thornhill, A. (2009). Research methods for business students. Pearson education.
18. Sawaneh, I. A. (2020). Cybercrimes: Threats, challenges, awareness, and solutions in Sierra Leone. Asian J. Interdicip. Res, 185(195), 185.
19. Schneier, B. (2015). Secrets and lies: digital security in a networked world. John Wiley & Sons.
20. Schwab, W., & Poujol, M. (2018). The state of industrial cybersecurity 2018. Trend Study Kaspersky Reports, 33.
21. Sekaran, U., & Bougie, R. (2016). Research methods for business: A skill building approach. john wiley & sons.

22. Shackelford, S. J., & Craig, A. N. (2014). Beyond the new digital divide: Analyzing the evolving role of national governments in internet governance and enhancing cybersecurity. Stan. J. Int'l L., 50, 119.
23. Shuttleworth, W. J. (2008). Evapotranspiration measurement methods. Southwest Hydrology, 7(1), 22-23.
24. Wood, A. J., Graham, M., Lehdonvirta, V., & Hjorth, I. (2019). Good gig, bad gig: autonomy and algorithmic control in the global gig economy. Work, employment and society, 33(1), 56-75.
25. Younies, H., & Al-Tawil, T. N. E. (2020). Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE). Journal of Financial Crime, 27(4), 1089-1105.
26. Younies, H., & Na, T. (2020). Hospitality workers' reward and recognition. International Journal of Law and Management, 63(2), 157-171.
27. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2022). Cyber security awareness, knowledge and behavior: A comparative study. Journal of Computer Information Systems, 62(1), 82-97.