DS Journal of Cyber Security
Volume 2 Issue 2, 1-8, Apr - Jun 2024
ISSN: 2584-0665/ https://doi.org/10.59232/CYS-V2I2P101

Original Article

The Impact of Employees Social Media Use on Corporate Cyber Security Posture

Frankline Makokha

School of Computing and Informatics, University of Nairobi, Nairobi, Kenya.

goldmedalist321@gmail.com

Received: 05 April 2024; Revised: 07 May 2024; Accepted: 29 May 2024; Published: 13 June 2024;

Abstract - This paper sought to establish the impact of employee's social media use on the corporate cyber security posture. The behavioural metrics used in the study include the impact of accessing private social media accounts using the same computing tool used for work-related duties, the linkage of personal accounts hacking to consequent successful work systems hacking, the connection of personal devices to corporate systems and the impact of corporate-sponsored training on cyber security posture. The adopted research design involved collection of primary data via a set of questions requirement a yes or no response. The paper used a cross-sectional study as the study design, with a questionnaire as the research method and online administration of the questionnaire as the research technique. The study sample was computed using the Yamane formula, which gave a sample size of 400 participants, from which the response rate to the questionnaires was 62%. An analysis of the responses showed that there is a high correlation between accessing private social media accounts while working using the same computing device with increased chances of corporate cyber attacks. There is also a statistical linkage between an employee's private email account having been hacked or impersonated, as well as connecting private computing devices to the company's systems (internet, printers) to execute either official duties or private. Those who reported having been facilitated with cyber security training reported lower cyber attacks on their corporate systems than those who reported having been facilitated with cyber security training by the companies they work for. It is therefore advised that companies deter employees from accessing private social media accounts and executing official duties using the same computing devices, private devices are not connected to corporate systems, and basic cyber security training is facilitated to all employees.

Keywords - Cyber security, Cyber security posture, CIA, Yamane formula, Social media.

1. Introduction

Cyber Security, defined as the collection of tools, policies, and practices aimed at protecting information as contained in computing nodes and transit between the computing nodes [1], has become a fundamental determinant for the success of any organisation [2]. Cyber security aims to achieve three key objectives of information and information assets, namely, Confidentiality, Integrity and Availability (CIA) [3], which have to be pursued within the constraints of Functionality, Security and Usability (FSU) of the system to be protected [4].

Cyber security posture is how effective the mitigations put in place to harden computing systems are in their ability to deter, detect, respond and recover from a Cyber incident [5] is used to gauge organisations' maturity on the Cyber front. Organisations, therefore, use various ethical hacking techniques, which, in order of complexity, range from security audits, vulnerability assessments, penetration testing, red teaming and bug bounty hunting [6] to enhance their corporate security posture.

Despite the existence of measures to enhance Cyber security, cases of Cyber-attacks have been on an upward trajectory [7]. Studies show that the success of an attack is majorly due to vulnerabilities on the victim's end, like human error, inherent weakness in systems, and insufficient security controls, than is the knowledge and skills of the attacker [8].

The main thematic attack drivers are categorised as intent to attack, human error and inherent system vulnerabilities [8]. Empirical studies show that despite an organisation having a high number of knowledgeable, skilled and cyber security-conscious professionals in their workforce, the presence of any member in the workforce with inherently limited knowledge of cyber security presents a conspicuous cyber-attack vector [9].

A systematic literature review undertaken to ascertain key human factors in cyber security enhancement efforts revealed two key human factors, namely, risk perception and awareness. Risk perception is considered an instinctive and scientific reaction to a cyber threat, while awareness is the possession of general knowledge of cyber security [10].

An exploratory analysis of human factors in electronic health records Cyber security breach [11] showed that 73% of the data breaches occurred due to unintentional human errors. The unintentional human errors can be occasioned by various facets of human activities, ranging from social media use, disposal of paper documents containing sensitive information, use of passwords linked to personally identifying information like date of birth, and through social engineering.

As to why employees would access social media while working at the same time, this study is guided by the Self-Determination Theory (SDT), which postulates that social contexts and individual basic needs work in harmony, leading to the satisfaction of three human psychological needs, namely, autonomy, competence and relatedness [12].

Based on the Self-Determination Theory (SDT), employees will always, therefore, seek to satisfy the three psychological needs as they go about their official duties, hence the high possibility of accessing social media and working concurrently. A study on the impact of social media use, but for work purposes, using the Self-Determination Theory (SDT) showed that it increases need satisfaction and intrinsic work motivation, but excessive use could have the opposite effect [13].

This paper sought to explore the correlation between social media use and cases of cyber security incidents on social media users and the firms they work for. Further, the paper also seeks to establish, if any, a statistical linkage between the connection of personal computing devices to corporate systems and increased incidences of successful cyber attacks. This study, therefore, aimed to answer two main questions, namely, can the use of the same computing device to perform official duties and access private social media platforms increase the chances of a successful cyber attack on corporate systems?.

Moreover, can connecting personal computing devices to corporate systems increase the chances of successful cyber attacks?. The type of statistical analysis method used was descriptive statistical analysis, where collected data was simplified in a table, and each number of responses per question was converted to a percentage of the total sample for easier visualization of linkage to a successful cyber attack. The specific method of statistical analysis used was hypothesis testing. The paper advances the hypothesis, H1, that the use of the same devices on private social media platforms and for official duties by employees and the connection of personal computing devices to corporate systems compromises the security posture of an organisation.

2. Related Works

A doctoral thesis on cyber security challenges in social media, aimed at establishing whether social media platforms put users at more privacy and security risks, showed that 99% of the respondents had faced a privacy issue or concern on social media, while 80 % reported having been stalked online [14].

The approach in the doctoral thesis was focused on establishing whether the social media users used their real names,40% reported using real names; how often they used social media, with 55 % reporting daily usage; third-party access to personal data authorisation, where 85 % reported having granted access; real personal information shared on the platforms, with 92 % reporting having used real picture and birthdays; and whether they read the privacy information on the social media platforms 75 % stating they have never read the privacy guidance on the social media platforms. Whereas the questions asked provided a dimension for studying the impact of social media use on cyber security, the study did not collect data on whether cyber incidences materialised due to the data on the collected dimensions, nor did it draw any correlation or causation between the collected data and Cyber security incidences.

A study on misinformation about technological topics via social media shows that at least 7% of information on social media about a certain technology is not correct [15]. From the study, the misinformation on social media ranged from security and privacy threats against other social media platforms, as well as technological solutions in use. The study developed a framework based on classifiers, from which 3% of posts on Instagram,18 % of posts on Facebook, 4% of posts on Reddit, and 3%of posts on Twitter were found to be misinformation.

The study also found about 9% of all obfuscated URLs and about 22% of tweets about phishing websites to be misinformation. Whereas the study identified this misinformation on various social media platforms, it did not establish if the misinformation resulted in cyber security incidences or security attack attempts.

In a survey carried out about the opinion of users on the possibility of social networking sites linking them to malicious sites, about 41 % of the respondents said they do not know or are not sure about their opinion on social sites linking them to malicious sites. In comparison, about 19 % said they are not concerned, with 23% saying they are very much concerned [16].

From the figures, more than half of the users are not very concerned about the social networking sites linking them to malicious sites. They would, therefore, be less cautious with links and clicking on prompts presented to them on social media sites. The sites could be used to harvest information which can be used to launch cyber attacks. The study, falls short in linking this attitude to actual cyber attacks or cyber attack attempts.

In an assessment of cybersecurity awareness among students [17], only 4.2 (%) of the respondents reported being aware of the cybersecurity issues encountered through social networking. This is a point of concern to organisations, noting that they offer apprenticeships, internships and attachment to students. The student's online activities can compromise cyber security measures rolled out by organisations if a huge number of them are not equipped with cyber security knowledge.

The study, however, has no statistical correlation between the lack of awareness among students and Cyber security attempts or attacks at the organisations that have offered the students apprentices, internships or attachments. Whereas social networking sites are used for bringing people together with a view of people getting to know each other, a paper on predicting individuals' vulnerability to social engineering in social networks [18] showed that in the study, only 48% of the participants stated that they knew less than 10% of their Facebook network at a personal level.

The revelation in the study [18] presents a prime social engineering attack vector, which can be exploited to spy or collect information through phishing. The revelation, though disturbing, did not link the lack of knowledge of social media friends at the personal level, to cyber security incidences to themselves or the organisation they work for. A study to look into the potential for information security risk posed by the disclosure of organizational information by employees on Facebook showed that 45% of the respondents discussed work with colleagues. In comparison, 18% of the participants used Facebook to perform job tasks [19]. The study [19] falls short by not linking the usage of Facebook for work activities with cyber security incidences in the companies the employees work. Whereas a study to establish attitudes, behaviours and unintended consequences of Facebook users and their related online privacy [20], found 91% of the respondents to be aware of the Facebook privacy issues and were also likely to restrict their profile. Despite this knowledge, however, only 61 % of those with security knowledge actually changed the default security settings. The study [20] does not draw a causation or correlation relationship between the lack of changing default settings with cyber crime incidences. This paper, therefore, sought to address the gulf that exists in the highlighted studies by drawing a statistical linkage between social media use and cases of Cyber security at their places of work.

3. Materials and Methods

The study universe in this paper were persons in formal employment in Kenya who use computers in their day-to-day work. This selection was premised on the fact that these are people who are likely to juggle between social media and work at the same time, using the same computers. An economic survey of Kenya for the year 2023 shows that approximately three (3) million Kenyans are in formal employment [21]. This figure was, therefore, used in the computation of the sample size used in this study. Sample size can be computed using either census, in the case of small populations, using sample sizes used in past similar studies, or by use of published tables, and finally by use of formulas advanced for calculating sample sizes [22]. With the study universe of more than three (3) million not explicitly covered by the published tables, and not possible for a census, and the gaps in the cited similar studies, this paper adopted the formula approach. The formula approach uses either the desired level of precision, or the degree of variability, and the confidence level in sample size computation [22]. This study had only two parameters prior to the study, namely, desired precision and confidence interval, premised on the most commonly used values of confidence level of 95% and precision level of 0.05. From the parameters at hand, this study used the Yamane formula of sample size computation [23], namely,

$$n = \frac{N}{1+N(e)^2}$$

Where n = Sample Size; N = Universe of Study; e = Level of Precision. The formula yields a sample size of 400 participants.

In view of the number of participants, data collection was done via an online questionnaire, where a link was sent via email. The platform used in questionnaire development was Survey Planet due to its simplicity in usage, free access, and configurable to allow strictly one response from each device. The selection of the study population was done through snowballing, where persons acquainted with and in the network of the authors are selected and who then, in turn, identify other people in their network to participate in the study. To increase the response rate, the questions consisted of a set of ten (10) multiple-choice questions, as detailed in Appendix 1. The questions centred around the number of hours spent on computers for work, the use of the same computer for both personal social media and work-related tasks, whether their personal accounts and work systems have ever been hacked, authentication of those requesting information via social media, and use of the real name on social media. The study design utilized in this paper was a cross-sectional study, on the strength that cross-sectional studies are useful in obtaining an overall picture as it stands at the time of the study [24]. The results were analyzed using a table that showed the number of respondents who responded with a ”YES” to a certain question. From the responses,

questions linked to one another were further analyzed to identify those who responded with a ”YES” and had a ”YES” in a consequent question.

4. Results and Discussion

A total of two hundred fifty-two (252) responses were received from the four hundred target respondents, indicating a sixty-two 62% response rate. In an article on Response Rates and Responsiveness for Surveys, Standards, and the Journal [25], response rates of 60% for most research should be the goal of researchers. This percentage has been corroborated in an article titled Instruments for obtaining student feedback: a review of the literature [26]. From the responses received, the notable findings are that 77% of the respondents stated that they concurrently work and access private social media accounts using the same working device,67% change the default security settings on the social media platforms, 70% perform background checks on new social media contacts before connections, 63% connect private devices to corporate networks, while 72% of the respondents ‘place of work has ever been hacked.

Detailed results are contained in the appendix section. Further analysis reveals that from the 77% of the respondents who reported working and accessing private social media accounts using the same working tool, 80% of them reported their corporate systems having been hacked. There is also a correlation between the respondents who connect their private computing devices to corporate networks and systems, at 63% and those whose corporate networks and systems have ever been hacked, at 72%, of the respondents. Of the 19% of the respondents who reported having suffered from personal emails and impersonation attacks, 89% of them reported their corporate systems having been hacked. This shows a linkage between successful personal account hacks and successful corporate systems hacking. Among the 62% of the respondents who reported connecting their private computing devices on their company’s systems (internet, printers) to execute either official or private duties 62% of them reported their corporate systems having been hacked. This is another correlation statistic. With regards to company-facilitated cyber security training, it was observed that from the 56% of the respondents who stated they had not been facilitated by company-sponsored cyber security training, 71% of them reported their company systems having been hacked. This could be attributed to a lack of basic cyber security knowledge among the employees of companies that have been hacked.

5. Conclusion

Based on the responses from the respondents, it is observed that there is a strong correlation between accessing private social media accounts and using the same terminal device for executing official duties by employees and successful cyber attacks on corporate systems and networks. The same is true with connecting private computing devices on the company’s systems (internet, printers) to execute either official or private duties. It is also evident that facilitating employees with basic cyber security training reduces the chances of successful cyber attacks on corporate systems and networks. Noting the usefulness of social media in so far as an employee needs satisfaction and intrinsic work motivation is concerned, its use concurrently and during work breaks should not be completely banned. However, moderating measures can be put in place from a corporate cyber security posture perspective. From the findings, it is recommended, therefore, that corporates deter employees from accessing private social media accounts and executing official duties using the same computing devices, private devices are not connected to corporate systems, and basic cyber security training is facilitated to all employees.

Data Availability

The raw data collected from the study questionnaire is available on request from the Author.

Authors’ Contributions

The sole author contributed to all tasks associated with paper development.

References

[1] ITU, Recommendation X.1205: Overview of Cybersecurity, ITU Standard, 2008. [Online]. Available: https://www.itu.int/rec/t-rec-x.1205-200804-i

[2] Ajitabh Ambastha et al., "Implication of Cyber Security in a Digital Economy: Learning from Corporate Sector with Special Reference to BFSI," *Artificial Intelligence for Sustainable Finance and Sustainable Technology*, pp. 543-552, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Sagar Ajay Rahalkar, *Certified Ethical Hacker (CEH) Foundation Guide*, New York City: Apress, pp. 85-87, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[4] N.A. Khan, A. Saeed, and M. Yousuf, *CEH v10: EC-Council Certified Ethical Hacker Complete Training Guide with Practice Questions & Labs: Exam: 312-50*, England: IP Specialist LTD., pp. 46-48, 2018. [Publisher Link]

[5] Australian Signals Directorate, "The Commonwealth Cyber Security Posture in 2022," *Australian Government,* Technical Report, 2022. [Publisher Link]

[6] K. Graves, *CEH: Certified Ethical Hacker Study Guide*, Indianapolis, Indiana, Wiley Publishing, Inc, pp. 344-350, 2010. [Google Scholar]

[7] Intel Security, Mcafee Labs Threats report, 2015. [Online]. Available: https://scadahacker.com/library/Documents/Threat_Intelligence/McAfee%20-%20Threat%20Report%202015-2Q.pdf

[8] Andreea Bendovschi, "Cyber-Attacks – Trends, Patterns and Security Counter-Measures," *Procedia Economics and Finance*, vol. 28, pp. 24–31, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[9] Uchenna Daniel Ani, Hongmei He, and Ashutosh Tiwari, "Human Factor Security: Evaluating the Cybersecurity Capacity of the Industrial Workforce," *Journal of Systems and Information Technology*, vol. 21, no. 12, pp. 2-35, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[10] Ahmed Alghamdi, "A Systematic Review on Human Factors in Cybersecurity," *JIJCSNS International Journal of Computer Science and Network Security*, vol. 22, no. 10, pp. 282-290, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[11] Liu Hua Yeo, and James Banfield, "Human Factors in Electronic Health Records Cybersecurity Breach: An Exploratory Analysis," *Perspect Health Information Management*, vol. 19, no. 3, 2022. [Google Scholar] [Publisher Link]

[12] Edward L. Deci, and Richard M. Ryan, *Intrinsic Motivation and Self-Determination in Human Behavior,* New York: Springer Nature, 1985. [CrossRef] [Google Scholar] [Publisher Link]

[13] Mehmet Akif Demircioglu, and Chung-An Chen, "Public Employees' Use of Social Media: Its Impact on Need Satisfaction and Intrinsic Work Motivation," *Government Information Quarterly*, vol. 36, no. 1, pp. 51-60, 1998. [CrossRef] [Google Scholar] [Publisher Link]

[14] Erdal Ozkaya, "*Cybersecurity Challenges in Social Media*," PhD Thesis, Charles Sturt University, Australia, Australia, 2018. [Google Scholar] [Publisher Link]

[15] Mohit Singhal et al., "Cybersecurity Misinformation Detection on Social Media: Case Studies on Phishing Reports and Zoom's Threat," *Proceedings of the Seventeenth International AAAI Conference on Web and Social Media*, vol. 17, no. 1, pp. 796-807, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Thilagaraj Ramasubbu, and Deepak Raj Rao G., "Vulnerabilities of Social Networking Sites- An Open Attack Vector for Cybercriminals," *Journal of Network and Information Security*, vol. 6, no. 1, pp. 12-17, 2018. [Google Scholar] [Publisher Link]

[17] Talal Alharbi, and Asifa Tassaddiq, "Assessment of Cybersecurity Awareness among Students of Majmaah University," *Big Data Cognitive Computing*, vol. 5, no. 2, pp. 1-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Samar Muslah Albladi, and George R.S. Weir, "Predicting Individuals' Vulnerability to Social Engineering in Social Networks," *Cybersecurity*, vol. 3, pp. 1-19, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Nurul Nuha, and Abdul Molok, "Disclosure of Organizational Information by Employees on Facebook: Looking at the Potential for Information Security Risks," *22nd Australasian Conference on Information Systems*, vol. 78, pp. 1-11, 2011. [Google Scholar] [Publisher Link]

[20] Bernhard Debatin et al., "Facebook and Online Privacy: Attitudes, Behaviors, and Unintended Consequences," *Journal of Computer-Mediated Communication*, vol. 15, no. 1, pp. 83-108, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[21] KNBS, "*2023 Economic Survey*," Kenya National Bureau of Statistics, Nairobi, Technical Report, pp. 1-510, 2023. [Publisher Link]

[22] Glenn D. Israel, "*Determining Sample Size,*" Florida Cooperative Extension Services, Institue of Food and Agricultural Sciences, University of Florida, Gainesville, Fact Sheet POED-6, 1992. [Google Scholar] [Publisher Link]

[23] Taro Yamane, *Statistics: An Introductory Analysis*, 2nd ed., New York: Harper and Row, 1967. [Google Scholar]

[24] Ranjith Kumar, *Research Methodology: A Step by Step Guide for Beginners*, 4th ed., London: Sage, pp. 104-127, 2011. [Google Scholar] [Publisher Link]

[25] Jack E. Fincham, "Response Rates and Responsiveness for Surveys, Standards, and the Journal," *American Journal of Pharmaceutical Education*, vol. 72, no. 2, pp. 1- 4, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[26] John T.E. Richardson, "Instruments for Obtaining Student Feedback: A Review of the Literature," *Assessment and Evaluation in Higher Education*, vol. 30, no. 4, pp. 387-415, 2010. [CrossRef] [Google Scholar] [Publisher Link]

Appendix

Study questionnaire

Please Tick (√) as Appropriate			
No.	Question	YES	NO
1	Do you work and access your private social media accounts at the same time using the same computing device?		
2	Do you execute part of your official duties on official company social media accounts?		
3	Do you use your real names and other real identity (email, place of work, place of school, place of origin and relatives etc) on your social media accounts?		
4	Do you always change the default security settings of your social media accounts?		
5	Do you perform authentication checks before connecting or communicating with new social media contacts?		
6	Have you ever suffered from an online or email impersonation attack?		
7	Has your private social media account ever been hacked?		
8	Do you sometimes connect your private computing devices to your company's systems (internet, printers) to execute official or private duties?		
9	Has your company's systems (Email, software, applications, network, etc)ever been hacked?		
10	Has your company ever facilitated you to attend a Cyber Security training?		

Summary results from the responses

Please Tick (√) as Appropriate			
No.	Question	YES	NO
1	Do you work and access your private social media accounts at the same time using the same computing device?	32	10
2	Do you execute part of your official duties on official company social media accounts?	10	32
3	Do you use your real name and another real identity (email, place of work, place of school, place of origin, relatives, etc) on your social media accounts?	23	19

4	Do you always change the default security settings of your social media accounts?	28	14
5	Do you perform authentication checks before connecting or communicating with new social media contacts?	29	13
6	Have you ever suffered from an online or email impersonation attack?	8	34
7	Has your private social media account ever been hacked?	5	37
8	Do you sometimes connect your private computing devices to your company's systems (internet, printers) to execute official or private duties?	27	15
9	Has your company's systems (Email, software, applications, network, etc) ever been hacked?	30	12
10	Has your company ever facilitated you to attend a Cyber Security training?	18	24