Assessment of the Effectiveness of Non-Technical Approach to Cyber Security Management for NLIMS System in the Ministry of Lands and Physical Planning, in Kenya

***Gabriel Chebbe*[1]*, Lawrence Mwenda Muriira[1], *Edwin Mkhganga*[1], *Robert Mutua Murungi*[1], *Patricia Kavuli Ndambuki*[1]**

[1]*Kenya Methodist University P.O. Box 627 – 60200, Meru, Kenya*
** Correspondence email: thgabu@gmail.com*

Abstract

The study determined whether NLIMS has adequately addressed the social aspect of their information security system. The study was conducted at Ministry of Land and Physical Planning Headquarters in Nairobi. The study adopted descriptive research design, and utilized stratified sampling technique to select respondents. Close-ended questionnaires were used to collect quantitative on social engineering cyber threats. Results indicated that 70% of staff using NLIMS system lack knowledge about social engineering attacks, their conduct, weaknesses, and the skills necessary to prevent or stop cyber threats. The findings further indicated that the 70% of Ministry of Lands' staff use insecure methods to dispose waste that may contain information that could be used to launch an attack. This lack of attention to secure waste disposal puts NLIMS at risk of accessing sensitive information through dumb star diving. Unauthorized personnel can easily access information on staff computers or working desks through shoulder surfing. Workstation privacy is compromised by workstation resource sharing policies, allowing malicious staff to exploit them. Over 60% of staff lack proper social engineering awareness. Further, lower rank staff accesses information they are not authorized to access through the workstation resource sharing policy. The non-technical aspect of information security at KMLPP towards NLIMS has weaknesses, impairing the overall effectiveness of the security. This study establishes, as a key take away, that despite global awareness, less attention is given to the social aspect of cyber security despite being labelled the major weakness in any information security system. The study concludes that holistic approach, technical and non-technical aspects in KMLPP's use of secure waste disposal methods, such as shredding and burning, is essential for effective management of non-technical vulnerabilities. This study recommends that KMLPP on NLIMS should pay more attention to workstation privacy, secure waste disposal and educating staff on cyber security awareness.

Keywords: *Complexity theory, NLIMS, socio-technical, socio-technical cybernetic enterprise model, Cyber Security Management, Ministry of Lands and Physical Planning*

IJPP 12(3); 15-30

1.0. Introduction

System digitization which was initiated in 2019/2020 financial year in Kenya's Ministry of Lands and Physical Planning has remained a key priority (National Land Information Management System [NLIMS], 2023). This study posits that the nature and framework of the new NLIMS used in the Ministry of Lands and Physical Planning is not accurately known (NLIMS, 2023). As such, the intended purpose of NLIMS including to enhancing security of land records, improving accessibility, cutting down land transaction costs, enhancing transparency, and promoting paperless transactions has not been fully realized (NLIMS, 2023).

Considering the advanced nature of cyber threat, information security in of key importance in any Information Communication Technology, ICT based system, especially one that handles bulk information transactions nationwide (NLIMS, 2023). A system is as secure as its last security patch; therefore, to improve cyber security nations have embraced global collaboration in information sharing pertaining security threats. It is apparent that the developers of the NLIMS have had security in mind, but its ability to match global standards and to leverage current technology is wanting. The most valuable resource that the NLIMS handle is the information of land transactions in form of land record. The security of this information is affected by the application security, network security, end- users and operation security among other factors.

Within an information security framework there are two issues that are a subject of concern in designing deterrence approaches and analyzing failures, which include the technical part, which deals with hardware; and the software infrastructure and the non-technical or sociotechnical part. Salim and Stuart (2014) observes that;

> *"Existing cyber security approaches mostly focus on technical aspects, with goal of creating a secure fence around technology assets of an organization. This limits systemic thinking for three main reasons: First, it does not view cyber security holistically at an organizational level, which includes people and processes. Second, focus on security technology reinforces the perception that it is solely an Information Technology department problem. Third, within the context of the cyber ecosystem, focusing only on a technical solution ignores interactions with other systems/sub-systems operating beyond an organizational boundary"* (Salim & Stuart, 2014).

Cyber security is a comprehensive property of an information system and not merely one of its components (Yunos, Ab, & Ahmad, 2016; Savage & Schneide, 2010). This paper extends the Salim and Stuart's concerns on the role of people in the security of the information system. The study therefore focuses on the non-technical aspect of the NLIMS.

The primary weakness of information security system has been established to be the social factor (Gandhi , Devishree , & Sathish , 2013). Many organizations have fortified the technical aspect of their information security system, but have paid little attention to the social aspect of the system. According to Kioskli and Polemi (2020), information leak or data breach can easily happen through the social aspect of the information system. NLIMS hosts critical confidential national land information in Kenya. Therefore, all aspects of this information system software needs to be secured. This study intends to establish whether due diligence has been observed in keeping NLIMS secure.

"The study found that KMLPP's use of secure waste disposal is inconsistent among staff and unauthorized personnel can easily access information on staff computers ."

Objectives

i. To evaluate work station privacy among employees linked to NLIMS system
ii. To assess office garbage disposal techniques used in work stations and offices linked to NLIMS system
iii. Appraise the awareness of social engineering by staff linked to NLIMS

The complexity theory by Mason (2022) posits that in every behavior of complex systems, there is an underlying order to which cannot be properly exemplified by the mere analysis of all its constituting components. A complex system is a system whose parts and their interaction collectively embody a unique behavior. This theory exemplifies the information system under study, as well as its security.

Most cyber security management approaches are based on a reductionist ideology (Tajfel et al., 1979). Under the lens of reductionist, cyber security is approached from specific point solution where attacks on known vulnerability can be anticipated (Gandhi, 2014). In the modern cyber system, there are sub-systems such as human behavior and socio –cyber system to mention but a few that a reductionist approach is limited to. Holism theory proposes a holistic approach to cyber security is analogous to the immunity of biological being in which there is robust, adaptive and constantly learning of the ever-dynamic behavior of threats such as mutation of a pathogen (Gandhi, 2014). With that in mind non- technical vulnerabilities which are human based and influence cannot be effectively managed the same way as technical vulnerabilities.

The socio-technical system method considers a system's community, person component, hardware, and software components while designing it for a specific use (What Are Socio-Technical Systems, 2023b). Thus, a combination of people and technology is involved systems security management (Geeks for Geeks, 2022). Social Technical Systems (STS) offers a chance to identify moral lapses and hazards in the systems'

social components. It is made up of numerous parts; namely, people, hardware, software, data, and laws and regulations, which constitute its five essential components (Geeks for Geeks, 2022).

2.0. Materials and methods

The study was carried out in the Ministry of Land and Physical Planning headquarters in Nairobi (KMLPP). The study adopted a descriptive research design that focused on quantifiable qualitative data (Kothari, 2004).

Study Population and Sample Selection Procedures (sampling techniques)

Magigi proposes a Slovin's formula by Taro Yamane (1967) (Jeffry and Joyce, 2012) for calculation of sample size (Stephan, Wakuru, & Boniphace, 2015). There were 53 employees who are linked directly and indirectly to NLIMS, thus,

$$n \approx \frac{N}{(1+N(\varepsilon)2)}$$

Where;

n = Sample size (Staff linked to the NLIMS to be interviewed)

N = Population (Total number of staff linked to the NLIMS) =53

e = Level of precision (5 – 10%)

Our N is 53 individuals; therefore, based on the above formula the sample frame n is 40 respondents

Quota sampling technique was further used to isolate the key population. Singh and Masuku (2014) recommends this method if the research has preset determinant that the key population must meet (Singh & Masuku, 2014). The determining key factor in this study is that the staff working in the ministry of land and physical planning must have access to the NLIMS system via workstation.

Data Collection Techniques and tools

Data was collected through administration of close ended questionnaires. Close ended questions were used to capture respondent's opinion or perspectives, and attitude toward social engineering cyber threat from predefined options.

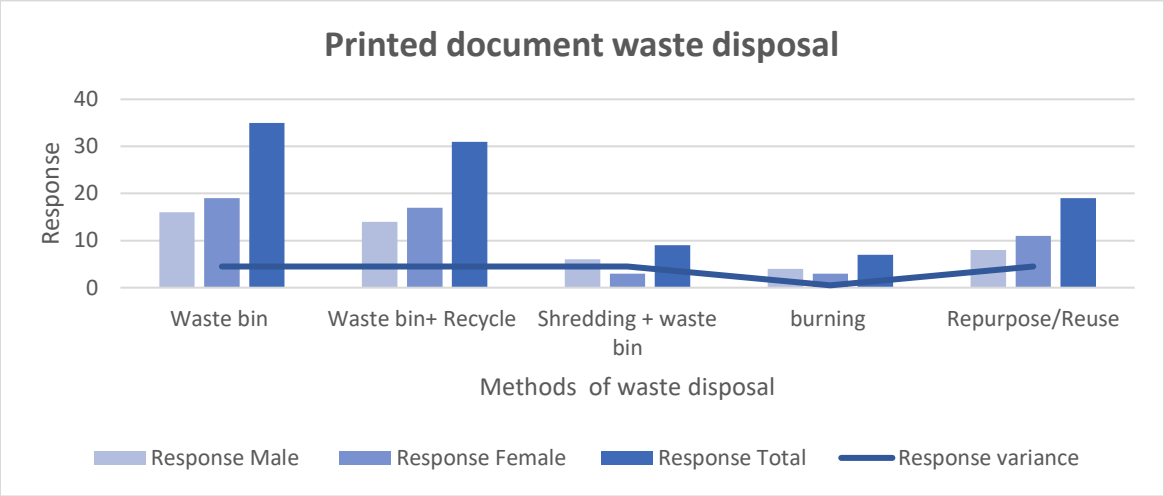
3.0. Results and Discussion

Access Control (test factors: waste disposal, should surfing) Printed document Waste Disposal (Sample size = 40)

Access to information pertains avenues that allow unauthorized individual to get access to highly restricted information or data. For the case of NLIMS, avenues include waste disposal, and surfing. Figure 1, 2 and 3 show how different waste disposal approach are insecure and which methods are predominantly used.

Figure 1

Printed document waste disposal



Results in Figure 1 indicate that waste bin disposal at 77.5% and waste bin + recycle at 87.5% are the two desirable methods that the staff linked to NLIMS prefer to use to dispose printed paper waste. This high percentage indicate that majority of waste printed paper can be accessed by the public as waste. These two methods do not safeguard NLIMS system against dumb star diving- an avenue for cybercriminal to access data that be instrumental in launching attacks against NLIMS. Only 15 % prefer shredding paper waste before waste disposal, while 10% prefer burning which is the 100% effective way of disposing printed paper waste that may contain usable data to the cyber criminals

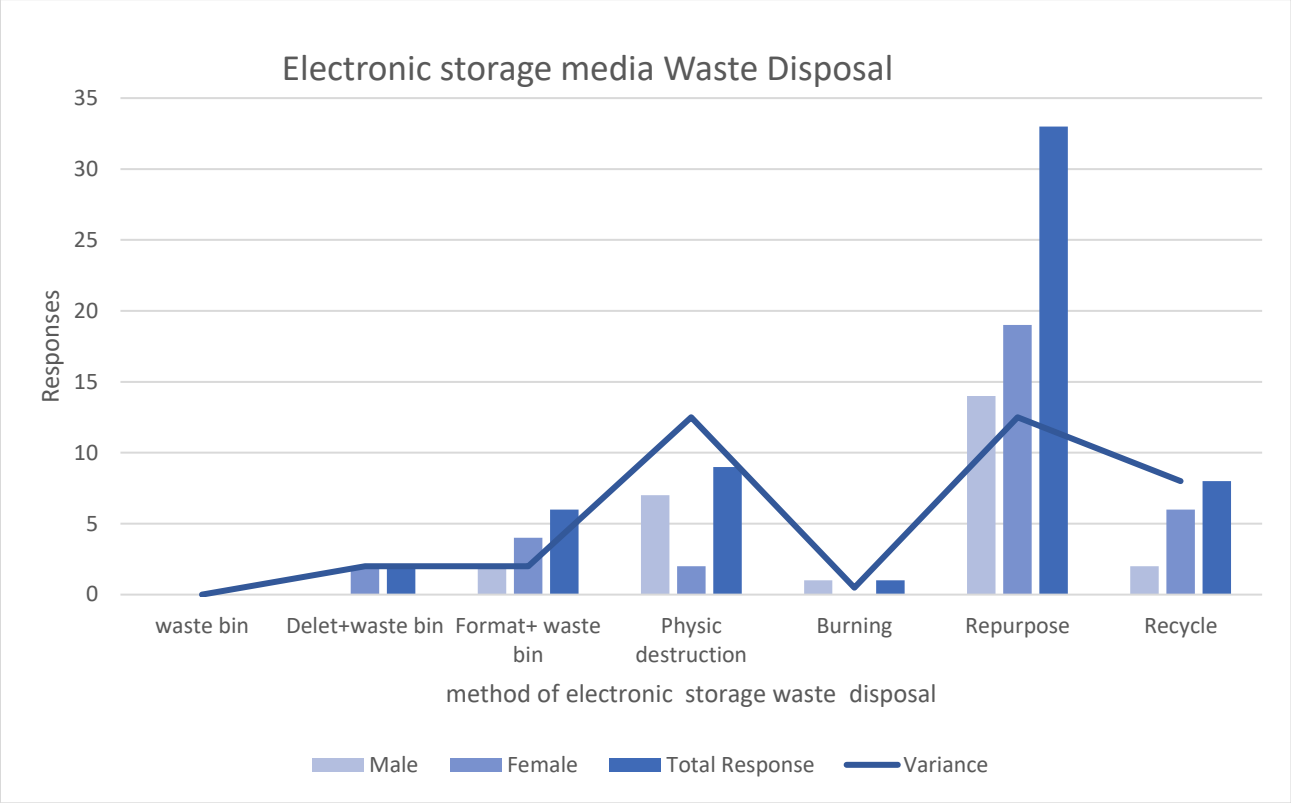
Shredding before disposal makes it hard to reconstruct information from printed paper waste. In aggregate, 25 % (burning 10% and shredding 5%) constitute effective methods of proper secure printed paper waste disposal against, 75% unsecured methods. Finally, the need to securely dispose waste is apparent for male staff more than it is for female staff where male staff prefer shredding at 67%, and female at 33%; while57% of male staff prefer burning to 42 % female staff

Storage media waste disposal

Storage media consist of hard drives, thumb drives and optical disks. When this media develops minor fault, they are bound to be disposed. Figure 2 and 3 shows disposal approaches at NLIMS.

Figure 2

Electronic storage waste disposal



Majority of the staff, 82.5% prefer to repurpose digital storage device such USB thumb drive and external storage such as memory card and hard drive. This means that once a staff takes home a storage devise such a thumb drive without securely erasing it there is a risk that unauthorized individuals can access data storage. Studies indicate that the risk of data breach electronic storage media is higher than that in printed papers because data in the storage device consist of complete actionable information and may be in larger quantity and variety compared to that on one-page printed document (GLOBAL, 2023). It has also been established that personal use of the storage device also ensures more unauthorized people can easily access the content of storage device with ease or even make a copy of the entire storage device (GLOBAL, 2023). Other publications have proposed that secure disposal of such devices as burning at 2.5% and recycling at 5%, constituting only 7.5% (GLOBAL, 2023). This means staff linked to NLIMS chose the least secure option to dispose storage devices that may contain secure information. Female staff are more inclined to repurpose at 47.5% than male counterpart at 35%.

Figure 3

Optical storage waste disposal

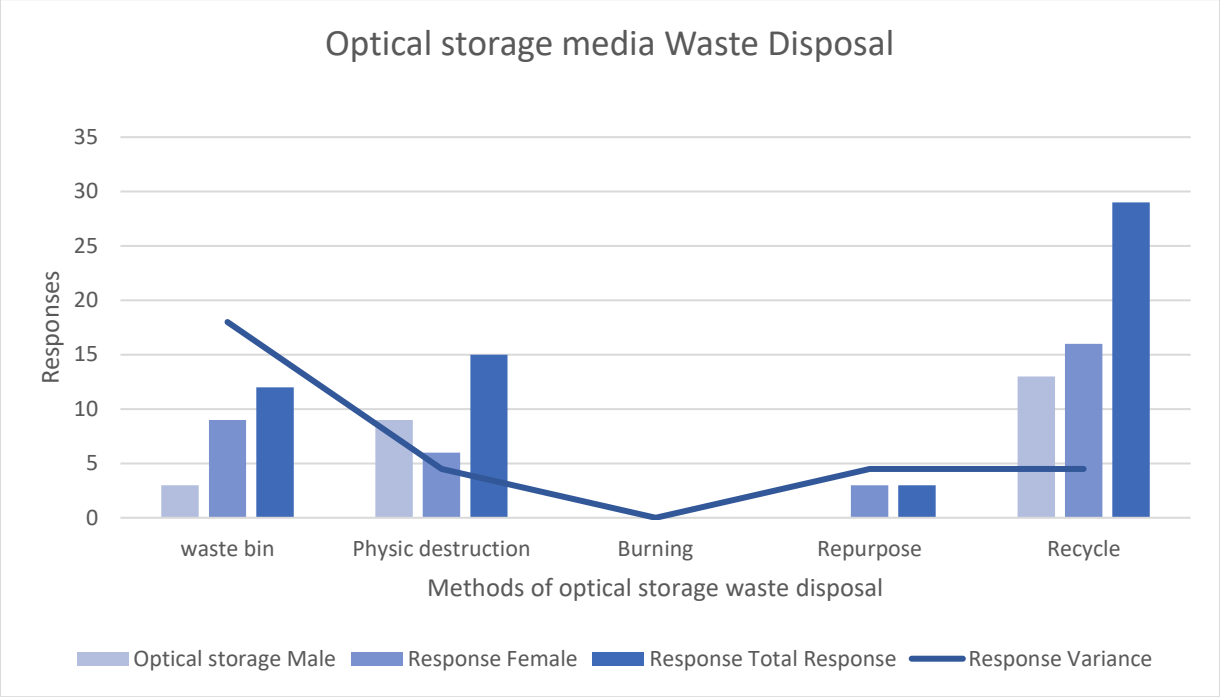


Figure 3 indicates that 72% of the respondents prefer to recycle the optical drives, while 69% choose to first physically shred the media before disposing. Optical drives are uncommon methods of storage in the present time, but were common ten years ago. In the attempt to digitalize all the NLIMS data, some of the data stored in Optical drives will be transferred into hard drive, therefore, the optical drive may become unnecessarily redundant. In this regard many old optical disks will be disposed as waste. Of 72% respondents who opted to recycle the disk, 3% do so without shredding them (GLOBAL, 2023). Here, disks are not physically destroyed as they go to be recycled and therefore, data can be accessed by unauthorized individuals. As such, they are handed over to third party with the data tacked inside. Studies have shown breaches among electronic recycling plants and the ramification has been far damaging to the company. Therefore, the approach used by NLIMS to dispose optical drive is not secure (GLOBAL, 2023). Information security breach does not need to be by majority, but only a small percentage as long as actionable information is accessed. In this regard 3% can cause severe damage (Siponen et al., 2007).

These findings therefore, indicate that a degree of weaknesses in the non-technical area that may compromise the technical area. Analysis shows that waste disposal of material that may contain data and information on day to day operations in NLIMS are not effectively and securely disposed to prevent unwanted access. Burning and physical destruction of such

waste is done by very few staff, leaving a large percentage of staff disposing waste using methods that dumb star divers can exploit to launch attack on the system.

Working station privacy: Shoulder Surfing

Unauthorized access to data and information can happen at workplace and public (home) through the following avenues; shoulder surfing both at work and at home, and access to work station shared resources such as common storage cabinet. Figures 4, and 5 show how information can be access by various individual through shoulder surfing and shared resources.

Figure 4

How shoulder surfing occurs in the work place and home

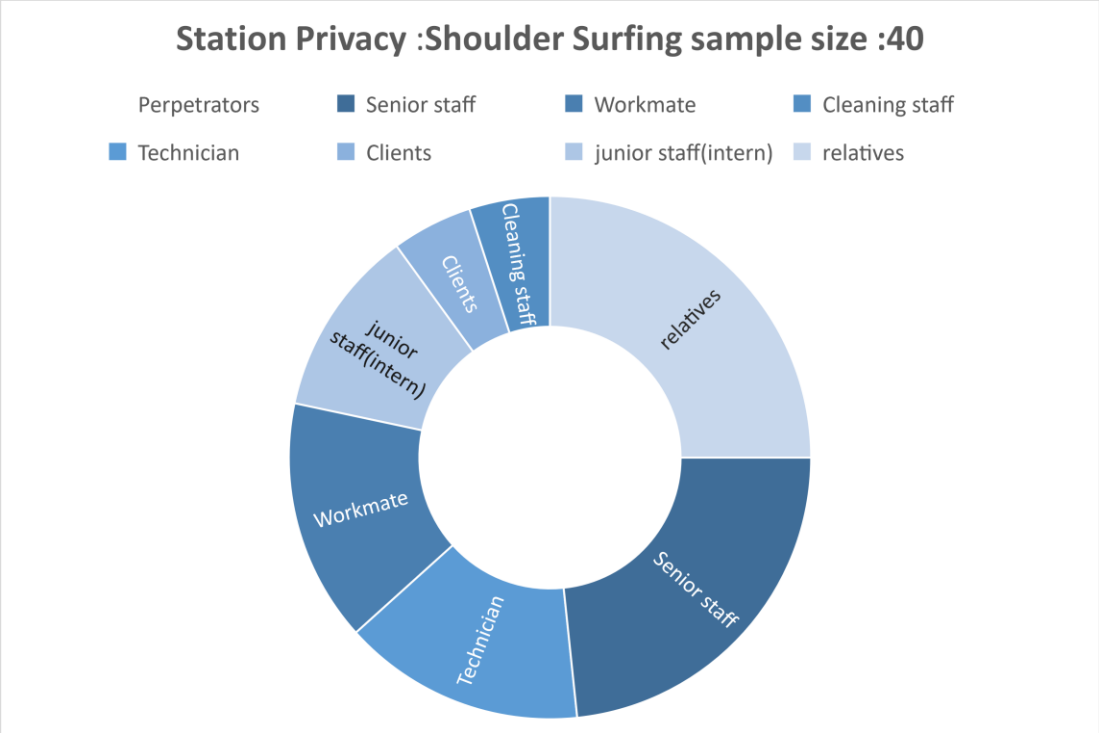
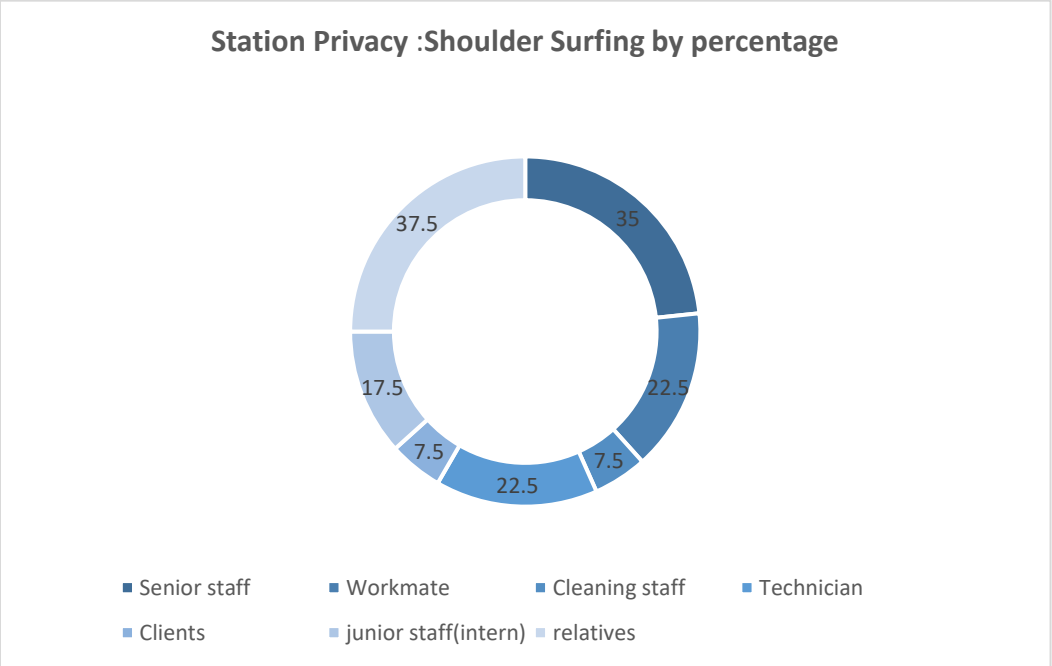


Figure 5

Station Privacy: Shoulder Surfing by percentage



Up to 37.5% of NLIMS linked staff agree that unauthorized personnel can access their computer through shoulder surfing. The percentage of the staff shoulder surfer 35%, indicates that more unauthorized people can access NLIMS information than those that are authorized through shoulder surfing. Studies indicate that individual who access information for which they are not authorized to in most case lack the knowledge pertaining the responsibility that comes with having access. As such, they are more likely to avail the accessed information to the public (Siponen et al., 2007). Therefore, shoulder surfing can course severe data breaches. According to these findings, NLIMS risks data breach both in offices and the public (staff relatives)

The data for shoulder surfing has been divided into two groups, one for perpetrators of shoulder surfing with access privileges, such as key staff directly linked to the NLIMS system (not subordinates staff such as cleaners), and those without access privileges such as client, relatives and interns. The ability to shoulder surf among the two groups were compared. The comparison is to establish if the level of access between the groups is significant. A t-test was conducted between the two groups. Null hypothesis was used for this t-test. The null hypothesis states that; "There is no difference in the level of access between the two groups." The outcome of t-test of the hypothesis are; the p- value of two-tail was 0.5913 which was slightly greater than the significant acceptable value of 0.05. In the

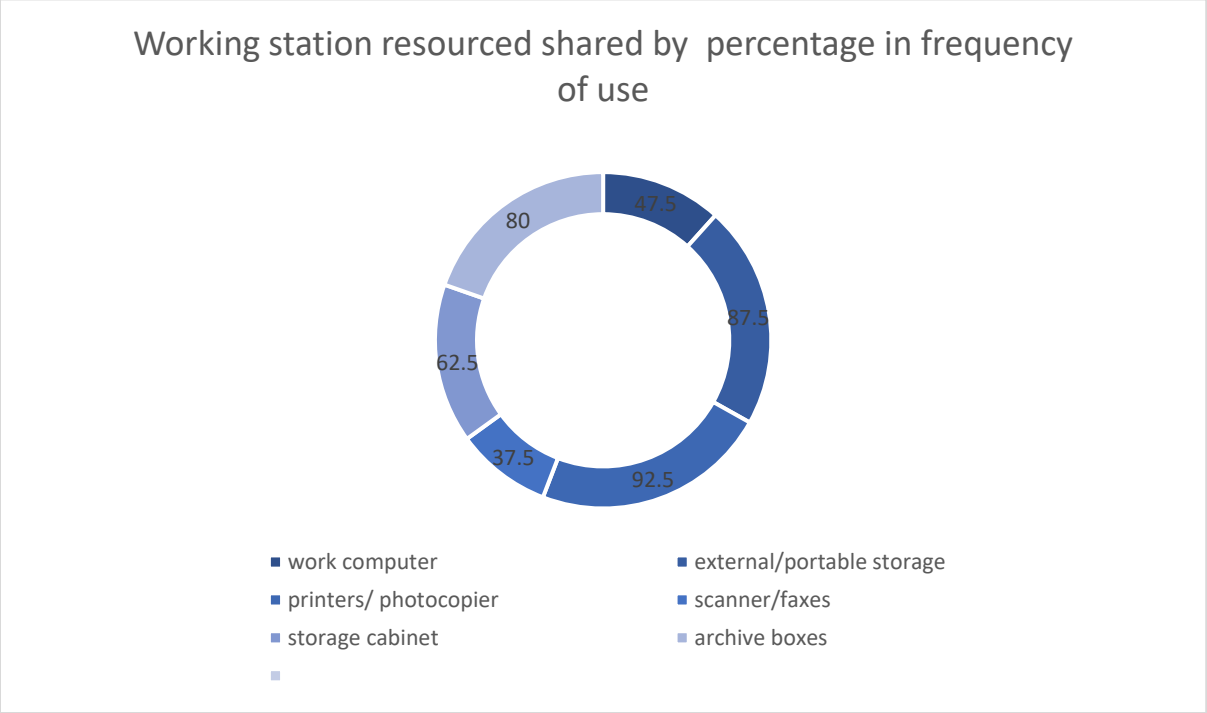
case where the null hypothesis was rejected, the implication would have been that unauthorized perpetrators of shoulder surfers were able to shoulder surf at almost same frequency as those that have access privileges.

Workstation resource sharing

It is important to point out that cybercrime is not always from external sources; however, staff have also been known to initiate the attack or help outsiders to launch attack by providing internal information about the system only accessible to the staff. This leads to the third aspect of access control; that is, through work station resource sharing, information or data can be easily accessed by unauthorized staff.

Figure 6

Working station resource shared by percentage in frequency of use



Work pace resource sharing indicates the ability of other staff to access information from other staff which they may not be authorized to access. Findings indicate that access to work computer is at 47.5%, external/portable storage at 87.5% and storage cabinet at 62.5%. These are direct access points to actionable information by unauthorized staff which predisposes the NLIMS system data leakage. Cybercrime is not limited to non-staff only, but also unfairly dismissed staff can leverage the easy access to information or the accessed information sabotage of the NLIMS system.

Unceremonious dismissals are found to leak confidential information to the public as means of retaliation (Salim & Stuart, 2014). As such NLIMS risk data breach due the ability of unauthorized staff being able to easily access information which they allowed to dismissed personnel.

Findings have indicated that sharing storage cabinets, and external drive such thumb drives or computer give unauthorized staff access to information or data (Von Roessing, 2010). These avenues are a loophole to access of limited accessibility data or information that they are not cleared to access. In aggregate, this study has sufficiently established that unsecure waste disposal, shoulder surfing, and unsecured resource sharing are non-technical weakness in KMLPP that can be easily exploited with limited effort by individual with malicious intent to attack the NLIMS system. It has also been established that available secure methods, such as burning for waste disposal are used by minority of the staff at less than 20% leaving at least 70% to unsecure methods.

Social engineering awareness: Social engineering awareness test

Social engineering is an approach that cyber criminals use to gather information on their target through exploitation of personal lifestyle of individuals. Many people are attacked and vital information about them is stolen. Information collected through social engineering is usually sold to highest bidder who can exploit it for a far larger and sinister attack. People directly linked to a critical information system such as NLIMS, are prime target for social engineering. In this case, staff associated or linked to NLIMS are expected to be well equipped with knowledge and skills to prevent themselves from being victims of social engineering. Attack on such personnel can have far more dangerous ramifications.

Figure 7

Social engineering awareness test sample size 4

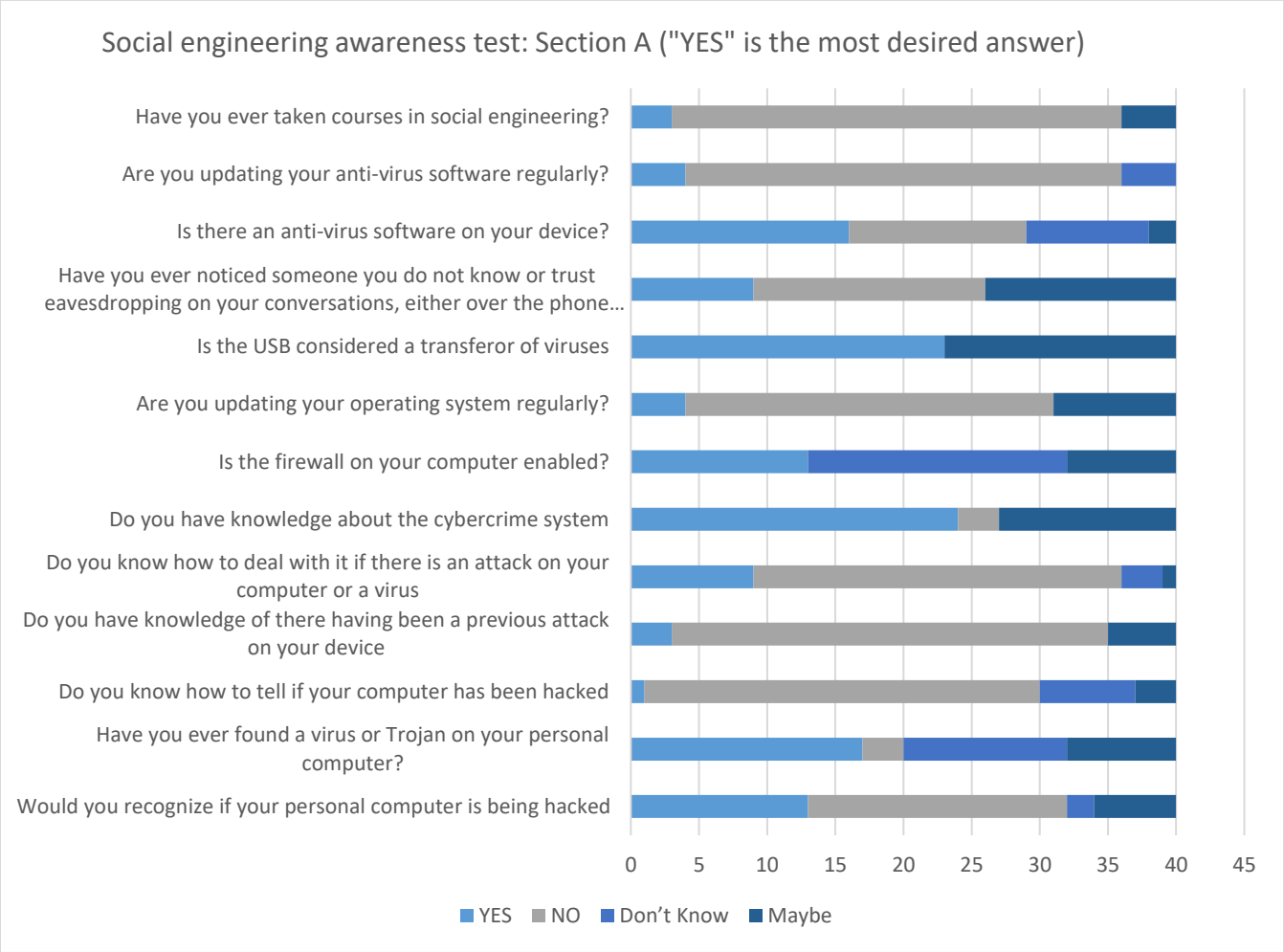


Figure 7 indicates awareness level on the knowledge pertaining cyber security protection measures. Out 40 respondents, 45% lack knowledge, experience and skills necessary to safeguard themselves against a social engineering attack. 17.3% are not sure if they are capable of avoiding, preventing or stopping the attack. 10.75% do not know what social engineering is or what it is all about. In aggregate, 73% of the staff are incapable of securely protecting themselves against a social engineering attack. At least 82% of the staff have never taken any cyber security training, while 32% of the respondent lack a proper antivirus software installed in their computers; and those that do 80% of them do not bother to frequently update it. 72% of the respondents do not know how to tell if their computer is being hacked, while 67.5% do not know how to go about stopping an ongoing attack.

Summary of discussion

70% of staff linked to NLIMS system lacks necessary knowledge on what is social engineering attack, how it is conducted, the

weakness that the attack relays on; and the skills and experience to prevent or stop the attack. This data is further supported by findings on how the staff dispose of waste that may contain information or data that can be used to launch an attack on the said system. Findings also indicate that lower rank staff access information which they are not authorized or cleared to access through the work station resource sharing policy. In this regard, the non-technical aspect of information security at KMLPP towards NLIMS has weaknesses which impair the overall effectiveness of the information security. With regard to cyber security, Gandhi postulates that despite complex barrier set up to deter cyberattack, most often attacker still manage to break through (Gagan, 2014). Gandhi, states observes that more often than not, computer break-ins are a collision of circumstances rather than a standalone vulnerability being exploited for a cyber-attack to succeed. In other words, it is the "whole" of the circumstances and actions of the attackers that cause the damage (Gagan, 2014). In reference to KMLPP weaknesses established by this study, it clear that KMLPP focuses more on the reductionist approach which strengthens the technical aspect of information security and pays less attention to the holistic approach which factors in both technical and non-technical.

Social engineering attack is highly mutable because it exploits people's lifestyle and thus their tricks and techniques keep changing and cannot be predicted. There is therefore an inherent need for KMLPP to be adaptive in their approach to non-technical aspects of information security. This can be supported by Gandhi where he suggests that holistic approach to cyber security is analogous to the immunity of biological being where robust, adaptive and constantly learning the ever-dynamic behavior of threat such as mutation of a pathogen is done (Gagan, 2014). With that in mind non-technical vulnerabilities which are human based and influenced cannot be effectively managed the same way as technical vulnerabilities.

4.0 Conclusion

KMLPP's use of secure waste disposal methods, such as shredding and burning, is inconsistent among staff, with at least 70% using unsecure methods. This lack of attention to secure waste disposal puts NLIMS at risk of access through dumb star diving. Further, unauthorized personnel can easily access information on staff computers or working desks through shoulder surfing. In addition, workstation privacy is compromised by workstation resource sharing policies, allowing malicious staff to exploit them, while over 60% of staff lack proper social engineering awareness, indicating that non-technical approaches to cyber security are ineffective against evolving cybercrime tactics.

5.0 Recommendations

This study recommends that, KMLPPS on NLIMS should invest in sensitizing her staff on cyber security awareness and measures that can be used to prevent and protect themselves against social engineering attacks. Secondly, they should employ secure waste disposal policies that will prevent information leakage. Thirdly KMLPS on NLIMS should secure and strongly regulate the sharing of work resources that contain confidential information so as to prevent

unauthorized staff from inadvertently getting access to confidential information. Lastly, the ministry should establish secure workstation privacy policy that will limit information sharing to unauthorized staff.

References

Armstrong, R. C., & Mayo, J. R. (n.d.). Leveraging complexity in software for cybersecurity. *the 5th Annual Workshop on Cyber Security and Information Intelligence Research: Cyber Security and Information Intelligence Challenges and Strategies*, (pp. 1-4). https://dl.acm.org/doi/abs/10.1145/1558607.1558643

BCS. (2023, June 5). *Complexity in cyber security*. BCS-chartered institute of IT. https://www.bcs.org/articles-opinion-and-research/complexity-in-cyber-security/

Chrispus, N. J. (2012). *Factors influencing performance of small and medium enterprises in Bungoma South District, Kenya* [Doctoral dissertation, University of Nairobi, Kenya]. kenya. http://erepository.uonbi.ac.ke/handle/11295/8221

Gagan, G. (2014). *Complexity theory in Cyber Security.* University of Warwick. https://www.researchgate.net/publication/263652176_Complexity_theory_in_Cyber_Security

Gandhi, S. M., Devishree, J., & Sathish Mohan, S. (2014). A New Reversible SMG Gate and Its Application for Designing Two's Complement Adder/Subtractor with Overflow Detection Logic for Quantum Computer-Based Systems. In *Computational Intelligence, Cyber Security and Computational Models: Proceedings of ICC3, 2013* (pp. 259-266). Springer India. https://link.springer.com/chapter/10.1007/978-81-322-1680-3_28

Gandhi, G. (2014). *Complexity theory in Cyber Security*. University of Warwick.

Hildick, S. A. (2005). Security for critical infrastructure scada systems. *SANS Reading Room, GSEC Practical Assignment,* , 498-506. https://www.researchgate.net/publication/242782760_Security_for_Critical_Infrastructure_SCADA_Systems

Jeffry, J. T., & Joyce, R. P. (2012). On the Misuse of Slovin's Formula. *The philippine statistician, 61*(1), 129-136. https://www.psai.ph/docs/publications/tps/tps_2012_61_1_9.pdf

Kioskli , K., & Nineta , P. (2020). A Socio-Technical Approach to Cyber-Risk Assessment. *ICCSITCSRA 2020 : International Conference on Cyber Security for Internet of Things, Cyber Security Riskand Analytics* (pp. 305-309.). Amsterdam, Netherlands: International Scholarly and Scientific Research & Innovation 14(11) 2020. https://publications.waset.org/abstracts/130520/a-socio-technical-approach-to-cyber-risk-assessment#:~:text=In%20this%20paper%2C%20a%20socio-technical%20approach%20is%20pro

posed,by%20considering%20the%20personality%20traits%20of%20the%20attackers.

Konstantinia, C., & Andrew , B. (2013). A Socio-Technical Approach to Cyber Risk Management and Impact Assessment. *Journal of Information Security, 4*(01), 33-41. doi:http://dx.doi.org/10.4236/jis.2013.41005

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques* (2nd ed.). NNew Age International (P) Ltd.

Mason, M. (2022). Complexity theory and the enhancement of learning in higher education The case of the University of Cape Town. *Educational Philosophy and Theory*, 1-10. https://www.researchgate.net/publication/365141317_Complexity_theory_and_the_enhancement_of_learning_in_higher_education_The_case_of_the_University_of_Cape_Town

McLeod, S. (2023, April 14). *Social Identity Theory: Definition, History, Examples, & Facts*. simplypsychology. https://www.simplypsychology.org/social-identity-theory.html#sthash.UsNnjwtA.dpbs

Mikko , S., Seppo, P., & Adam , M. (2007). Employees' Adherence to Information Employees' Adherence to Information . *International Federation for Information Processing, 232*, 133-144. https://link.springer.com/chapter/10.1007/978-0-387-72367-9_12

Morin, E. (1992). From the concept of system to the paradigm of complexity. *Journal of social and evolutionary systems, 5*(4), 371-385. https://www.sciencedirect.com/science/article/abs/pii/1061736192900248

National Land Information Management System. (2023, July 1). *National Land Information Management System (NLIMS)*. Retrieved from national-land-information-management-system-nlim: https://lands.go.ke/national-land-information-management-system-nlims/

Norman, D. (2022). *Socio-Technical Systems*. Interaction Design Foundation: https://www.interaction-design.org/literature/topics/socio-technical-systems

Prashant , K., & Supriya , B. (2010). Sample size calculation. *International Journal of Ayurveda, 1*(1), 55-57. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2876926/

Rangwala, H. (2022). *Socio-technical Systems*. Geeks for Geeks: https://www.geeksforgeeks.org/socio-technical-systems/

Salim, H., & Stuart, M. (2014). *Cyber Safety: A Systems Theory Approach to Managing Cyber Security Risks – Applied to TJX Cyber Attack.* Cybersecurity Interdisciplinary Systems Laboratory (CISL).

Savage , S., & Schneide, F. B. (2010, May 31). *Security is not a commodity: The road forward for cybersecurity research.* https://doi.org/10.17226/1581

Singh, A. S., & Masuku, M. B. (2014). Sampling techniques & determination of sample size in applied statistics research:. *International Journal of economics, commerce and management, 2*(11), 1-22. https://d1wqtxts1xzle7.cloudfront.net/65225177/21131

Stephan, S., Wakuru, M., & Boniphace, G. (2015). The organization of urban agriculture: Farmer associations and urbanization in Tanzania. *Cities, 1*(42), 153-159. https://www.sciencedirect.com/science/article/abs/pii/S0264275114000882

Tajfel, H., Turner, J. C., & Austin, W. G. (1979). An integrative theory of intergroup conflict:Organizational identity. (G.-E. Olivia, Ed.) *A reader, 56*(65), 56-65. https://doi.org/10.1093/oso/9780199269464.003.0005

Yunos, Z., Ab, H., & Ahmad, M. (2016). Development of a cyber security awareness strategy using focus group discussion. *SAI Computing Conference* (pp. 1063-1067). London: SAI IEEE. https://ieeexplore.ieee.org/abstract/document/7556109