Improving Information Privacy and Security: Strengthening Digital Literacy in Organisations

Guy Toko[1] and Kagisho Losaba[2]
[1]College of Business and Economics, Department of Applied Information Systems, University of Johannesburg, Johannesburg, South Africa
[2]Department of Applied Information Systems, University of Johannesburg, Johannesburg, South Africa

Keywords: Information, Privacy, Security, Digital Literacy.

Abstract: In a world of instant information, information privacy and security are under constant attack. With that being the case, organisations are expected to comply with regulations of securing and ensuring that information assets are protected. Employees are also expected to operate within the set frameworks that have been adopted by the organisation, which brings about the question of digital literacy among the workforce in order to achieve the set goals. The security of information alludes to the manner in which information is stored, processed and transmitted in order to comply with the organisation's information systems frameworks. The privacy of information can be described as the safeguarding of information related to a particular subject's identity. In addition, the security of information is a significant instrument for ensuring information resources and business goals, while privacy is centred on the safety of a person's rights and privileges concerning similar information.

1 INTRODUCTION

Technology is part of our daily lives. It has been entrenched in such a manner that everything we do, be it in the working space or private space, involves interaction with technology.

With the use of technology came other added requirements of how to ensure information privacy and security while enjoying the benefits or convenience of making use of such technology. Then the question of digital literacy comes into mind. Years ago, the use of technology was limited to use by experts, and this has changed radically over the years. Interaction with technology has indeed become part of our daily activities. In the working environment, a certain level of skills is required or needs to be acquired for employees to be effective and efficient in carrying out their duties.

Organisations should consider digital literacy as an ongoing process, which can be viewed in terms of personal development for employees (based on working conditions) and technological development. Information or data are one of the most valuable assets in any organisation. Therefore, how it is handled and protected is important.

In line with our research topic, we focus on the perception around the use or interaction with technology from the employee's point of view.

This research was undertaken to assess how to improve information privacy and security in strengthening digital literacy in the organisation and to evaluate the challenges they face in using or interacting with different technological platforms. Furthermore, to see which interventions can assist in closing the gap.

For this study, four research questions were generated to assess how digital literacy affects information privacy and security in an organisation, so as to investigate issues faced by employees when interacting or using technology.

2 LITTERATURE REVIEW

The South African Constitution of (1996), the Bill of Rights, sets out that all people have the right to privacy. This is a basic human right. Many countries in the world have this right in their constitution and have gone further to include digital privacy and data protection.

Toko, G. and Losaba, K.
Improving Information Privacy and Security: Strengthening Digital Literacy in Organisations.
DOI: 10.5220/0010534501170122
In *Proceedings of the 2nd International Conference on Deep Learning Theory and Applications (DeLTA 2021)*, pages 117-122
ISBN: 978-989-758-526-5
Copyright © 2021 by SCITEPRESS – Science and Technology Publications, Lda. All rights reserved

The National Institute of Standards and Technology (NIST) describes information security as the protection of information or data and information technology systems from unapproved access, usage, unauthorised leaks of information, disruption, change, or destruction, in order to provide integrity, availability and confidentiality.

Digitisation has sped up the rate of globalisation at an alarming pace. This was or is in the hope of assisting organisations to increase their competitive edge. This requires certain skills: technical, professional and specialised skills in ICT. Employers need to ensure that policymakers involve all stakeholders in taking part and learning new skills in an increasingly digitised world.

Information Privacy and Security. Governance and risk management associated with information privacy and security are indeed critical to many job categories, which include aspects coming from areas of information and knowledge management responsibilities (Burkell, Fortier, & Di Valentino, 2015).

Digital Literacy. It is of importance to recognise the need for employees to acquire or develop digital literacy skills and capabilities in order to operate effectively in the digital society. Furthermore, digital literacy cannot have a finite definition, as this depends on different life situations, which vary. Digital literacy cannot be viewed from a one-glove-fits-all in terms of applicable courses or assessments (Nelson, Courier, & Joseph, 2011).

Bawden (2001) argued that, as digital technology is ever-present in whatever we do, employees need to increase in number in an effort to acquire appropriate sets of digital abilities to gain access and process information, using digital systems and tools.

Challenges on Digital/ICT Platforms. Because of a lack of adequate or appropriate information management practices by employees, they are often the main cause of organisational vulnerabilities or threats regarding information privacy and security. Employees reveal insufficient abilities and expertise, coupled with unsuitable practices in these areas of focus, and comparable shortcomings at the organisational level are widely captured (Cox, 2012).

Interventions to Address the Gaps. The risk factor compels organisations to consider investing more in the awareness and training of users and employees.

It is therefore important when strengthening digital literacy to consider different digital-literacy frameworks in an effort to address a specific area of interest, in this instance information privacy and security in organisations (DQ Digital Intelligence, 2019). An example of a digital-literacy framework is the Digital Intelligence Framework, which was created in association with World Economic Forum, Economic Cooperation and Development, IEEE Standards Association and DQ Institute. An umbrella framework aims to address digital skills, digital literacy and digital readiness across all sectors and demographics.

3 METHODOLOGY

Research methodology is a set of processes in which information pertaining to a research problem is analysed, processed, selected and identified, based on a specific procedure or technique. This is in an effort to identify and assess the levels of digital literacy among employees in order to improve information privacy and security in an organisation and to evaluate the levels of compliance, with measures put in place for information privacy and security (Fernandez-Aleman, Senor, Lozoya, & Toval, 2013; Yang, & Tate, 2012; Zeng, Wang, Deng, Cao, & Khundker, 2012).

Furthermore, it is known that research methodologies can be categorised into quantitative and qualitative research methodologies. This is to set out how information pertaining to the research is going to be gathered and presented.

For the purposes of this research project, a quantitative research methodology was used. A survey questionnaire (electronic) was distributed to approximately 50 computer end users. People of interest were managers, engineers, supervisors and junior staff members with varying job functions (various departments) within the organisation (City of Ekurhuleni).

4 RESULTS AND ANALYSIS

Quantitative data analysis was utilised in this research and can be characterised into different viewpoints, which incorporate descriptive statistics, exploratory data analysis, corroborative information investigation

and connection and relapse information investigation. In this research, descriptive data analysis was utilised to analyse the collected data. Descriptive data analysis is utilised to depict the essential features of the data in a research study or an exploration venture and they offer fundamental outlines about the example and the measures. Descriptive data analysis is utilised to introduce quantitative clarification in a helpful structure. Descriptive data analysis likewise encourages us to gather immense measures of data in a sensible manner with basic illustrations investigation.

Demographics. The demography for this research was based on gender, age and ethnicity. See charts below.

Table 1: Gender.

Gender

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Male	5	33.3	33.3	33.3
	Female	10	66.7	66.7	100.0
	Total	15	100.0	100.0	

Gender

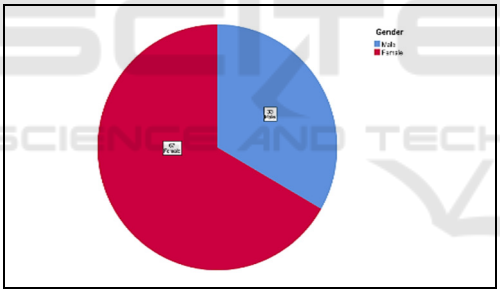

Figure 1: Gender.

The analysis of the gender data collection shows that the female respondents wherein the majority (67%) as compared to the male respondents (33%).

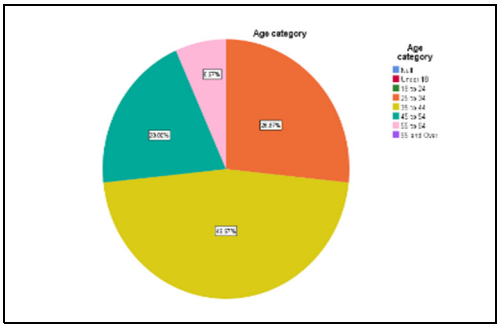

Figure 2: Age Categories.

The respondents comprised the following age groups: 26.67% were 25-34; 46.67% were 35-44; 20% were 45-54 and 6.67% were 55+.

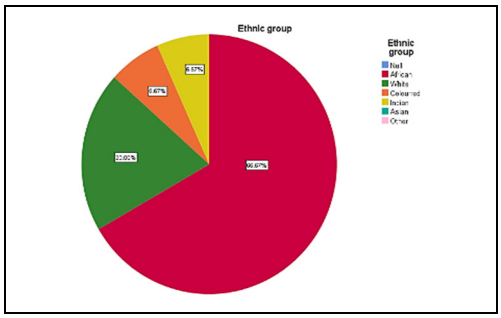

Figure 3: Participants circle.

The participants were Black (66.67%), White (20%), Indian (6.67%) and Coloured (6.67%). This analysis allows us to know how many employees in each ethnic group participated.

Answers Collected from Research Questions.

What is information privacy and security?

(How to keep information private/secure while online – what measures are taken while making use?)

Question 1: Which of the following best describes your thinking, does not have to be exactly right? The data collected and analysed from this question showed that 20% of the respondents said, "Following security policies at our organization prevents me from doing my work" and 80% said, "Following security policies at our organization helps me to do my work better".

Question 2: I am capable of identifying a security issue/incident if I saw one? Information systems are exposed to different types of threats, which can result in huge financial losses (Gerić & Hutinski, 2007). Early detection can save the organisation from such incidents. The data collected and analysed from the respondents showed that 60% "Agreed", 26.7% "Strongly Agreed", 6.7% "Disagreed" and 6.7% were "Neutral".

Question 3: The management and the security team regularly share security information and have awareness programs? On this question, the responses were as follows: 20% "Agreed", 13.3% "Strongly Agreed", 46.7% "Disagreed", 13.3 "Strongly Disagreed" and 6.7% were "Neutral". According to the literature reviewed, instilling an information-security-aware culture will reduce the risk to information assets (Da Veiga & Eloff, 2010). However, strengthening information security requires

employees to comply with security rules and regulations (Bulgurcu et al., 2010).

Question 4: In general, which is more important to you: CONVENIENCE or PRIVACY? The data analysis showed that 33.3% answered "Convenience" and 66.7 answered "Convenience". According to the reviewed literature, the convenience and efficiency brought by IoT applications also bring privacy and security to the spotlight (Pu et al., 2019).

Question 5: Content providers have the right to resell information about its users to other companies? The analysis showed that 13.3% "Agreed", 6.7% "Strongly Agreed", 13.3% "Disagreed", 60% "Strongly Disagreed" and 6.7% were "Neutral".

According to the literature that was reviewed, to benefit from important shopper and value-based information on versatile applications, organisations should utilise ethical decisions and strategies that can reduce privacy concerns, because such concerns present critical challenges for corporate social duty (Libaque-Sáenz, 2020).

Question 6: The organisation should update user privacy notices and privacy policies?

The responses for the question were 46.7% "Agreed", 40% "Strongly Agreed" 6.7% "Strongly Disagreed" and 6.7% were "Neutral". Basic elements were associated with privacy policy. The organisations require principles to govern their information practices and to ensure that a process compliance is put into daily operations (Pfadenhauer, et al., 2019). Privacy policy should reflect fair information practices (FIPs)

What is digital literacy?

(How to examine the credibility of information – the level of digital literacy while interacting with technological platforms?).

Question 7: How often do you use PC/Laptop at work? The data collected and analysed from this question showed that 97.3% "Regularly" used the PC/Laptop at work and 6.7% "Never" used the PC/Laptop at work. Bawden (2001) argued that, as digital technology is ever-present in whatever we do, workers would need to increase in number in an effort to acquire appropriate sets of digital abilities to gain access and process information, using digital systems and tools.

Question 8: How do you acquire digital literacy skill? (Experience – on the job learning) The analysis of the data showed that 53.3% "Strongly Agreed" and 46.7% "Agreed" that respondents acquired digital literacy through experience (on the job learning). A number of studies among adults finding "that only about 10 percent of learning represents formal learning in the work-place, compared with 70 per cent self- or on-the-job learning and 20 percent peer-to-peer learning" (Grant-Clement, 2017), provide further evidence of this.

What are the challenges experienced on digital platforms?

Question 9: Cannot use the databases? The responses to the question were as follows: 60% "Strongly disagreed", 33.3% "Disagreed" and 6.7% "Agreed". Database technologies are a centre segment of many processing frameworks. They permit data to be held and shared electronically and the measure of data contained in these frameworks keeps on developing at a dramatic rate and so does the need to safeguard the integrity of the data and secure the data from unintended access (Murray, 2010).

Question 10: Cannot fully apply security features as and when required? The responses were that 33.3% "Agreed", 33.3% "Disagreed", 6.7% "Strongly Agreed" and 26.7 "Strongly disagreed". Security features control how users and systems interact with systems. Access controls give organisations the ability to control, restrict, monitor, and protect resource availability, integrity and confidentiality. It is of importance to impart such skills to those who have been given the authority to administer such. According to Jaeger (2013), the major causes of data breaches is errors committed by employees, rather than hackers.

What interventions to put in place to address the shortcomings of digital literacy?

Question 11: Intervention -Information security (passwords, data security, etc).

Among respondents, 86.7% see this intervention as "Very Essential", 6.7% as "Essential" and 6.7% as "Quite Essential". Information security implies ensuring data (information) and data systems from unapproved access, use, revelation, interruption, adjustment, or obliteration.

Information security management is a cycle of characterising security controls to ensure information resources/assets.

(Kissel, 2011) creation of information security awareness is more effective than other measures. However, this requires support from management, as top management participation in information security management has a significant influence on employees' attitude and behaviour over compliance with information security policies (Hu, Dinev, Hart & Cooke, 2012).

Question 12: Intervention - Electronic banking. Among respondents, 80% saws this as "Very Essential" and 20% as "Essential".

According to Soomro, Shah, & Ahmed (2016), awareness and training courses are the responsibility of management. The inclusion of overall management for a holistic approach to information security may make organisation information more secure.

5 RECOMMENDATIONS

The research was seeking to investigate how employees perceived information privacy and security. Digital literacy plays a part in how employees interact with digital platforms. The crux of the matter is how to safeguard information assets while making use of technology. This can be affected by external factors.

Digitisation is here to stay, empowering the workforce is of real importance within any organisation. Safeguarding information assets is also important, by investing in employees, by imparting the required skill sets and ensuring that there is more awareness around technological new and existing platforms.

Even though the net was cast wide for participants, only a few responded.

Future research will be required to further investigate and interrogate how employees interact and perceive technology. Measures required ensuring that digital literacy is strengthened and information privacy and security is improved through learning and awareness programmes.

6 CONCLUSIONS

Due to the Covid-19 outbreak, physical contact was kept at a minimum and lockdown regulations were adhered to.

The approval process for ethical clearance took a long time, as well as permission from COE.

The other shortcoming with the research was that some of the respondents did not complete the questionnaire. As a result, the sample size was smaller than expected.

A broad literature review was done to gain further knowledge and understanding of information privacy and security as well as digital literacy in general.

Digitisation has changed our way of life and we should adapt otherwise face being left behind.

A large percentage of the data and information came from the point of view of the research participants.

REFERENCES

Bawden, D. (2001). Information and digital literacies: A review of concepts. Retrieved 7 April 7, 2020, from http://arizona.openrepository.eom/arizona/bitstream/10150/105803/1/bawden.pdf

Bulgurcu, B., Cavusoglu, H. and Benbasat, I. (2010), "Information security policy compliance: An

Burkell, J.A., Fortier, A. & Di Valentino, L. (2015). Enhancing Key Digital Literacy Skills: Information Privacy, Information Security, and Copyright/Intellectual Property: FIMS library and information science publications. FIMS Library and Information Science Publications.

Constitution of the Republic of South Africa No 108 of 1996 (RSA).

Cox, J. (2012). Information systems user security: A structured model of the knowing–doing gap. *Computers in Human Behavior*, 28(5):1849-1858.

culture", *Computers and Security*, Vol. 29 No. 2, pp. 196-207.

Da Veiga, A. and Eloff, J. (2010), "A framework and assessment instrument for information security

DQ Global Standards Report (2019). DQ Global Standards Report 2019. Common Framework for Digital Literacy, Skills and Readiness. https://www.dqinstitute.org/wp-content/uploads/2019/03/DQGlobalStandardsReport2019.pdf empirical study of rationality-based beliefs and information security awareness", *Management*

Fatima, R., Yasin, A., Liu, L., Wang, J., Afzal, W. & Yasin, A. (2019). Sharing information online rationally: An observation of user privacy concerns and awareness using serious game. *Journal of Information Security and Applications*, 48102351.

J.L. Fernandez-Aleman, J.L., I.C. Senor, I.C., P.A.O. Lozoya, P.A.O., A. Toval, A. Security and privacy in electronic health records: A systematic literature review, *Journal of Biomedical Informatics*, 46 (3) (2013), pp. 541-562.

Gerić, S. and Hutinski, Ž. (2007). Available from: https://hrcak.srce.hr/21445.

Grant-Clement S (2017). Digital learning: education and skills in the digital age. An overview of the consultation on digital learning held as part of the Corsham Institute Thought Leadership Programme 2017. RAND Corporation and Corsham Institution. Available athttps://www.rand.org/content/dam/rand/pubs/conf_proceedings/CF300/CF369/RAND_CF369.pdf.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, 43(4), 615–660.

Information Systems Quarterly, Vol. 34 No. 3, pp. 523-548.

Jaeger, J. (2013). Human error, not hackers, cause most data breaches. *ComplianceWeek*, 10(110),56–57.

R. Kissel R., "Glossary of Key Information Security Terms," 2011.

Libaque-Sáenz, C.F., Wong, S.F., Chang, Y. & Bravo, E.R. (2020). The effect of fair information practices and data collection methods on privacy-related behaviors: A study of mobile apps. *Information & Management,* 103284.

Murray, M.C. (2010). Database security: What students need to know. *Journal of Information Technology Education*, 9IIP-61.

Nelson, K., Courier, M., & Joseph, G.W. (2011). Teaching tip: An investigation of digital literacy needs of students. *Journal of Information Systems Education*, 22(2):95-109.

Pfadenhauer, M., Banse, G., Böhn, A., et al. (2019). *Editorial*KIT Scientific Publishing.

Pu, Y., Luo, J., Hu, C., Yu, J., Zhao, R., Huang, H. & Xiang, T. (2019). Two secure privacy-preserving data aggregation schemes for IoT. *Wireless Communications and Mobile Computing*, 20191-11.

Soomro, Z.A., Shah, M.H. & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2):215-225.

Yang, H. & Tate, M. (2012). A descriptive literature review and classification of cloud computing research. Communications of the Association for Information Systems, 3135.

Zeng, Y., Wang, L., Deng, X., Cao, X., & Khundker, N. (2012). Secure collaboration in global design and supply chain environment: Problem analysis and literature review. *Computers in Industry*, 63(6), 545e556.

SCITEPRESS SCIENCE AND TECHNOLOGY PUBLICATIONS