The Relationship between Human-centric Cybersecurity and Cybercrime

Anesu Robin Dikito[1] and M Shamim Kaiser[2]

[1]Binary University of Management & Entrepreneurship, Selangor, Malaysia
[2] Institute of Information Technology, Jahangirnagar University, Savar, Dhaka-1342, Bangladesh
mskaiser@juniv.edu

Abstract. The aim of this study is to propose a model of human-centric cybersecurity and its relationship to curbing cybercrime in Zimbabwean commercial banks. The effects of human-centric cyber-crimes (e.g. email phishing, identity theft, hacking and malware) are increasing irrespective of the use of cyber security techniques (such as firewalls, antispyware and antivirus). In order to prevent security breaches, the role of the human element should always be emphasized. The study proposed a model of human-centric cyber security solutions in Zimbabwean commercial banks to counter identity theft. Item frameworks were modified to illustrate how human cyber security measures would effectively curb cybercrime from the theory of protection motivation and the theory of routine activity. Solutions to cybercrime centered on human beings include raising aware- ness about cyber security, top management support and cyber security policies. Quantitative data collected through survey questionnaires which were distributed to 118 key informants across thirteen commercial banks in Zimbabwe. Gathered data were analyzed using SPSS 23 and Smart PLS Version 3.2.8 for partial list structural equation modeling. The findings were interesting, the human solutions such as raising awareness, top management support, and cybersecurity policy indicated a negative and moderate effect on identity theft, R^2 value was of 0.64. The standardized root mean square residual value for the human structural model was 0.08 indicating a good model fit. The findings show that the human factor is key for the successful cybersecurity of any banking institution.

Keywords: Cybersecurity, Cybercrime, Identity theft.

1 Introduction

With the expeditious expansion of the information and communication technology, the rate of cybercrime or electronic-crimes is increasing at an alarming rate. Cybercriminals use computing technology to carry illegitimate activities such as hacking, phishing, malware, mail scams, and identity theft, etc. On the other hand, cybersecurity refers to techniques for shielding computer systems and networks from the cybercrime.

Cybercrime refers to all crimes committed in cyberspace. Cyberspace is the environment created when both hardware and software infrastructure are connected. In Zimbabwe, cybercrime continues to rise. According to the Reserve Bank of Zimbabwe, Zimbabwe loses on average about USD 1.8 billion dollars every year owing to cybercrime. The various types of cybercrimes in Zimbabwe include identity theft, phishing, hacking and malware victimization. [14]. This study focused on human cybersecurity solutions to eradicate identity theft.

Over the last decade (2009 to 2020), there has been an increase of interest in (a) Cybersecurity and (b) Cybercrime, as shown in Figure 2. The graph was made with the help of the Google Trends (https://trends.google.com/) result. The graph depicts how interest in cybersecurity is increasing at an unprecedented rate in order to combat cybercrime.

Identity theft refers to illegal use of private and personal information such as passwords and pins for financial gain. In Zimbabwe identity theft is the most common form of cybercrime. The problem of identity theft requires enhanced cybersecurity solutions. Gone are the days of relying on technical solutions alone, banking institutions should seriously consider introducing human solutions to cybercrime. Banks continue to experience identity theft victimization leading to financial losses. Human based solutions such as raising

awareness, top management support and cybersecurity policy emerge as potential solutions to identity theft.

This study sought to analyze human cybersecurity and its relationship to curbing identity theft. The study was focused on thirteen commercial banks in Zimbabwe. The unit of analysis were senior managers and employees from audit, risk and compliance departments.

In this paper, our contribution is to

- Identify human-centric factors which influence the cybercrime reduction,
- Verify a human-centric cybersecurity model in reducing cybercrime.

The rest of the paper is structured as – Section 2 discusses the human-centric factors which help reduce cybercrime. The most common cybercrimes are in Sec- tion 3. Section 4 talks about the theories applied to human-centric cybersecurity and cybercrime. Section 5 presents the Human-centric cybersecurity conceptual model, the research methodology is explained in section 6. The data are analyzed in section 7 and discussions are given in section 8. Lastly, the work is concluded in section 9. Some future research directions are also provided.

2 Human cybersecurity factors

Cybersecurity refers to all the precautionary activities including both technical and non-technical measures intended to protect computers and elements of the cyberspace from all threats [5]. According to the international telecommunication union (ITU) cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organizational assets. Organizational assets include connected computing devices computing infrastructure, applications, service, communication systems and data in the cyberenvironment [9]. Cybersecurity refers to the availability, integrity and confidentiality of resources domiciled in the cyberspace. The study focused on human aspects of cybersecurity. Reliance on technical solutions alone will not eliminate cybercrime; emphasis should be given to the human factor. The human factors in include awareness, top management support, and cybersecurity policies.

Top management support exists when senior managers create a supportive environment through budgetary funding and skills development [4, 3]. Awareness occurs when employees understand and know an organization's cybersecurity goals and requirements. Awareness is mostly achieved through training, posters, notice boards and via emails campaigns [15]. The cybersecurity policy defines the dos and don'ts or the expected employee behavior whilst on the cyberspace [16, 13]. Complying with cybersecurity policy leads to cybersecurity.

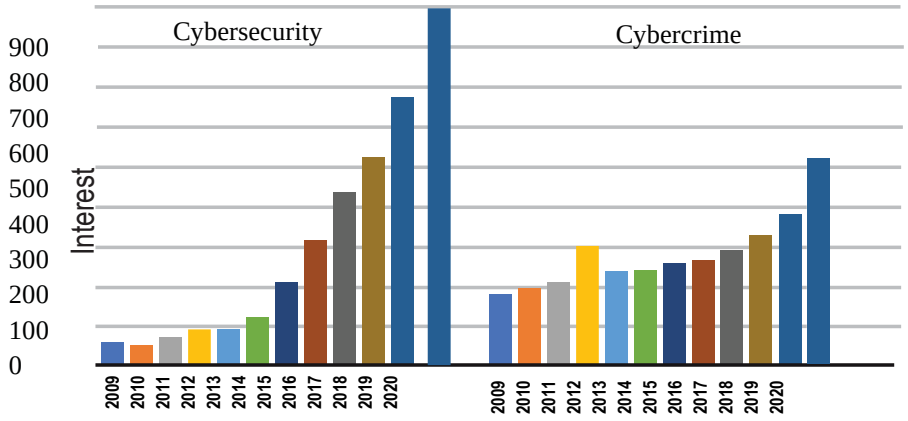

Fig. 1. Interest on (a) Cybersecurity and (b) Cybercrime in the last decade.

3 Cybercrime

Cybercrime refers to all the illegal actions which are detrimental to the confidentiality, integrity and availability of cyberinfrastructure. Cybercrime can also be defined as criminal activities perpetrated though use of computer related devices and the internet [10]. Cyberinfrastructure includes both hardware and software resources existing in the cyberspace. The most common and significant cybercrime in Zimbabwe is identity theft, which is the focus of this study.

3.1 Identity Theft

Identity theft refers to using another person's private information for fraudulent activities. Private information can be gained through email phishing, hacking and malware victimization. In email phishing humans are tricked into providing their private personal details by being requested to click on malicious links and opening attachments. Hacking entails the illegal access to cyberinfrastructure to obtain private personal or organizational information. Techniques employed by hackers may include key logging, denial of services, sniffing and fake messages. Hackers use identity related data to commit a range of fraud.

4 The Human-centric Cybersecurity Model

Human involvement in the cybersecurity chain has potential to improve and reshape cybersecurity in the banking sector. Technical factors alone would not solve the problem of cybercrime, but human factors should be included in order to combat cybercrime. This necessitated the development of a conceptual model that realizes the importance of the human factor and its relationship to curbing identity theft. Figure 2 depicts the Human centric Cybersecurity Model.

The following hypotheses were developed to analyze the relationship between the human cybersecurity and cybercrime.

- **H1:** Awareness has a direct negative effect on identity theft
- **H2:** Top management support has a direct negative effect on identity theft
- **H3:** Cybersecurity policy has a direct negative effect on identity theft

Awareness plays an important part in cybersecurity in that it develops an employee's understanding of potential risk and threats including appropriate actions to take in order to protect the cyberinfrastructure. Likewise, [19] suggested that cybersecurity success depended on awareness. [11] employed learning analytics to build cybersecurity awareness programs and found out that awareness campaigns were a key component of cybersecurity. Another study, [15] found out that awareness programs promoted secure employee behavior such as use of strong passwords, and compliance to policy. [12] recognized that awareness was a key factor in combating cybercrime. Therefore, it is hypothesized that Awareness has a negative effect on identity theft

Top Management support entails the creation of a cybersecurity supportive environment by top managers via skills development, technology investments and budgets. [2] opined that Top managers were key in aligning cybersecurity with overall business goals. Top Management helps to positively change and shape employee attitudes via training, collaboration and knowledge sharing. A study by [1] concluded that management commitment was a key driver of information security. Therefore, the hypothesis that Top management support has a direct negative effect on identity theft

According to [18] *cybersecurity policy* is a communication document from management which conveys a specific message [8] posited that an organization whose employees do not comply with an information security

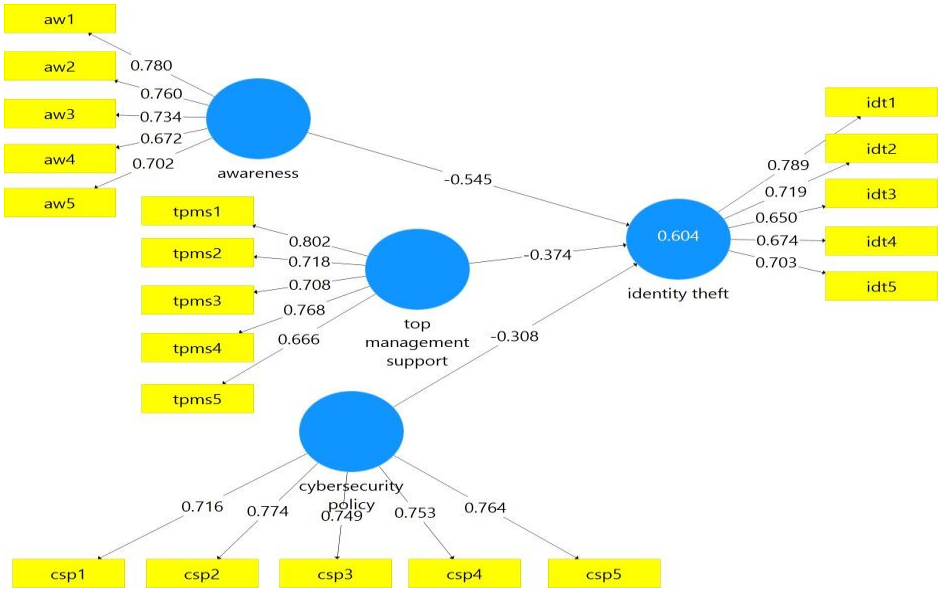

Fig. 2. The Human-centric Cybersecurity Model

policy, will continue to have security violations. This view was supported in [16] who conducted a study in Nigeria, and recommended that a national policy should cover citizen identification and relationships with internet service providers. [17] concluded that adherence to policy improves cybersecurity. Therefore, the hypothesis that Cybersecurity policy has a direct negative effect on identity theft

5 Research Methods

This section focuses on population and sampling, design of the survey questionnaire, and the various methods of analysis adopted in the study. The target population was non-information technology employees from commercial banks of Zimbabwe. The employees were selected for their role in dealing with cybersecurity on one way or another. The sampling units were senior man- agers and employees from the audit, risk and compliance departments across thirteen commercial banks in Zimbabwe.

The total for respondents was 118, the majority were males 79, constituting 66.9% of the total representation against females who were 39, constituting 33.1% of the representation. Forty eight percent of the respondents were aged between 40 and 49 years, 30% were aged between 50 and 59 years while 22% were aged between 30 and 39 years. The departments were as shown in Table 1. A survey questionnaire on a five points likert scale was used to gather data for each construct in the Human-centric cybersecurity model.

Table 1. Departments

Department	Count	Percent
Audit and Risk Management	57	48.3
Compliance	25	21.2
Credit	5	4.2
Client Coverage	4	3.4
Personal and Business Banking	15	12.7
Transaction	6	5.1
Operations	2	1.7
Business Development	3	2.5
Corporate and Investment banking	1	0.8
Total	118	100.0

The respondents were each requested to judge 20 statements which were tagged from 1 = Strongly disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, 5 = Strongly Agree. All the constructs were adapted from previous literature and were slightly modified to suit the measured phenomena. Respondents were randomly selected and data were entered in Smart PLS 3.2.8 for partial least squares structural equation modeling. The analysis and results are explained in the next section.

6 Analysis and Results

In order to determine the most significant factors negatively affecting identity theft data were first assessed for convergent and discriminant validity, followed by path coefficient analysis.

6.1 Convergent Validity

Convergent validity refers to how well the indicator items measure the same construct. Indicators of a construct should share a high proportion of variance. According to [6] convergent validity can be accessed via factor loadings, composite reliability and average variance extracted. Table 5.1 depicts the factor loadings for all the constructs exceeded the recommended value of 0.5. Composite reliability is the extent to which the construct indicators actually measure the construct. The composite reliability values ranged from 0.834 to 0.866. The composite reliability values were all above 0.7, demonstrated high levels of in- ternal consistency among the reflective latent variables. The average variance extracted measures the variance captured by the indicators relative to measurement error, and it should be greater or equal 0.5. The average variance extracted for all constructs were all greater than 0.5 as shown in Table 2. The cronbach alpha for all the constructs was above 0.7. The results show that all the three constructs awareness, top management support, and cybersecurity policy were indeed measuring what they were intended to measure.

Table 2. Validity and Reliability of Human-centric cybersecurity Model Constructs

Constructs	Items	Loading	Cronbach	CR	AVE
Awareness	I know the rules and regulations prescribed by the bank's Cybersecurity policy	0.78	0.783	0.851	0.534
	I understand the rules and regulations prescribed by the bank's Cybersecurity policy	0.76			
	I know my responsibility as prescribed in the Cybersecurity policy to enhance the bank cybersecurity	0.734			
	I am aware of the bank cybersecurity policy				
	I am aware of the dos and don'ts prescribed in cybersecurity	0.702			
Cybersecurity Policy	The bank has cybersecurity policy in place	0.716	0.807	0.866	0.564
	I know where to get the cybersecurity policy copy				
	Cybersecurity policy drives the acceptable use of the bank's cybersecurity resources	0.774			
		0.749			
	Cybersecurity policy provides instruction for the implementation of the bank security posture	0.753			
	The bank cybersecurity policy is easily accessible	0.764			
Top Manage- ment Support	In my bank, top management actively supports cybersecurity management as a vital enterprise-wide function	0.802	0.787	0.853	0.538
	The bank funds and allocate resources for cybersecurity	0.718			
	A formal organization unit for cybersecurity is established within my bank	0.708			
	Senior management actively enforce cybersecurity polices at my bank	0.768			
	Top managers set aside a budget for cybersecurity	0.666			
	every year				
Identity Theft	Individual bank cards had been illegally used with-	0.789	0.751	0.834	0.502
	out permission of the card holder	0.719			
	Unauthorized charge on accounts have occurred in some way	0.65			
	Stolen identity had been used to conduct purchases				
	Personal information had been used to apply for benefits	0.674			
	Money has been deducted from personal accounts without permission	0.703			

6.2 Discriminant Validity

Discriminant validity refers to the extent to which a construct is truly distinct from another constructs and is indicated by low correlations between the measure of interest and the measures of other constructs. Indicator items should load more on their constructs in the model and the average variance shared between each construct and its indicators should be greater than the variance shared between the construct and other constructs (Fornell & Larcker, 1981).

Discriminant validity was assessed via the cross loadings criteria and the Heterotrait-Monotrait Ratio (HTMT) criterion. 2 and Figure 2 show that the model demonstrated adequate discriminant validity.

Table 3. Cross Loadings

	aw	csp	idt	tpms
aw1	0.78	0.138	-0.415	-0.071
aw2	0.76	0.165	-0.32	-0.147
aw3	0.734	0.125	-0.527	0.081
aw4	0.672	0.048	-0.372	-0.014
aw5	0.702	0.066	-0.41	-0.053
csp1	0.036	0.716	-0.325	0.222
csp2	0.22	0.774	-0.39	0.048
csp3	0.039	0.749	-0.335	0.171
csp4	0.095	0.753	-0.297	-0.001
csp5	0.144	0.764	-0.337	0.194
idt1	-0.41	-0.409	0.789	-0.323
idt2	-0.471	-0.328	0.719	-0.249
idt3	-0.311	-0.277	0.65	-0.276
idt4	-0.368	-0.241	0.674	-0.355
idt5	-0.463	-0.328	0.703	-0.237
tpms1	-0.032	0.022	-0.305	0.802
tpms2	-0.14	0.048	-0.218	0.718
tpms3	0.036	0.063	-0.267	0.708
tpms4	0.004	0.245	-0.384	0.768
tpms5	-0.053	0.191	-0.262	0.666

Legend: Awareness(aw) Cybersecurity policy(csp) Identity Theft(idt) Top Management Support(tpms)

6.3 Hypothesis Testing

A path analysis to test the hypothesis generated earlier in the literature review section is summarized in Table 4. A closer look at Table 4 shows that all the three hypotheses (H1-H3) were confirmed. This concludes that Awareness, cyber- security policy and top management have a direct and negative effect on identity theft.

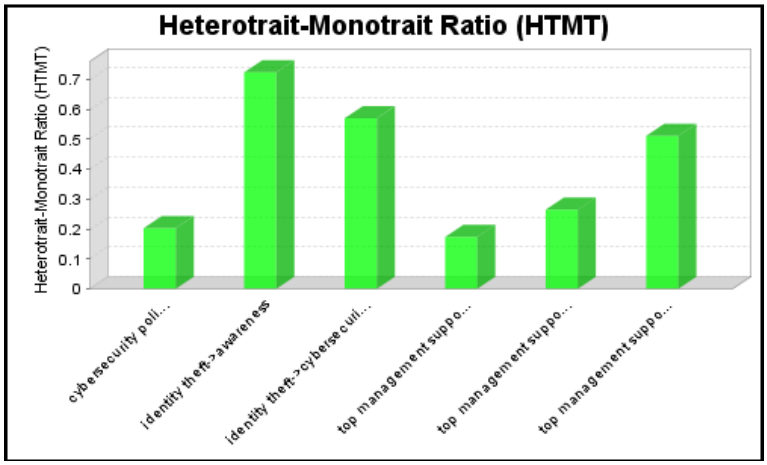

Fig. 3. Heterotrait-Monotrait ratio (HTMT)

Table 4. Path Coefficients

	Original Sample	t-Stat.	*p*-value	Decision
Awareness →Identity Theft	-0.545	10.43	0	Supported
Cybersecurity policy →Identity Theft	-0.308	4.209	0	Supported
Top Management Support →Identity Theft	-0.374	4.817	0	Supported

Determination of Coefficient R^2 The determination of coefficient R^2 indi- cates the share of the latent construct's explained variance, it therefore measures the regression function's goodness-of-fit against the empirically obtained manifest items. R^2 values ranges from 0 to 1, where larger values closer to 1 indicate a higher predictive accuracy or higher percentage of variance explained. The acceptable thresholds for R^2 nearer 0.19, 0.33 and 0.67 indicate a weak, moderate and substantial effect on the particular latent endogenous variable. Table 5 shows the R^2 value of 0.604 which suggest that 60.4% of the variance in identity theft can be explained by awareness, top management support and cybersecurity policy

Table 5. R^2 Coefficient

	R^2	Adjusted R^2	t-Statistics	*p*-value
Identity theft	0.604	0.594	7.573	0.000

6.4 The Standardized Root Mean Square Residual

The Standardized Root Mean Square Residual (SRMR) is a goodness of fit measure that was introduced by [7], it measures the difference between the observed and expected residual correlations. According to [6], a value of less or equal 0.10 is generally considered a good fit. In this study the SRMR was 0.08, confirming a good model fit.

7 Discussion

Cybersecurity is both a technical and human issue. Technical solutions alone would not eliminate cybercrime. Thus, the importance of the human factor should not be under estimated. The research analyses the impact of human factors i.e awareness, top management support and cybersecurity policy on identity theft. The findings indicate that all the human factors had a direct and negative impact on identity theft; awareness (β = -0.545, t-value = 10.300, and p-value = 0.000.), top management support (β = -0.374, t-value = 4.817, and p-value = 0.000.), cybersecurity policy (β = -0.308, *t*-value = 4.209, and *p*-value = 0.000). It is clear that cybercrime, in particular identity theft can be reduced in banking institutions if efforts were made to raise awareness, increase top management support and ensure good and sound cybersecurity policies are put in place.

8 Conclusion

The main objective of this study was to provide a model for analyzing human cybersecurity and its relationship to curbing cybercrime in the banking sector. The protection motivation theory, theory of reasoned action and the routine activity theory prescribed the guidelines for the analysis. Emphasis was put on the human factor as a key element of cybersecurity in the fight against cybercrime. This study analyzed survey data collected from 118 senior managers and employees from audit, risk and compliance department across 13 commercial banks in Zimbabwe. A Human-centric cybersecurity model was evaluated and it was empirically found that the human factors awareness (β = -0.545), top management support (β = -0.374) and cybersecurity policy (β = -0.308) had a negative and significant impact on identity theft.

Studies that have investigated the factors influencing cybercrime reduction in commercial banks of Zimbabwe are scarce. This study focused on addressing this knowledge gap. Theoretically the study extends the current body of knowledge by establishing that awareness, top management support and cyber-security policy all have significant and negative impact on identity theft. The study strengthened the understanding that cybersecurity must always consider the human factor. Practically, banking institutions are advised to seriously consider the human factor i.e raising awareness, providing top management support to cybersecurity and ensure cybersecurity policies are put in place if they need to meaningfully mitigate the risk of cybercrime. Cybercrime continues to be perpetrated despite the availability of technical solutions such as data encryptions, firewalls and antivirus scanners. A more fitting solution would be to combine both technical and human solutions in combatting cybercrime. Future work involves investigating the technical solutions impacting identity theft in commercial banks of Zimbabwe.

Compliance with Ethical Standards

Funding: This research was funded by Chinhoyi University of Technology, Zimbabwe.

Conflicts of Interest: All authors declare that they have no conflict of interest.

Ethical Approval: All procedures reported in this study were adhered to ethical standards.

Informed Consent: This study used data - survey responses related to consent.

Authors and Contributors: This work was carried out in close collaboration between co-authors. All authors have contributed to, seen and approved the final manuscript.

References

1. Alkalbani, A., Deng, H., Kam, B.: A Conceptual Framework for Information Security in Public Organizations for E-Government Development. In: Proceed- ings of the 25th Australasian Conference on Information Systems. ACIS (2014), http://aut.researchgateway.ac.nz/handle/10292/8031
2. Anupriya, K., Sebastian, M.P.: Understanding the Human, Managerial and Or- ganisational Aspects of Information Security Management: A Literature Review (2018)
3. Chitechi, V.K., Mbugua, S., Omieno, K., Mugisha Akandwanaho, S.: Facilitating Factors for Cybersecurity Vulnerabilities in Kenyan County Governments. Asian Journal of Research in Computer Sci- ence **2**(1), 1–11 (2018). https://doi.org/10.9734/AJRCOS/2018/45049,
4. Choejey,P.,Che Fung,C.,Wai Wong, K.,Murray, D.,Xie, H.:Cybersecurity Practices for E-Government:An Assessment in Bhutan. In: The 10th International Conference on e-Business (2015), https://pdfs.semanticscholar.org/7fa0/82bd6407f3502933f89c27d2b5212ab971d1.pdf
5. GHATE, S., AGRAWAL, P.K.: A Literature Review on Cyber Se- curity in Indian Context. Journal of Computer & Information Tech- nology **8**(05), 30–36 (oct 2017). https://doi.org/10.22147/jucit/080501, http://www.compitjournal.org/paper/348/a-literature-review-on-cyber-security- in-indian-context
6. Hair, j.F., Tomas, G., Hult, M., Ringle, C., Sarstedt, M.: A Primer on Partial Least Squares Structural Equation Modeling. Thousand Oaks:Sage, 2nd edn. (2017)
7. Henseler, J., Ringle, C.M., Sarstedt, M.: A new criterion for assessing discriminant validity in variancebased structural equation modeling. Journal of the academy of marketing science. Journal of the academy of marketing science **43**(1), 115 – 135 (2015)
8. Herath, T., Rao, H.: Protection motivation and deterrence: A framework for secu- rity policy compliance in organisations. European Journal of Information Systems **18**(106-125) (2009)
9. ITU: Definition of Cybersecurity (2018), https://www.itu.int/en/ITU- T/studygroups/com17/Pages/cybersecurity.aspx
10. Kharb, L.: Cyber Crimes Becoming Threat to Cyber Security. International Jour- nal of Engineering and Management Research **7**(2) (2017), www.ijemr.net
11. Korpela, K.: Improving Cyber Security Awareness and Training Pro- grams with Data Analytics. Information Security Journal: A Global Perspective **24** (2015). https://doi.org/10.1080/19393555.2015.1051676, http://www.tandfonline.com/action/journalInformation?journalCode=uiss20
12. Kuru, H., Ocak, M.A.: Determination of Cyber Security Aware- ness of Public Employees and Consciousness-rising Suggestions. Jour- nal of learning and teaching in digital age **1**(2), 57–65 (jul 2016), http://joltida.org/index.php/joltida/article/view/18
13. Mikolic-Torreira, I., Snyder, D., Price, M., Shlapak, D., Beaghley, S., Bishop, M., Harting, S., Oberholtzer, J., Pettyjohn, S., Weinbaum, C., Westerman, E.: Exploring Cyber Security Policy Options in Australia. Tech. rep. (2016), https://cybersecuritystrategy.dpmc.gov.au
14. Mugari, I., Gona, S., Maunga, M., Chiyambiro, R.: Cybercrime - The Emerg- ing Threat to the Financial Services Sector in Zimbabwe. Mediterranean Jour- nal of Social Sciences (may 2016). https://doi.org/10.5901/mjss.2016.v7n3s1p135, http://www.mcser.org/journal/index.php/mjss/article/view/9092
15. Neaimi, A.A., Tago Ranginya, P.L.: A CRITICAL ANALYSIS OF THE EF- FECTIVENESS OF CYBER SECURITY DEFENSES IN UAE GOVERN- MENT AGENCIES (2014), http://sdiwc.net/digital-library/a-critical-analysis-of- the-effectiveness-of-cyber-security-defenses-in-uae-government-agencies.html
16. Osho, O., Onoja, A.D.: National Policy and Strategy of Nigeria: A Qualitative Analysis The Cyber-state of Nigeria View project Cyber Forensics View project. Article in International Journal of Cyber Criminology (2015). https://doi.org/10.5281/zenodo.22390, https://www.researchgate.net/publication/282026229
17. Rajendran, S., Shenbagaraman, V.M.: A Study on Protection Motiva- tion Theory and Information Systems Security Policy Compliance. International Journal of Pharmaceutical Sciences Review and Research (2016), www.globalresearchonline.net
18. von Solms, R., von Solms, B.: From policies to culture. Computers & Security **23**(4), 275–279 (jun 2004). https://doi.org/10.1016/j.cose.2004.01.013, http://linkinghub.elsevier.com/retrieve/pii/S0167404804000331
19. Yunos, Z., Hamid, R.S.A., Ahmad, M.: Development of a cyber security aware- ness strategy using focus group discussion. In: 2016 SAI Computing Conference (SAI). pp. 1063–1067. IEEE (jul 2016). https://doi.org/10.1109/SAI.2016.7556109, http://ieeexplore.ieee.org/document/7556109/