International Journal of Scientific Research and Management (IJSRM)
||Volume||12||Issue||12||Pages||8037-8046||2024||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v12i12.em02

Factors That Influence Cybersecurity Compliance Behaviours by Bank Employees: A Case of Banks Operating In Kenya

CPA Dr. Leonard W. Wakoli

Jaramogi Oginga Odinga University of Science and Technology, School of Informatics and Innovative Systems,
P. O. Box 210 – 40601, Bondo - Kenya

Abstract
Digitization of transactions in Banks has developed exponentially since the advent of the internet technology. This has brought about efficiency and high quality service delivery at all times. However, cyber threats also continue to grow exponentially in spite of various initiatives to counter the threats. There are numerous technology initiatives to address the issue of cyber threats but the problem still persists. There is very limited research on how to leverage on human behaviours to effectively improve Cyber security compliance behaviours in Banks. Investigating Cyber security Compliance behaviours in Banks has therefore become inevitable. The main purpose of this study was to determine the factors that influence cyber security compliance behaviours in banks operating in Kenya. This was accomplished using a model that was based on an integration of three theories: Institutional Theory, the Protection Motivational Theory (PMT) and the General Deterrence Theory (GDT). In order to empirically test the relationships between the independent and dependent variables, data were collected from 75 purposively selected bank employees in Kenya. The Research was carried out using the mixed (both quantitative and qualitative) approach and survey tools used to collect data were verified for reliability and validity before being used. Data analysis was carried out using SPSS Version 25.0, MS Excel 2013, and WarpPLS (SEM) Version 7.0. The findings of our study indicate that the direct paths from the independent variables "Normative pressure" ($p = 0.026$, $\beta = 0.213$), "Self-Efficacy" ($p < 0.001$, $\beta = 0.440$), "Punishment certainty" ($p = 0.024$, $\beta = 0.217$), "Age" ($p = 0.013$, $\beta = 0.243$), "Prior experience with computers" ($p = 0.004$, $\beta = -0.284$) were found to have a positive, direct and significant influence on a bank employee cyber security compliance behaviours. "Top management commitment" was found to partially mediate between self-efficacy and Cyber security compliance behaviours.

Bank management may find the results useful for future policy formulation in relation to cyber-security compliance behaviours. Researchers and scholars may also find the results useful in terms of contribution to the body of knowledge and further investigation to fill the gaps identified by the study.

Keywords: cyber security, employees, human behaviours, bank, compliance

1. Introduction

A. 1.1 Background Information

Kenyan banks have completely embraced information and communication technology (ICT), collaborating with telecoms companies to fully use currency exchange and transmission systems. Mobile Banking (m-Banking), for example, is presently the most desired service across all Kenyan banks, since this technology has given users several platforms to handle their cash transactions. Banks have reaped the benefits as well; for example, they have increased their efficiency and reduced lengthy lines in banking halls, reducing the need for vast office space as consumers interact remotely. Customers may, for example, do business with their banks at any time and from any location with Internet access using m-banking. Despite this, innovation has its limits, which are manifested in cybercrime. Hacking, attacks, and other security breaches are on the rise, according to Bohme and Moore (2012); Arachchilage et al. (2014), as ICT usage continues.

Approximately 400,000 malware-related occurrences were recorded in Ghana's financial institutions in 2016 (Nir, 2019).

Kenya's situation is no better. According to the Serianu Report from 2019, Kenya's economy was hit by cyber-attacks in 2018, resulting in a loss of around KES 29.5 billion.

2. Literature Review

Cyber security compliance has been researched in both a corporate and a personal setting, according to several research findings. The assumption that the expectations of superiors and peers have a significant impact on compliance behaviour is supported by social influence and normative beliefs/pressures (Rao, 2009). Computer users, for example, are more prone to dismiss secure regulations and policies as simply procedures and instructions, rather than seeing them as standards that aid in Cyber security (Herath & Rao, 2009, as cited in Dinesh and Glenn, 2017).

Several determinants of cyber security compliance behaviours have been investigated in the past, including fear deterrence, fear appeals, user awareness, and many more, as Dinesh and Glenn observed (2017).

Users might be hesitant conformers, reluctant conformers, or enthusiastic conformers, according to Dinesh and Glenn (2017). To encourage unwilling conformers, strong deterrent tactics are required.

Fear appeals, social influence, and danger perception, among other things, may inspire hesitant conformers.

Willing conformers are driven to follow Cyber security rules and policies, but they may be hindered by a lack of knowledge of possible dangers, a lack of comprehension of security-related issues, and a lack of skills to safeguard information assets (Dinesh and Glenn) (2017).

Research Gaps

The impact of top management commitment on coercive pressure, normative pressure, mimetic pressure, gender, and self-efficacy is mostly unknown in the research. In addition, there is a study gap in the use of employee cyber security compliance behaviours in resolving cyber security challenges in banks. We performed an empirical quantitative study to fill this gap by examining the elements that impact bank employee cyber security compliance behaviours and determining the mediating effect of top management commitment to improve cyber security compliance behaviours in this study.

Although there has been a surge of interest in cyber security in recent years, little empirical study has looked at the subject of cyber security compliance behaviours in its entirety. Xiaofeng et al. (2018), for example, claim that previous efforts to integrate technology-based solutions with the human aspect in terms of cyber security compliance/non-compliance behaviours have failed. Poor findings on the human factor side have been reported, for example, in a research using the General Deterrence Theory (GDT), which might be due to a lack of moderating variables (D'Arcy and Herath, 2011). A Mediating variable, we believe, might be the solution to the problem.

Tim et al. (2009) discovered that perceived vulnerability, perceived serenity, response efficacy, and response cost all had a significant impact on users' intention to adopt anti-spyware protective technology in their study on application of Protective Motivation Theory to Adoption of Protective Technologies (Proceedings of the 42nd Hawaii International Conference on System Science – 2009). Self-efficacy, on the other hand, had no effect on a user's behavioural intention to use anti-spyware software, according to the research.

This conclusion was found to be in opposition to the role of self-efficacy in many PMT studies on health.

As a result, we thought it would be appropriate to research self-efficacy in a Bank setting.

Piyapong (2017) discovered that perceived severity had a significant influence on waste disposal behaviours and reuse and recycle behaviours, whereas perceived vulnerability had a significant effect on reuse and recycle behaviours in his study on the application of Protection Motivation Theory to investigate Sustainable Waste Management Behaviours (SWMBs).

What about the perceived severity of bankers' cyber security compliance behaviours? In terms of self-impact efficacy's on office employees, the study discovered that self-efficacy has a major impact on an office worker's motivation to participate in any and all forms of SWMBs. What about the impact of self-efficacy on bankers' cyber security compliance behaviours?

3. Methodology

In this study, we used the mixed method – both the quantitative and qualitative methodologies to examine the extent and type of relationships amongst coercive pressure, normative pressure, mimetic pressure, self-efficacy, perceived severity, punishment certainty, punishment severity, gender, age, prior experience with computers and cyber security compliance behaviours. The same approach was used to examine the mediating effect of top management commitment on coercive pressure, normative pressure, mimetic pressure, self-efficacy and gender. A cross sectional descriptive survey design was adopted with questions being asked once in the entire period of the research as described by Saunders et al. (2007).

Target Population

The survey was carried out by categorizing the banks into three groups for this study: Commercial domestic public banks, commercial domestic private banks, and commercial foreign banks are the three types of commercial domestic banks. A list was made accessible for each group, and the individuals were picked using a random numbers table, which can be found in many basic statistics manuals. A sample size formula found in many survey manuals was used to calculate the number of Banks in the sample.

Sampling Size

The Yamane Taro (1967) formula was employed in this investigation.

The required sample size is a function of the target population and the greatest allowed margin of error (also known as the sampling error), and it is defined mathematically as follows:

$$n = N/(1+ N^*(e)^2)$$

Where

n - The sample size,

N - The population size,

e - The acceptable sampling error

95% confidence level and p = 0.5 are assumed.

Hence $n = 43/(1 + 43^*(0.05)^2)$

$= 43/1.1075$

$= 38.826185$

~ 39

Hence the targeted number of respondents was 117 (3 per Bank for 39 Banks).

The research used a 5% margin of error, and 39 Banks were targeted by the use of questionnaires.

Data Collection Instruments

We used two instruments to collect data: a questionnaire and interviews.

Copies of raw data for the study are available upon request from the researcher.

Respondents indicated their responses to the questionnaire based on an ordinal Likert's 5-point scale ranging from 1 (strongly disagree) to 5 (strongly agree) to score the individual items in the instrument.

Pilot Study

Validity Of The Research Instrument

This study was carried out to improve the odds of success in the main study by evaluating the content validity and reliability of the instruments that would be utilized (Questionnaire and Interviews).

We used 10% of the sample size projected for the larger parent study as our sample size for our pilot study as recommended by Connelly (2008). Given that our study's sample size was 117, 10% of this value is approximately 12 respondents.

Main Study

The main study was conducted across 35 Banks from the initial sample of 39 Banks since 4 Banks participated in the pilot study and hence were excluded from the main study. Hence, a total of 105 respondents were purposively identified.

Reliability Of The Research Instrument

In this study, we tried to minimize bias and ambiguity to obtain valid and reliable data. The Research tool was revised several times after a series of discussions with peers to ensure reliability and validity.

Descriptive Statistics for Indicators

Table 4.1 shows the descriptive statistics for indicators

Table 4.1: Descriptive Statistics for Indicators

S/No.		Mean	SD	Min	Max	Median	Mode	Skewness	Exc Kurt	Normal? (Skewness)	Normal? (ExcKurt)
1	Age	3.613	0.853	2.000	5.000	4.000	3.000	0.170	-0.744	Yes	Yes

2	Gender	1.267	0.445	1.000	2.000	1.000	1.000	1.055	-0.886	No	No
3	Duration	2.800	1.027	1.000	5.000	3.000	3.000	-0.045	-0.494	Yes	Yes
4	Department	2.453	1.427	1.000	5.000	2.000	1.000	0.629	-0.944	No	No
5	Position	2.600	0.493	2.000	3.000	3.000	3.000	-0.408	-1.833	No	No
6	Terms	1.507	0.665	1.000	3.000	1.000	1.000	0.946	-0.263	No	No
7	CoerciveP1	4.667	0.475	4.000	5.000	5.000	5.000	0.707	-1.500	No	No
8	CoerciveP2	4.653	0.479	4.000	5.000	5.000	5.000	-0.644	-1.585	No	No
9	CoerciveP3	4.653	0.479	4.000	5.000	5.000	5.000	-0.644	-1.585	No	No
10	NormativP1	4.640	0.483	4.000	5.000	5.000	5.000	-0.583	-1.660	No	No
11	NormativP2	4.680	0.470	4.000	5.000	5.000	5.000	-0.772	-1.404	No	No
12	NormativP3	4.707	0.458	4.000	5.000	5.000	5.000	-0.908	-1.176	No	No
13	MimeticP1	4.707	0.458	4.000	5.000	5.000	5.000	-0.908	-1.176	No	No
14	MimeticP2	4.720	0.452	4.000	5.000	5.000	5.000	-0.980	-1.040	No	No
15	MimeticP3	4.600	0.520	3.000	5.000	5.000	5.000	-0.697	-0.870	No	No
16	PercvSev1	4.733	0.475	3.000	5.000	5.000	5.000	-1.431	0.919	No	No
17	PercvSev2	4.560	0.575	2.000	5.000	5.000	5.000	-1.308	2.951	No	No
18	PercvSev3	4.387	0.517	3.000	5.000	4.000	4.000	0.168	-1.290	Yes	Yes
19	SelfEffc1	4.000	0.986	2.000	5.000	4.000	5.000	-0.595	-0.743	No	Yes
20	SelfEffc2	3.747	1.001	2.000	5.000	4.000	4.000	-0.534	-0.735	Yes	No
21	SelfEffc3	3.613	0.943	2.000	5.000	4.000	3.000	-0.038	-0.909	Yes	Yes
22	PuniSev1	4.520	0.554	4.000	5.000	5.000	5.000	-0.559	-0.793	No	No
23	PuniSev2	4.493	0.503	3.000	5.000	4.000	4.000	0.027	-1.999	No	No
24	PuniSev3	4.467	0.528	1.000	5.000	4.000	4.000	-0.143	-1.360	No	Yes
25	PuniCert1	3.600	0.615	1.000	5.000	4.000	4.000	-0.912	2.571	No	No
26	PuniCert2	3.640	0.799	1.000	5.000	4.000	4.000	-0.544	1.481	No	No
27	PuniCert3	3.893	0.481	3.000	5.000	4.000	4.000	-0.295	1.027	Yes	No

28	TopMaC1	4.240	0.516	3.000	5.000	4.000	4.000	0.277	-0.237	Yes	No
29	TopMaC2	4.147	0.485	3.000	5.000	4.000	4.000	0.372	0.695	Yes	No
30	TopMaC3	4.093	0.440	3.000	5.000	4.000	4.000	0.466	1.793	No	No
31	PriorExp1	4.267	0.528	2.000	5.000	4.000	4.000	-0.365	2.799	No	No
32	PriorExp2	4.453	0.501	4.000	5.000	4.000	4.000	0.187	-1.965	No	No
33	PriorExp3	4.533	0.502	4.000	5.000	5.000	5.000	-0.134	-1.982	No	No
34	PriorExp4	4.587	0.496	4.000	5.000	5.000	5.000	-0.352	-1.876	No	No
35	CybsecCB1	3.840	0.806	3.000	5.000	4.000	3.000	0.296	-1.383	No	Yes
36	CybsecCB2	4.587	0.522	3.000	5.000	5.000	5.000	-0.637	-0.960	No	No
37	CybsecCB3	3.520	1.319	1.000	5.000	4.000	3.000	-0.666	-0.500	No	Yes

Source: Researcher (2022

6. Inferential Statistics

Reliability and Validity Model Assessment (Confirmation Factor Analysis)

Composite Reliability

Composite reliability and Cronbach's alpha were determined to be greater than 0.6 and 0.7, respectively (see table 3.3).

This condition was met by all latent variables except for Coercive pressure (0.028), Normative pressure (0.000), Mimetic pressure (0.024), and Top management commitment (0.168). (0.127). The remainder was as follows: Sanctions severity (0.658), Sanctions certainty (0.732) Prior experience with computers (0.850) Age distribution (1.000), self-efficacy (0.787), and Cybersecurity Compliance Behaviours (0.613).

Convergent Validity

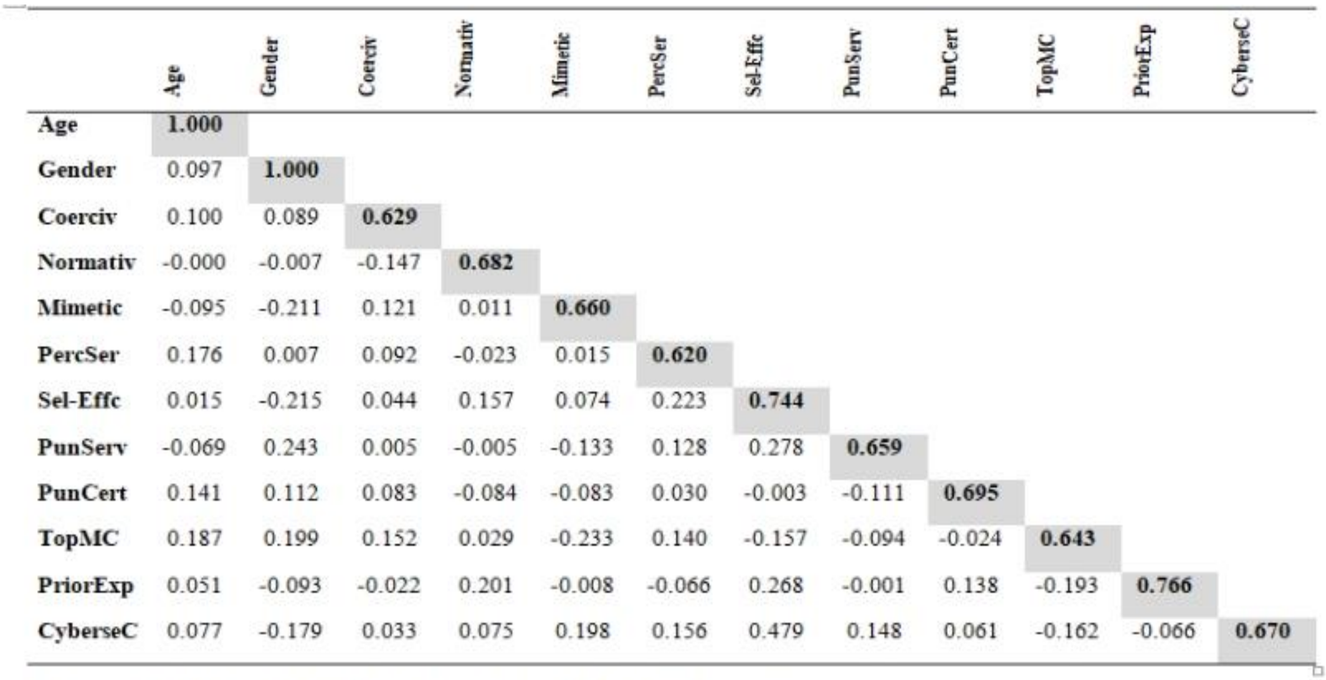
When PLS-SEM is utilized, the minimal need for indicator loading in a model is 0.70 (Hair et al (2017a). This is because the square of that value (0.70) is nearly equal to the variable variation divided by 0.5 (50 percent). It was recommended to eliminate indicators with factor loadings ranging from 0.40 to 0.70. The minimal AVE value is 0.50, indicating that more than 50% of indicator variance is explained by the concept score.

The values found were as follows: Coercive pressure (0.642), Normative pressure (0.565), Mimetic pressure (0.535), Self-efficacy (0.554), Gender (1.000), Punishment certainty (0.483), Perceived severity (0.385), Punishment severity (0.434), Top management commitment (0.414), Prior computer experience (0.586), Age-range (1.000), and Cyber security Compliance Behaviours (0.559). As a result, the majority of constructions met the requirement.

Discriminant/Divergent Validity

The results of the calculation in Table 4.3 indicate that the value The AVE of each component is more than the correlation between the research concepts, implying that the discriminant validity of all constructs used in this investigation was satisfactory (Ghozali & Latan, 2014). Simply put, there is evidence for high validity because each square root of the average variance extracted (AVE) indicated on the diagonal is bigger than the value to its left in the same row and also greater than the value to its right in the same column

Table 4.3: Correlations among Lvs with square roots of AVEs



	Age	Gender	Coerciv	Normativ	Mimetic	PercSer	Sel-Effc	PunServ	PunCert	TopMC	PriorExp	CyberseC
Age	**1.000**											
Gender	0.097	**1.000**										
Coerciv	0.100	0.089	**0.629**									
Normativ	-0.000	-0.007	-0.147	**0.682**								
Mimetic	-0.095	-0.211	0.121	0.011	**0.660**							
PercSer	0.176	0.007	0.092	-0.023	0.015	**0.620**						
Sel-Effc	0.015	-0.215	0.044	0.157	0.074	0.223	**0.744**					
PunServ	-0.069	0.243	0.005	-0.005	-0.133	0.128	0.278	**0.659**				
PunCert	0.141	0.112	0.083	-0.084	-0.083	0.030	-0.003	-0.111	**0.695**			
TopMC	0.187	0.199	0.152	0.029	-0.233	0.140	-0.157	-0.094	-0.024	**0.643**		
PriorExp	0.051	-0.093	-0.022	0.201	-0.008	-0.066	0.268	-0.001	0.138	-0.193	**0.766**	
CyberseC	0.077	-0.179	0.033	0.075	0.198	0.156	0.479	0.148	0.061	-0.162	-0.066	**0.670**

Note: Square roots of average variances extracted (AVEs) shown on diagonal.
Source: Researcher (2022)

Path Coefficient Estimates
Figure 4.1 shows the inner model path coefficient sizes (β values) and significance (p-values).

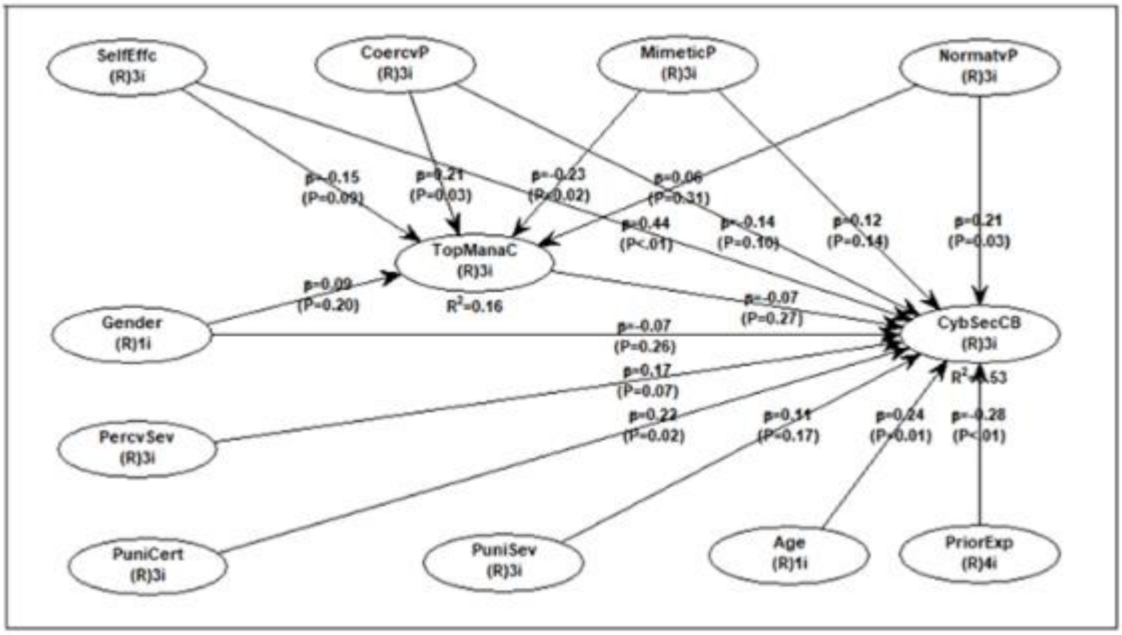


Figure 4.1: PLS-SEM Path Analysis
Source: Researcher (2022)

As illustrated in Figure 4.1, the inner model indicates that coercive coercion has a negative and insignificant effect on bank workers' cyber security compliance behaviours (p = 0.103, = -0.141). Normative pressure appears to have a favourable and significant effect on bank workers' cyber security compliance behaviours (p = 0.026, = 0.213). Mimetic pressure appears to have a beneficial but insignificant effect on bank workers' cyber security compliance behaviours (p = 0.143, = 0.119). Self-efficacy appears to have a significant favourable effect on bank workers' cyber security compliance behaviours (p 0.001, = 0.440). Gender appears to have a negative and insignificant effect on bank workers' cyber security compliance behaviours (p = 0.263, = -0.072). Perceived severity appears to have a favourable but insignificant effect on bank workers' cyber security compliance behaviours (p = 0.066, = 0.167). Certainty of punishment appears to have a favourable and significant effect on bank workers' cyber security compliance behaviours (p = 0.024, = 0.217).

Hypothesis Testing

Table 4.5 shows the results of the hypothesis testing

Table 4.5: Hypotheses Testing Results

Hyp Code	Hypothesis Description	Supported/Unsupported
Ho1	Coercive pressure has no significant influence on the Cyber security Compliance behaviours of bank employees in Kenya	Supported
Ha1	Coercive pressure has a significant influence on the Cyber security Compliance behaviours of bank employees in Kenya	Unsupported
Ho2	Normative pressure has no significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Unsupported
Ha2	Normative pressure has a significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Supported
Ho3	Mimetic pressure has no significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Supported
Ha3	Mimetic pressure has a significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Unsupported
Ho4	Self-efficacy has no significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Unsupported
Ha4	Self-efficacy has a significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Supported
Ho5	Gender difference has no significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Supported
Ha5	Gender difference has a significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Unsupported
Ho6	Perceive severity has no significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Supported
Ha6	Perceive severity has a significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Unsupported
Ho7	Punishment certainty has no significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Unsupported
Ha7	Punishment certainty has no significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Supported
Ho8	Punishment severity has no significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Supported
Ha8	Punishment severity has no significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Unsupported
Ho9	Age diffence has no significant influence on the Cyber security compliance behaviours of bank employees in Kenya	Unsupported
Ha9	Age diffence has a significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Supported
Ho10	Prior experience with computers has no significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Unsupported
Ha10	Prior experience with computers has a significant influence on the Cyber security compliance behaviours of bank employees in Kenya.	Supported
Ho11	Top Management commitment has no significant effect on Cyber security Compliance Behaviours of the bank employees in Kenya.	Supported

Ha11	Top Management commitment has a significant effect on Cyber security Compliance Behaviours of the bank employees in Kenya.	Unsupported
Ho12	Top Management commitment has no significant mediating effect on Coercive pressure.	Supported
Ha12	Top Management commitment has a significant mediating effect on Coercive pressure.	Unsupported
Ho13	Top Management commitment has no significant mediating effect on Normative pressure.	Supported
Ha13	Top Management commitment has a significant mediating effect on Normative pressure.	Unsupported
Ho14	Top Management commitment has a significant mediating effect on Mimetic pressure.	Supported
Ha14	Top Management commitment has a significant mediating effect on Mimetic pressure.	Unsupported
Ho15	Top Management commitment has no significant mediating effect on Gender	Supported
Ho15	Top Management commitment has a significant mediating effect on Gender	Unsupported
Ha16	Top Management commitment has no significant mediating effect on Self-efficacy.	Unsupported
Ha16	Top Management commitment has a significant mediating effect on Self-efficacy	Supported

Source: Researcher (2022)

Research Model for Cyber Security Compliance Behaviours

The proposed Model for Cyber security Compliance Behaviours has 10 independent latent variables: coercive pressure, normative pressure, harshness of punishment, top management commitment, and self-efficacy. At the same time, top management commitment was analyzed as a mediating latent variable. The ability of top management commitment to mediate Coercive and Normative pressure was examined. The developed model is depicted in Figure 4.1.

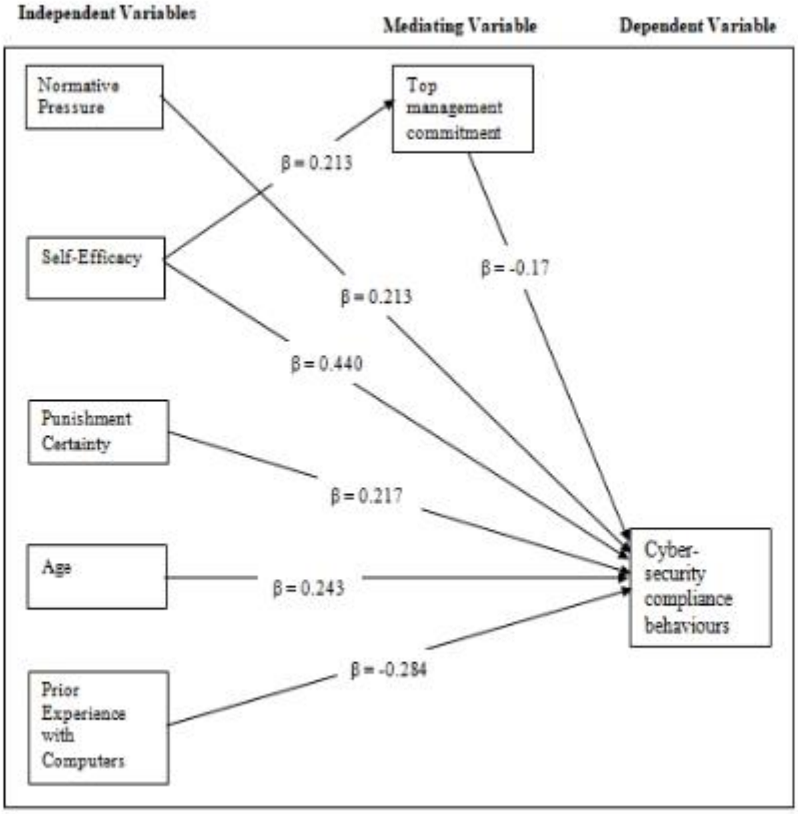


Figure 4.1: Research Model
Source: Researcher (2022)

Discussion of Results

The study's outcome is a model that banks may apply to improve their cyber-security compliance behaviours, hence increasing cyber-security (see Figure 5.16).

The created model is based on Rogers's (1983) Protection Motivation Theory, DiMaggio and Powell's General Deterrence Theory, and the Institutional Theory (1983). The model was developed by integrating these three notions (see Figure 5.16).

The model establishes a link between top management commitment and cyber-security compliance behaviours, normative pressure and cyber-security compliance behaviours, coercive pressure and cyber-security compliance behaviours, severity of punishment and cyber-security compliance behaviours, and self-efficacy and cyber-security compliance behaviours.

The rationale for this integration is that the three theories of protective motivation, general deterrence, and institutional theory have all been found to be beneficial in the management of information security in businesses on their own. There have been very few studies integrating the three theories and evaluating their utility in managing information security within enterprises and government bodies.

In general, the path analysis findings demonstrate that the independent factors normative pressure, harshness of punishment, self-efficacy, and top management commitment all predict the dependent variable - cyber-security compliance behaviours. Coercive pressure, on the other hand, is not a predictor of cyber-security compliance behaviour. Additionally, neither coercive nor normative pressure predicts top management commitment

Conclusion

The factors that influence Cyber security compliance behaviours positively were found to be Normative pressure, Self efficacy, punishment certainty and age. Top management commitment was found to partially influence cyber security compliance behaviours. However, prior experience with computers was found to influence negatively influence cyber security compliance behaviours.

References

1. Arachchilage, N. A. G., & Love, S. (2014). Security awareness of computer users: A phishing threat avoidance perspective. *Computers in Human Behaviours*, *38*, 304-312.
2. Babbie, ER (2004). The Practice of Social Research – 10th Edition Journal of
3. Asynchronous Learning Networks (JALN), 4(2) 7-41, available at http://www.sloan-c.org/publications/jaln/v4n2/pdf/v4n2_fredericksen.pdf.
4. Beniteza J., Henseler J., Castillo A., Schuberth F. How to perform and report an impactful analysis using partial least squares: Guidelines for confirmatory and explanatory IS research. Information & Management 57(2020) 103168 Available at https://doi.org/10.1016/j.im.2019.05.003 [Accessed on 23/07/2022]
5. Bohme, R., & Moore, T. (2012). *Challenges in empirical security research*. Technical report, Singapore Management University.
6. Boss S. R., Galletta D. F., Lowry P. B., Moody G. D., Polak P., What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors, MIS Q. 39 (4) (2015) 837–864
7. Connelly, L. M. (2008). Pilot studies. Medsurg Nursing, 17(6), 411-412.
8. Dinesh Reddy & Glenn Dietrich. Cyber security Training and the End-User: Pathways to Compliance Journal of The Colloquium for Information System Security Education (CISSE) Edition 5, Issue 1 - October 2017
9. Fornell, C. & Larcker D. F. (1881). Evaluating structural equation models with unobservable variables and measurement error. JMR, JOURNAL OF Marketing Research, 18(1), 39-50. doi: 10.2307/3151312

10. Hayduk L., Shame for disrespecting evidence: the personal consequences of insufficient respect for structural equation model testing, BMC Med. Res. Methodol. 14 (124) (2014) 1–10.
11. Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. Journal of the Academy of Marketing Science, 43(1), 115–135. https://doi.org/10.1007/s11747-014-0403-8
12. Herath T, Rao HR. Encouraging information security behaviors in organisations:Role of penalties, pressures and perceived effectiveness. Decision Support Systems. 200; p. 154-165.
13. Lynne, Pam Briggs, John Blythe and Minh. Using behavioural insights to improve the public's use of cyber security best practices – 2014 Available at https://www.gov.uk/go-science [Accessed on 12/03/2022]
14. Saunders, M., Lewis, P. & Thornhill, A. (2012) "Research Methods for Business Students" 6th edition, Pearson Education Limited
15. Serianu (2019) Kenya Cyber security Report 2019 Nairobi, Kenya: Serianu Cyber Threat Intelligence Team. Available at: https://www.serianu.com/downloads/KenyaCyberSecurityReport2019.pdf [Accessed on 23/9/2022]
16. Tim Chenoweth, Robert Minch & Tom Gattiker; Application of Protection Motivation Theory to Adoption of Protective Technologies proceedings of 42nd Hawaii International Conference on System Science – 2009.
17. Vijayan J., Target Breach Happened Because of a Basic Network Segmentation Error, Computerworld, Feb. 6, 2014, available online at http://www. computerworld.com/article/2487425/cybercrime-hacking/target-breachhappened-because-of-a-basic-network-segmentation-error.html
18. Xiaofeng Chen, Dazhong Wu, Liqiang Chen, Joe Teng K. L..(2018) Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables Information & Management journal Available at: www.elsevier.com/locate/im [Accessed on 12/09/2022]

Author Profile

Dr. CPA Leonard Wakoli, PhD.

CPA Dr. Leonard Wakoli is currently a Lecturer at Jaramogi Oginga Odinga University of Science & Technology (JOOUST), School of Informatics & Innovative Systems (SIIS). He is the Acting Dean, School of informatics and innovative systems. Leonard has a PhD in Information Technology (IT) Security and Audit from Jaramogi Oginga Odinga University of Science and Technology, a Master of Science in Software Engineering, a Bachelor of Science Degree in Mathematics and Computing, a a Post Graduate Diploma in the Management of Information Systems from University of Greenwich UK, a Diploma in Science Education (Mathematics & Physics). Leonard is also a Certified Public Accountant - CPA(K).