A MODEL FOR ASSESSING THE URBAN COMMERCIAL BANKS EMPLOYEES' CYBER SECURITY ETHICAL BEHAVIOUR IN UGANDA.

NAKATO RUTH

2016/PhD/029/PS

A THESIS SUBMITTED TO THE FACULTY OF COMPUTING AND INFORMATICS IN FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF DOCTOR OF PHILOSOPHY OF MBARARA UNIVERSITY OF SCIENCE AND TECHNOLOGY

MARCH 2023

DECLARATION

I hereby declare that this thesis is my original work and has never been submitted to any other institution of higher learning for any academic award to the best of my knowledge.

Signature: .....

Date: 15/3/2023

Approval

This is to certify that this research thesis has been submitted to the higher Degrees department for examination with the approval of the Supervisors:

Prof. Mayoka. G. Kituyi,Ph.D.

Faculty of Computing and Informatics

Makerere University Business School

Signature.....

Date 13/03/2023

Dr. Fred Kaggwa

Faculty of Computing and Informatics

Mbarara University of Science and Technology

Signature.....

Date 13/03/2023

Dedication

This dissertation is dedicated to God The Almighty who gave me the breath and life to see it complete.

To my Parents, Dinah Kemirembe Nalongo and the late Eliasaph Tibirekwa Salongo. You believed in education and you would tell me "***OBUTASHOMA BWINE AKAKWATE NOBWORO" meaning; Illiteracy is Related to Poverty***. You were always proud of me. And I am sure I have kept you proud.

To my beloved husband for believing in me when I struggled to believe in myself. I will never let You down I will always be on your side.

To my Handsome Sons; Dr. Rodney Bashabe, Albert Agaba, Rhene Didas Keita and my Beautiful Daughter Nicole Atuhairwe. You are a blessing to the Family and our little Angels.

Alibakabya amaziga Katonda alimukabya omusayi.

Acknowledgement

I thank God most of all, because without God I wouldn't be able to do any of this. Thank You LORD for Everything. I would like to say a very big thank you to my supervisors Assoc. Prof. Mayoka. G. Kituyi and Dr. Fred Kaggwa, for all the support and encouragement they gave me while writing this Thesis. Without their guidance and constant feedback this PhD thesis would not have been achievable.

The greatest thanks go to my Awesome husband Didace! You encouraged me take on this work! Didace you read the early drafts, edited and gave me advice on almost all the sections in this thesis. You are as important to this work getting done as I am. Thanks for all the support, the honest feedback, and for everything else you do to make my life Amazing! Thank you so much, beloved."

I gratefully acknowledge the funding received towards my PhD from the African Development Bank (AfDB) - Support to Higher Education, Science and Technology (HEST) PROJECT ACADEMIC STAFF SCHOLARSHIP.

Thanks to Prof. Nixon Kamukama, Prof. V. Batwala and Dr. Evarist Nabaasa for your encouragement. Thanks to Prof. Annabella Habinka Ejiri, for reading every sentence of this work, edited it and you gave me constructive feedback, thank you. I want to thank Prof. Paul Ssemalulu, Dr. Jane Katusiime, Dr. Deborah Natumanya, Dr. Simon Kawuma, Dr. Pius Ariho, for all the encouragement and efforts provided towards making this PhD thesis a better one.

To everyone at Mbarara University of Science and Technology (MUST), who enable me to be one of the best lecturers of a University that I'm honored to be a part of, thank you for letting me serve, for being a part of our astonishing University. Thank you to everyone who strives to grow and help others grow. Without the experiences and support plus ideas and criticism from my peers and entire team at the Faculty of Computing and Informatics this research thesis would not exist. Thank you FCI Team Members.

To all the individuals and the students, I have had the opportunity to inspire, lecture, be lectured by, or watch my lecturing from a far, I want to say thank you for being the inspiration and foundation for my career manifesto. I want to thank EVERYONE who ever supported me in anyway, said anything positive to me or taught me something. I heard it all, and it meant something.

Last but not the least, I thank all my respondents from ABSA and Centenary Banks' branches in Kampala, for sparing your precious time to fill my lengthy questionnaire. You are the reason this research is complete. I thank you all.

Good moral character is the first essential in a man. ***George Washington***

Contents

Approval i

Dedication iii

Acknowledgement iv

List of figures xi

List of acronyms. xiv

CHAPTER ONE: INTRODUCTION 1

1.1 Background to the Study 1

1.2. Theoretical background 3

1.2.1 Philosophical theories 3

1.2.2. Theory of Planned Behavior (TPB) 5

1.3. Definition of Key Operating Terms 7

1.4 The Context of employees' ethical behavior and Cyber security breaches in the banking sector 9

1.5 Problem Statement 14

1.6. Justification 15

1.7. Main objective 16

1.7.1 Specific Objectives 16

1.8 Research Questions 16

1.9 Scope of the study 17

1.9.1 Subject Scope of the study 17

1.9.2 Geographical scope 17

1.10. Outline of the Thesis. 18

CHAPTER TWO: LITERATURE REVIEW 19

Introduction 19

2.1. Employees' Ethical Behavior and Cyber security 19

2.2. Types of Information Security Behaviors in Organizations 20

2.3 The effect of Cyber security breaches in organizations. 21

2.4 Cyber security Technical Protection Measures are ineffective 24

2.5 Cyber security Goals 26

2.5.1 The Availability, Integrity and Confidentiality of Cyber Assets 26

2.6. Cybersecurity in Developed Countries compared to Developing Countries. 28

2.7. The importance of Cyber security in the modern banking sector 29

2.8. Cyber security strategies in Uganda 32
2.9. Factors affecting Cyber security protections in Uganda 34
2.10. Philosophical Theories of Ethics 35
2.10.1. Consequentialism 36
2.10.2. The deontological class of ethical theories 36
2.10.3. The virtue ethics theories 38
2.11. Theories for Ethical behavior 40
2.12. Conceptual Framework and Developing Hypotheses. 51
2.12.1 Prudence and behavior intention 53
2.12.2 Temperance and behavior intention 54
2.12.3. Courage and behavior intention 55
2.12.4. Justice and behavior intention 56
2.12.5. Ethical Climate and Ethical Behavior 57
2.13. Cyber security ethical behavior intention and improved Cyber security ethical behavior. 60
2.14. Approaches to Cyber security ethical behavior Assessment 63
CHAPTER THREE: METHODOLOGY 65
Introduction 65
3.1 Philosophical Foundation (Philosophy, the Love of Knowledge) 65
3.1.1 Research Paradigm 65
3.1.2 Positivism paradigm 67
3.1.3 Epistemology of positivism 68
3.1.4 The Ontology of Positivism; (ontology the Theory of Being) 70
3.2 Research design 71
3.3 A Research Approach 72
3.3.1 Dual essential paradigms 72
3.3.2 Employing Design Science in this Research 72
3.4 Awareness of the Problem: Objective 1 methods 77
3.4.1. Employing Behavioral Science in this Research 77
3.4.2 Study Population 78
3.4.3 Sampling design and procedure 79
3.4.4 Questionnaire Design 80
3.4.5 Stages of Research Study 81
3.4.6. Reliability and validity of instruments 82

3.4.7. Unit of Analysis and Inquiry 83
3.4. 8. Data and sources 84
3.4.9. Data Collection Methods 85
3.5. Approach to establishing the influence of cardinal virtues moderated by ethical climate on Cyber security ethical behavioral intentions in commercial banks in Uganda. (Objective one methods) 86
3.5.1 Participants 86
3.5.2. Instrumentation 86
3.5.3 Measurement of Constructs 88
3.5.4 The cardinal virtue Constructs 88
3.5.5 Data Processing and Analysis 91
3.7 Confirmatory Factor Analysis (CFA) & Structural equation modelling 96
3.8 Evaluation of measurement model 97
3.9 Suggestions to the Solution 99
3.9.1 A Conceptual Framework of the Proposed Solution 99
3.10 Phase 3: Artifact development 100
3.10.1. Objective two; Approach to developing an employees' Cyber security ethical behavior assessment model for commercial banks in Uganda. 100
3.10.2 Requirement gathering and analysis 101
3.10.3 Model design 101
3.10.4 Model Development 101
3.11. Ethical Considerations 103
3.12 Consent from participants to carry out the study on them 103
3.13 Confidentiality of the respondents 103
3.14. Permission to carry out the study 104
3.15 Acknowledging information sources and materials 105
3.16 Chapter Conclusion 105
CHAPTER FOUR: PRESENTATION AND DISCUSSION OF FINDINGS 106
Introduction 106
4.1 Data Analysis 106
4.1.1 Demographic Data 106
4.1.2 Respondents Gender 106
4.1.3 Respondents age group 107
4.1.4 Respondents' bank 108

4.1.5 Respondents Education level 108
4.1.6 Speciality 109
4.1.7. Current professional role 109
4.2 Data cleaning 110
4.2.1 Outliers 110
4.2.2. Test for Statistical Normality 110
4.2.3. Test of homogeneity of variance 111
4.2.4. Test for Linearity 111
4.2.5 Test for Multicollinearity 112
4.2.6 The Standardized Root Mean Square Residual (SRMR) 113
4.2.7 Path Weight 113
4.2.8 p-value 114
4.3 Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) 114
4.3.1 Exploratory Factor Analysis 114
4.3.2 Confirmatory Factor Analysis (CFA) 123
4.3.3 Estimation of Total Effects: The Original Structural Equation Model 136
4.3.4 Estimation of mediation effect (Indirect Effects) for the Original Structural Equation Model 137
4.4 Hypotheses Testing 138
4.4.1 Moderation test results; Modgraphs 139
4.5 Summary of Findings 143
CHAPTER FIVE: DISCUSSION OF FINDINGS 147
Introduction 147
5.1 Findings for objective 1 147
5.2 Estimation of mediation relationships (Indirect Effects) for the final Structural Equation Model 153
5.3 Discussion for objective 2 154
5.4 Discussion for objective 3 155
5.5 Conclusions 155
CHAPTER SIX: DEVELOPMENT OF THE MODEL 158
Introduction 158
6.1 Description of the ECEBA model 158
6.1.1 Requirements for the ECEBA model 160
6.1.2. The ECEBA Modules (Architecture) 160

6.2 The ECEBA Model Architecture 160
6.3 ECEBA Model design tools 164
6.3.1The ECEBA Use Case Diagram 164
Eceba Model reaction to the Use Case 164
6.4 Non-Functional requirements for Ethica Application 168
6.4.2 Sequence diagram 168
6.5 The Ethica Web based System's Requirements 170
6.5.1 Software requirements 170
6.5.2 Software Specifications 171
6.6 Architectural design 171
6.6.1 Account of the Designed System 171
6.7 System Flow 172
6.7.1 System Flow Chart 172
6.8. Database Design 173
6.8.1. Entity Relationship Diagram (EERD) 173
6.9 Graphical User Interface 175
6.9.1 User Login Interface 175
6.9.2 New Staff/Employee registration form 176
6.9.3 Attempting a questionnaire 178
6.10 Marking and tot up 179
6.10.1 Computing the Employee Assessment Score (EAS) 179
6.10.2 Computing the Maximum Score Possible (MsP) 179
6.10.3 Computing the Total Response Score (TrS) 180
6.10.4 Computing the Final Assessment Results (FaR) 180
6.10.5 Determining the Employee Recommendation 180
6.10.6 Assessment Results 181
6.10.7 Complete assessment Certificate 182
6.11 Ethica Application Testing 183
6.11.1 Individual Component Testing 183
6.11.2 Entire model Testing 183
6.11.3 Usability Testing 183
6.12 Usability Testing Results 184
6.12.1 User Friendliness 184

6.12.2 Usefulness of the System 184
CHAPTER SEVEN: STUDY CONCLUSIONS, RECOMMENDATIONS AND IMPLICATIONS 185
Introduction 185
7.1 Study Conclusion 185
7.2 Implications 187
7.2.1 implications to theory 187
7.2.2. Practitioner Implications 188
7.2.3. Researcher Implications 190
7.2.4 Research contributions 190
7.2.5 Limitations of the study 191
7.2.6 Data collection Challenges 193
7.3 Recommendations and Future Research 194
7.3.1 List of papers 196
REFERENCES 197
7.5 Appendices 214
7.5.1 Appendix A 214
7.5.2 Appendix B 215
7.5.3 Appendix C; Survey Instrument 217
An Employees' Cyber Security Ethical Behavior, ethical Climate and Influences Survey 217
7.5.3.3 SECTION A: BACKGROUND INFORMATION 218
7.5.4 Appendix D Research Ethics approval from Mbarara University of Science and Technology 228
7.5.5 Appendix E Research Approval: from Uganda National Council For Science and Technology 230
7.5.6 Appendix F Research Approval: from Centenary Bank 231
7.5.7 Appendix G Research Approval: from ABSA Bank. 232
7.5.8 Appendix H Missing Values Outliers 233
7.5.9 Appendix I A list of commercial banks in Uganda 238
7.5.10 Appendix J Usability questionnaire 239

List of figures

Figure 1. 1 Theory of Reasoned Action (TRA) (Ajzen and Fishbein (1969,1980) 5
Figure 1. 2 Theory of Planned Behavior components, (Icek Ajzen 2019). 6

Figure 2. 1 Normative Ethical Theories' components 35
Figure 2. 2 Theory of Reasoned Action components 40
Figure 2. 3 Showing the Extended TRA to include Behavior control construct. 42
Figure 2. 4 Theory of Planned Behavior components, (Icek Ajzen 2019). 45
Figure 2. 5 Components of Contingency Framework for Understanding Ethical Decision Making in Marketing. 46
Figure 2. 6 A Theoretical Model for Ethical and Unethical Decision Making (Bommer et al. 1987). 47
Figure 2. 7 The Hunt-Vitell General Theory of Ethics components, (Hunt & Vitell 1986). 48
Figure 2. 8 General Deterrence Theory (GDT). 49
Figure 2. 9 A theoretical model derived from the general deterrence theory. 50
Figure 2. 10 A conceptual frame work. 52

Figure 3. 1 Stages of deductive approach. 69
Figure 3. 2 Design science research process model Source: Adapted from (Hevner & Chatterjee, 2010; Vaishnavi, V. & Kuechler, 2007). 76

Figure 4. 1 Ethical virtues. 126
Figure 4. 2 Ethical Climate. 129
Figure 4. 3 Behavioral intentions and Actual Ethical Behavior. 132
Figure 4. 4 Ethical Behaviour. 134
Figure 4. 5 The Original Structural Equation Model. 135
Figure 4. 6 Moderation Effect of ethical climate on cardinal virtue constructs and ethical behaviour. 139

Figure 5. 1 Final model. 151

Figure 6. 1 The ECEBA model architecture. 163
Figure 6. 2 The ECEBA use case; diagram. 164
Figure 6. 3 illustrates how Eceba model is used during employees' cyber security ethical behavior assessment. 166
Figure 6. 4 The Ethica web based Application Development to test ECEBA model. 169
Figure 6. 5 Showing the Flow of the system, system users and their designated tasks. 172
Figure 6. 6 An Enhanced Entity-relationship diagram showing database entities and their relationships. 174
Figure 6. 7 System Login Interface. 175
Figure 6. 8 New User Account Creation Interface. 176
Figure 6. 9 Attempting the questionnaire. 178

Figure 6. 10 Assessment Results. 181
Figure 6. 11 Complete assessment Certificate. 182

List of tables.

Table 1. 1 Recent Cyber Security Breaches in Ugandan Commercial Banks 11
Table 1. 2 Data Breaches in Finance industry in developed countries (Kost, 2022) 12

Table 2. 1 Showing the Theoretical Gap Analysis. 50
Table 2. 2 Theoretical Types of Ethical Climate (Victor & Cullen, 1988 p. 668). 57

Table 3. 1 Summarized Comparison of Research Viewpoints in Social Sciences Research; (Paulinus &Eaton 2013). 66
Table 3. 2 Some Key Terms and Definitions Related to Understanding the Research Paradigm of Positivism (Park et al., 2020). 67
Table 3. 3 Design-science research guidelines Source: (Hevner et al., 2004). 73
Table 3. 4 Sample Size of Respondents and Sampling Technique. 80
Table 3. 5 Test of homogeneity of variance. 94
Table 3. 6 Multicollinearity. 95

Table 4. 1 Respondents Gender. 107
Table 4. 2 Respondents age. 107
Table 4. 3 Respondents' bank. 108
Table 4. 4 Respondents Education level. 108
Table 4. 5 Speciality. 109
Table 4. 6 Current professional role. 109
Table 4. 7 Test for Normality. 110
Table 4. 8 Test of homogeneity of variance. 111
Table 4. 9 shows bivariate correlation analysis results. 112
Table 4. 10 Estimates of the Variance Inflation Factor (VIF). 113
Table 4. 11 Rotated component matrix for Cardinal Virtue Constructs. 115
Table 4. 12 Rotated component matrix for ethical climate Constructs. 117
Table 4. 13 The exploratory factor analysis of ethical Behavioral Intentions constructs. 121
Table 4. 14 The exploratory factor analysis of ethical Behavioral Intentions constructs. 122
Table 4. 15 Indicator validity. 127
Table 4. 16 Construct reliability and validity. 128
Table 4. 17 Fornell-Larcker Criterion/Test for discriminant validity. 128
Table 4. 18 Indicator validity. 130
Table 4. 19 Construct Reliability and validity. 131
Table 4. 20 Fornell-Larcker Criterion/Test for discriminant validity. 132
Table 4. 21 Indicator validity. 133
Table 4. 22 Construct Reliability and validity. 133
Table 4. 23 Indicator validity. 134
Table 4. 24 Estimation of Total Effects: The Original Structural Equation Model. 136
Table 4. 25 Estimation of mediation effect (Indirect Effects) for the Original Structural Equation Model. 137

Table 4. 26 Hypothesis influence Results. 145

Table 5. 1 Estimation results for the Structural Equation Model for Ethical Behavior. 152
Table 5. 2 Estimation results for the regression of factors on ethical behavior. 152
Table 5. 3 Estimation of mediation relationships (Indirect Effects) for the final Structural Equation Model. 153
Table 5. 4 Model fit for Final Structural Model for Ethical Behavior. 153

Table 6. 1 Software requirements of the developed model. 170
Table 6. 2 Usability Testing Results. 184

Table 7. 1 Determining Sample Size from a Given Population. 214
Table 7. 2 Study population. 215

,ist of acronyms.

ABSA	Amalgamated Banks of South Africa Limited
ACM	The Association for Computing Machinery
AfDB-HEST	African Development Bank Support to Higher Education, Science and Technology (HEST) Project.
AJAX	Asynchronous JavaScript and XML Extensible Markup Language.
API	Application Programming Interface
ATMs	Automatic Teller Machines
AVE	Average Variance Extracted
BoU	Bank of Uganda
CERT-UG	Uganda National Computer Emergency Response Team
CFA	Confirmatory Factor Analysis
CFI	Comparative Fit Index
CIA	Confidentiality, Integrity, Availability
CID	Criminal Investigations Department
CISSP	Certified Information System Security Professional
CR	Composite Reliability
CSS	Cascading Style Sheet
DDoS	Distributed Denial Of Service
ECQ	Ethical Climate Questionnaire
EERD	Enhanced Entity-Relationship Diagrams,
EFA	Exploratory Factor Analysis
FCI	Faculty of Computing and Informatics
GUI	Graphical user interface
GDT	General Deterrence Theory

GoU	Government of Uganda
HTML	Hyper Text Markup Language
ICT	Information and Communications Technologies
IEEE	Institute of Electrical and Electronics Engineers.
IP	Intellectual Property
IRB	Institutional Review Board
IS	Information Systems
ISO	International Organization for Organizations
IT	Information Technology
ITU	International Telecommunication Union
JS	JavaScript
KMO	Kaiser-Meyer-Olkin
LTD	Limited
MAR	Missing At Random
MCAR	Missing Completely at Random
MoICT&NG	Ministry of Information Communication Technology and National Guidance
MUST	Mbarara University of Science Technology
NDP	National Development Plan
NFI	Normed Fit Index
NISS	National Information Security Strategy
NITA-U	National Information Technology Authority -Uganda
PBC	Perceived Behavioral Control
PDO	PHP Data Objects

PHP	Hypertext Processor
PLS	Patial List Squares Regression
RMR	Root Mean Square Residual
RMSEA	Root Mean Square Error of Approximation
SD	Standard Deviation
SeBIS	Security Behavior Intentions Scale
SEM	Structural Equation Modeling
SEM	Structural equation modeling
SIM	Subscriber Identity Module
SMEs	Small And Medium-Sized Business
SN	Subjective Norms
SQL	Structured Query Langauge
SRMR	The Standardized Root Mean Square Residual
SRMR	Standardized Root Mean Squared Residual
TPB	Theory of Planned Behavior
TRA	Theory of Reasoned Action
TV	Tolerance Value
UBA	Uganda Bankers' Association
UCC	Uganda Communications Commission
UI	User Interface (UI)
UID	Unique Identification Number
URL	Uniform Resource Locator
VIF	Variance Inflation Factor
XAMPP	X-operating system, Apache, MySQL, Php, Perl.

Abstract

Introduction: Banks have built many robust Cyber security measures and set up codes of conduct to deter undesirable behaviour, but unethically behaved employees overlook and bypass all these. Thus ethical issues continue to be a problem. There is an urgent need for banks to understand employee threats for Cyber security to inhibit unethical behaviour better. This research developed an ethical behaviour model that analyses Employees' character traits which may influence Cyber security ethical behaviour.

Objectives: The research was guided by four specific objectives: i) To study the Existing ethical behavior models and identify the model requirements. ii) To establish the influence of ethical virtue constructs moderated by ethical climate on employees' Cyber security ethical behavior intention in Ugandan commercial banks. iii) To Develop a Cyber security ethical behaviour assessment model for Ugandan commercial banks. iv) To test and validate developed model. The study was guided by virtue ethical theory, supplemented by the Theory of Planned Behavior (TPB) and ethical climate theory.

Methodology: The research applied dual essential paradigms. behavioral-science paradigm in establishing the influence of Ethical Virtues moderated by ethical climate on employee's Cyber security ethical behaviour and the design science paradigm in developing an artefact in the form of a model for assessing employees' Cyber security ethical behaviour. Testing the model was done with the System Usability Scale. The researcher conducted exploratory research using a focus group of 10 beta testers from ABSA bank Mbarara and a cross-sectional survey using quantitative methods through an online questionnaire. And Data from a sample of 240 commercial bank employees from Centenary and ABSA banks' branches located in Kampala capital city of Uganda. The study purposively selected the commercial banks' employees with access to banks' sensitive information, including; bank tellers, Information Systems Security Officers, Financial Managers, branch managers, and loan officers.

Partial Least Squares Structural Equation Modeling (PLS-SEM) was employed to analyze the indicators, constructs, and path relationships and to test for casual relations between the model's constructs. The study conducted a confirmatory factor analysis to determine causal patterns in the

variables and assess them for validity and reliability. The moderating effects of Ethical climate were tested using Modgraphs.

Results: The results reveal a positive but insignificant effect of prudence Beta 0.094. p = 0.277 on Behavioral Intentions; that there is a positive and significant influence of Temperance; Beta 0.255, p = .000; on Behavioral Intentions; There is a positive and considerable influence of courage; Beta 0.247, p = .001; on ethical behaviour, that there is a positive and significant influence of Justice; Beta 0.452, p = .000; on Behavioral Intentions. The results further showed that a Strong ethical climate gave rise to a positive effect on Ethical Behavior. Results further showed that a positive change in behaviour intentions leads to a positive shift in ethical Behavior towards Cyber security. The usefulness of the assessment report was rated excellent by 9 of the respondents.

Contribution: The contribution of this thesis is An Employees' Cyber security Ethical Behavior Assessment Model for Ugandan Commercial Banks (ECEBA), deployed to the internet via the URL http://Cybersecurity.groxels.com.

Recommendations: The research recommends banks use the developed model in conducting Employee pre-hire screening and periodic assessments of current employees. It could be a means of detecting an employee's ethical decision-making style and growing more ethical employees.

Policymakers should develop virtue ethical-based training programs with dedicated, continuous learning and teaching undertakings geared towards monitoring and enhancing the overall Cyber security ethical behaviour in the banks. Banks are encouraged to establish a moral climate to allow employees to continue observing ethical conduct among themselves. When the ethical environment is robust, employees experience less force to breach the banks' Cyber security. The results are a platform for the Government of Uganda through the Ministry of ICT to generate appropriate national policies related to Cyber security ethics as a strategy aimed at improving Cyber security ethical behaviour in the banking sector.

Key words: *Cyber security, Ethical Behavior, Ethical Climate, ethical Virtues.*

CHAPTER ONE: INTRODUCTION

1.1 Background to the Study

Since the 1960s, when computers first became widely used, information security has become a major current problem. Information security, according to Safa et al., (2015), is crucial for businesses and has improved over time. The first antiviral program, named Reaper, was created in the 1970s by Ray Tomlinson, the inventor of electronic mail. The worldwide web was made publically accessible in 1989, which caused the demand for security to expand. The public had greater access to the internet in the 1990s, and dangers to network security grew. As necessity is the mother of invention, widespread production of firewalls and antiviral software was required to protect the public.

The International Telecommunication Union (ITU), (2018) describe the evolution of internet from a platform for information sharing to the foundation of modern business, essential services and infrastructure, social networks, and the global economy since 2010. The development and density of cyberspace have significantly expanded throughout this time. Concerns about Cyber security have also grown in an effort to keep up with the rapidly advancing capabilities of the cyber realm (Edgar & Manz 2017).

Safa et al., (2015) contend that although there are significant opportunities and advantages for people in the cyber world, there are also significant risks and difficulties. Cybercriminals have attempted to use the cyber space for everything from theft and espionage to college mischief. The weakest link is typically made by internal organizational staff members who work with outside attackers to wreak havoc. For instance, Yahoo reported that a cyberattack had compromised more than one billion accounts in December 2016. Target agreed to pay $18.5 million in settlements in May 2017, bringing the total price of the 2013 data breach at the corporation to $292 million, (Kan 2016). It was revealed in August 2014 that 500 million email addresses and 1.2 billion usernames and passwords had been hacked by Russian cybercriminals. As a result, the US communications regulator, imposed a USD25 million penalties on AT&T, (Chandarman and Niekerk,2017). Significant cyberattacks in recent years have not only resulted in monetary loss but have also compromised other sensitive data.

While many international companies have been greatly affected by cyberattacks, Tariq, (2018) argues that the financial services industry has been a primary target for attacks globally.

This is because banks have money and the information they hold is very valuable. Nikki et al. (2018), expound that financial companies experience Cyber security problems 300 times more frequently than other types of companies. This was echoed by Carter & Crumpler, (2019) that the financial industry, notably large institutions, continue to be the target of the majority of cyberattacks. For example, customers of Bank of America, JPMorgan Chase, Citigroup, U.S. Bank, Wells Fargo, and PNC, expressed frustration in 2012 when they were unable to access their accounts or make online bill payments due to a cyber-assault. According to a 2014 article in USA Today, hackers broke into bank networks and stole more than 500 million financial records over the course of a year. A cyberattack that the Bangladesh Central Bank experienced in February 2016 cost them $81 million. 36 financial organizations disclosed breaches, and 46 major American financial institutions were the targets of distributed denial of service (DDoS) assaults in 2016. When hackers stole the data of 83 million customers from JPMorgan in 2014, it was the largest data breach from a financial company. Experian experienced the largest credit bureau breach in 2015 when information on 15 million consumers was made public. Using money transfer messaging services, hackers stole $81 million from the Federal Reserve Bank of New York in 2019. Additionally, in 2016, the "Carbanak" spear phishing campaign targeted banks in Australia. 100 banks in 30 countries were the targets of cybercriminals, and Over the course of 18 months, cybercriminals stole around 1.3 billion dollars from 100 institutions in 30 different countries (Nikki et al., 2018).

In 2016, a hacker collective known as the Lazarus Group allegedly waged devastating operations against retail and central banks all throughout the world, (Dupont, 2019). The organization attempted to move more than a billion dollars unlawfully between 2015 and 2018 by hacking into bank systems in Vietnam, the Philippines, Africa, Asia, Europe, and North America. Additionally, it broke into the networks of finance that control ATM transactions and stole tens of millions of dollars from banks in more than 30 nations (Dupont, 2019).

The region's electronic financial transactions have been breached by suspected fraudsters, a senior official of Cyber security Africa has warned.

At a news conference held in advance of a workshop on banking and Cyber security in Kigali, Rwanda, Cyber security Africa Alliance manager Mr. Sammy Kioko stated that a survey done by

Deloitte in 2018 shows that banks in Kenya, Rwanda, Uganda, Tanzania, and Zambia lose $245 million (roughly Sh367 billion) annually to cyber fraud.

A Cyber security assessment on Uganda published in 2017 reveal that the banking sector in Uganda has also been targeted by cybercriminals. The Chief Information Officer of Stanbic Bank Uganda Herbert Olowo, explicate that the Ugandan banking sector continues to be the most targeted by cybercriminals, for instance in its official announcement from July 2019, DFCU Bank acknowledged that its system discovered a cyberattack in May 2019 which was immediately reported to the police, (CID HDQTRS GEF 604/2019). Between January 2016 and January 2017, 800 fraud occurrences were reported by Stanbic Bank Uganda, this was reported by the bank's managing director Patrick Mweheire.

Fraudsters frequently have bank employees assist them in carrying out their mission. On the same note Malaba, (2018) stated in the daily monitor newspaper of Sunday, April 15, 2018, that insider fraud occurs in nearly all Commercial Banks. McAlaney et al., (2018), posit that one of the reasons Cyber security assaults succeed is that systems designed to protect enterprises do not take the psychological makeup of the users into account. Yet, people are the weakest link in cyber insecurity chain that puts the company at risk of losing sensitive information and other assets. (Kearney & Kruger, 2016). For the Ugandan commercial banks, this research developed an Employees' Cyber security ethical behavior assessment model for evaluating the ethical behavior of employees towards Cyber security.

1.2. Theoretical background

This study model is supported by the Philosophical Virtue Theory, the Theory of Planned Behavior (TPB), and the Ethical Climate Theory. An assessment model for employees' ethical behavior in relation to Cyber security was created using these theories as a foundation.

1.2.1 Philosophical theories

Plato and Aristotle were the founders of virtue ethics, which were later revitalized and strengthened by Averroes & Thomas Aquinas, (2005). One of the three main approaches to normative ethics is virtue theory.

Normative ethics examines whether a person's moral actions are right or wrong in relation to the moral laws of society (Gray and Tejay, 2014). In normative ethical theory, Cyber security ethics

is a subset of applied ethics that addresses the real-world moral issues that arise from using computers and networks of computers in the information age on a daily basis.

Deontological and consequentialist ethics have frequently been favored in contemporary studies as being appropriate for computer ethics, while traditional theories of ethics, such as virtue ethics, are typically neglected as being outmoded and unsuitable for the Information Communication Technology (ICT) age. But during the past few decades, considerable efforts have been made to apply Aristotelian version of virtue ethics to computer and cyber ethics in modern research. According to MacIntrye, (1984), a virtue is a cultivated trait or personality that constitutes the fundamental components of admirable character. Virtues are advantageous for leading a contented, successful, or flourishing human existence; this good life may also entail defending particular values against opposing values. By having and using virtue, one develops self-awareness, a sense of goodness, and ultimately benefits both internally and externally (MacIntyre, 1984). Gray, (2015) asserts that values may be taught and, with time and effort, embedded in a person's character.

Aristotle considered 15 virtues, including bravery, temperance, liberality, magnificence, pride, and honor, as well as respect and adoration. Good nature, friendliness, and honesty intelligence, humor, and friendship Justice/impartiality. However, because all other virtues are built on cardinal virtues, the virtues of Courage, Temperance, Justice, and Prudence are carefully thought out as cardinal virtues. They are fundamental in the sense that they are dependent upon the other virtues. According to Aquinas, the other virtues are the most important of the four. Therefore, one requires elements of the four cardinal virtues in order to possess any of the other moral virtues. Aquinas provided an explanation of the cardinal virtues (2005) as:

Prudence: is the demonstration of knowledge, intellect, and good judgment in making decisions that are appropriate for the circumstances at hand (Aquinas, 2005).

Fortitude: The ability to face and withstand fear, uncertainty, or intimidation; the ability to overcome challenges that may prevent taking effective action (Aquinas, 2005).

Justice: In relationships with other people, the ongoing readiness to give each person what they justly deserve; righteous deeds (Aquinas, 2005).

Temperance: willpower, and moderation in one's actions, wants, and emotions (Aquinas, 2005).

Cybersecurity professionals can better understand their moral obligations with the aid of the cardinal virtues of ethics (Vallor, 2017). Employees and professionals in the field of Cyber security have ethical duties to other people, organizations, and the computing industry as a whole. Cardinal virtues should be incorporated into the information systems protection paradigm, Gray & Tejay, 2014). Theoretical work on virtue ethics in social work has grown in recent years, but little has been done to examine how the virtues are really put to use in the field of computing, and more specifically, in Cyber security. In contrast to other fields like medical, nursing, education, and psychology, there is still a dearth of research on the ethics of Cyber security.

The current research created a web-based Cyber security ethical behavior assessment model to assist banks in analyzing the Cyber security ethical conduct of their personnel. The model also identifies an employee's ethical blind spots and behavioral gaps, and this data is used to develop awareness and training programs for Cyber security ethics.

1.2.2. Theory of Planned Behavior (TPB)

The two best known Theoretical models of behavior are the Theory of Reasoned Action (TRA) and the Theory of Planned Behavior (TPB). The TRA was developed by Ajzen and Fishbein (1969,1980);

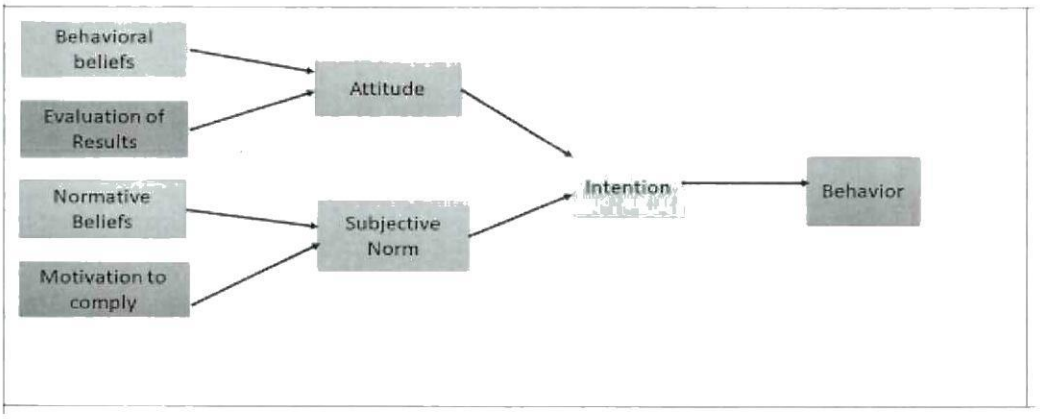


Figure 1. 1 Theory of Reasoned Action (TRA) (Ajzen and Fishbein (1969,1980)

It was assumed that one's behavioral intention, was the immediate precursor to their actual behavior. The TRA model identified two factors attitude toward the conduct and subjective norms that influence behavioral intention. In determining whether an action is good or bad and whether an actor supports or opposes engaging in it, attitude is involved.

Uffen and Breitner, (2013), content that earlier researchers have employed the theory of planned behavior (TPB) to explain user behavior in information system studies. Some other studies, with the backing of Jafarkarimi, et al., (2016; 2017), have also asserted that TPB is applicable in the context of ICT. The majority of studies mention TPB (Ajzen, 1991) Loch & Conger (1996) as being more useful in foretelling IT-related behavior.

1.3. Definition of Key Operating Terms

Explanations of the main terms of this research are essential to offer understanding to those intending to read this work.

Cyber space; Apvera, (2018) expose, cyber space as a composite environment that was created via the combined efforts of users, software and services on the Internet. Virtual technology methods and the networks that connect to it enable this.

Cybersecurity; refers to procedures and actions taken to prevent unauthorized access to, alteration of, or destruction of digital assets and data. Technologies, rules, and practices for securing assets in cyberspace are all part of Cyber security. Cyberspace is made secure through Cyber security, (Edgar & Manz 2017).

Vries, (2017) defines Cybersecurity as a group of models, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that can be used to defend an organization's information assets from both internal and external threats.

Merriam Webster describes Cybersecurity as the measures used to protect a computer, computer system, and the internet from unauthorized access or assault.

The International Telecommunication Union (ITU, 2018), describe Cyber security as a collection of policies, plans, guiding principles, threat management techniques, actions, teachings, best practices, assurance, and technological advancements that can be used to protect the confidentiality, availability, and integrity of assets in connected infrastructures owned by public and private organizations and individuals.

These assets include connected computing devices, personnel, infrastructure, applications, and services. Brey, (2007) clarifies that Cyber security also refers to the effects and outcomes that follow the application of Cyber security strategies and tactics.

Toch, et al., (2018) designates Cyber security as a way of guarding networks, computers, programs, and data from assaults and proscribed access. Von Solms & Van Niekerk, (2013), define Cyber security as the safeguard of Cyberspace, electronic information, and Cyber space users from malicious damage done by people and different categories of technologies that support Cyberspace. Cyber security is described as those actions and other methods, technical and non-technical, envisioned to defend computers, computer networks, and the computer system devices, and the information they contain and other components of Cyberspace, from all kinds of threats (Igwe & Ibegwam, 2014). This study adopts the definition of ITU (2018) and Odumesi, (2014) to be the guide in explaining Cyber security variables in this research.

As more gadgets are connected to the Internet, Cyber security becomes more crucial to all enterprises (Hamburg & Grosch, 2017). By assuring their supply chain, partners, stakeholders, and consumers of their commitment to Cyber security, enterprises may protect their most important assets, customer information, and operating systems and gain new business. Today's enterprises must acknowledge that using specialized software to protect themselves solely from online attacks is insufficient if they want to achieve true Cyber security. Effective Cyber security relies on three key areas: people, processes, and technology.

Ethics: Laudon & Laudon, (2006), define ethics as the main beliefs of right and wrong where persons performing as free moral agents use to make choices to guide their behavior. The Macquarie Dictionary, describes ethics as a set of moral rules that determine whether a person's actions and recommendations are good or evil, right or wrong. A subfield of philosophy known as ethics is focused on how people behave, particularly how they act in social situations. Ethics looks at how our moral judgments are rationally justified. What is ethically right or wrong, just or unjust, is the subject of ethics. A person's, a religion's, or a group's code of ethics is their set of moral principles.

Ethical behavior intention: Behavior intention is the decision to carry out or refrain from acting. In ethics, the intention principle states that whether an action is morally permissible sometimes depends on the agent's intention for performing this action.

Trevio, Nieuwenboer, & Kish-Gephart, (2014), describe ethical behavior as both morally right and wrong choices and actions that are evaluated in relation to societal norms.

In a given situation, ethical behavior is that which is morally regarded as "good" and "right" as opposed to "bad" or "wrong."

An ethical climate: Deliberate the understanding of appropriate behavior deriving from organizational architecture, which affects behavior and decision-making (Victor & Cullen, 1988).

Commercial bank; Commercial banks are a type of financial institution that are permitted to manage checking, savings, and time deposit accounts for people and organizations in local and foreign currencies. The issuance of letters of credit, the purchase and sale of foreign currency, and customer loans are all permitted activities for commercial banks. Uganda has 25 commercial banks. (Appendix 2). Uganda had 2.5 commercial bank branches per 100,000 adults in 2020. Uganda's commercial bank branches grew at an average annual rate of 5.89% from 1.2 per 100,000 adults in 2006 to 2.5 per 100,000 adults in 2020.

1.4 The Context of employees' ethical behavior and Cyber security breaches in the banking sector

The banking industry is gradually embracing the use of the internet to improve access and efficiency for their customers and to streamline corporate practices, Gana et al, (2019). Banks have quickly shifted their banking operations to online banking in order to reduce operational expenses and improve consumer satisfaction. (Kazmi et al., 2017). Rao (2019), expound that the development of information technologies has made it possible for bank customers to interact with their bank's operations around-the-clock via automatic teller machines (ATMs), mobile devices, and other Web-based methods. However, there has been an upsurge in Cyber security breaches, and they are common in all facets of the banking sector.

Cyber security breaches affect banks 300 times more frequently than other types of businesses, and most of the time, staff are directly responsible, they conspire with foreign attackers to sow havoc, (Zahoor et al, 2016; Carter & Crumpler, 2019).

Financial institutions in Uganda, have been wrestling with employees who swindle money from customers and the banks. For instance, Centenary bank Bagala (2021), like several other financial institutions in Uganda, have been victims.

For instance, in December 2020, six Centenary Bank employees were charged in court with conspiracy to defraud the bank and unapproved disclosure of bank information.

They conspired by deceit or fraudulent means to defraud Shs152m from Centenary Bank account no. 5020008320 held in Isingiro branch. Centenary Bank Bwaise branch Officer Steven Zziwa, the branch assistant manager Diana Musisi Namubiru, the branch supervisor Nasir Doka, and other workers, including Oscar Mukombozi, Annet Nalumansi and Hassan Kintu Musoke, were remanded to prison, Bagala (2021).

Uganda Police report (2020) indicate that the bank fraud involves tellers, bank managers, top bank office executives and auditors. Dupont (2019) echoes that bank staff, such as bank tellers, are thought to be a greater threat to financial organizations than hackers. The management of the banks is urgently required to fully understand the issue posed by the threats posed by their employees to Cyber security. Mukisa (2019) contends that 35% of Cyber security breaches in banks originate from the outside, while 65% originate from within. Over 95% of the 35% are helped by insiders. According to Mukisa, internal workers are involved in over 90% of all instances of electronic bank fraud. For instance, in 2019, hackers who colluded with DFCU Bank executives Kiirya stole billions of shillings from the bank (2019). As an illustration, it is alleged that between May 14, 2019, and May 28, 2019, four DFCU Bank customers' simcards were switched without their knowledge, resulting in the transfer of money to 15 DFCU Bank accounts, which was then withdrawn using ATMs and various mobile money accounts on both MTN and Airtel. The crime was carried out, according to police records, by two outsiders and four junior bank employees. Additionally, in 2018, the officers of Bank of Uganda (BoU), which oversees all commercial banks, colluded with fraudster Kahjjhjh Mukasa and stole Sh285 million.

This issue is exacerbated by the absence of effective employee Cyber security ethical behavior assessments. The Annual Crime and Traffic Safety report 2020, indicates that Uganda lost money and other assets valued at Shs11.5t in economic crimes in 2020. This is a registered increase from a Shs297b loss due to economic crimes in 2019.

User behavior is responsible for 80% of security failures in businesses, (Humaidi & Balakrishnan 2018). Employee unlawful conduct remains to be the biggest danger to information security, (Xue et al., 2018). Fraud in banks continues to be one of the most alarming cyber threats to any financial organization, (Malaba, 2018). Commercial banks suffered losses from electronic fraud totaling Sh15 billion in 2018, according to information from the Ugandan police.

Malaba also claims that banks suffer from frauds or attempted scams, which are frequently orchestrated by bank workers. Fraud is one of the major problems in the banking sector.

Instances of electronic fraud are increasing in Uganda's commercial banks, and the majority of these crimes are planned and carried out by insiders, (Mukisa,2019). The Uganda Police Annual Crime and Traffic Safety report of 2020, showed that banks lost Shs2.4b. Directorate of Criminal Investigations spokesperson Mr. Charles Twine, (2021) said bank frauds involve connivance between high-level executives and lower cadre employees. The most typical type of fraud in banks, involves internal coordination amongst the banking staff who have access to critical information with outsiders. For example; Lule & Buregyeya, (2023) reporting for New vision newspaper of Tuesday February, 14, 2023 opine that the Stanbic branch managers of garden city, Freedom city, and others allegedly connived and transferred the funds frequently into bank accounts they had set up specifically to receive the stolen money. The investigations by CID and the bank show that the money was withdrawn and stolen on the directive of branch managers. Using computer system intrusions, they gained un authorized access to banks' clients' accounts and stole $1.8m.

Financial institutions have been recommended to restrict personnel access to important data in order to reduce cyberattacks, as most attacks are inside jobs. A top priority should be given to safeguarding financial institutions from Cyber security attacks. To ensure greater Cyber security of the banks' information systems and assets, management of the banks must find ways to comprehend, encourage, and support the moral values and behavioral objectives of their employees with those of the business (Gray, 2015). Shoemaker et al. (2019), contend that when firms are developing their Cyber security strategy, ethics is likely the last thing on their minds.

Table 1. 1 Recent Cyber Security Breaches in Ugandan Commercial Banks

Case	Date	Employee involved	Reference
Centenary Bank loses Shs3b in internal fraud	2021		Andrew Bagala Monitor, Wednesday, April 21 2021
Shs 14bn lost as hackers wreak havoc across Ugandan banks	2021	Insiders involved	URN October 18, 2021 Observor news paper

Stanbic Bank Uganda recorded 800 fraud incidents	January 2016 and January 2017,	Collaborated by internal employees	Mweheire, (2017)
DFCU bank lost billions of shillings	May 14, 2019 and May 28, 2019,	crime executed by four junior bank staff and two outsiders. hackers had connivance with the DFCU Bank officials .	Kiirya (2019).
Shs285 million stolen from Bank of Uganda.	2018	BoU officers connived with Kahjjhjh Mukasa a fraudster	
Total customer base of Centenary bank Uganda declined by 11.4% and customer deposit declined by 7%, after electronic fraud increased by 6.3% in 2016.	2016/2017	Insiders involved	Matovu (2018)
Cyber-attack on stanbic bank, telecoms (MTN and Airtel). Over shs1 billion stolen	2019	forced to temporarily suspend bank-to-mobile money/wallet and mobile money to bank transactions.	S. Masaba, (2019)

Table 1. 2 Data Breaches in Finance industry in developed countries (Kost, 2022)

Bank	Date:	Impact:	Type of data compromised
First American Financial Corp Data Breach	May 2019	885 million credit card applications	• Names • Email addresses • Phone numbers of closing agents and buyers
Equifax Data Breach	Sep 2017	147 million customers	• Personally Identifiable Information (PII) • and financial information. • Equifax was fined $700 million for the breach.
Heartland Payment Systems Data Breach	January 2008	130 million debit and credit card numbers	• Credit card numbers • Card expiration dates • Cardholder names

Capital One Data Breach	March 2019	100 million credit card applications	• Social security numbers (about 140,000 records) • Canadian Social Insurance numbers (about 1 million records) • Bank account numbers (80,000)
JPMorgan Chase Data Breach	October 2014		• Internal login details for a JPMorgan employee • Customer names • Email addresses • Phone numbers
Experian	August 2020	24 million customers and almost 800,000 businesses were impacted by the breach.	• Mobile phone numbers • Home phone numbers • Work numbers • Email addresses • Residential addresses • Places of work • Work addresses • Job titles • Job start dates
Block	Apr 2022 damage costs, which rose from $70 million to $108 million.	8.2 million employees	• Full names • Brokerage account numbers • Brokerage portfolio values • Brokerage portfolio holdings • Stock trading activity for one trading day
Desjardins Group	June 2019	access to 4.2 million members' data with an intent to cause harm to the company.	• Social security numbers • Names • Email addresses • Transaction records
Westpac Banking Corporation	June 2013	98,000 customers	• Full names • Email addresses • Phone numbers • Account information
Flagstar Bank	June 2022		• Social Security numbers (SSN) • Banking information • Personal information (names, addresses

It's not easy for internal security teams to watch for insider threats because they're busy handling other risk management tasks.

Banks must implement additional cybersecurity systems for instance cyber threat training in the workplace because People remain the feeblest links in a cybersecurity program.

The core problem of this research is "increased cyber insecurity boosted by employees in banks". Banks must hire employees that are morally upright, able to abstain from committing cybercrimes, maintain a commitment to their jobs, and diligent in their work. Ait Maalem et al. (2020) acknowledge that ethical conduct may contribute to increased Cyber security and incident avoidance. Safa et al., (2016), contend that user behavior needs to be taken seriously. To close that gap, immediate tangible efforts are required; otherwise, security dangers would probably increase. Therefore, it is becoming increasingly important to evaluate how ethically responsible banking sector employees are when it comes to Cyber security.

1.5 Problem Statement

Banks have established codes of conduct and put in place a number of strong Cyber security measures as a deterrent to unwanted behavior, (Zahoor et al., 2016). However, employees who act unethically ignore and bypass all of these protections (Gray, 2015) leading to the increase in Cyber insecurity in the banks which results into sensitive information falling into the hands of cybercriminals, (Kosk, 2022).

Running anti-virus software, installing software updates, turning on personal firewalls, avoiding adware/spyware, protecting passwords, using spam filtering techniques, are all important cyber-safety measures but they haven't been successful in addressing these human issues because their focus is placed on technological applicability. Uganda has three cyber space laws (the Eletronic transaction Act, Computer misuse Act, and the Electronic Signatures' Act), to govern fraud online, but they are difficult to implement and they are not known by the public (Lule & Buregyeya; 2023). Ethical conduct may contribute to increased Cyber security but behavioral components of Cyber security are still understudied, Ait Maalem et al., (2020), as a result, ethical considerations remain a challenge. In order to prevent employees 'unethical activities, banks urgently need to better comprehend the issue of Cyber security ethical concerns (Gray, 2015; Carter & Crumpler 2019).

Gray, (2015), posited that there is little research into how the positive characteristics of employee virtue ethics and Ethical climate can improve Cyber security ethical behavior. This research addressed this gap.

To the best of the researcher's knowledge, the existing frameworks for Cyber security ethical behavior assessment for instance the Security Behavior Intentions Scale, Egelman & Peer (2016), are implemented through face-to-face which are restricted by geographical boundaries, and are time consuming. Further still there is lack of proper tools to analyse employees' ethical behavior to identify their ethical blind spots and ethical behavioral gaps; (Nkonge 2017, Gray 2015). There is lack of proper models for guiding the design of web-based applications that analyse employees' character traits which may influence ethical behavior and ultimately Cyber security.

Therefore, this research developed a model for assessing the urban commercial banks employees' Cyber security ethical behavior in Uganda.

1.6. Justification

Improving computerized and online information security is one of Uganda's Vision 2040 goals for information communication technologies, as per the country' Third national development plan (NDPIII) 2020/21 - 2024/25. Goal 9: ICTs can be found explicitly as a target under SDG 9 "Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation" Global efforts need to be stepped up to address an increase in cross-border cyberattacks, hate speech and security breaches. However, Kuepper, (2019) contends that Cyber security incidents in the banking industry have increased, which has an impact on the performance of the banks. A Cyber security breach hurts the afflicted bank's reputation and finances; this can cause bank clients to lose faith in the institution. On the same note Dupont, (2019), echoed that a bank would incur an average loss of $1.8 million from a cyberattack particularly directed at their online banking services. after an increase in electronic fraud of 6.3% in 2016, the overall number of customers at Centenary Bank Uganda decreased by 11.4%, and client deposits decreased by 7%, (Matovu, 2018). The banking sector is a crucial component of a strong economy because it plays a key role in financial mobilization, facilitates a reliable payment system, and helps implement monetary policy.

Malik et al., (2018), warn that if bank workers' breaches of Cyber security are not addressed, both the micro and macro levels of the economy may suffer.

This could make it harder for Uganda to realize Vision 2040. Breach of Cyber security may potentially deter international investors.

They control a significant portion of the financial sector, and if their money is taken through cybercrime, the entire economy of Uganda could suffer. Standard of living, availability of jobs National development, savings, and welfare may all be impacted.

1.7. Main objective

This research aimed at improving Cyber security by developing a model for assessing the urban commercial banks employees' Cyber security ethical behavior in Uganda.

1.7.1 Specific Objectives

The specific objectives of this research are;

1. To identify the key elements of virtue ethics moderated by ethical climate and establish their influence on employees' Cyber security ethical behavior in Ugandan commercial banks.
2. To identify the requirements for the Employees' Cyber security ethical behavior assessment model in Ugandan commercial banks.
3. To design a model for guiding the design of a web-based application that analyses Employees' character traits which may influence Cyber security ethical behavior.
4. To test and validate the developed model.

1.8 Research Questions

I. What are the key elements of virtue ethics moderated by ethical climate and what are their influence on employees' Cyber security ethical behavior in Ugandan commercial banks?

II. What are the requirements for the Employees' Cyber security ethical behavior assessment model in Ugandan commercial banks?

III. What is required in Developing a model that guides the design of a web-based application that analyses Employees' character traits which may influence Cyber security ethical behavior?

IV. To what extent can the developed model be tested and validated?

1.9 Scope of the study

1.9.1 Subject Scope of the study

The subject matter was limited to investigating how the virtue constructs of Prudence, temperance, courage, justice behavior intentions, moderated by ethical climate, positively influence Cyber security employees' ethical behavior intention. The study identified the requirements for the Employees' Cyber security ethical behavior assessment model in Ugandan commercial banks. The research designed a model for guiding the design of a web-based application that analyses Employees' character traits which may influence Cyber security ethical behavior. The research tested and validated the developed model. This research presents the creation of a theoretical ethical behavior model and presents its applicability among the banking sector employees in Uganda. The Cyber security ethical behavior questions covering the cardinal virtues and ethical climate, are created by the system administrator and stored in a database. XAMPP version 7.2.32 was used to act as the local database server to locally host the MYSQL database where the system data is stored. The server also hosted the web application files which were accessed in a client server environment using Google Chrome web browser. MYSQL Workbench 8.0 CE was used to design the database model to illustrate the flow of data between entities. This helped in designing the logical database model which was later converted into a physical database after forward engineering. Sublime Text Editor version 3 32bit was also used as the source code editor for editing the developed web system source code.

1.9.2 Geographical scope

This study was carried out in the banking sector. The banking sector is chosen because Cyber security has become a major concern in banks (Babu 2018). Abreau, et al., (2015) proposed that ethical issues and understanding of bank personnel ethical behavior may help to reduce frauds in e-banking services. The research was conducted on selected commercial banks. The banks selected were centenary and ABSA Banks because they consented to taking part in this study and they are among the banks that have been grappling with their employees stealing money from customers and the bank (Bagala 2021).

The technical employees of the banks' branches in Uganda's capital city of Kampala participated in the study. Kampala has the largest percentage of banked adults (42%), (Finscope, 2018).

Kampala hosts the majority of banks' headquarters and has one of the highest numbers of bank branches and ATM outlets. The presence of a number of internet hotspots and easy accessibility to other forms of information technology makes Kampala more ideal for electronic bank fraud.

1.10. Outline of the Thesis.

This dissertation comprises of 7 chapters: Chapter one details the back ground of the study, the research problem, offers a justification for the study and defines the research objectives, research questions and hypotheses., the significance of the research is also presented.

Chapter two presents a critical assessment of literature on the study variables, the theoretical review, the current state of employees' ethical behavior intention towards Cyber security, the state of practice of Cyber Security Protection Measures, Cyber security Goals The importance of Cyber security in the modern banking sector, Conceptual Framework and Developing Hypotheses, behavior intention and Cyber security ethical behavior.

Chapter three describes the steps and procedures followed in order to accomplish the research. The online questionnaire was used to investigate the influence of cardinal virtues moderated by ethical climate on employees' Cyber security ethical behavior intentions in Ugandan commercial banks. Data collection was largely quantitative based on the use of questionnaires. Chapter four describes the analysis and findings of the objectives one. The descriptive statistics of background information and exploratory factor analysis of the hypothesized variables. It also presents correlation and Partial Least Squares Structural Equation Modeling (PLS-SEM) and hypotheses testing. Further, this chapter presents the findings from the objective one.

Chapter five describes the discussion of research findings of objective one. Presents the results of the hypothesized influences of cardinal virtues moderated by ethical climate. The Cyber security ethical behavior assessment model values were studied using p-values.

Chapter six presents objective two, this entails the development of a cyber-security ethical behavior assessment model. The chapter explains the different requirements that were used in the development of the system. Software and hardware models used together with the different sketches/ images of the developed system and their description are also clarified.

Chapter seven presents the study conclusions, implications to theory, Practitioner implications, Researcher implications, Limitations of the study and the Recommendations and Future Research.

CHAPTER TWO: LITERATURE REVIEW

Introduction

This chapter includes a review of literature and an exploration of the study concepts and theories that underpin the research. The aim of this chapter is to bring out a summary of the pertinent works of other authors and researchers to give a contextual and setting for the study. This is done to help the investigator appreciate the current information concerning the topic, verify the study problem, enable theory development, and recognize the research gap. Pertinent journal papers, organizational reports, newspapers, related books, and other important literature are got from internet sources (Kyeyune, 2017). The research further gets the study materials from various literature presented by numerous authors in platforms like; Science direct, Google, Google Scholar, Emerald, Research Gate, research databases like IEEE, ACM, the Association for Computing Machinery, among others.

The chapter reviewed literature related to the existing ethical behavior models, the influence of cardinal virtue constructs on Cyber security behavioral intention and actual ethical behavior of banking sector employees. The moderation effect of ethical climate on the virtue constructs in connection with influencing the behavioral intention of organizational employees towards Cyber security ethical behavior. The chapter further reviewed literature on existing models that assess the employees' ethical behavior towards Cyber security.

2.1. Employees' Ethical Behavior and Cyber security

Worldwide, governments and companies place a high importance on Cyber security and are investing billions of dollars to safeguard economies from cybercrime (Volz & Hosenball, 2016; Guardian, 2017). Wang et al. (2011), Opine that Cyber security is a crucial component of an organization's core operations and interactions. Thomson, (2018) makes the case that individuals working in the cyberspace require a mix of technological know-how, subject-matter expertise, social intelligence, and ethics to succeed. Similar to the webs they operate, these people must be trustworthy, accountable, and strong. And ethical behavior governs all of these. According to Vallor et al., (2017), When connected evils or profits significantly increase a person, group, or entity's chances of living well and experiencing happiness in a social environment, that is when an ethical issue is relevant.

When using Cyber security, humans either purposefully or unintentionally engage in fraud, malicious behavior, casual errors, retaliatory harm, misinformation, etc., which are difficult to identify and even more difficult to correct permanently. Identity theft is one of the cyber dangers to privacy. An individual's identifying information is stolen and used to falsely represent victims in financial transactions or for other illegal purposes (Burkell et al., 2015). Hacking and other network intrusions that allow for the access of private information for the purpose of extortion, blackmail, and other unethical operations. Discreet client information, trade secrets, espionage, and other wrongdoing are all revealed through privacy violations. All of these are due to inadequate or unethical Cyber security behavior (Jones, 2016). Confidential information cannot be preserved in its original digital form, where it was created and shared, in networked situations.

In order to uphold their ethical position in cyberspace, organizations must establish and sustain good behavior. However, the Cyberspace is vast and moral behavior relies on the individual. It becomes challenging for a corporation to ensure moral behavior in day-to-day operations, (SANS, 2019). Shoemaker et al., (2019), uphold that a company's level of security will depend on how prepared and committed its employees are to Cyber security. Echoed by Sommestad et al., (2015), an organization's employees' behavior is particularly important for information security and the overall stance on Cyber security. In order to guide and support their employees' ethical conduct, organizations develop and communicate Cyber security strategies, regulations, policies, and procedures. However, Gray, (2015) and Hatfield, (2019) contend that employees' bad behavior in committing Cyber security vulnerabilities have persisted and continue to harm enterprises.

Therefore, there is a pressing need for Cyber security professionals to remain motivated in maintaining their professional ethical conduct. They are trusted to secure and protect this confidential information in its original form, as described in Valor, (2017), and to guard against privacy violations.

2.2. Types of Information Security Behaviors in Organizations

Organizations may have personnel who are purposefully risk averse, purposefully risk inclined, or naive and incidental in their information security practices (Shamsudin eta.l, 2019; Pattinson et al., 2016).

The employees' attitudes toward information security are made clear by their naive and accidental behaviors, such as leaving computers unattended, using social networking sites, opening impulsive email attachments, using passwords that are simple to guess, failing to report security incidents, and visiting dubious websites. Deliberate Risk Averse Behaviors are the kinds of actions people take when they are aware of the privacy and information security safeguards put in place by the organization, such as turning off computers when not in use, reporting security threats and mishaps, changing passwords frequently, installing antivirus software, and blocking spam.

Deliberate risk-taking conduct refers to actions taken with the intent to commit crimes or pose a security risk, such as hacking into accounts and obtaining private information. committing information security offenses, sending spam, and getting unauthorized access to forbidden places.

According to Shamsudin et al., (2019), employee behavior is the most frequent barrier to information security compliance. Good work performance is linked to good employee behavior. Positive attitudes and self-assurance will result in better behavior, whilst negative behavior will result in incompetence at work. Shamsudin et al. state further that it is the responsibility of information security personnel to safeguard data and follow security protocols.

2.3 The effect of Cyber security breaches in organizations.

Cybercrime is on the rise and is distressing businesses, people, families, financial institutions like banks, and governmental agencies. Uganda Cyber Security Report, (2018) indicate that commercial and state businesses collectively lost more than Sh155.5 billion in 2018. On the same vein cybercrime costed Africa $3.5 billion in 2017, (Serianu, 2017; Dahir, 2018). Serianu further reveals that, by 2017, 90% of African firms were operating below the "poverty line" for Cyber security, demonstrating that these establishments are unable to protect themselves from cyberattacks. According to Serianu, 60% of firms' Cyber security strategies and policies are out-of-date, and 96% of Cyber security cases in Africa are not disclosed. These have a negative effect on the organizations, for instance, Mr. Sammy Kioko speaking at a news briefing ahead of banking and Cyber security workshop in Kigali Rwanda said that a survey conducted by Deloitte in 2018, indicates that banks in Kenya, Rwanda, Uganda, Tanzania and Zambia lose $245 million (about Sh367 billion) annually in Cyber fraud.

Profits are lost as a result of breaches in Cyber security. Millions of Shillings have been lost by Ugandans as a result of hackers duplicating SIM cards and accessing their personal information (Ogong, 2018). For instance, breaches in Uganda are anticipated to cost enterprises and ministries more than $50 million, or sh180 billion, a year, excluding recovery expenses (Muhawe, 2017). Business advancements can also be hindered by Cyber security breaches; for instance, in 2017, Makerere University's computer systems were breached, and 50 students' names were removed from the list of graduates after being accused of faking grades in 2018. Violations of Cyber security undermine client confidence (Global Economic Crime and Fraud Survey Uganda Report 2018; Leung ,2018).

Uganda Police's chief of the cyber unit, Richard Ndaboine, report that there were 400 or so cases of cybercrime in 2017, involving data tampering, money laundering, and electronic fraud. Ndaboine claims that the majority of them are still pending in court. He adds that in 2018, more than 50 additional instances were reported. According to the 2018 Africa Cyber Security Report, cyber-attacks cost Uganda 155 billion (or $42 million) annually. Uganda Police's report (2016) figures show that cybercrime cost the nation UGX. 122 billion in 2016. About 400 cases were recorded in 2017, according to Richard Ndabione, chief of the cyber unit at the Uganda Police. It is believed that these cases have cost both private and state businesses more than 150 billion shillings. The majority of the recorded offenses involve electronic fraud, information tampering, and money laundering. Uganda police CID recorded 198 instances of electronic fraud in 2018 that cost billions of shillings in Uganda. Property violations cause serious ethical harms to owners and other persons who rely upon such property for their wellbeing to secure good lives for themselves and others. Business establishments must ensure that their intellectual property is protected against unjustified usage. They must also ensure that they and their employees use information and inventions produced by others in ways that respect intellectual property protections and guidelines.

Vallor, (2017), posit that persons in charge of Cyber security have a moral obligation to protect the networks of their company or their clients against the majority of threats and intrusions.

Sakka and Spyrou (2015) concluded that new societal requirements are being noticed, and that understanding of cyber ethics is necessary to address these needs and provide rules for proper online conduct. Blanken-Webb (2018), echoed that it is crucial that Cyber security professionals receive education that fosters comprehensive capacities, talents, and temperaments since doing so will enable them to understand and handle the ethical and technological problems that lie ahead. Thus this research recommends that when Cyber security ethical behavior assessment is carried out gaps identified, cyber ethics trainings should be carried out among employees.

Ethics is a set of moral guidelines that assist people in determining how they ought to act in various situations. Igwe and Ibegwam, (2014), opine that it is crucial to impart the correct knowledge and attitudes in people so that they can live well and contribute positively to the society in which they reside. Cybercrime is expected to cost the globe $6 trillion yearly, up from $3 trillion in 2015, according to (Cyber Security Ventures, 2016). This indicates that cybercrime is on the rise and might result in significant financial loss, which can discourage and demoralize investors.

The majority of internet and other computing resource users, are very complacent, which makes them an easy target for cyberattacks (Chandarman & Niekerk, 2017). Cybercriminals are now focusing on the weakest link in the chain: the ignorant computer user (Korovessis, et al., 2017; Chandarman & Niekerk, 2017). The human aspect has been more exposed as a result, and is now referred to as the threat to Cyber security (Anwar, et al., 2016; Pfleeger, 2012; Kaspr Prei 2017). Spyrou & Sakka, (2015), posit that the most varied, unpredictable, and flexible component of any system is its people. Ethics and behavioral norms should be adhered to if serious, informed, and capable individuals truly desire to be both technically and psychologically on top of the issue makers in real time.

Despite the fact that ethics may be applied to IS security and that human behavior has a large impact on systems, most practitioners and researchers have downplayed the significance of ethics (Gray, 2015). The role of ethics is not mentioned in standardized models, such as those described by Jones, (2007) or Ketel, (2008). Ethics should be emphasized when providing a clear understanding of risks, incorporating the best methods of addressing risks within an organizational security plan, when assessing risk exposure and when providing processes to protect an information system.

Ma &Pearson, (2005), echoed that one of the most important and pertinent standards for information system security, ISO 17799, does not take into account the function and impact of employee ethics. There is virtually little historical research in the field of ISS on ethics in general and particularly on philosophy-based ethics (Adam & Bull, 2008). Halawi, (2013) laments the lack of research in the field of ethical concerning Cyber security.

2.4 Cyber security Technical Protection Measures are ineffective

Cyber assets and information are protected by various Cyber security protection methods that have been implemented in computers, the internet, and other networked computing systems. Thakur et al., (2016), contend that a solid security and control system that safeguards business information assets can therefore result in a significant return on investment. Businesses must safeguard not only their own data and digital assets but also those of their clients, staff, partners, and other stakeholders. Failure to do so may result in expensive legal action for data theft or exposure.

The 10 Basic Cyber Security Measures proposed by WaterISAC, (2015) comprise the following: i) Maintain a correct inventory of control system devices and prevent any exposure of this equipment to external networks. ii) Implement network segmentation and apply firewalls; iii) Use secure remote access techniques; iv) Use only strong passwords, change default passwords, and take other access controls into consideration; v) Use strong passwords to protect your systems and information and have different passwords for different accounts; vi) Maintain awareness of vulnerabilities and implement necessary patches and updates; and vii) Establish role-based access controls and implement system logging. Viii) Implementing an employee Cyber security training program, ix) involving executives in Cyber security, x) implementing measures to detect compromises, and developing an incident response plan for Cyber security.

The current set of information security countermeasures are categorized by Cherdantseva & Hilton ,(2013) into four categories: organizational, technical, human-oriented, and legal, a) Policies, governance, audit, procedures, and strategy make up an organization, b) Cryptography, authentication, firewalls, and antivirus software are all part of the technological aspect, c) Education, training, and awareness programs, motivation, rules, penalties, and rewards, and culture are all part of the human-oriented dimension, d) Laws, contracts, and agreements are all part of the legal realm.

Thakur et al., (2016) state that running anti-virus software, installing software updates, preventing identity theft, turning on personal firewalls, avoiding adware/spyware, protecting passwords, using spam filtering techniques, and backing up important files are all important cyber-safety measures to take. Veksler, et al., (2018), revealed that technical solutions to cyber-security are crucial for a successful security endeavor. Utilizing access control methods, using encryption for communication, and using monitoring and auditing models are all effective countermeasures. However, Siponen et al., (2010) posit that policies alone are not a deterrent against internal threats. Workman & Gathegi, (2007) opine that formal policies and procedures are meaningless if the persons they are directed at are insensitive to ethical matters. This was echoed by Lapuh Bele, (2014), that although the current mechanisms for enhancing Cyber security have made some progress, the issue continues to exacerbate. Lapuh Bele further notes that IT specialists can set up firewalls, antivirus programs, and enable routine operating system and antivirus software updates to increase technical security, but the weakest link, human beings are still a threat to systems and Cyber security. The effectiveness of technical strategies such as the deployment of firewalls, intrusion detection and prevention systems, secure setup of IT assets, and physical security measures is restricted against dangers posed by employee misbehavior. Safa et al. (2015), opine that Cyber security technology techniques have not been able to completely ensure the protection of cyber assets. Emphasis should be paid to human information security conduct. Employee attitudes and views strongly influence whether they will abide by these techniques, (Dhillon et al., 2007). The majority of organizational staff members, especially those in IT positions, have valid credentials to access the IS they intend to abuse, (Yu, & Liang, 2012).

The values and ethics of the workforce must support the existence of these countermeasures. Information system security non-technical activities including developing policies, guidelines, awareness campaigns, training materials, employees' background checks (Thakur et al.,2016) and ethics should be incorporated in the Cyber security planning model. Internet users need to be taught the proper moral and ethical online behavior. Blanken-Webb, (2018), argue that professionals in Cyber security are mandated to make significant decisions while engaged in their line of work therefore ethical behavior in all this is important. Cybersecurity so strongly implies the ethical component of society as a whole. Organizations can utilize virtue ethics to shape the opinions, deeds, and conduct of the moral personnel. Predicted employee conduct ought to be based on the core values of the particular ethical perspective being studied (Weber, 1993).

The virtue ethics method places more emphasis on a person's character than on a particular act. It also makes the point that a person's moral behavior will be guided by and defined by the attributes that make up their character. There are substantial security challenges that technical measures may not address since it is assumed that system security is a social or human issue (Chang & Ho; 2006). D'Arcy & Hovav, (2009) demonstrated that technical measures that work as a deterrent to some people are useless against others, which lends weight to this position. However, the majority of practitioners and researchers still concentrate on finding answers to technical problems. When developing Cyber security strategies, ethical behavior toward security is crucial and should be taken into consideration, (Dunkerley &Tejay, 2011).

2.5 Cyber security Goals

2.5.1 The Availability, Integrity and Confidentiality of Cyber Assets

The major objective of Cyber security is to protect digital assets, such as data and computer systems, from hackers and other dangerous users Odumesi, (2014). The CIA Triad confidentiality, integrity, and availability are three crucial components of any computer-related system that are addressed by computer security (Pfleeger's, 2003); Samonas & Coss 2014). Cybersecurity is the process of securing digital assets, such as data and computer systems, from hackers and other dangerous users. The CIA trinity of confidentiality, integrity, and availability of information is given top priority in this process. Hatfield, (2019), emphasize that protecting the confidentiality, integrity, and availability of data within computer networks is only one aspect of Cyber security. It also encompasses broader issues with regard to actual access to buildings, computer hardware, and online virtual access. The CIA triad of confidentiality, integrity, and availability of information is given significant weight in this regard. Pfleeger, (2003) claimed that confidentiality verifies those with permission to access the assets associated to computers. Information dissemination to third parties without authorization is avoided through confidentiality. Confidentiality in information security is the attribute that prevents information from being made available to or disclosed to unapproved people, groups, or procedures. Beckers, (2015). Only those with permission are able to access the assets associated to computers thanks to confidentiality.

Data integrity in information security refers to preserving and guaranteeing the accuracy and completeness of data across its full lifecycle. This ensures that data cannot be altered without authorization or detection. Integrity preserves the status quo by preventing illegal file alteration.

Data integrity refers to the fact that assets can only be changed by authorized persons or in permitted methods and that the data stored on a computer is the same as the source documents.

Information cannot be improperly withheld from individuals who require it at the time they require it thanks to availability. It also stops information from being disclosed without authorization to outside parties.

Access control and non-repudiation are two more significant issues that computer security experts are concerned with. Maintaining access control: This entails not only limiting user access to resources and services to which they are legally entitled, but also ensuring that users are not denied access to resources to which they have a right.

Nonrepudiation suggests that a sender of a communication cannot retract it, and that a recipient also cannot retract a message that he has received. The absence of any denial of a communicated message by either the sender or the receiver is known as non-repudiation. A computer system must be able to demonstrate the sending and receiving of specific messages. The difficulty this presents to computer users is that if someone acquires authorized access to the computer resources, he or she can send a message on the person's behalf that is problematic to repudiate.

Computing security experts consider the CIA security model to be the industry standard and use it as a reference when putting security into place for information systems (Pfleeger, 2003). The CIA is also used to identify issues or holes and to identify the best security fixes. The CIA Triangle is the paradigm used by the Certified Information System Security Professional (CISSP) to implement IS security. The International Organization for Standardization (ISO) recognizes the CISSP certification, and researchers contend that availability, confidentiality, and integrity make up the foundation of an effective security system.

The CIA triad was created in the early days of computers and has served its purpose as a well-known conceptual model of information systems security, (Cherdantseva & Hilton, 2013). But more recently, the CIA triad's suitability as a comprehensive set of ISS objectives has come under fire as a tactic that ignores new dangers that arise because of networked environments. The typical form of the CIA triad is lengthened by the appropriate list of security objectives that Cherdantseva & Hilton (2013) defined and recorded. Accountability, auditability, authenticity/trustworthiness, authenticity, availability, integrity, confidentiality, non-repudiation, and privacy are on the list.

2.6. Cybersecurity in Developed Countries compared to Developing Countries.

Khan et al., (2022), contend that Cybersecurity occupies a significant position in the aftermath of globalization and the intricate integration of Information Systems with Information and Communication Technologies (ICTs). The influence of information and communication technologies (ICT) on improving the quality of services in today's networked global village is unsurpassed (Otieno, 2020). Developed countries are already taking strides towards sustaining multifaceted Cyber security approaches.

Cyber threats however, to developing countries could impede their economic growth and destabilize the global financial system.

Mars, (2021) opines that while rich nations are moving forward with diverse Cyber security strategies, developing nations are negotiating their own muddle of internal problems while advocating for regulations for digital infrastructures and have even failed to understand the digital transition that is taking place. Developing countries are at the forefront of the digital transition and are still having trouble understanding. Poorer countries have insufficient institutional capacity, limited ICT skills and knowledge, and limited protection of crucial national infrastructures. They also have weak interagency coordination and emergency responses. Indeed, developing nations lag behind the developed world by a few decades

Russu, (2022) contend that Developed nations have gathered strong Cyber security resources. Developing nations try to imitate developed countries because they are seen as major models of Cyber security tactics, policies, and technological innovation. Reluctant leaders of developing countries hurriedly pass legislation, launch extensive proposals, establish CERTs, and look for methods to raise money for national Cyber security infrastructures. They do so without looking at their own ICT roadmaps or first enhancing the very pillars of their technological state, including communications, internet services, law and order, business costs, resources, and investment security. For instance, the cybercrime in Bangladesh Heist, which cost a local bank $81 million (from an attempted $951 million), was sent to a bank in the Philippines. But lax anti-money laundering regulations and broken cybercrime laws made investigations unsuccessful.

Africa's Cameroon is one of the countries where cybercrime is having the biggest impact. A few years ago, there were ideas about launching various Cyber security training programs to help address this issue. Policymakers were worried that after training, students might use their newly acquired skills to engage in cybercrime. Nigeria has become the gold standard for phishing. Despite being simple, the technique has already stolen billions from trusting people and stupid people all across the world. Nigerian fraud networks have been discovered in numerous countries, nevertheless the countries where they are captured determine whether they will be charged. Other socioeconomic issues are significantly impacted if the populace lacks confidence to protect them. A reliable and stable justice system, as well as competent law enforcement, are essential for sustainable growth.

While underdeveloped nations detest responsible vulnerability reports and pursue security researchers as criminals, developed nations see bug glut programs as a helpful tool in defending their national infrastructure and government systems.

Although most developed countries have in place comprehensive ICTs and Cyber security policies and plans or are at an advanced stage of implementing them, developing countries are short of the capabilities and infrastructure when it comes to Cyber security countermeasures. Most hardware and software products used in the developing world are developed from the western world and without proper measures on how to secure these products, these countries are vulnerable to cyber exploitation due to inherent vulnerabilities on these products.

Low-income states are targeted by both money-driven attacks (such as ransomware), and serve as training grounds for criminal groups in preparation for more ambitious attacks in developed countries (Owiny, 2023). Developing countries are aware of the need for Cyber security, but many would contend that they are more concerned with serious issues like HIV/AIDS or poverty. Developing countries lack well-trained cybersecurity experts. Level of understanding and education in cybersecurity issues among law enforcements agents, judiciary are not up to the standard.

2.7. The importance of Cyber security in the modern banking sector

Global enterprises have benefited greatly from the network of networks and computing devices, including smartphones, wireless connections, multiple Information Communication Technologies (ICTs), and other Infrastructure.

The management and oversight of the banking industry are now better structured and resourceful thanks to the internet. But since the beginning of time, criminals have always targeted the banking industry. At first, the assailants would take actual cash. Then it turned into a computer scam. The current trend is to break into bank servers and commit cyber fraud and also steal personally identifying information about customers.

Banks use Cyber security techniques to safeguard the private data of their staff, clients, and other stakeholders. Cybersecurity aids in preventing this information from ending up in the hands of cybercriminals who are adept at selling it or even using it to steal money. This increases the significance of Cyber security in banking. Protecting personal information is one of the most prized possessions in the digital world, according to Apvera, (2018). Cybersecurity is required to safeguard the assets of banks, including their clients.

The risk of a data breach grows daily as the banking sector transfers the majority of its transactions online, (More et al., 2016). There is a stronger focus on examining the value of Cyber security in banking sector processes. Banking sector employees are constantly at risk from impending cyberattacks if there are no essential Cyber security measures in place; bank-related cybercrimes are surging in number, (Zahoor et al., (2016). Cyberattacks on the financial industry are increasing relative to other industries. There are four times as many attacks on banks as there are on businesses in other industries. Successful cyberattacks cost banks and their clients a great deal of money. Banks must consider employee behavior in addition to the Cyber security measures they have put in place to protect the money, personal data, and other banks' treasured assets from cyberattacks.

Ample Spyware, a sort of cyber contaminant designed to infect bank computers and relay data back to cybercriminals, can be prevented by Cyber security and ensures that employees' activities remain private and confidential at work. Financial institutions, have made every effort to keep their transactions secure (Bhatt & Pant 2011). They categorized the many anti-cybercrime measures taken by banks, such as password encryption, virtual keyboards, Secure Socket Layer, SMS Alerts, and User Awareness Programs. Banks utilize the most up-to-date technology for online security, but security threats to the banks continue growing at an incredibly fast rate. While banks have adopted solid security measures to protect their assets, more work is still required to ensure that these assaults are limited or stopped. Bank security is becoming more problematic, necessitating tighter controls and enhanced Cyber security measures.

Enhanced Cyber security boosts customers' trust in banks. Businesses can inspire trust in their customers and clients by demonstrating that their operations are commendably secure from all types of cyber threats (Apvera, 2018).

Improved Cyber security can protect professional endeavors. Offering comprehensive digital defense to an organization's business processes is the best IT security strategy. This enables workers at the organization to visit and browse the internet without being concerned about potential risks. Computer infections like viruses, worms, and Trojan horses can make personal computers practically unusable by drastically slowing down their performance and making operations on them difficult to manage. Considering how much time is wasted by employees, this may have an impact on productivity. This frequently causes the entire operation to cease. Thus, Apvera lists the following benefits of Cyber security;

Cyber security protects Personal Information - In the digital age, personal information is one of the most important commodities. A virus is highly capable of selling or even utilizing personal information about your clients or employees to steal their money if it can get its hands on it.

It enables staffs to perform work safely - You and your staff are continuously at risk from a potential cyber-attack if your company doesn't have the strongest Cyber security solutions. Your system's efficiency may be seriously hampered by infection, and you might even need to replace individual machines.

Cyber security Repudiates Spyware – A type of cyber virus known as spyware is created to spy on your computer's activities and transmit that information back to the cybercriminal. High-quality Cyber security can stop this spyware from operating and guarantee that your employees' actions are kept private and confidential at work.

It Can Protect Your Business - The biggest benefit is that your company can receive complete digital protection from the top IT security solutions. This will protect your staff from potential hazards while enabling them to use the internet whenever they need to.

It Protects Productivity - Viruses can make using personal computers nearly difficult by slowing them down to a crawl. This can result in a great deal of lost time for your staff and frequently causes the entire operation to halt.

Prevents Adware - Adware is a type of computer virus that is fairly popular and inundates your computer with adverts. All of these advertisements, though, can seriously hinder productivity and frequently let other infections into your computer when they are unintentionally clicked.

You probably host your own website if you are a business. Stop Your Website from Going Down. There is a very real chance that your website may have to go offline if your machine is infected. This implies that in addition to losing money from declined transactions, you will also lose the trust of your customers and risk system harm from specific malware.

2.8. Cyber security strategies in Uganda

Information and communication technologies (ICTs) are widely acknowledged in Uganda as providing a significant contribution to the National Development Plan (2010). ICTs are also capable of supporting all contemporary activities carried out in the nation, such as e-Government, e-Commerce, and other ICT-based facilities. However, a number of cybercrimes and other breaches of Cyber security have jeopardized the ICT sector. Wamala (2011) contended that it is the responsibility of the government to safeguard the general security of the nation, its people, and their property. As a result, Cyber security becomes a government responsibility.

The East African Community established a task force in January 2008 to create a cyber-security frame work, NISS (2011). The framework gives the East African states approval to change their state laws so that activities that compromise the availability, confidentiality, and integrity of information and communication technology are minimized, electronic commerce can be improved, and personal privacy is protected.

A national information security policy for Uganda was released in 2014. The policy describes the minimal security procedures that must be implemented by all organizations in the public and private sectors. In order to lessen their vulnerability to cyber-attacks, the policy outlines how to use, own and/or operate protected computers, manage official communications, and handle personal data. The terms "critical infrastructure" and "critical information infrastructure" are also defined in the policy.

Uganda has a National Information Security Strategy (NISS), but it does not contain any specific, practical guidance about Cyber security.

To coordinate the response to Cyber security incidents, the Uganda National Computer Emergency Response Team (CERT-UG) was founded in 2014. The principal agency in charge of Uganda's Cyber security is NITA-U. In addition, NITA-U is accountable to the National CERT-UG and works closely with other CERTs. The National Information Consulting Group, which is headquartered under NITA-U, offers the Government of Uganda (GoU) free advisory services on information security. In order to fill in any gaps, it also solicits knowledge and guidance from other stakeholders, including the telecommunications sectors (Cyber security Capacity Review of the Republic of Uganda, 2016).

Internal security policies set the parameters for how public administration entities and ministries can use their networks. Every entity should be included in the preparation of the national Cyber security plan in order to identify and close any gaps, it was decided during the 2016 Cyber security Capacity Review of the Republic of Uganda by various stakeholders. This was due to Uganda's lack of a centralized budget for Cyber security. Each ministry allocates its budget individually and bases the amount it spends on Cyber security on both its past performance and its future ambitions. The Ugandan telecommunications regulators Uganda Communications Commission (UCC) and NITA-U work together with law enforcement. Under the Ugandan Ministry of ICT are NITA-U and UCC.

Cyber regulations in Uganda are designed to protect the online world. The relevant laws include the Data Protection and Privacy Bill, which was signed into law by His Excellency Yoweri Kaguta Museveni on February 25, 2019. The Anti-Terrorism Act of 2002 is a legislation that permits message interception and the surveillance of those who are thought to be engaging in or preparing terrorist crimes (Analyzed Cyber Laws of Uganda, 2016). A Monitoring Center must be established in order to intercept communications under the Regulation of Interception of Communications Act, RICA 2010, Section 3 of RICA.

The Electronic Signatures Act (ESA) regulates the use of electronic signatures in Uganda. The Computer Misuse Act (CMA) prescribes liability for offences related to computers. The Electronic Transactions Act (ETA) provides for the use, security, facilitation and regulation of electronic communications and transactions. The Uganda Communications Act, 2013. The Uganda Communications Act (UCA) regulates the Ugandan communications services. The Anti-Pornography Act, 2014 criminalizes all forms of pornography.

Certain initiatives are already in place to promote Cyber security in the nation, but nothing has been done to analyze organizational employees' ethical conduct in relation to Cyber security in the nation (Cyber security Capacity Review of the Republic of Uganda, 2016). According to Wamala (2011), businesses should hire Cyber security specialists who are committed to safeguarding the personnel as well as the organization's Cyber security assets. Gray, (2015), posit that it is improper to judge an employee's fit with the organization based on their ethical behavior while on the work. It is preferable to do this before hiring them. This seems to be essential for stopping trusted insiders from violating the ISS.

2.9. Factors affecting Cyber security protections in Uganda

Uganda currently faces a number of internet-related issues connected to security risk, IP infringement, and inadequate data protection. Furthermore, the technical and financial resources needed to tackle cybercrime are insufficient. The majority of organizations in Uganda, both public and private, now see Cyber security as an IT problem rather than a business concern. Upper-level management places more emphasis on business performance and IT departments are only concerned with network and database infrastructure, ignoring the organizations' expanding security requirements.

In accordance with accepted international best practices, law enforcement organizations have a restricted capacity to investigate crimes involving computers. This is because cybercrime cases lack enough technical skills in digital forensics. And it is made worse by the personnel mix between the public and private sectors, which includes government-sponsored trained officials (Cyber security Capacity Review of the Republic of Uganda, 2016). The incapacity of Ugandan society and the legal system to keep up with the rate of technological advancement only increases this burden.

Additionally, to ensure service delivery, public entities hold a wealth of government and citizen information in various databases collected by various organs, such as SIM card registration, voter registration, and national identity card databases, while oblivious to the common threats this data is exposed to. Reviewing Uganda's current legal system reveals that concerns about data protection and privacy are not sufficiently addressed. Although some laws provide provisions for certain areas of data protection, they are fragmented and only apply to certain industries.

There is currently no comprehensive law to safeguard personal data by regulating how personal information is collected or to ensure that it is used only for the purpose for which it is collected, despite the fact that article 27(2) of the constitution stipulates that no person shall be subjected to the interference of that person's privacy of that person's home, correspondence, communication, or other property. Other people and organizations, such as banks, hospitals, hotels, schools, and others nationwide, collect and use personal information. However, there is no arrangement or proper regulation that is in charge of this sort of information being collected or its storage in order to preserve its integrity and the purposes, for the intended use and it is available in many scattered databases.

Significant information leaks occur when some companies in Uganda don't follow the necessary security procedures, putting those organizations in danger. For example, in 2018, Mulengera News published confidential information regarding the staff pay at public universities. The employees at Mbarara University of Science and Technology was caught off guard, and several vowed to sue university personnel.

2.10. Philosophical Theories of Ethics

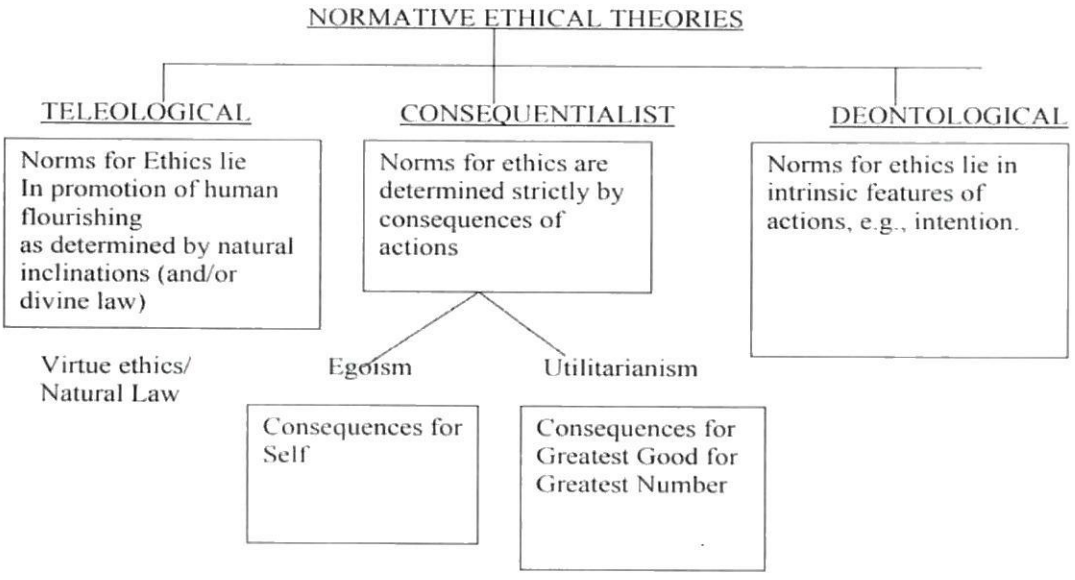


Figure 2. 1 Normative Ethical Theories' components

2.10.1. Consequentialism

Moral principles in consequentialist theories of ethics consider the likely effects of certain actions (Vallor, 2017). The most notable application of consequentialism is utilitarianism, which holds that the morally just thing to do is what will benefit the largest number of people in any given situation. Consequentialism, for instance, encourages activities that lead to human satisfaction, provide the greatest benefit, and do the least harm to all parties involved, including as consumers, employees, shareholders, the community, and the environment. This is true, for instance, of Cyber security. Cybersecurity plans and policies should strike a balance between the good that is gained by stopping cybercrimes and the less harm that is caused to all parties through monetary loss, business loss, injuries, and destruction. The founder of utilitarianism is the English moral philosopher Jeremy Bentham (1748–1832). Bentham thought that the highest moral standard was to maximize happiness and ensure that joy outweighed sorrow.

In utilitarian ethics, the "good" is measured in terms of happiness and contentment, which include intellectual, emotional, and bodily pleasures. According to Vallor (2017), refraining from causing harm to another person's bodily or psychological well-being is also thought to be beneficial. Choose a course of action with the least potential for harm or expense. Bentham (1907:3) (1907:3) According to Bentham, the standard for right and evil is the greatest happiness of the greatest number. According to "the greatest pleasure principle," Harrison, (2014), an action's moral value is only determined by its outcomes.

Bentham, (1907) recognized the idea of "utility," which he defined as everything that brings delight and avoids suffering. Therefore, carrying out the appropriate deed entails doing whatever raises utility, which in turn raises delight. Harrison, (2014) argues that utilitarianism should provide guidelines for specific situations and serve as a helpful manual on how to behave in any given moral predicament. It is difficult to predict consequences and thereby establish them, this theory has faced criticism. Duquency et al., (2008), echoes that utilitarianism is criticized for failing to recognize the individual or minority groups. Therefore, it was not taken into account for this study.

2.10.2. The deontological class of ethical theories

The name "Deontology" derives its meaning from the Greek word "deon," which is translated as "that which is bound or duty" (Harrison, 2014, p. 24). Immanuel Kant championed deontology, (1724-1804). All persons are rational beings, and are thus deserving of respect and dignity.

Deontology holds that when faced with an ethical choice, people should uphold their duties and responsibilities.

Only when a deontological action respects and complies with key criteria is it deemed to be ethical. This indicates that a person will uphold his or her duties to another person or society since doing so is what is morally right.

Ethics studies the morality of individuals, behaviors, policies, laws, and societal institutions (Duquency et al., 2008). Ocholla (2008), opines that ethics serves to uphold people's inherent goodness, prevent anarchy, and provide guidelines for moral behavior as well as moralities and principles that bring people together rather than divide them.

A number of studies have critiqued deontology because it is viewed as an insufficient morality manual. Deontology is challenging to put into practice Harrison (2014). He claims that not all circumstances are guided by pre-existing rules, and that in situations when there are no norms in existence, the canon may not offer ethical advice.

As approaches that might not be able to tackle complicated challenges in information and computer security ethics, the previous theories Rule-based and consequences have been contested by several authors. For instance, Volkman claims that rule-based and consequence-based ethics may not be able to manage an act if a person is unable to analyze the results of an accomplishment or even determine their reasonableness. Volkman maintains that no one can choose to act in a way that will result in the best outcome if there are no standards for evaluating the implications of that action and no means of predicting the outcomes.

Thus, the moral challenge of the complexity of Cyber security in cyber society may not be adequately addressed by consequences-based ethics theory. This is true because moral judgments are made personally and on an individual basis. Vallor (2017), posit that Cyber security experts work primarily "behind the scenes," which means that the majority of the time, the interested parties, such as their supervisors, employers, customers, and end users, may not be aware of what these professionals are doing. It is challenging to determine whether Cyber security actions are moral. Therefore, the rule-based and consequences techniques of ethics are insufficient for carrying out Cyber security work in the face of these moral conundrums.

2.10.3. The virtue ethics theories

In the Middle Ages, Averroes and Thomas Aquinas reinvigorated and strengthened virtue ethics, which had its roots in Plato and Aristotle. It is possible to define virtues as human traits that, when properly used, can make a person's life more enjoyable in the society in which they live. However, society members who lack qualities have lives that are unhappy and less content (Chatterjee et al.,2015). Aristotle, (2005) asserts that a person's free activities serve as examples of their virtues. Quinas, (2015), contended that virtues are personal qualities and conduct that might enhance a person's excellence. Löfquist, (2018) reaffirmed that virtues are crucial to human existence and that they enable people to lead moral lives. This was echoed by Hawking et al. (2017), that a virtue is what makes the owner good and his work morally equivalent. An ancient ethical foundation for moral behavior is virtue ethics. Individual ethics is more action-based than virtue-based. In contrast to ethical obligations, ethical standards, or the results of specific actions, virtue ethics is concerned with the virtue or moral character of the person performing an activity. Virtue morality emphasizes the need of upholding moral principles through effective instruction (Hackett & Wang, 2012). Stamatellos (2011), reaffirmed that virtue ethics mold a person's values. The four cardinal virtues of prudence, justice, courage, and temperance serve as the foundation of virtue ethics. Before humans may possess any other virtues, they must possess these four (Oderberg, 1999).

Gray, (2015) said that morality is important in the field of information security since ethical judgments, decisions, and choices must be made. Regarding moral conduct and adherence to Cyber security, virtue ethics controls may be an alternative approach. Chatterjee et al. (2015) posit that when it comes to adhering to Cyber security strategies, a professional's judgment may be influenced by their morality and behavior. Virtues encourage moral behavior in people. (Hackett &Wang, 2012; Chatterjee et al., 2015).

Information systems workers may be motivated to act honorably when performing their duties via virtue ethics. Virtue ethics help Cyber security experts realize that they have a moral responsibility to develop their moral character in order to advance the field. Cyber security professionals can understand the ethical principles that should guide their actions and decision-making by using virtue theories. virtue theories help Cyber security professionals locate exemplary people to imitate by using standards of behavior from role models who already exist in their local communities, (Vallor, 2017).

The three normative moral theories would offer useful theoretical support that could be utilized to evaluate the employees in the banking sector's ethical behavior with regard to Cyber security. For instance, if a deontological theory is accepted, then a discussion of what Cyber security laws, duties, and obligations the personnel of the banking industry need to abide by would be an intriguing subject for this research. Banks desire strong Cyber security for the data they store on computer systems. It is important to follow sound Cyber security policies, practices, and methods that promote human flourishing.

To increase Cyber security in banks, staff in the banking sector should follow the laws as they are. The question would have been whether or not Cyber security was bringing consumers of the internet the enjoyment they desired. Whether the policies and procedures for Cyber security in place are fair and just for fostering a happy society. Despite how worthwhile they may be, unfair Cyber security policies, laws, and procedures may eventually impair the desired results.

On the other hand, if a consequentialist approach is used, the research findings would take into account the moral value of the banking industry's online employees based on the idea of utility. However, virtue ethics also present an alluring prism through which to examine employee behavior. Virtuous Cyber security experts are advised to persevere and put good ethical judgment into practice. They enjoy their life and always act honorably toward everyone in their social circles, including coworkers, superiors, and customers. By enhancing their wellness, these Cyber security professionals serve as an ethical role model for others to follow.

There exists scanty research in information security that have used virtue theory, with the current research, virtue-based ethical theories might be a preferable choice. The focus of virtues is on helping people make better decisions and judgments that are based on righteous ethical practices rather than on standards and consequences. Although there has been recent research on virtue ethics in social work, (Papouli, 2018) there is still a void in the literature about the applicability of virtues to daily tasks. In comparison to fields like psychology, medicine, nursing, and education, the study of virtue ethics in computing, and specifically in Cyber security, is still in its infancy.

The Aristotelian ethical virtues and their impact on social work professions like Cyber security are another area where understanding is lacking (Papouli, 2018). Since virtue ethics are more of a personal character, virtue ethics may not be appropriate for usage in Cyber communities due to the diversity of worldwide tenets, (Floridi & Sanders 2006).

Relying on virtue ethics, moral people may attempt to use their own fundamental moral convictions to address global ethical problems, which could have unintended or undesirable global effects. However, a framework based on virtues is fit for use in information systems including the Internet is (Adam & Bull, 2008; Gray, 2015). Ethical obligations for a person to think about and act against their own interests have always been a part of virtue ethicsm (Hart, 2001; Aristotle, 2005). In order to improve employees' ethical behavior and conduct with regard to Cyber security, this study explicitly looked at Aristotle's virtue ethics in Cyber security.

Myyry et al. (2009), contended that employee decisions to violate policies are a result of moral conflict, hence moral reasoning theories are applicable to Cyber security. The study also provided a clear model of virtue ethics that may be utilized for study and practice in order to enhance moral behavior in the field of Cyber security. This model incorporates the Aristotelian cardinal virtue ethics structures with organizational ethical climates. Nussbaum and Sen (1993), assert that virtues are desirable traits that help people face life's problems. The cardinal virtues in this instance are character attributes required to overcome difficulties in Cyber security practice.

2.11. Theories for Ethical behavior

2.10.1. Theory of Reasoned Action (TRA)

The Theory of Reasoned Action (TRA), which has its roots in social psychology, was developed by Ajzen and Fishbein in 1980.

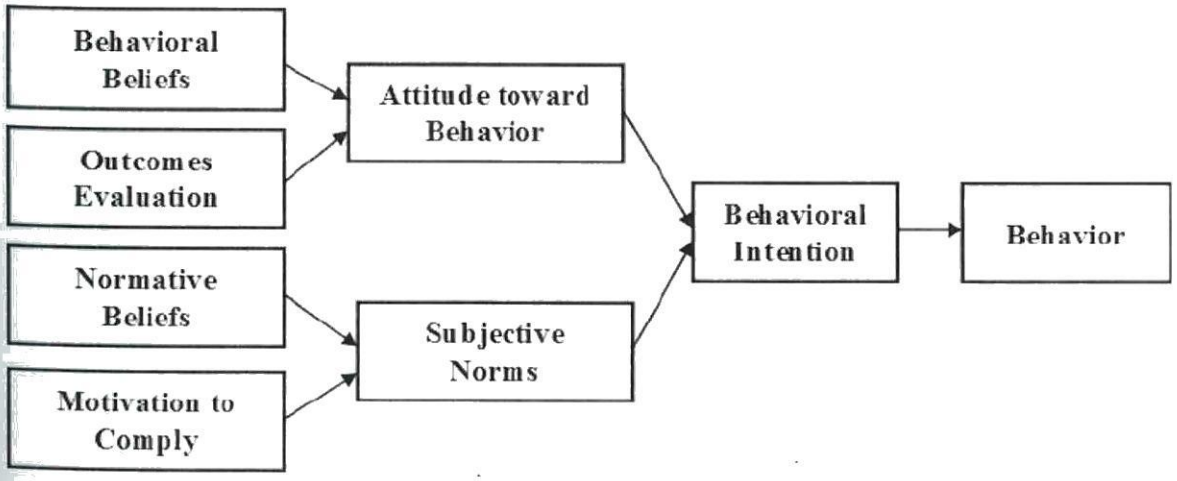


Figure 2. 2 Theory of Reasoned Action components

The TRA emphasizes the function of intention, social influence, and attitude variables in predicting behavior. According to TRA, a person's intents determine their conduct, attitudes and subjective norms are influenced by behavioral intention, and behavioral and normative beliefs are mediated by an individual's attitude and subjective norm. Ami-Narh & Williams (2012), opine that the external variables include demographic parameters, personality traits, ideas about things, attitudes toward objects, task characteristics, and situational variables. The applicability of this theory as well as its limitations have, however, come under fire. The model has a significant risk of confounding between attitudes and norms since attitudes can often be reframed as norms and vice versa. A second limitation is the assumption that when someone forms an intention to act, they will be free to act without limitation.

TRA is most successful when applied to behaviors that are under an individual's voluntary control. Although while attitudes and subjective norms may be highly motivating, if behaviors are not totally under the control of the individual, intervening contextual factors may prevent the behavior from being carried out.

The Theory of Planned Behavior (Ajzen &Fishbein, 1991) is an extension of the Theory of Reasoned Action by adding a construct called perceived behavioral control in an effort to account for factors outside the individual's control that may affect one's intention and behavior. This extension was based on the idea that behavioral performance is determined jointly by motivation (intention) and ability (behavioral control).

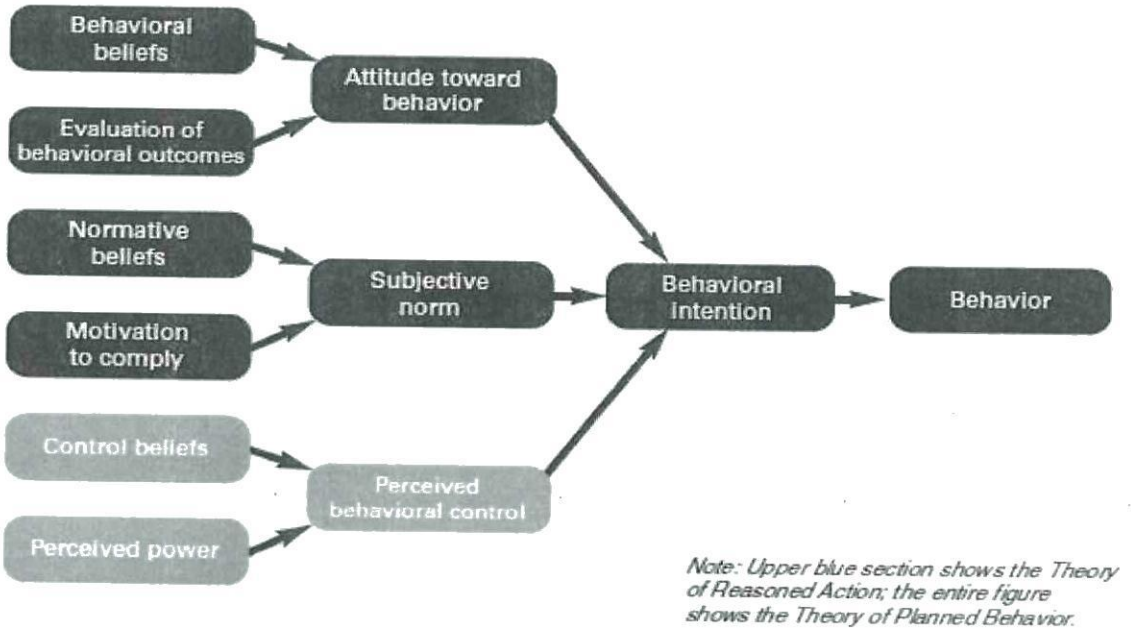


Figure 2. 3 Showing the Extended TRA to include Behavior control construct.

The TPB was created to forecast actions in which people have only partial voluntary control. The TPB develops the idea of perceived behavioral control by taking into account self-esteem and self-efficacy.

the theory of reasoned action (TRA) is a special case of the theory of planned behavior (TPB). The only difference between the two theories is that the TPB includes behavioral control as an additional determinant of intentions and behavior. The main difference between the Theory of Planned Behavior and the Theory of Reasoned Action is that there is a greater chance of being able to understand a person's actual attitudes through the Theory of Planned Behavior that result in the physical behavior that is being carried out (Martin, 2017).

2.11.2 The Theory of Planned Behavior

The Theory of Planned Behavior (TPB), was proposed by Ajzen in 1991. The theory opines that one's behavioral intention, or desire to carry out or refrain from acting, predicts their actual behavior.

The TPB concepts of perceived behavior control, attitude toward the activity, and subjective norms can predict intention and also account for a sizable portion of actual behavior, (Pham et al., 2017).

Armitage & Conner's, (2001) carried out an analysis of 185 works and found out that TPB is a useful predictor of behavior. With TPB, a significant portion of actual conduct is explained by perceived behavior control, attitude toward the activity, and subjective standards that predict intention (Pham et al., 2017). TPB has five components (Jafarkarimi et al., 2017).

- Behavior, which is an individual's activity in a specific situation and the result of intention and Perceived Behavioral Control (PBC). This suggests that a strong PBC is required for a desirable intention to become behavior. A behaviour is likely to occur based whether there is a high level of intent. If a behaviour is perceived as appealing, socially acceptable and is easy to do, it is likely to happen.
- Intention is a person's willingness to engage in a specific behavior. Its' a product of the behavioural attitudes, normative beliefs and the control beliefs. The combination of the three will produce an intention as to whether or not an individual will undertake a certain behaviour.
- A person's attitude can be defined as their assessment of how favorable or negative an action is. Attitude refers to how appealing or favorable a behaviour or act might be to the individual and the anticipated outcomes of undertaking behaviour. This is when an individual will weigh up the advantages and disadvantages. It's the propensity to respond predictably favorably or unfavorably with a thing, someone, or situation.
- iv. Subjective Norms (SN) are the opinions of a person about what most of the people who are significant to them believe they should do. Subjective norm includes the influence that other individuals, such as friends or coworkers, have.
- Perceived Behavioural Control (PBC) describes how easy or difficult a task is perceived to be. It's the level of control an individual believes they have in order to carry out a behaviour or an act.

Humaidi & Balakrishnan, (2018), contend that prior researchers have employed the theory of planned behavior (TPB) to explain user behavior in information system studies. TPB was used by Schwager et al., (2016) to investigate how people use social networking security settings. The findings of the study demonstrated that Subjective Norm, Attitude, and Perceived Behavioral Control were predictive of Behavioral Intention. Positive behavioral intention had a causal effect on behavior.

While Perceived Behavioral Control positively influenced Social Trust, Apathy negatively predicted Attitude. TPB and the Theory of General Deterrence were integrated by Cronan et al., (2006) to analyze students' intents to misuse software and data. TPB was used by Wong et al., (2013) to investigate the effect of video game console piracy on consumer adoption.

The intention of users and their actual reading of computer usage policies have both been examined using the Theory of Planned Behavior. One study looked into the purpose and actual reading of computer usage policies using an enhanced version of the TPB that included Social Trust and Apathy. The study's findings imply that attitudes, social trust, and apathy have an impact on whether people read computer usage regulations. A comparable study examined employee attitudes toward compliance with organizational information using the TPB, Normative Belief, and Self-Efficacy.

The user acceptance of information systems that are intended to anticipate human behavior has been extensively examined using TPB (Uffen & Breitner, 2013; Liao et al., 2007). Rahman & Loukaka (2017, Fishbein & Ajzen (2010), TPB, is a reliable hypothesis for predicting actions related to information security policy compliance. Toe et al. (2016), posit that TPB has faced criticism because of its apparent poor predictive efficiency, which is linked to the use of an insufficient number of constructs to explain why people agree to a particular behavior in a given situation.

Pham et al. (2017), opine that there are several behavioral models that offer a solid foundation for explaining employees' security decisions. Shemroske (2011) asserts that social behavior-related existing IS research is lacking in ethical components. The Theory of Planned Behavior (TPB) is cited in the majority of studies (Ajzen 1991) Tommasetti et al., (2018) argue that TPB is used in some studies as a foundation for explaining behaviors related to IT and has proven to be reliable, however it lacks any component that fits in directly and precisely the philosophical considerations that affect ethical behavior.

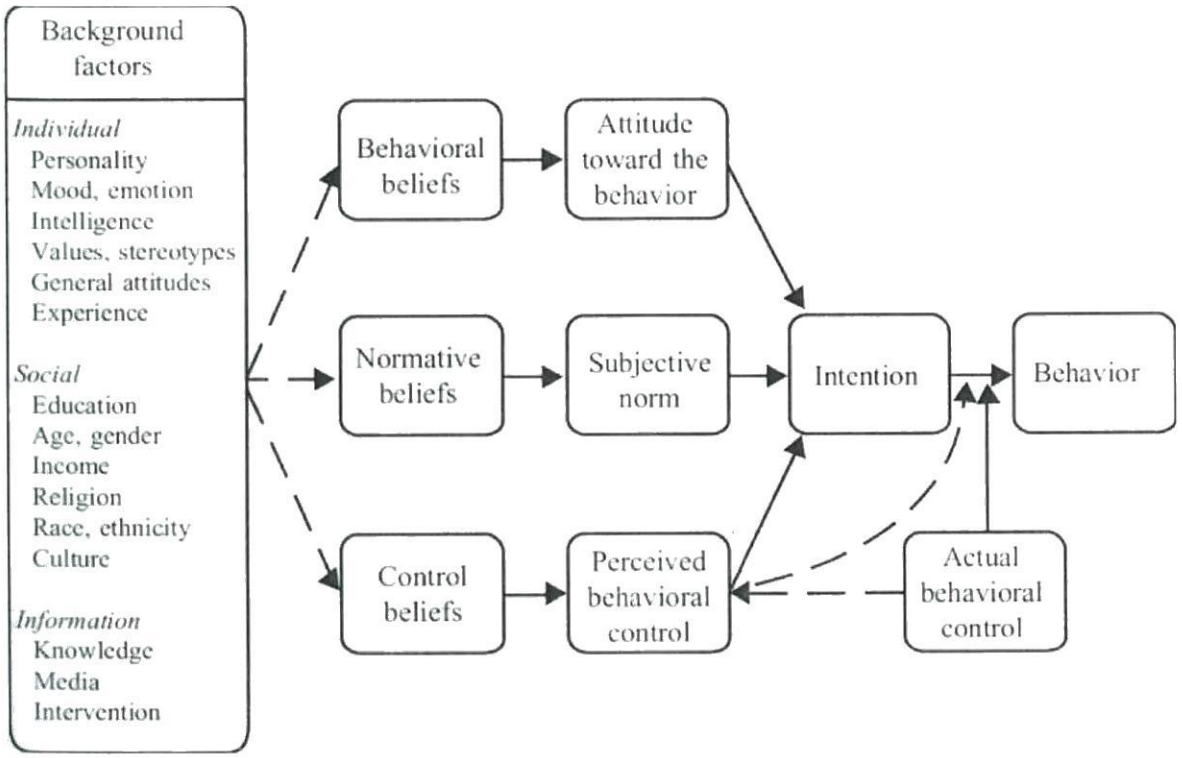


Figure 2. 4 Theory of Planned Behavior components, (Icek Ajzen 2019).

2.10.3. Contingency Framework for Understanding Ethical Decision Making in Marketing

A contingency framework was developed by Ferrell and Gresham in 1985 to explain how ethical choices are made in marketing. They provided a model that takes into account both organizational and personal considerations.

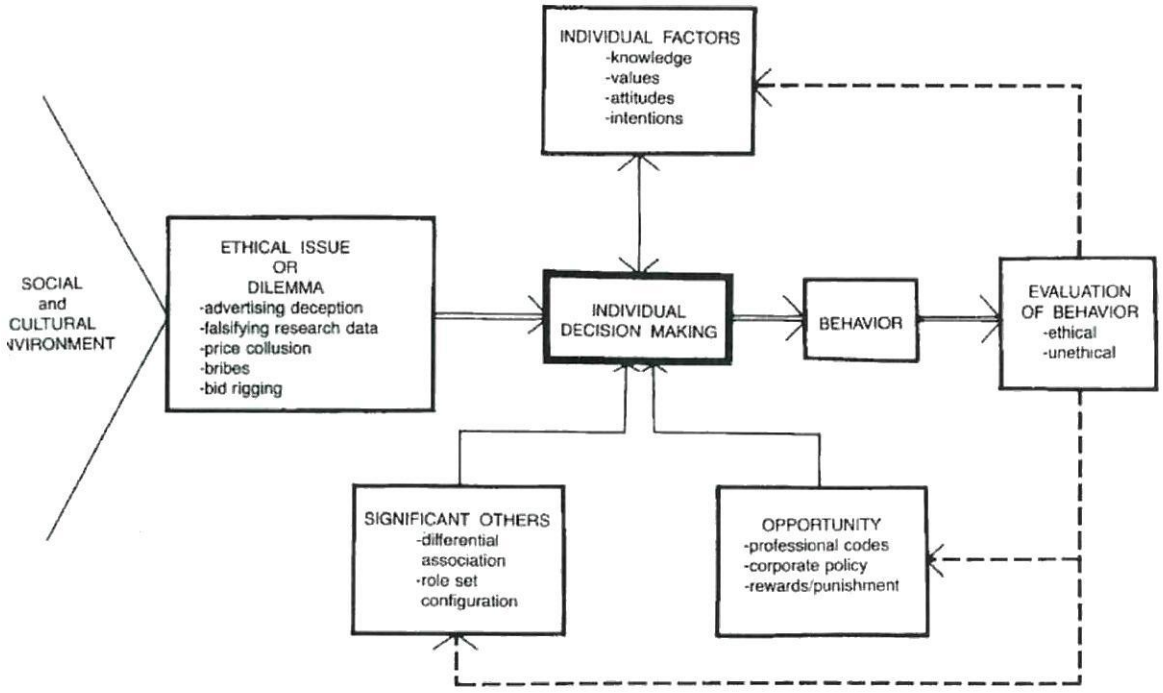


Figure 2. 5 Components of Contingency Framework for Understanding Ethical Decision Making in Marketing.

Knowledge, values, attitudes, and intentions are only a few of the personal factors assessed. Organizational issues, such as differential association theory, role set configuration, and organizational openings like corporate policy, professional codes, and rewards/punishments). To be formalized in their contingency model, Ferrell & Gresham, (1985) abandoned their normative ethical theories, which they claimed had a vital impact on specific factors. Furthermore, their model has not been empirically tested; thus not used in the current research.

2.11.4. Bommer, Gratto, Gravander Tuttle's behavior model of ethical and unethical decision making

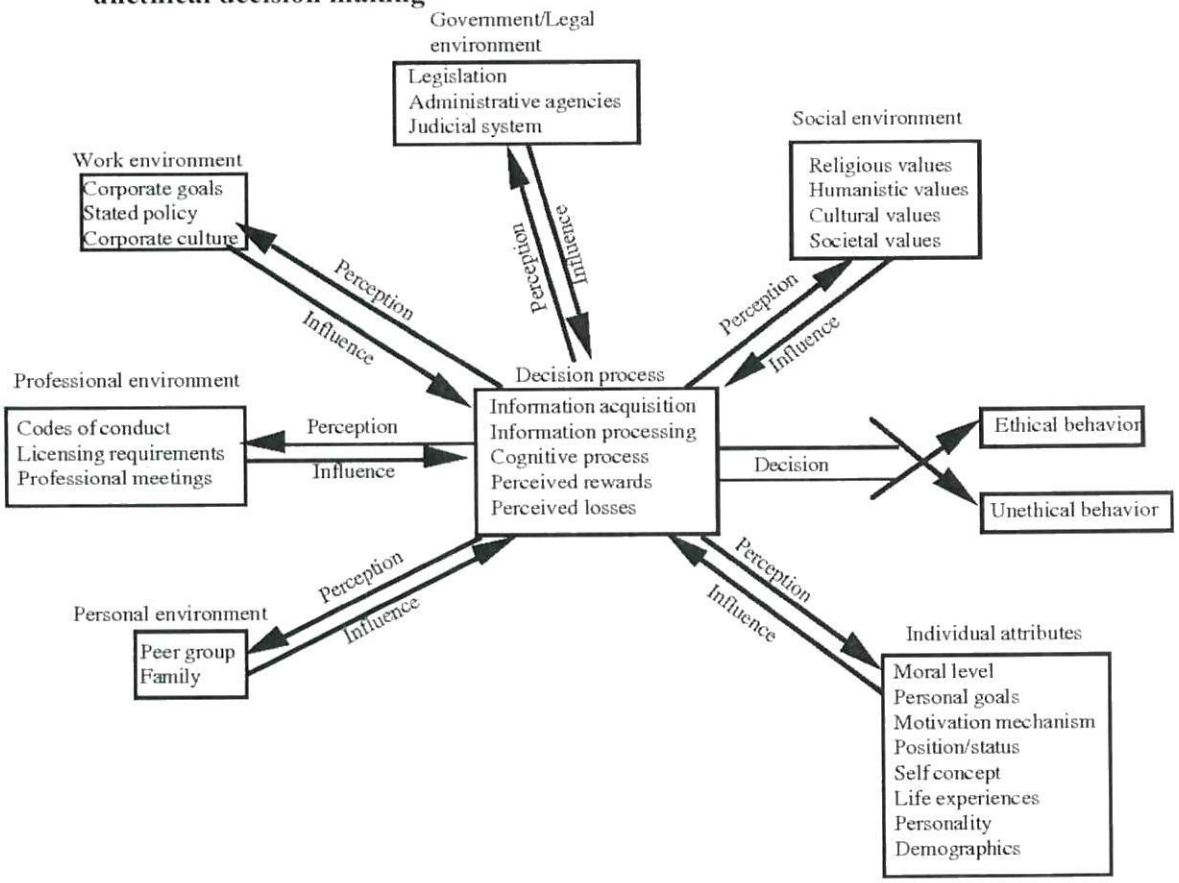


Figure 2. 6 A Theoretical Model for Ethical and Unethical Decision Making (Bommer et al. 1987).

In order to determine whether a decision should be made in an ethical or unethical manner, Bommer et al., (1987) proposed a theoretical model that included perception and the degree of influence of individual attributes, personal environments, professional environments, work environments, government/legal environments, and social environments. Additionally, there is no empirical support for this model.

2.11.5. The Hunt-Vitell General Theory of Ethics (Hunt & Vitell 1986)

Hunt & Vitell created this model in 1986 to guide research on the moral conduct of marketers. The generalizability of this paradigm, however, allows it to be used in different contexts. For instance, Gopal, et al., (2004). The name was altered to the "Hunt-Vitell Theory of Ethics" because this model had a wide range of applications (Hunt & Vitell 2006). The model's ethical practices are teleological and deontological in nature. The model's goal is to more clearly explain how ethical actions are thought about and how that thought affects subsequent behaviors. Each of these stages results in a cognitive assessment of a particular action, which is then used to create an intention to act. Vitell &Hunt submit to Ajzen & Fishbein suggesting intentions lead to behavior.

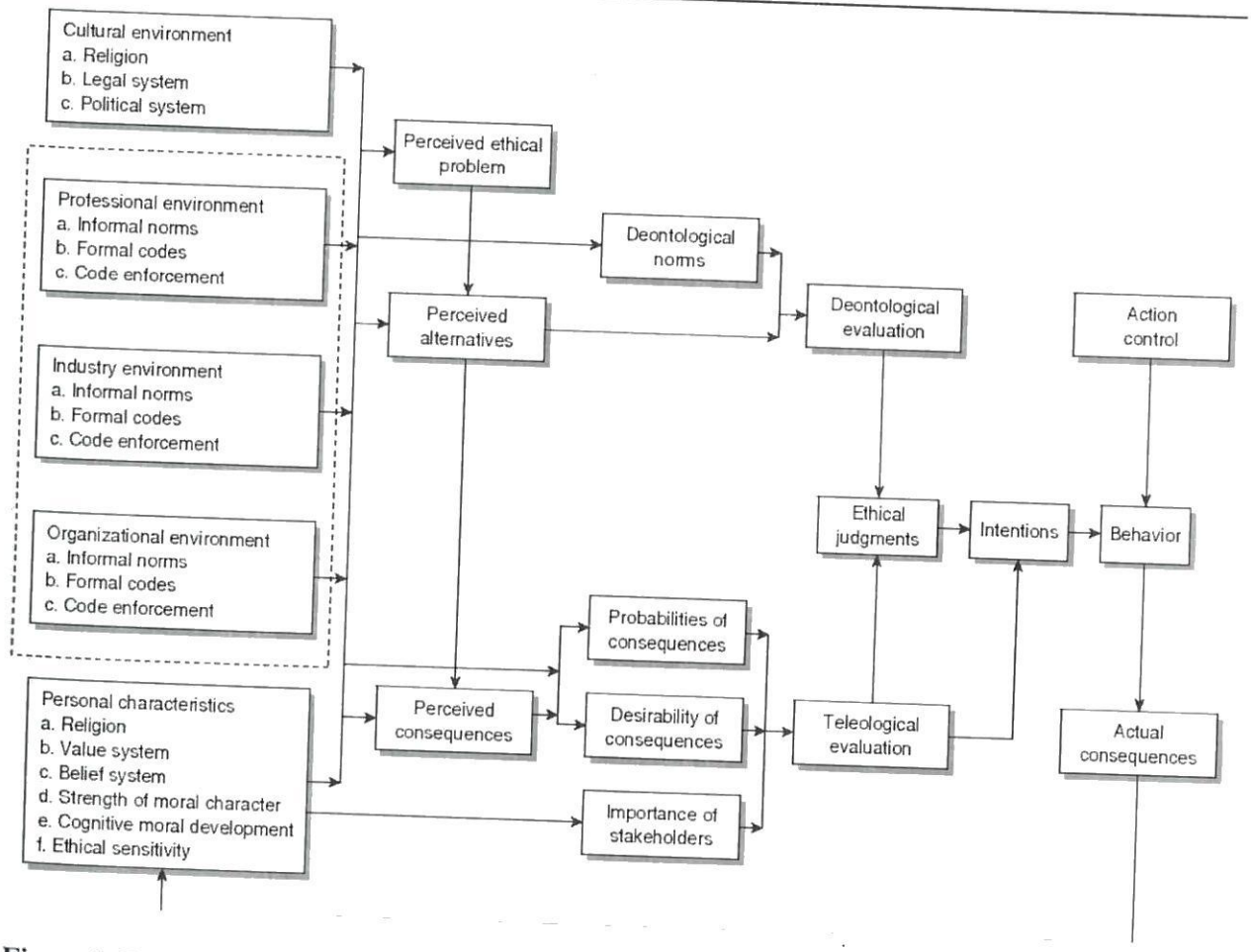


Figure 2. 7 The Hunt-Vitell General Theory of Ethics components, (Hunt & Vitell 1986).

However, studies investigating the use of the HV model tend to test only a portion of the model Shemroske (2011). The HV model states that while the ethical judgment might select a specific decision as the most ethical, the evaluation of consequences might override any decision about what is most ethical for sake of desirability of a specific consequence.

2.11.6. General Deterrence Theory (GDT)

Gundu, (2019), explains that the deterrence theory primarily focuses on employees' intentional non-compliance with Cyber security policies and procedures. Employees may choose not to follow Cyber security protocols out of convenience, because they choose to disregard rules, or because they don't comprehend them. Fear is used as a control mechanism in deterrence along with the prospect of punishment. Utilizing this control strategy, an employee assesses the behavior's results and weighs them against the danger. GDT provides useful insights into how protections act as deterrents by preventing punishments. However, the argument is flawed when a criminal goes beyond the point of deterrence and turns to cybercrime (Willison, 2006). GDT have been used as preventative measures in information security research. Straub & Welke (1998), posit that IS security measures Deterrence, prevention, detection, and recovery are said to be the four interrelated actions that make up argument of IS security controls.

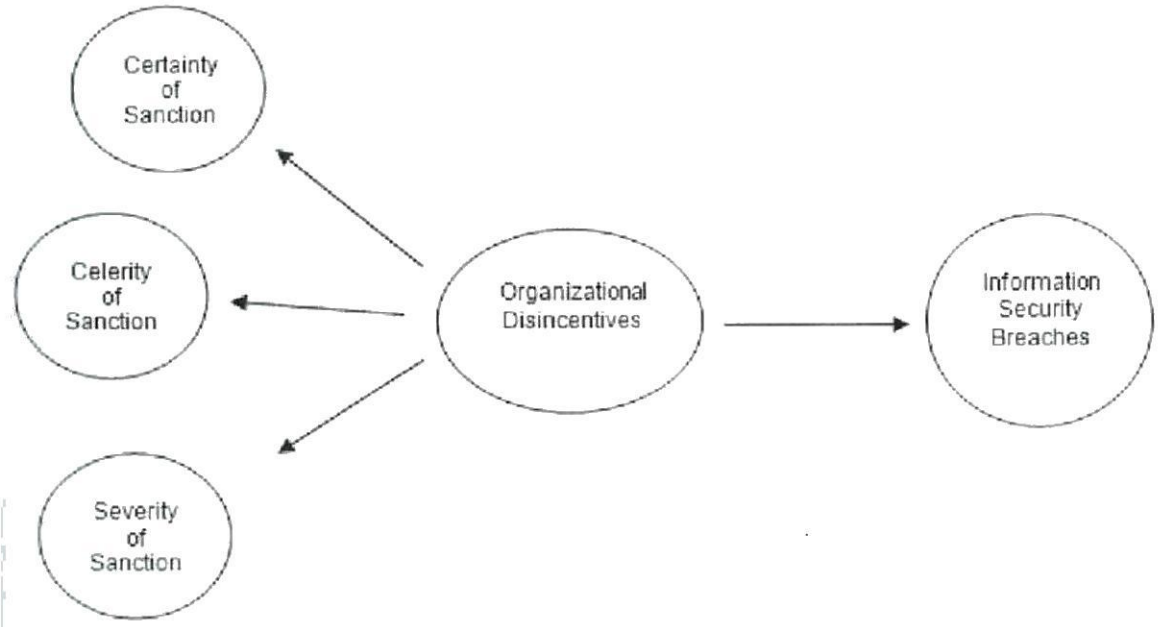


Figure 2. 8 General Deterrence Theory (GDT).

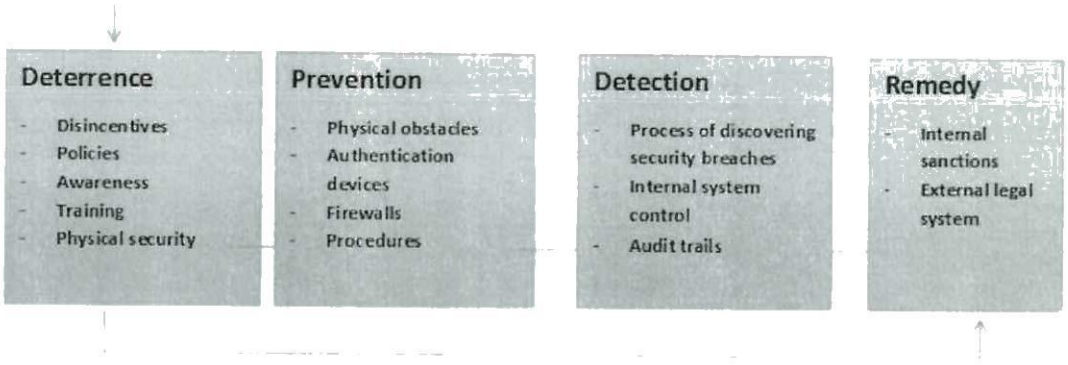


Figure 2. 9 A theoretical model derived from the general deterrence theory.

By reducing system risk, these initiatives seek to increase IS security. Halawi (2013), conclude that employing and enforcing harsh judgments or penalties may deter aspiring criminals from engaging in illegal or undesirable activity. Straub & Welke (1998), argue that the threat of punishment should be used to deter someone from acting inappropriately. When everyone is aware of the consequence, it will similarly deter them from carrying out similar undesirable activities (Gray, 2015; Theoharidou et al., 2005). The application of GDT techniques can stop the abuse of IS.

Although punishment has been demonstrated to be mostly effective in deterring essentially just minor inspired potential criminals, deterrents may not be effective for those significantly inspired criminals. While the GDT has seen some success, it is evident that deterrence is frequently ineffective at stopping transgressions especially from highly motivated criminals.

The current research borrowed the virtue constructs of prudence temperance, courage, and justice together with the theory of planned behavior elements of behavior intention and actual behavior moderated by ethical climate. These constructs were studied and used as assessment constructs in a Cybersecurity ethical behavior assessment model and its web based ethical behavior assessment application.

Table 2. 1 Showing the Theoretical Gap Analysis.

Construct	Virtue Ethics Theory	Theory of Planned Behavior
Prudence		x

Justice		x
Courage		x
temperance		x
Behavior intention	x	
Ethical behavior	x	
Ethical climate	x	x

The virtue ethics theory Aristotle, (2005) helped to identify and describe the cardinal constructs for Cyber security ethical behavior intention of the employees in the commercial banks in Uganda. The major contributions of virtue theories are the cardinal constructs of prudence, justice, courage, and temperance. However, the theory is short on explaining behavior intentions towards Cyber security. These four-virtue ethics-based constructs never solely or directly affect employee's ethical behavior; they are always filtered through ethical climate which moderate their effect. The virtue ethical theory lacks the behavior intention, ethical behavior and ethical climate.

The idea of planned behavior cannot be used by itself to explain behavior because it does not demonstrate how moral behavior could be accomplished. While TPB is helpful in understanding attitudes and other antecedents, it is lacking in the ethical component and does not provide an explanation for how ethical action develops. None of the two theories address the ethical climate, according to the theoretical gap analysis table. Employees can develop ethical behavior through being exposed to an ethical workplace culture. Practice has shown that there is an issue. Organizations need to foster an ethical environment. Employees are encouraged and required by EC to adopt appropriate ethical behavior when carrying out their organizational obligations.

2.12. Conceptual Framework and Developing Hypotheses.

A conceptual framework is a structure that the researcher uses to explain how the phenomenon under study is likely to develop (Camp, 2001). It is consistent with the theories, practical research, and essential ideas utilized to support and organize the researcher's knowledge (Peshkin, 1993).

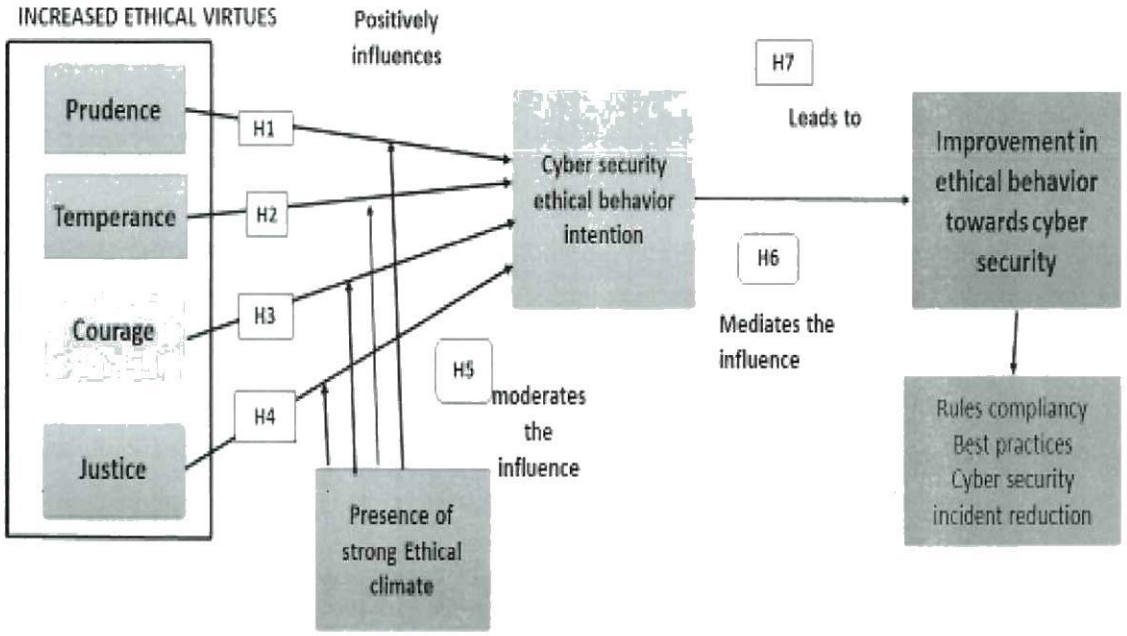


Figure 2. 10 A conceptual frame work.

Waithaka, (2016) expounded a conceptual framework as an explanation of the researcher's perspective on the issue and advances the research. The conceptual framework aids the researcher in determining the connections between the many constructs under investigation. The virtue theory and the theory of planned behavior serve as the foundation for this conceptual framework. The conceptual framework depicts how the constructs have an impact on "intention," which in turn has an impact on "behavior." Prudence, Temperance, Courage, and Justice are the four components of the Cardinal Virtue Ethics, which serves as the study's independent variable.

The dependent variable of the study is employees' Cyber security ethical behavior. The moderating variable is the organizational ethical climate. And the mediator variable is the behavior intention.

The researcher hypothesizes that Cyber security is realized where; (1) prudence is high, (2) Temperance is high, (3) courage is high, (4) Justice is present (5) Organizational ethical climates are in favor of Cyber security.

2.12.1 Prudence and behavior intention

Prudence, according to Aquinas, (2005), is the presentation of wisdom or the right reason when appropriate action is being examined in light of a particular situation. Prudence is the ability to decide, based on knowledge, the best course of action to take, especially in a field where situations and fundamentals are always changing. Prudence is the inclination and ability to make wise judgements about acts that are good for other people (Bartunek &Trullen, 2007). Prudence takes into account what is morally sound, good for oneself and others, and healthy throughout life. Cyber security breaches that cause harm to others frequently result in catastrophic circumstances to people and organizations. Riggio et al., (2015), uphold that prudence is the wisdom that maintains a suitable balance between two extremes. it's used to make the appropriate choice that minimizes harm while maximizing the use of the intention for virtuous conduct. Pisk, (2017), posit that the foundation of human nature and all moral behavior is reason.

Alfawaz et al., (2010), advance that a person's knowledge, professional skills, and values, together with consistent behavior, have an impact on their Cyber security behavior. Virtuous deeds involve the ability to overcome conflicts between organizational goals and security policies. Prudence is a virtue that aids in reasoning, (Siponen & Iivari, 2006). Aquinas, (2005), opines that moral behavior stems from reason. Echoed by Aristotle, (2004), reason is a distinctive human talent and the highest faculty of the human being, and it governs a happy existence.

Moral behavior should be consistent with reason, and evil behavior should be opposed by reason. Therefore, reasoning and making decisions are the tasks of prudence as a virtue. Additionally, it enables quick decisions to be made under any condition. A person can fight against the temptation of unfairness and fearfulness with the support of wisdom. Gray & Tejay (2014) conclude that the ability to think clearly, reason well, and make the right choice at the right time is what is meant by prudence. Bartunek & Trullen, (2007), opine that routine daily hiccups typically call for caution. This was repeated by Vallor, (2017) that daily Cyber security activities, roles, and interests need caution because these obligations can result in serious consequences.

Lack of prudence could lead to financial problems, fatalities, and a decline in client faith in a company. Therefore, taking into account the value of caution, a Cyber security professional should exercise caution in their ethical decisions in order to manage the complexity of the cyber society.

Therefore, the study proposes;

H1. *Increased Prudence positively influences the Cyber security ethical behavior intention.*

2.12.2 Temperance and behavior intention

Gray & Tejay (2014), explained temperance as the capacity to control one's emotions and behavior as well as personal humility and self-discipline. temperance is defined in terms of what a person voluntarily refrains from doing, such as refraining from retaliation and choosing to be calm and merciful instead, renouncing arrogance in favor of self-effacement and humility, refraining from excesses and refraining from excessive anger and instead exercising self-discipline (Schwarzer & Ralf, 2012). Papouli, (2018), said self-control allows a person to refrain from acting in ways that are harmful to him or others. Employee morale promotes ethical behavior and can improve Cyber security. Increasing employees' morals and expertise has a clear impact on their ethics, which can help to advance Cyber security.

Employees working in Cyber security can apply and use the idea of Aristotelian temperance as a self-care strategy to minimize tiredness and avoid wrongdoing, (Papouli, 2018). This study considered temperance as the ability of the Cyber security professionals to uphold control and to desist and avoid acting in excess on their security responsibilities, regulate their yearnings, activities, and conducts, and be true to themselves and others particularly in their Cyber security dealings. An ethical individual, (Myyry et al., (2009), is self-reliant and restrains his temptation to violate security. The attitudes and behaviors of professionals, and how they manage their emotions, promote moral behavior and aid in the security of information systems. People are intemperate if they refuse to acknowledge that they are weak in some areas or if they cannot accept that they are flawed. As a result, managers who have little regard for people and are constantly curious in what happens at their workplaces end up interfering and intervening. Then, this need for information is bad, poorly reasoned, and can be described as intemperate.

McManaman, (2006) asserts that egocentric professionals who get overly preoccupied with themselves and end up becoming materialistic and selfish are viewed as being out of control. Additionally, intemperate frontrunners include Cyber security managers who make an effort to act dishonestly, pretend to be meek by giving up on themselves or their reasonable demands, and ultimately display fake humility. Employees of an organization should be conscious of work ethics in both their conduct goals and when performing their daily tasks.

By honing their virtue ethics and competence, professionals' work ethics are frequently improved and impacted, which can increase Cyber security (Gray &Tejay, 2014).

The study therefore hypotheses that;

H2: *Increased temperance positively influences the Cyber security ethical behavior intention.*

2.12.3. Courage and behavior intention

Courage: The quality of courage aids the possessor in their efforts to promote an organization's long-term wellbeing and prosperity. Bravery is the capacity to face fear, reluctance, or coercion. Employees in positions of leadership display bravery (Caldwell et al. 2015; Gray & Tejay 2014). Employees who are courageous endeavor to ensure the future safety and security of the company. A possessor performs successfully when they combine courage with a wise and modern evaluation of their options and possibilities. Professionals in Cyber security who exhibit courage are more likely to increase the protection of their assets. According to Papouli, (2018), a courageous social worker must make a difficult choice in order to carry out the right deed in spite of threats and dangers. Cooper, (2015) said that social labor is an act of bravery since it frequently requires its participants to put courage into practice in the face of overwhelming challenges and difficulties at work. Making an ethical decision requires courage. Leaders who exhibit courage as a virtue support the continued success of their businesses. Employees of the firm who exhibit courage in this scenario have admirable demeanors that aid them in overcoming difficulties in Cyber security activities. Valor, (2017), contended that a cyber-security professional who is tasked with protecting a company's network and sensitive data from hostile attacks must valiantly carry out his duties despite all obstacles. This is due to the possibility that the success or failure of the Cyber security expert could affect the company's information confidentiality and their ability to remain in business. Stamatelos, (2011) asserts that adhering to the demands of Cyber security requires employees in that field to have enhanced personalities, individual growth and enhancement,

developing ethical and precise selections, adopting good security tactics, along with courage. As a result, ethical issues are crucial and at the heart of Cyber security procedures. To better protect and shield people's capacity to live fulfilling lives, Cyber security experts should develop the virtue of courage (Valor, 2017). Cyber security is likely to be improved by professionals who exhibit the virtue of courage, who are willing to embrace excellent security techniques, and have the guts to take and monitor the proper measures even in difficult circumstances.

Consequently, this study suggests that;

H3. *Increased courage positively influences the Cyber security ethical behavior intention.*

2.12.4. Justice and behavior intention

Justice is explained as a means of ensuring that each person is able to exercise their legal rights (Mumcu & Döven, 2016). Organizational justice is a crucial idea that helps organizations carry out their tasks and gives employees happiness from their work, in addition to explaining the role of justice in the workplace (Greenberg, 1987). The idea of organizational justice is based on how people within the organization view justice. General justice and particular justice are two different types of justice that Aristotle (2005) discusses. General justice monitors the law (Riggio, et al, 2010). If a behavior is illegal, it is unjust. Fairness is a key component of specific justice; an act is deemed unjust if it is thought to be unfair. Papouli, (2018) contends that, Justice is a fundamental value for social work and other forms of social practice. Social Justice involves a constructive view of society that ensures that all members of the community receive an equitable share of resources and wealth, which is distributed in a safe and secure way. Faithfulness, appreciation, and trust are fostered and encouraged, which shapes virtue-based responsibility ethics. This is especially important for safeguarding and maintaining private information belonging to people and organizations (Gray & Tejay, 2014). Using information systems ethically means taking into account all parties involved, including staff members, customers, and the administration. Additionally, Cyber security experts should make morally righteous judgments and conclusions regarding Cyber security and safety regulations.

Stamatelos, (2011), argued that cyber ethics and proper behaviour include methods for being sensitive and kind. Additionally, it involves making more informed decisions about personal policies, societal norms, and decisions that could have an impact on society.

Employees in IT jobs should have good moral character in order to improve and enrich Cyber security in the digital society. Justice, Aquinas, (2005), takes into account the interactions among other people. The ongoing commitment to giving each person what they rightfully deserve; just or fair deeds. Gray & Tejay (2014), justice entails acting responsibly, being fair, and being considerate of the rights of others. The technology is the issue here, according to justice (Valor, 2017). Justice is a moral and legal issue. Chatterjee et al., (2015), Aristotle had two ways of defining justice as a virtue: distributive justice and corrective justice.

The focus of corrective justice is mainly on the law. Distributive justice was considered in this study. (Chatterjee et al., 2015) assert that distributive fairness strengthens confidence. Additionally, a key component of social capital is trust. Those who have access to the huge benefits promised by new technologies should be done and ensured in the right manner, (Valor, 2017). Cyber-security professionals should disclose the technology hazards, in the correct way. Virtues are thus behaviors of fascination refined through practice that result in the actions essential for an individual to flourish. Aristotle deliberated that virtues are important in community management. Dyck & Kleysen, (2001) echoed that virtues are good at enhancing professional activities. Hackett & Wang, (2012) noted that virtues are required of an "exceptional" leader.

Basing on these arguments this study proposes;

H4; *Increased justice positively influences the Cyber security ethical behavior intention.*

2.12.5. Ethical Climate and Ethical Behavior

Table 2. 2 Theoretical Types of Ethical Climate (Victor & Cullen, 1988 p. 668).

		Locus of analysis		
		individual	local	cosmopolitan
Ethical theory	Egoism	Self interest	Company's profits	efficiency
	Benevolence	friendship	Team interest	Social responsibility
	Principal	Personal molarity	Company's rules and procedures	Law and professional codes

Egotism, helpfulness, and principlism, (Mumcu & Döven, 2016), are all unquestionable rules that reflect ethical judgments. The first and most significant component of the structure, egoism, concentrates on actions that aim to maximize self-interest and selfishness. The other two additional structures, helpfulness and principlism, speak to the caliber of the workforce.

Helpfulness accomplishes this through making choices and acting in ways that will benefit the greatest number of people. According to the principlism idea, the actions and behaviors that determine a person's goodness are determined by rules, regulations, codes, and processes.

A shared understanding of what establishes moral behavior and appropriate behavior among organizational members is referred to as the ethical atmosphere (Martin & Cullen, 2006). It also entails the notion that specific moral principles or behaviors ought to be recognized as rules for business decision-making. Xue et al., (2018), assert that an organization's ethical atmosphere sends out signals to its employees about appropriate behavior and ethics. Sabiu (2016), posit that improving the ethical climate in a business enterprise may have a major impact on organizational performance. The degree to which an organization experiences genuine ethical problems is influenced by the ethical climate. Decision-making and subsequent conduct in the face of ethical difficulties are influenced by the ethical climate (Martin & Cullen, 2006). Employees who thought that success and moral conduct were very consistent ideas also appeared to be happier at work. This may suggest that encouraging moral behavior could foster a climate that increases job satisfaction (Vitell & Davis, 1990). An organization's ethical code of conduct can have an impact on the ethical climate (Otaye-Ebede et al, 2019). These codes of ethics embrace a formal regulation that establishes expectations for employees' behaviors. Models of corporate moral decision-making also identify the influence of organizational problems on an individual's moral or ethical choices. Victor & Cullen proposed that ethical climate is one of the several organizational work climate types and backed the work of Schneider & Snyder 1975; Schneider & Reichers,1983). Trevino (1986), opined that people typically seek outside assistance when they have ethical questions. Therefore, organizational elements like guidelines, rewards, and the organization's influence can serve as a link and have an effect on employees' ethical behavior.

In Florida, a study was conducted by Kessler et al., (2019) on 261 workers from the four occupational groups of hospitals, doctor's offices, rehabilitation facilities, and nursing homes. The Information Security Climate Index was linked to better employee information security motivation

and information security practices, according to the study's findings. The study also showed that the environment of information systems has the ability to have a beneficial influence on employees' behavior and motivation, ultimately resulting in a decrease in the incidence of data breaches.

Dinc, (2018) conducted a study to investigate the connection between employees' organizational commitment, job satisfaction, and ethical climate in Bosnia and Herzegovina. A caring workplace culture has a good impact on overall job satisfaction, according to results based on a sample of 151 employees from three private banks.

A quantitative survey from 181 educational agencies in Nigeria was conducted by (Sabiu et al. 2019). The goal of this study was to comprehend how the ethical climate mediated the relationship between performance evaluation and organizational performance. The results showed that the relationship between performance evaluation and organizational performance can be mediated by ethical climate.

A thorough assessment of the literature exploring the causes, effects, and moderators of ethical climates in relation to other variables was conducted by (Newman et al., 2017). Their article highlights the need for future research to include a dynamic perspective to study ethical climates, examine the impacts of ethical climates on work outcomes, extend the study of ethical climates to various organizational levels, and investigate the influences of culture on ethical climates. Baron & Kenny, (1986) argued that the inclusion of mediator or moderator variable could best address the inconsistencies in research findings hence the inclusion of Ethical Climate variable in the current study.

Despite the fact that there is significant research about ethical climate little research has been conducted on the mediating potential of the influence of virtue ethics on organizational employees' Cyber security ethical behavioral. Such research is theoretically significant because it presents insights into what ethical climate really exists and what organizations leaders essentially do to influence employees' behavioral intention towards Cyber security. This basically affects how firms make decisions and predict employee misconduct with regard to Cyber security. On the same note Kuenzi et al., (2019), expounded that a company's employees are able to uphold ethical behavior within the workplace if there is presence of a strong ethical climate. Employees are less likely to violate the organization's ethical standards in order to accomplish goals and objectives when the ethical climate within the workplace is robust. Hence, this study argues that EC may play

a moderating role on the connection between virtue ethics and employees' ethical behavior intentions.

The study tested the influence of Ethical Climate to moderate the link between cardinal virtue constructs and employees' ethical behavior intentions specifically in the Ugandan commercial banks.

Therefore, on the basis of literature this study hypothesizes that:

H5 *Ethical climate moderates the influence of virtue ethics on Cyber security ethical behavioral intention.*

H5a. The presence of strong ethical climate moderates the influence of prudence on Cyber security ethical behavior intention

H5b. The presence of strong ethical climate moderates the influence of courage on Cyber security ethical behavior intention

H5c. The presence of strong ethical climate moderates the influence of Temperance on behavior intentions of employes'ethical behavior towards Cyber security.

H5d. The presence of strong ethical climate moderates the influence of Justice on Cyber security ethical behavior intention.

2.13. Cyber security ethical behavior intention and improved Cyber security ethical behavior.

Ajzen, (1991) defined intents as the indication of the degree and quantity of efforts that people are willing to apply to complete a given conduct. Three elements attitude toward the conduct, subjective norms, and perceived behavioral control are said to be the foundation of intentions (Schwager et al., 2016). The majority of studies on security compliance examined security intention as the dependent construct and claimed that intention would result in real conduct, in line with the TPB's fundamental premise regarding the link between intention and behavior (Sommestad et al., 2014). Leonard et al., (2004), argue that one's behavioral intention comes before the actual activity in a direct manner. Though it's also possible that virtue appraisal and assessment have a direct impact on intention. In order to establish a framework for intended outcomes while implementing an ethics-based model, a company must define what constitutes ethical behavior (Gray, 2015).

Behavioral Intention positively influenced users' behavior toward modifying social networking privacy and security settings, (Schwager et al., 2016). A person's intention to engage in or refrain from engaging in a particular conduct is known as intention to behave.

In their editorial preface, Cronan & Douglas noted that ethical behavior is still a crucial global concern. They put out a theoretical framework that supports the idea that a person's attitude affects their intention to act ethically. This is also affected by a number of other factors, including as beliefs, the perceived importance of the subject, and the results of the action. Gray (2015) provided concise guidelines for moral conduct when it comes to information system security. These include; i). Rules compliance, which is seen when staff members follow the organization's security requirements, policies, and regulations, adhere to prescribed norms of proper conduct, and show the ability to make morally responsible decisions. ii) Adopting best practices, which means that when faced with information system security challenges, personnel will apply the appropriate processes and practices that guide the industry and their professions in the lack of particular instruction. Reduction of security incidents, loyalty, and dedication to security. iii) Incident reduction is evidence that there are fewer instances overall of information loss, breach, disclosure, or theft. iv) Loyalty that demonstrates self-control and reliability by upholding ethical principles and being ethically dependable (Gray, 2015). An employee's views and beliefs greatly influence whether or not they will abide by ISS standards.

Yoon & Kim, (2013) conducted study, using structural equation modeling to experimentally examine data from 162 employees across several Korean firms. The study's findings, organizational standards and moral responsibility have a big impact on how employees behave with regard to computer security. The study also revealed that an employee's inclination to conduct computer security behavior was significantly predicted by their moral responsibility and attitude toward it.

Schwager et al., (2016) surveyed issues that affect users' behaviour when updating their social networking security settings using the Theory of Planned Behavior. The findings supported the theory that Behavioral Intention was predicted by Attitude. This support is in line with the belief that users' attitudes toward engaging in a behavior are influenced by those attitudes.

To examine the variables that might affect a person's attitude toward ethical behavior in the context of information systems (IS), Leonard & Cronan (2005) conducted a study.

They compared their findings to those of a previous study to see if any changes had occurred. The results demonstrated that a variety of factors, depending on the specific sort of ethical issue at hand, influence attitudes toward ethical decisions. The impact of attitude on behavioral intention was proven by (Leonard et al.,2004).

The organization's overall security posture, is maintained when the attitudes of its workforces are in line with its security objectives and requirements (Gundu, 2019). Employees with "strong" attitudes display adaptable attitudes and behavioral intention linkages, whereas "weak" attitudes may exhibit weaker relationships. Bhattacherjee & Sanford (2009) contend that more time investments for learning secure practices, and better Cyber security compliance is seen from employees with strong attitudes towards Cyber security as compared to those with weak attitudes who usually just buy into the information security initiatives as they begin but do not commit to complying over the long term and, thus leaving organizations exposed to numerous risks.

H7: organizational employees' ethical behavioral intention leads to improved Cyber security ethical behavior.

Based on the literature review and the goal of this research which is to enhance Cyber security performance through a model for assessing the Employees' Ethical Commitment and Behavior Towards Cyber security the following statistical hypotheses was tested:

H1. Increased Prudence positively influences employees 'Cyber security ethical behavioral intention.

H2: Increased temperance has a positive influence on the behavioral intention of employees 'ethical behavior towards Cyber security.

H3: Increased courage has a positive influence on the behavioral intention of employees 'ethical behavior towards Cyber security.

H4: Increased justice has a positive influence on the behavioral intention of employees' ethical behavior towards Cyber security.

H5: The presence of strong ethical climate moderates the attitude towards ethical behavior intention of employees' ethical behavior towards Cyber security.

H6; employees Behavior intention has a mediation effect on the influence of cardinal virtue ethics and ethical behavior towards Cyber security.

H6a. employees Behavior intention has a mediation effect on the influence of courage and ethical behavior towards Cyber security.

H6b. Behavior intention of organisational employees has a mediation effect on the influence of Justice and ethical behavior towards Cyber security.

H6c. Behavior intention of organisational employees has a mediation effect on the influence of Temperence and ethical behavior towards Cyber security.

H6d. Behavior intention of organisational employees has a mediation effect on the influence of Prudence and ethical behavior towards Cyber security.

H7: Employees' ethical behavioral intention leads to improved ethical behavior towards Cyber security.

2.14. Approaches to Cyber security ethical behavior Assessment

Yatich & Musebe, (2017), posit that acting ethically means abiding by and reflecting one's personal morals as well as the generally accepted standards of the organization and society. A vital component of life and the cornerstone of a cultured society is ethical behavior. An important asset and source of competitive advantage in the workplace is ethical behavior by employees. A successful business adheres to strict ethical standards. Andrews, (1989) posited that unethical behavior has a negative bearing on an employee, the colleagues, and the entire business.

Egelman & Peer, (2016) created a scale called the Security Behavior Intentions Scale to evaluate end-users' computer security practices (SeBIS). The scale gauges' users' self-reported compliance with security recommendations for computers. The 16 items on the Security Behavior Intentions Scale (SeBIS) are specifically mapped to four factors: device security, password creation, p Faklaris et al. (2019) assert that while SeBIS explains how much a user strives to follow these professional suggestions, it is unable to express people's attitudes toward security practices. Additionally, it avoided discussing the intentions behind security ethical action based on virtue ethical theories.

A web-based Employees' Cyber Security Ethical Behavior Model for Ugandan Commercial Banks was created as a result of this research (ECEB). roactive awareness of security indicators, and updating.

CHAPTER THREE: METHODOLOGY

Introduction

This chapter brings forward the methods and approaches that were followed to achieve the stated objectives. It again discusses the philosophical foundation of the study. The chapter looks at research design and target population. The chapter discusses crucial concerns of this study with the help of various research paradigm and philosophies, various approaches and strategies to collect data and evaluate the responses of the respondents. It contains an argument of the sampling plan that was used, unit of analysis, questionnaire development and measurement strategy.

3.1 Philosophical Foundation (Philosophy, the Love of Knowledge)

The Research Philosophical Paradigms, Shah and Al-Bargi (2013), explained research as an investigative process in which a researcher tries to connect, build, and add to existing knowledge. Vijay Vaishnavi (2019) defined Research as activities that advance knowledge of a topic.

The broad approach to the design of doing research, comprising all aspects from the theoretical foundation through the collecting and interpretation of data, is known as research methodology Creswell (2009). In a different view Paulinus & Eaton, (2013), explained Research methodology as a philosophical stance of worldview that underlies and informs the style of research. From these explanations, its concluded that the philosophical worldview of things is important to the meaning of research methodology. Therefore, research philosophy is concerned with the way in which things are viewed in the world (Saunders et al., 2009; Yin, 2009). It addresses the assumptions that support the research strategy and the methods chosen as part of a research paradigm.

3.1.1 Research Paradigm

Shah and Al-Bargi, (2013) assert that the interpretive paradigm wants to understand, the critical paradigm aims to free and emancipate, and the positivist paradigm seeks to generalize. Paradigms are essential because they provide beliefs and direct and guide a researcher in choosing the study to do, how to conduct the study, and how to evaluate the analysis and study results (Kivunja & Kuyini, 2017).

Table 3. 1 Summarized Comparison of Research Viewpoints in Social Sciences Research; (Paulinus &Eaton 2013).

	Interpretative	Positivism	Pragmatism	Realism
Ontology	Since everything is socially created, thinking is subjective and liable to change in response to various realities.	emphasizes that the researcher is unbiased, impartial, and external to the study.	Researcher is External, multidisciplinary, and with a perspective chosen to best address the study questions.	Researcher is objective and exists autonomously of human mind but interpreted out of social situation
Epistemology	Looking at the specifics and underlying reality of social issues while taking inspiring action	Objects are seen to support claims made by facts, emphasizing causality and law generalizations to simplify events.	Facts about a study question may have either subjective or objective interpretations; concentrate on real-world applications by combining perspectives to evaluate the data.	the conviction that watching an occurrence establishes the veracity of facts; a lack of facts and data leads to imprecision and misunderstandings; only pay attention to context or contexts within explanations cross
Axiology	The research is value bound; such that the researcher is part of what is being studied, not isolated from the studied and will be subjective	The research is value free, hence independent of the data and objective in the analysis of the data	Values play a vital role to interpret results using subjective and objective reasoning	The research is value laden; hence, the researcher is biased by world views, culture, values, experiences and will affect the results/research
Approach	Qualitative	Quantitative but can still use qualitative	Uses both qualitative and quantitative	Approach adopted depends on the research matter
Method	Mixed or multiple methods	Mono-method but can use mixed in certain cases	Mixed or multiple methods	Method to use is based on the research problem or situation

This study considered the positivism and deductivism (pragmatism) paradigms;

3.1.2 Positivism paradigm

The French philosopher Auguste Comte promoted positivism, which he defines as a system that defines observation and reason as a means of comprehending conduct (Shah & Al-Bargi, 2013). Definition and components of positivism relies on the hypothetic deductive method to verify a priori hypotheses that are often stated quantitatively, where functional relationships can be derived between causal and explanatory factors (independent variables) and outcomes (dependent variables).

Bryman, (2008) suggested four important characteristics of positivism:

Phenomenalism; only knowledge confirmed by the sciences is genuine knowledge.

Deductivism; theory generates hypotheses that can be tested for provable 'laws'.

Objectivity; science must be value-free.

Inductivism; knowledge is gained by gathering facts that provide the basis for laws

Table 3. 2 Some Key Terms and Definitions Related to Understanding the Research Paradigm of Positivism (Park et al., 2020).

Dependent variable:	Measures of interest (outcomes) in the study; unlike independent variables, dependent variables can only be measured, not manipulated.
Dualism:	Separation of researcher and participants in study design and data collection to minimize bias.
Hypothesis:	A statement or idea derived from theory or literature that can be tested through experimentation.
Hypothetico-deductive model:	Scientific model based on forming a testable hypothesis and developing an empirical study to confirm or reject the hypothesis.
Independent variable:	Factors that influence outcomes of the study; in this study; Virtue ethics, ethical climate, ethical

	behavior intention influence cyber security ethical behavior.
Internal validity:	Evidence and inference supporting the "causal" relationship between the independent and dependent variables.
Objectivity:	Absence of bias due to researcher influences, flaws in experimental design, or outliers in data.

3.1.3 Epistemology of positivism

Positivists view knowledge as solid data that is objective, as noted by Chilisa and Kawulich. According to Creswell (2009), positivism is independent of the researcher's values, interests, and emotional condition. They don't affect each other in any way. This study took the positivist paradigm into consideration. This study on cyber security ethics is classified as positivist because it uses quantifiable factors. This kind of research methodology is a recognized approach for advancing scientific understanding (Gray, 2015). Using this paradigm, the researcher collected data from the two banking institutions; Centenary and ABSA banks. With the help of this philosophy, the current study focused on the facts and figures corresponding to the research problem. The positivist philosophical approach made it possible for the researcher to understand the employees' ethical behavior towards Cyber security. Using positivism, the researcher considered Centenary and ABSA banks branches located in Kampala the capital city of Uganda. Positivist paradigm approach is considered because generalization and replicability become possible for other different organizational environments (Garretta & Cutting ,2015; Shah & Al-Bargi 2013).

An organized investigation of research on ethical behavior and their application to improve Cyber security among employees in developing countries is limited.

The little research that is there revealed that much of the emphasis had been put on interpretative insights (Hawking et al., 2017). Therefore, a positivist epistemology is essential to close the gap.

Literature shows that many investigative contributions in Cyber security ethics need to be confirmed with hypothesis testing. This gap called for theoretical configuration in explaining the

beauty of embracing Cyber security ethical behavior and an explanation on which theory has greater predictive influence.

Thus, this study also applied deductive approach. Deductive approach can be explained by the means of hypotheses, which can be derived from the propositions of the theory. The researcher formulates a set of hypotheses at the start of the research. Then, relevant research methods are chosen and applied to test the hypotheses to prove them right or wrong. a quantitative research approach is an investigation into a social or human problem, based on testing a theory composed of variables, measured with numbers, and analyzed with numerical procedures, in order to determine whether the prognostic generalizations of the hypothesis hold true (Creswell, 2009). As a result, it is objective leading to positivist and deductive reasoning in a research study (Saunders et al., 2009; Yin, 2009).

Positivism is aligned with the hypothetico-deductive model of science that builds on verifying a priori hypotheses and experimentation by operationalizing variables and measures; results from hypothesis testing are used to inform and advance science.

Deductive reasoning is a logical approach where you progress from general ideas to specific conclusions. It's often contrasted with inductive reasoning, where you start with specific observations and form general conclusions. Deductive reasoning is also called deductive logic or top-down reasoning.

Positivism relies on the hypothetico deductive method to verify a priori hypotheses that are often stated quantitatively, where functional relationships can be derived between causal and explanatory factors (independent variables) and outcomes (dependent variables).

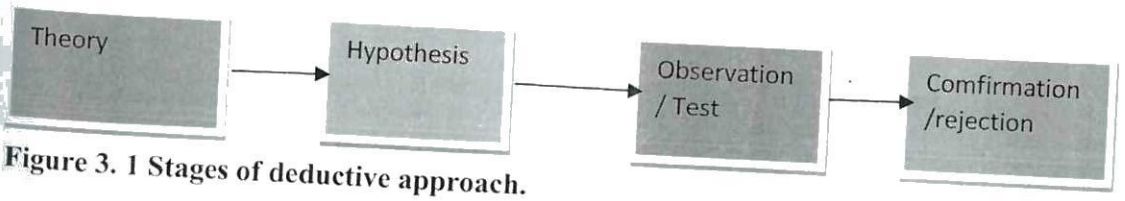


Figure 3. 1 Stages of deductive approach.

Guided by deductivism this study came up with research hypotheses see (chapter two). They address the influence of Prudence, temperance, courage, justice, and ethical climate subjects in influencing behavior intention of improving Cyber security ethical behavior. These variables are picked from literature as the body of knowledge.

This study offers possibilities to learn more about the nature and structure of the study variables' influences. The model's unsubstantiated hypotheses were eliminated, while empirically supported hypotheses were kept in place. Based on this contextual justification, it was crucial to do research in the area of information and communication technologies (ICTs), notably in the areas of computing and cyber security ethics. As a result, in order to develop a model that evaluates Cyber security ethical behavior, it was necessary to adopt and conduct research that was based on positivist epistemology, described the interactions and influences between the study variables, and used the best sample size possible.

Positivism paradigm was further considered for this study because it has particularly successful association with the physical and natural sciences. It is relevant to the current research because Cyber ethics and computing, involves the interaction of people and technology, thus this study is considered to be of the social sciences rather than the physical sciences (Hirschheim, 1985). Positivist accepts that generalization is applicable in social sciences. Due to lack of objectivity that is commonly associated with interpretivist research methods this study further embraced a positivist, quantitative approach to the development of the research model

3.1.4 The Ontology of Positivism; (ontology the Theory of Being)

Objectivism ontology

The current study adopted the objectivism ontology in order to assess the commercial banks employees' ethical behavior towards Cyber security without creating prejudices. This ontological stance is praised for separating the researcher from the research. This ontology is consistent with quantitative research methods where the researcher is detached from respondents. In this study, the researcher stood apart from the banking sector employees, who were the respondents thus reducing bias. Objectivism ontology similarly helped to ensure empirical investigation so that truth in reality is established.

Objectivism ontology helped the researcher to understand and register coherent justifications as to why the banking sector remains the main target of Cyber-attacks including big banks. Why are Cyber-attacks successful despite the fact that different Cyber security protection measures have been put in place. As previously argued in chapter one Xue et al., (2018) employees' unethical behaviors remain the utmost threat to information security. Therefore, there is an urgent need to come up with practical and scientifically verifiable solutions which could help assess and promote employees' ethical behavior towards Cyber security. The key assumption is that, the banking sector employees are rational individuals, in which rational clarifications offer solutions to rational problems.

3.2 Research design

A research design is defined by Ponelis, (2015), Aaker, Kumar, & Day (2003) as the detailed plan that guides a study in achieving its goals. The study plan outlines the investigational techniques required to answer the significant research issue (Wahyuni, 2012). The researcher can stay focused and put the research together with the aid of research design. The research approach that was chosen, which controlled how the information was obtained, was also supported by the study design.

The design of the study was cross-sectional. A cross section of a research population is a type of data that is gathered by watching several people at the same time or without taking into account changes in time. The use of cross-sectional time frame is both "cheaper and easier to organize. Over the course of two and a half months, data was gathered all at once. This form of survey study was taken into consideration because it makes it easier for the researcher to study bigger groups of people. By using numerous respondents and questionnaires to thoroughly describe a phenomenon, a cross-sectional study design was employed to describe and explain the conditions of the current study. In addition, a cross sectional study design was used for this investigation because the primary goal is to collect data from the key informants at only one point in time; mainly the current cardinal virtue ethics and organizational ethical climate and their influence on employees' Cyber security. Ethical behavior intention.

This study considered Cyber security ethical behavior at one point in time. The cross-sectional study design that is considered in this research allowed the researcher to compare many different variables at the same time. The study considered virtue ethics constructs, organizational ethical climate, and how they influence Cyber security ethical behavior.

3.3 A Research Approach

3.3.1 Dual essential paradigms

Hevner et al. (2004) claim that the fields of behavioral science and design science have contributed significantly to the study in information systems. To advance theories that describe or predict human or organizational behavior, the behavioral science paradigm studies and analyzes people or organizational behavior (Basel, 2019). While the design-science paradigm aims to push the boundaries of what is possible for people and organizations to do by creating novel and cutting-edge IT artifacts that are largely transparent as constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), and instantiations (implemented and prototype systems) (Hevner et al., 2004, Basel, 2019).This thesis applied the two paradigms; the design science paradigm to develop an artifact in form of a model for cyber security that supports banks when assessing employees' cyber security ethical behavior, (ref Chapter 6). Then the behavioral-science paradigm to investigate and establish the influence of Virtue Ethics moderated by ethical climate on employees' Cyber security ethical behavior in Ugandan commercial banks. (See chapter 4).

3.3.2 Employing Design Science in this Research

The current research used the design science as a research approach to address the research problem. The guidelines provided by (Hevner et al., 2004) were followed as shown in table 3.1.

Design Science Research (DSRM) is a methodology that "involves a rigorous process to design artifacts to solve observable problems, to make research contributions, to assess the designs, and to communicate the results to relevant audiences," according to Peffers et al. (2007).

Design science is used because it interacts with behavior science (Peffers et al 2007). This encouraged the researcher to apply a methodology for evaluating ethical cyber conduct in Ugandan commercial banks.

Peffers et al. also make the case that design science research informs the creation and assessment of fresh IT solutions to problems that have been recognized within a business. Constructs, procedures, models, and installations are among the artifacts.

Table 3. 3 Design-science research guidelines Source: (Hevner et al., 2004).

No	Guideline	Explanation
1	Design as an Artifact	Research in design science must result in a workable concept, model, technique, or instantiation.
2	Problem Relevance	Development is the goal of design-science research. solutions based on technology for significant and pertinent business issues
3	Design Evaluation	A design artifact must be extensively evaluated in order to show its utility, quality, and effectiveness.
4	Research Contributions	Clear and verifiable contributions must be made to the design artifact, design processes, or both in order for design-science research to be effective.
5.	Research Rigor	The construction and evaluation of the design artifact must both follow strict procedures in design-science research.
6	Design as a Search Process	Utilizing available resources to achieve desired goals while adhering to the laws of the problem environment is necessary in the quest for an effective artifact.
7	Communication of Research	Design-science findings must be communicated effectively to audiences focused on technology and management .

Using the first guideline of designing as an artifact, this research produced a web based cyber security ethical behavior assessment model that aids commercial banks to assess their employees' ethical behavior and forms the artifact of this research, as described in Chapter 6. Novelties known as "artifacts" characterize concepts, procedures, technological advancements, and items that make the successful and resourceful design, development, and use of information systems (Hevner et al., 2004). Design science satisfies the second criterion (problem relevance) by producing novel artifacts that aim to alter the processes that occur (Hevner et al., 2004). A problem is defined as the differences between the goal state and the existing state (Hevner et al., 2004; Basel, 2019). Literature suggests that staff security infractions in banks were promoted by a lack of efficient employee cyber security ethical behavior assessment, (Maalem et al. 2020). Additionally, findings and reports suggest that little research has been done on virtue ethics, ethical atmosphere, and how these affect cyber security. The cyber security ethical behavior assessment model may address this problem. Through its decision model, the artifact supports bank managers in the decision-making process when assessing ethical behavior towards cyber security. Ethical behavior assessments could be a continuous process and be used to identify and address employees' unethical behavior towards cyber security.

IT artifacts can be assessed for their functionality, usability, organizational fit, and other pertinent quality features (Hevner et al., 2004). The usability, quality, and efficacy of the cyber security ethical behavior assessment model were demonstrated using well-executed evaluation techniques after the third guideline (design evaluation) (see Chapter 6). In this research the Cyber security ethical behavior assessment model has been implemented as a web-based model. Hence a prototype that acts as a proof-of notion; that facilitated discussions with employees and other experts within the banks. It facilitated conversations with bank workers and other subject matter experts. Additionally, the evaluation conducted in this thesis is described in Chapter 6.

In the fourth guideline (research contributions), Design-science research made explicit contributions in the form of design objects, foundations (growing and refining the existing design-science knowledge base foundations), and procedures (measures and assessment metrics) (Hevner et al., 2004). This study makes a contribution by creatively incorporating previously acquired knowledge regarding virtue ethics, ethical conduct, and ethical atmosphere.

This thesis primarily addresses bank managers and bank staff by offering them a cutting-edge model that aids in better evaluating cyber security ethical behavior. Additionally, because information on ethical behavior in cyber security is kept in an organized approach that makes it easier to manage and expand this information, this model is also motivating for bank employees. Additionally, this study makes a contribution by introducing ethical cyber security practices. This research also contributes by adding the cyber security ethical behavior model to the knowledge base for future work.

In this study, the model was developed and evaluated using rigorous procedures, adhering to the fifth design-science guideline (research rigor) (Hevner et al., 2004). The research in this study was conducted using organized, precise methodologies. To guarantee rigor, quality checkpoints were put in place.

In this thesis, when developing the artifact ethical virtue constructs, ethical climate, behavior intention, and ethical behavior constructs were used as requirements that are assessed by the model. Also, the appraisal of the developed model was done using rigorous approaches guided by the third guideline "design evaluation".

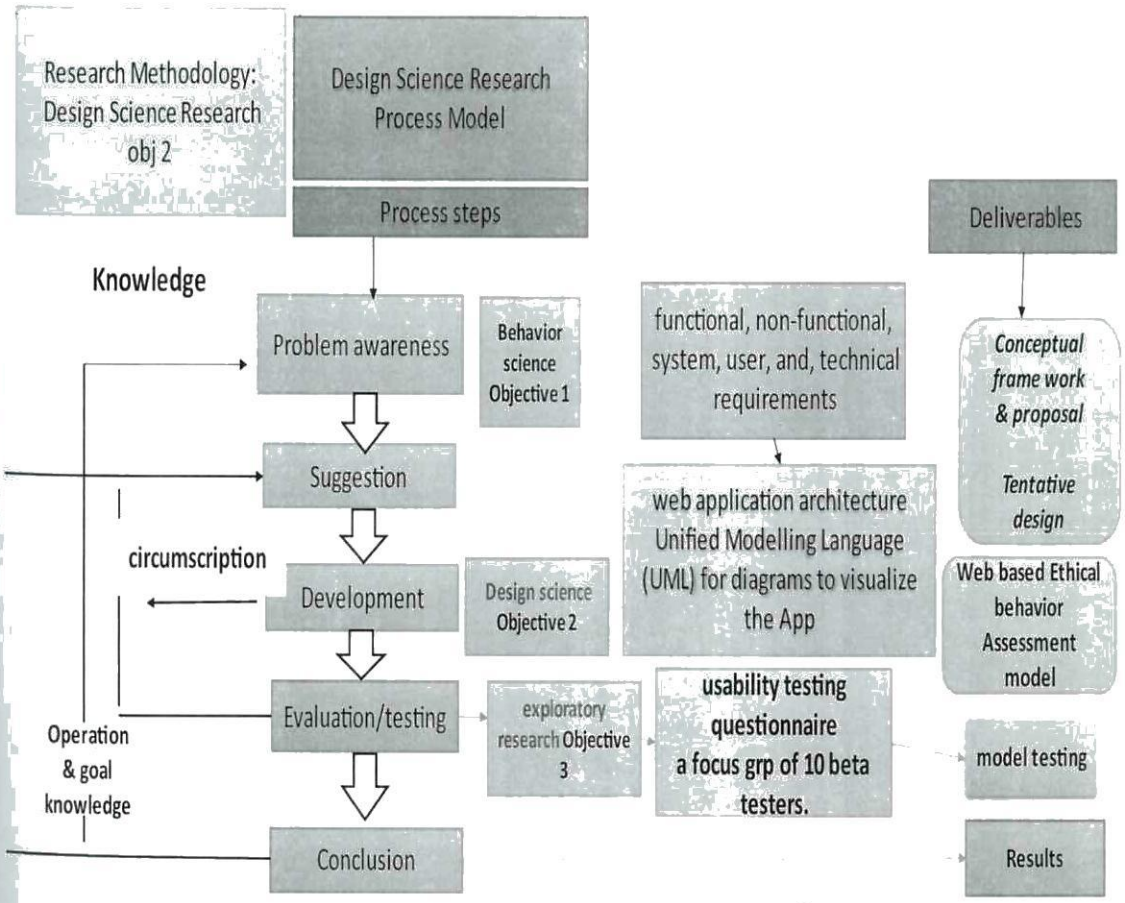
Hevner et al., 2004 posited in the sixth guideline (design as a search process) that; formation of operative artifact needs to use obtainable means to achieve desired goal without defying the existing laws. Designing and developing of the model in this research followed an extensive research procedure guided by the study objectives. The researcher continued carrying out literature review to get most information, identify strenghth and weaknesseses of the existing models and identified the study gap. Objective 1, Research was carried out using online questionnaire to establish influence of cardinal virtues moderated by ethical climate on employees' Cyber security ethical behavior intentions in commercial banks in Uganda, (ref chapter 4).

Objective 2. To develop a model for assessing the Employees' cyber security Ethical Behavior towards Cyber security in Ugandan commercial banks. See chapter 6. Objective 3, To test the developed model.ref chap 6 Section 6.8

This research developed a model that helps the managing of the banks' employees' ethical behavior by mapping cardinal virtues, ethical climate, ethical behavior intentions and actual cyber security ethical behavior.

Throughout the study the researcher kept it clear that the information provided within the model should be comprehensible to all the users. Thus, this research considered the best ways to extract, manage and share information about cyber security ethical behavior assessment in Ugandan commercial banks, and supporting them when they want to assess ethical behavior among the existing employees and the new recruits.

Ensuing the seventh guideline (communication of research) this thesis and the developed model are offered to the academic audience to add to the knowledge base. Also, the research results were communicated and presented to various different scientific conferences and workshops and papers were extracted and published in academic journals.



Design science research process model Source: Adapted from (Hevner & Chatterjee, 2010; Vaishnavi, V. & Kuechler, 2007)

Figure 3. 2 Design science research process model Source: Adapted from (Hevner & Chatterjee, 2010; Vaishnavi, V. & Kuechler, 2007).

3.4 Awareness of the Problem: Objective 1 methods

The current work follows the model provided by (Hevner & Chatterjee, 2010), as shown in Figure 1. above. The first phase is the awareness of problem. This phase considers guideline 2 "problem relevance". Using literature review Humaidi and Balakrishnan, (2018), Xue et al., (2018), and research conducted using online questionnaire with the banking employees revealed that security failures in the banks are attributed to employees' wrong behaviors that remain the utmost threat to information security. Thus the problem has been identified and defined here grounded on these discussions and literature review. The output of this phase was a conceptual frame work for this research effort.

The suggestion for a problem solution is the next step, and it is derived from the material already available, a hypothesis based on the problem area, or it is created using the right research process (Hevner & Chatterjee, 2010). The concept of the cyber security ethical behavior evaluation model was the end product of this phase. This stage takes into account Principle 6: "Design as a Search Process." The tentative design is further developed and implemented in phase development. This phase is creative and the design is further refined through many iterations (Hevner & Chatterjee, 2010). This phase follows the guideline 1 "design as an artifact" and the guideline 5 "research rigor", resulted in an artifact, the prototype or the proof-of-concept of the cyber security ethical behavior assessment model.

A prototype is tested when it is finished. The result of this stage establishes how effectively an artifact functions (Hevner et al., 2004). Iterations and feedback are referred to as circumscription in the "development" and "assessment" phases (Hevner & Chatterjee, 2010). The guidelines for this phase were 3 (design evaluation) and 5 (research rigor).

3.4.1. Employing Behavioral Science in this Research

While delivering technical answers is a part of computer science, it is also concerned with operational difficulties, project management, and human behavior (Basel 2019). The goal of behavioral science research is to create and test hypotheses that explain or predict organizational or human behavior in relation to information system analysis, design, implementation, management, and use (Basel 2019; Hevner et al., 2004).

Data on notions of virtue ethics and views of the ethical climate were gathered for the current study through surveys. Surveys that were conducted using a quantitative research approach with already provided questions and hypotheses. Quantitative research model has been chosen because of the significant amount of data and feedback it provides, the greater access it allows to participants, and the low cost involved. Utilizing questionnaires, useful data was gathered by soliciting the opinions of respondents. The acquired data was then put to an empirical test for validation under carefully monitored conditions to ensure that the outcomes remain unaffected (Shah & Al-Bargi 2013). The study tested views on ethical behavior and investigated the applicability of virtue ethical constructs and ethical climate and how they could help improve Cyber security ethical behavior. Deeper quantitative investigation on security ethics and planned behavior investigating the underlying virtue and the organizational variables would enhance understanding of the influence of these variables between employees in attempt to improve Cyber security in the banking industry.

3.4.2 Study Population

A population, Bryman & Bell (2003), is the total set of elements that the research focuses on in order to draw findings. Population was defined by Mugenda and Mugenda (2003) as a complete group of people, things, or events with a common identifiable trait. A targeted population is a group of individuals chosen based on standards consistent with the study's objectives (Wahyuni, 2012). The population for this study are the commercial banks' employees. This research's survey targeted the banks' employees who are knowledgeable about information and Cyber security issues and those who have access to the banks' sensitive data. Therefore, the particular individuals who handle the banks' information at different levels and Cyber security professionals in the same banks were targeted. Because they are better able to assess their own behavior (activity) in regard to the issue under inquiry, namely; their ethical behavior towards information and Cyber security, these were considered to comprise the target group. This is in line with the theories put out by Rutherford (1988) & Kang'ahi et al., (2012), which contend that a person is best qualified to characterize the nature of the conditions in effect at a particular time regarding oneself. The research targeted the top nine commercial banks in Uganda. These are Stan Bic bank, DFCU bank, Centenary bank, Standard chartered bank, ABSA bank, Bank of Baroda, Citi bank Uganda, Equity bank, Housing finance bank, Bank of Africa- Uganda LTD.

Appendix C presents the number of bank employees in each of the top 9 commercial banks in Uganda constituting the study population and their headquarters.

3.4.3 Sampling design and procedure

Sampling design

Using the two layers of a multistage sampling technique (Purakam & Koop, 1966), the research selected 9 commercial banks in stage 1 purposively. As such this study purposively selected the top 9 commercial banks in Uganda at stage one. At stage two, purposive sampling technique was also used to select the representative banks and purposively selected Centenary and ABSA banks because they have been grappling with employees who steal the banks' money Baggala, (2020).

The choice of the commercial banks was motivated by the fact that the Banks have a significant impact on economic growth, change, and their role in reducing unemployment and inflation, two factors that have a direct impact on people's daily lives. Banks are an important part of the economy, yet they are limited by insider-performed cyber security breaches. Understanding how the cardinal virtue ethics verified through the character growth of the banks' employees can add on the improvement of Cyber security. This is a vital area of probe for both policy makers and academics.

Sample Size

A sample, Oso & Onen, (2008), is a portion of the target population that has been carefully chosen to be representative. Since the population of interest is enormous, diversified, and distributed over a vast geographic area, sampling is crucial (Kothari, 2004). In addition, Sekaran (2003) notes that it would be exceedingly challenging to survey every component of the population and that gathering data from the entire population would be nearly impossible. Therefore, in this study a sample of respondents were selected from a total population of of commercial banks employees.

Selection of respondents

To get a better representation of participants from the two commercial banks purposive sampling technique was used to determine the sample size. The total population was purposely sampled according to the categories of employees in the bank as indicated in the table below.

The Krycie and Morgan formula was subjected to the total population to determine the sample size (Krejcie and Morgan 1970) (see appendix A). The population in the two banks was 320 and a total sample of 240 employees was obtained for the study basing on a 95.0% confidence level and a 0.05 margin of error.

Table 3. 4 Sample Size of Respondents and Sampling Technique.

BANK	Category of population	Population Size	Sample Size	Sampling Technique
ABSA	Financial Managers	15	**14**	
	information security managers	15	**14**	**Purposive sampling**
	loans officers	15	**14**	
	bank tellers .	90	**70**	
	Branch managers	15	**14**	
Centenary bank				
	Financial Managers	15	**14**	**purposive sampling**
	Information security managers	20	**15**	
	loans officers	20	**15**	
	bank tellers .	100	**70**	
	Branch manager	15	**14**	
total		**320**	**240**	

3.4.4 Questionnaire Design

For this research the questionnaires that was used to gather data were picked from literature.

The purpose of the questionnaire was to collect information that would be used to statistically validate the organizational ethical climate and the cardinal virtue ethics frameworks. This was accomplished by confirmatory factory analysis (CFA), and structural equation modeling was used to assess the reliability of the created Ethical Behavior Model (SEM).

There were three sections of questions in the survey. To establish the reliability and authenticity of the participants' information security or cyber security backgrounds, Section One was used to collect the demographic information about them. This was crucial since it might be presumed that the respondents' comments were valid if they demonstrated understanding of the subject being studied (Goodman, 1987). The indicator statements in Sections Two and Three of the survey were concerned with prospective ethical behaviors, behavioral factors, ethical climate, and their effects on enhancing cyber security. On a five-point likert scale, the things in Section Two and there were evaluated. To make the importance of the study clear and entice respondents to participate voluntarily, a statement of purpose and motivation was included at the outset of the questionnaire. A disclaimer referring to high secrecy was included on the questionnaire to ensure the respondents' privacy and to state that the study is solely for academic reasons. To ensure that each construct is measured with satisfactory psychometric qualities, this study used a multi-item technique (Miller et al., 2009). The participants were given one month to fill in and answer the questionnaires. The researcher sent emails to remind the respondents about the questionnaires and to confirm that they had received them. And respondents were asked to email them if they finish answering them.

3.4.5 Stages of Research Study

The emphasis of this research was the employee's Cyber security ethical behavior assessment model, consisting of seven concepts, and was based on the research results from objective one.

Pilot study

In order to avoid bias, pilot studies are usually carried out on individuals who are as similar as possible to the target population, but not on those who will be a part of the final sample. Since this research was carried out in the commercial banks, a pilot study was conducted to pre-test the survey instrument in the commercial banks' environment. Pilot studies are crucial since they serve as trials for carrying out the main study and assess the model's content. Pretesting is a way to determine whether research participants understand questions and phrases the way the researcher intends. Pilot studies assist in obtaining an overall assessment of respondents' aptitude to do necessary tasks as well as recommendations for question wording in the event that the original statements need to be rephrased. Pretesting helps uncover survey filling issues and spot any ambiguities or other participant problems or suggestions by getting feedback from respondents.

The researcher calculates the anticipated survey completion time during pretesting (Lewis et al., 2005). The researcher carried out a pilot study by picking 34 respondents from the banks and gave them the approved questionnaires. The pilot study was conducted among 34 banks employees over a period of three weeks, in the commercial banks in Uganda, after which 31 questionnaires were returned. The employees that participated in the pilot study comprised 8 employees from Post bank, 8 employees from DFCU bank, 5 employees from Centenary bank, 5 employees from Stanbic bank and 8 employees from ABSA bank. Most of the participants said that the survey was ok, with almost all the variables and indicators easy to understand, finely prearranged, and that it had good functionality. Results also indicated that the survey would take between 10 and 15 minutes to complete. After the pilot study, the final research instrument was finalized and ready for use.

3.4.6. Reliability and validity of instruments

Testing for reliability

The level of internal consistency among various measures of a variable is known as construct dependability (Hair et al., 2010). One of the popular ways to determine reliability is by using the coefficient alpha. The coefficient alpha was deemed appropriate since it can be used to assess how well the scale's items represent the area of the construct being evaluated. The reliability of a measurement scale is typically evaluated using the coefficient alpha, which is a measure of the interior consistency of a set of objects Kyeyune (2017). Cronbach coefficient is thought to be effective for measuring items on multi-point scales, according to Sekaran, 2000. In this study a 5-point Likert scale was used and Cronbach alpha estimate was used as a verification of the reliability of the many items encompassing each scale construct. Nunnally and Bernstein (1994) suggest a level of higher than 0.70, with a level as low as 0.60 being allowed for novel scales, when measuring reliability by Cronbach Alpha. According to Carmines and Zeller (1979), internal consistency must be found at a level of at least 0.80. In accordance with the literature, an alpha of 0.70 and above is acceptable. The cut-off point in this study was 0.70, and this was utilized as the minimum to assess the scale's internal consistency.

Validity Test

The degree of correlation between a construct and its indicators or measures is referred to as construct validity (Jarvis et al., 2003). According to Yin (2009), a trustworthy study should perform construct validity on both the internal and outside levels. Internal validity is the ability to build a causal link in which superior relationships are demonstrated to differ from other relationships and some conditions are proven to cause other conditions. The extent to which the research design can determine the area in which a study's results can be generalized is known as external validity (Yin 2009). Internal and external validity was carried out, internally the data collection tools were pre-tested by subjecting them to a similar population, see pilot study below. Externally Validity was ensured through correlating the findings with other related empirical studies to make the study credible.

Construct validity is defined by Hair et al. (2010) as the degree to which a gauge or set of measurements accurately represents the concept under study. This study examined construct validity and reliability. Confirmatory factor analysis (CFA) and exploratory factor analysis (EFA) were used. In order to perform structural equation modeling, the researcher first tried to test and confirm that the measurement model's validity and reliability are in place. The number of components and variables associated with each factor from a set of multiple measures were also determined using exploratory factor analysis. The measurement requirements were subsequently approved using confirmatory factor analysis.

3.4.7. Unit of Analysis and Inquiry

An important part of survey grounded study is the choice of suitable research participants because their knowledgeable sentiments form the foundation of the research results. The unit of analysis was the main object or individual being analyzed in this study. They composed of individual employees who are knowledgeable about information and Cyber security in the commercial banks in Uganda. This research focused on commercial banks' employees 'behavior intentions towards Cyber security. Because they are the main keepers of information systems and Cyber security in these banks. Therefore, the unit of analysis in this research was the commercial banks 'employees who handle banks information practically. Unit of analysis was individual employees. The answers they provided to the survey questions consisted of the data that was statistically analyzed.

The unit of inquiry are the commercial banks identified as; Absa bank and Centenary bank that served as focal places for this study.

Inclusion criteria;

Data was gathered from employees working as; Financial managers, information security managers, loans officers, bank tellers and branch managers. Goodman (1987) commended that the would-be survey participants should not be randomly targeted rather they should be renowned experts or informed advocates. Participant suitability and selection criteria included; working in the IT/IS department, position title that reflects direct participation with Cyber security, handling sensitive information, and or information systems security in the banks.

3.4. 8. Data and sources

Both primary and secondary data was collected and used. Primary data collected from respondents constituted the main source of data. On the other hand, secondary data was also gathered from different published literature. There was continuous literature review throughout this research. Different articles, journals, and reports were continually reviewed. Some of the bibliographic databases that were visited include; Google Scholar, Science direct, Web of Science, ACM, (Association for Computing Machinery), is the world's largest educational and scientific society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM Digital Library, SpringerLink, IEEE IEEE, (Institute of Electrical and Electronics Engineers), Computer Society Digital Library. Universally recognized peer review journals, websites including Google, Research gate, and others. Indigenous newspapers, articles, policy documents consultancy and annual reports published by different institutions on Cyber security, information systems security, computer ethics, and Cybercrime in the country. Literature review forms a strong foundation for progressing knowledge and it is a vital feature of any academic research. (Webster & Watson, 2002). Conducting a thorough literature review on an area, in this sea of information aids more scrutiny and synthesis. literature review conducted focused on applications and research outcomes and to assimilate findings from other writings. The literatures carefully chosen were evaluated concentrating on outcomes, and identifying gaps that were extracted, structured and mapped as requirements in the cyber security ethical behavior assessment model together with a stance of future research.

3.4.9. Data Collection Methods

There are a number of techniques for collecting data in research. These comprise observation, in-depth interviews, self-administered questionnaires, on-line questionnaires among others (Jenkins & Dillman, 1995).

Questionnaires are viewed as a reasonable method for a population that is distributed like the one in banking sector in Uganda. Ndwandwa (2009) describe a questionnaire as a data gathering model which contains a standardized set of questions concerning the study topic. Ndwandwa further explains a questionnaire as a number of queries on the same topic that a respondent must answer. This research used the questionnaire method to collect data from the identified banks. The survey consisted of 67 questions divided into three sections. Section A was used to gather the demographic data of the participants in order to establish the reliability and validity of their Cyber security background. This was important because the researcher needed to know if the respondents had knowledge of the topic under study to be sure of the validity of their responses (Goodman, 1987). Section B of the survey consisted of indicator statements that focused on Virtue ethics, potential behaviors, behavioral influences, and their implications on the banks' workers. The 28 items in Section B were rated on a five-point Likert-type scale with replies ranging from Strongly Agree to Strongly Disagree, reflecting the extent of the respondents' feelings or strength of agreement in regards to the question. Section C is the Ethical Climate Questionnaire. It rated on a five-point Likert-type scale with replies ranging from Mostly false to Completely true. It contained some questions about the general climate in the Banks. Respondents answered the questions in terms of how it really was in the banks and not how they would prefer it to be. These Likert-type scale closed question responses were used as the basis for developing the statistical comparisons and correlations between variables. Survey is a proven way to capture the ethical climate within an organization and an essential and recognized method for conducting theory validation and demonstrating exterior validity in the arena of information and computing security.

3.5. Approach to establishing the influence of cardinal virtues moderated by ethical climate on Cyber security ethical behavioral intentions in commercial banks in Uganda. (Objective one methods).

To achieve this objective, the researcher used the questionnaire method to collect data from the identified banks. This research employed quantitative methods to collect data from the identified banks. Quantitative methods were considered in this research because the research is emphasizing objective quantities and analyzed statistical data that was collected through questionnaires using computational techniques. This research further used quantitative method to focus on gathering numerical data and generalizing it across the Ugandan banking industry. The survey was used to investigate the proposed measures for cardinal virtue ethics constructs that may influence the behavioral intention of organizational employees' ethical behavior towards Cyber security. The virtue constructs were measured using the study conceptual frame work variables which were adapted from literature, Trusted Worker Ethical Behavior and Influences Survey, Gray (2015) provided the construct variables that were measured. The survey considered the cardinal virtue constructs of; Prudence, courage, justice, and temperance that should be possessed by Cyber security employees. Pertinent literature was reviewed to ascertain the acceptable indicators of the virtue ethics constructs. This research used multi-items approach to measure each construct, which is important in ensuring that satisfactory psychometric properties are measured (Miller et al., 2009).

3.5.1 Participants

A sample of 240 employees from commercial banks in Kampala participated in the study. The study was carried out among Centenary and ABSA banks' branches located in Kampala capital city of Uganda. The participants Speciality included; Information systems, Information technology Computer Science Data communication and other Specialties. The study also looked at current professional role; Financial Managers, information security managers, loans officers, bank tellers, internal auditors, Branch managers, customer service representatives, Assistant branch managers

3.5.2. Instrumentation

An instrument Trusted Worker Ethical Behavior and Influences Survey developed by Gray (2015) was used in this research.

The instrument measured the virtue constructs and proposed measures for cardinal virtue ethics constructs that may influence the behavioral intention of organizational employees' ethical behavior towards Cyber security. The survey considered the cardinal virtue constructs of; Prudence, courage, justice, and temperance that should be possessed by Cyber security employees. Also, the survey measured Behavioral intentions and ethical behavior towards Cybersecurity.

The survey consisted of questions divided into two sections. Section one was used to gather the demographic data of the participants in order to establish the credibility and validity of their Cyber security background. The first section of the instrument consisted of questions about Gender, age, Respondents' bank, Education level, Speciality, professional role and experience. The second section of survey consisted of 25 items/ indicator statements with a 5 item Likert scale as: Strongly Disagree, Disagree, Not Sure, agree to Strongly Agree that focused on virtue ethics constructs, potential behavior intentions, ethical behaviors and their implications on improvement of Cyber security among the commercial banks 'employees. Cronbach alpha estimate was used as a verification of the reliability of the multiple items including each scale construct. An alpha of 0.70 and above is acceptable according to literature. In this study the cut-off point was (0.70) and this was used as the minimum for determining internal consistency of scale.

The Ethical Climate Questionnaire (ECQ) developed by Victor & Cullen (1988) was adapted and the nine theoretical ethical climate types, were tested. Respondents were asked to fill the survey by answering to how it really is in the bank as they see it, rather than how they would wish it to be. The postulation is that participants should respond to the items unbiased in describing the bank's ethical climate to others external to the bank. The Ethical Climate Questionnaire measures the ethical climates at individual and organizational levels of analysis. Cullen et al., (1993) tested the EC questionnaire with 1,167 individuals through three studies. The outcomes at the individual level agreed that there is a strong support for the validity and reliability of the questionnaire.

The Ethical climate scales measured; 1. Self-interest, Organizational interest, efficiency, Friendship, Team interest, Stakeholder Orientation, Personal Molarity, Company's rules and procedures, Public Interest. The ethical climate scales, their items and their reliability were adapted from Victor and Cullen (1988). The ECQ consisted of 31 items/ indicator statements with a 5 item Likert scale used to measure agreement with each statement. The scale ranged from **(1) Mostly false, (2) Somewhat false, (3) somewhat true, (4) Mostly true, to (5) Completely true.**

Organizational climate, together with a persons' own ethical bearings, and the recognized rules, procedures and structures of the organization are all considered key items in determining the ethical behavior of employees, (Dark, & Rix, 2015).

3.5.3 Measurement of Constructs

The research variables that was used was picked from previous research and some of them have been modified for the purpose of this research. This study reviewed pertinent literature to ascertain the acceptable indicators of the virtue ethics constructs of temperance, fortitude, prudence, and justice. Ethical climate questionnaire provided variables from ethical climate theory that were assessed. Ethical behavior intentions and ethical behavior constructs were from the Theory of planned Behavior. An advantage of using variables from previous research is that the variables have already been verified.

Scales are noticeable items that capture pieces of the concept and when combined form the construct. The Likert scales that were adopted for this study provided answers on a scale and aimed at constructs that was measured. The constructs measured ranged from strongly agree, agree, not sure, disagree, to strongly disagree. In circumstances of uncertainty, a midpoint Likert scale can be implemented to escalate validity and reliability responses (Garland, 1991). These scales were based on previous research that was done in similar theoretical and empirically directed level of theory and measurements, (Kyeyune, 2017). In the case of Cyber security, virtue ethics can possibly improve the organizational employees' moral conduct through pinpointing the main personality traits and how to influence wanted behaviors. The desired behavior identified may help to forecast how an employee reacts or take a decision when s/he meets an ethical dilemma. Understanding that employees are implementers of Cyber security and have the knowledge and skill of how to evade the security controls and strategies an ethical approach that appeals to the inner inspirations of an individual has the potential to provide more effective Cyber security.

3.5.4 The cardinal virtue Constructs

Prudence (Practical Wisdom); An individual's deliberations, decisions, and actions are based on facts, understanding, and contribution from others and that they result in morally right judgements.

Measuring Prudence; Intrinsic in this virtue theory construct is the acceptance that employees 'moral or ethical conduct may guard against the temptation of committing Cyber security violations. Pisk, (2017) further propounds that the virtue of prudence could help Cyber space users and security professionals to take good decisions regarding good actions that benefit other humans. Artz (1994) upholds that virtue ethics main beliefs for computer systems comprises wisdom and mindfulness of appropriate activities and use. This was echoed by Alfawaz, et al. information systems security behavior is affected by an individual's knowledge, professional skills, and values coupled with consistent behavior. Cautious responses and avoiding Cyber security breaches that cause injury to others, might result into monetary gains, saving of lives and gaining of customer confidence in an organization. This may assist in handling the complexities in the Cyber society.

Temperance: is another virtue construct that was measured in this study. Papouli (2018) affirms that temperance consist of self-discipline such that an individual can evade doing things that are injurious to him and others. Myyry, eta l, (2009) contend that IS guiding principle compliance is determined by skill, creativeness, priority for moral values over personal values, correctly interpreting situations as involving moral issues, being motivated to act morally and rationalizing importance of policies. In this notion temperance can be considered as a self-care plan and it can be applied and used by Cyber security employees to avoid exhaustion and to evade misconduct.

Courage: was also measured in the current research. Courage entails the readiness to an accomplishment in dangerous situations and settings. An employee who possesses courage works for the long-lasting and continuing welfares and prosperities of an organization for the safety and security of its future. This should be combined with intelligent and up-to-date valuation of choices and opportunities. Cyber security professionals who possess the virtue of courage are likely to maintain and improve Cyber security of their organizations' assets and resources. Stamatellos (2011) contends that Computer ethics involves self-determination, how one should act in particular situations, character based development focusing on greater good over personal desires IS policy compliance determined by courage, working under pressure, right judgments and willpower. Policy requirements are internalized, (Gray, 2015)

Justice: is another virtue construct that was measured in the current study. Justice in Cyber security is responsibility ethics which are shaped by encouraging and promoting faithfulness, admiration, and trust, chiefly when protecting and preserving confidential and private information belonging to individuals and organizations, (Gray & Tejay 2014). Justice is precision of behavior and decisions that could affect information system security.

The Cyber security ethical behavioral intentions variables were adapted from the research done by Yoon & Kim, (2013). And the Cybersecurity Ethical behavior constructs were adapted from the study conducted by Gray, (2015). After each question a five-point Likert scale was provided. The Scale is; 1 = Strongly Disagree2 = Disagree3 = Neutral 4 = Agree 5 = Strongly Agree.

After each question a five-point Likert scale is provided. The Scale is; 1 = Strongly Disagree2 = Disagree3 = Neutral4 = Agree 5 = Strongly Agree. Participants remained anonymous to each other and all survey answers remained confidential. The survey instrument was centered on quantitative research which allows for investigation of phenomena through statistical techniques because the data was in numerical form (Sekaran & Bougie, 2010).

The Ethical climate scales measured; 1. Self-interest, Organizational interest, efficiency, Friendship, Team interest, Stakeholder Orientation, Personal Molarity, Company's rules and procedures, Public Interest. The ethical climate scales, their items and their reliability were adapted from Victor and Cullen (1988). The ECQ consisted of 31 items/ indicator statements with a 5 item Likert scale used to measure agreement with each statement. The scale ranged from (1) Mostly false, (2) Somewhat false, (3) somewhat true, (4) Mostly true, to (5) Completely true.

Data Collection

Primary data provided by the respondents constituted the main source of data. The researcher obtained a letter of introduction from the University to help with introductions to the identified banks. After making the instruments, the researcher took them for approval to the supervisor and there after they were taken for pretesting in selected banks in Kampala city. After obtaining the Research permit, the survey was disseminated using an email to potential participants with an invitation to participate through an Internet link which was provided for participation for ten weeks. The email that was sent to the prospective respondents included a link to the Google form containing the questionnaire and also an attachment of a Microsoft word version of the questionnaire.

Given that internet access is still an issue in Uganda, especially the banking industry, the two choices were provided to allow respondents to choose between completing the survey online or offline. During this period, the survey was accessible, and the Banks employees who were participating shared the survey link with their coworkers. The study participants volunteered to invite and suggest more of their coworkers who they believed qualified to participate in the survey. Throughout the survey's duration, the researcher kept track of the response rates. When 240 responses were received the results were reviewed for completeness and the main survey was closed

3.5.5 Data Processing and Analysis

Data analysis is the methodical examination of data to ascertain its significance, organization, linkages, historical context, and other characteristics. This is done in order to gather pertinent data and make decisions easier, (Ndwandwe, 2009).

The acquired information was cleaned and formatted. Before being entered into the data analysis program, the data was compiled, edited, and organized according to serial numbers. The exercise in cleaning the data includes looking for outliers and filling in the blanks. It was evaluated to see if the features of the cleaned data violated the assumptions for multivariate analysis and introduced bias that would weaken the analyses' robustness (Hair et al., 2010).

Data Cleaning

Missing Values Analysis

Having data without missing values is unusual. They are the result of incorrect data entry or incomplete participant completion of the entire questionnaire. A responder may purposefully choose not to answer the question(s) or unintentionally miss it if there are any missing values. At the time of data entering into a software, the researcher may also miss certain information Hair et al. (2010). Missing data must be accounted for to avoid biases in the analysis and misleading outcomes (Pollet & van der Meij, 2017). Although the reasons for missing data in this study were not clearly defined, the procedures involved in missing data were taken into consideration. To ascertain the extent, patterns, and relationships that result in the missing data while maintaining the original distribution of values, a missing value analysis was carried out (Hair et al., 2010).

The information might be missing at random or missing completely at random (MCAR) (MAR). When the data are MCAR, it indicates that the observed data is independent of the observed data. Missing Values Analysis was also done to determine;

If there were clear patterns that could be identified or if the missing data were dispersed randomly throughout the observations. ii) To ascertain the frequency of missing data in order to decide whether to replace them or remove cases, while also recording the initial distribution of the data. MCAR tests were used in this instance to determine the level and relationship of the missing data and determine whether there was a pattern or not (Little, 1988). So that a decision can be made regarding whether to eliminate cases or change the missing data. Therefore, if $P< 0.05$, it portrays that the pattern of the missing data is the same as the random pattern, and if $P>0.05$, then the missing data pattern is significantly different from the random pattern.

Thus Little's MCAR test was carried out to examine whether the data are MCAR by considering the levels of significance (sig. <.05). If the test is significant, then we can say that the data are not MCAR. However, when the test is not significant, then the data are said to be MCAR (sig.> .05)

Dealing with Outliers

Values that are anomalous in relation to the measuring scale are known as outliers. Outliers, are observations that deviate from the typical sample responses. They deviate from the test's values Hair et al. (2010). The extremely low or extremely high values skew the mean and inflate the standard deviation, the presence of outliers in the data on a variable may cause the distribution to be skewed (Pollet & van der Meij, 2017).

Consider the graphical tools, such as the Boxplots, as a coherent means of analyzing the outliers. Since boxplots display differences in data distribution without indicating whether the underlying distribution is normal or not, they are non-parametric in nature. Nevertheless, they demonstrate the range, especially when looking at the lower and upper ends of their whiskers (Vandervieren, 2008). The data from the pilot study's results showed that no other variable distributions had outliers; only the distribution of the Prudence variable did. By entering the appropriate numbers in the outlier's data, the outliers in the Prudence example were fixed.

Distribution Characteristics

The data characteristics tested were normality, homogeneity, linearity and multicollinearity.

Statistical Normality Test

The degree of skewness and kurtosis of the variables is referred to as the normality of a variable (Hair et al., 2010). When observations are unjustly concentrated on either the lower or upper side of a variable's arithmetic mean, the situation is referred to as skewness. When observations are evenly distributed on either side of the mean, a variable is said to have a normal distribution (symmetrical about the mean). On the other hand, kurtosis is the degree to which the distribution of a specific variable is peaked or flat (Field, 2009). Variables must be normally distributed at the univariate and multivariate levels for the majority of analyses that test hypotheses regarding specific parameters, such as correlation and regression coefficients, in order to prevent distortion in the detection of significance or non-significant of the parameter estimates.

Using the Kolmogorov-Smirnov and Shapiro-Wilk tests, the variables were examined for normality; a significance level of above 0.05 indicated that the variables are regularly distributed (Nornadiah & Bee, 2011). If a variable was not normally distributed, natural logarithmic transformation was applied to it.

Homogeneity

Another tenet of relational analysis is the homogeneity of variance, or just heterogeneity. If the variance of one variable is constant across all levels of the other variables, the data is said to be homogenous (Field, 2009). Differences in the impact of the independent factors on the dependent variable(s) in relation to the level of the independent variable result from the absence of homogeneity of variance (heterogeneity) in multivariate analysis (s).

Levene's test of variance was used in this study to assess homogeneity (Levene, 1960). The Levene's test statistic's significance threshold was less than or equal to 0.05, the null hypothesis that the population variances are equal was rejected.

Table 3. 5 Test of homogeneity of variance.

	Levene Statistic	df1	df2	Sig.
Prudence	1.575	1	238	.211
Courage	1.967	1	238	.162
Justice	.057	1	238	.812
Temperance	1.808	1	238	.180
Ethical Climate	2.192	1	238	.140
Behavioral Intentions	.276	1	238	.600
Ethical Behavior	2.208	1	238	.139

Linearity

A straight line relationship between two variables is referred to as linearity. This implies that variations in the independent variables occur at various points and result in correspondingly consistent variations in the dependent variables (Huber, 2004). The linearity of the correlations between the studied variables was confirmed by this investigation. By using correlational analysis and scatter plots, linearity was guaranteed. If the pattern of the plots shows a straight line rather than a curve, the relationship between the two variables is said to be linear. Additionally, if any pair of variables' correlation coefficient differs significantly from zero due to a significance level that is lower than the acceptable level of 5%.

Multi-Collinearity

If the predictors exhibit strong correlations when they are regressed against one another, multicollinearity exists. The variance inflation factor (VIF) and the correlation coefficients of the research variables were used to identify multicollinearity in the data. Menard (1995) said that VIF values above 10 imply multicollinearity; however, Table 6 shows that VIF is below 10, and correlations show correlation coefficients <.90, indicating that the variables are not multicollinear, and the assumption was therefore met.

Table 3. 6 Multicollinearity.

	Zero order correlation	Tolerance	VIF
(Constant)			
Prudence	.571**	.465	2.149
Courage	.522**	.710	1.409
Justice	.452**	.629	1.590
Temperance	.581**	.586	1.705
Ethical Climate	.633**	.500	2.001
Behavioral Intentions	.476**	.763	1.310

Exploratory Factor Analysis

The primary motivation behind component analysis was to distill variables from constructs with several questions into more significant and understandable factors. Additionally, to investigate theoretical structure (Barclay, Higgins & Thompson, 2001). Using explanatory factor analysis, the assessment of the indicators for content validity was further verified. Items with factor loading of 0.5 and above were kept, and factors with eigenvalues greater than one were retrieved using the Varimax rotation. However, the required qualities were carefully examined in order to judge whether the EFA application was appropriate for the data. The Kaiser-Meyer-Olkin (KMO) test, which should be over 0.60 (Kaiser, 1974), and Bartlett's Test of Sphericity, which should have statistical significance (Sig=0.000), are two examples of the qualities. The SEM modeling approach is appropriate for information systems research. Through the investigation of visible indicators or measures, it has the ability to determine correlations between pragmatic and hidden variables (Dow et al.,2008). With the help of this information, the constructs in the proposed model of ethical behavior in cyber security were evaluated for validity and reliability.

3.7 Confirmatory Factor Analysis (CFA) & Structural equation modelling

Software for Confirmatory Factor Analysis (CFA) and Structural Equation Modeling (PL-SEM) was used to analyze the quantitative data that was gathered. Confirmatory factor analysis (CFA), in accordance with Albright & Park (2009), is theory- or hypothesis-driven and is based on theoretical links between the seen and unobserved. CFA makes it feasible to apply constraints to the factor model that have real, practical value. Researchers can choose the number of components or the value at which one latent variable affects the observable variables. CFA enables academics to test theories on a certain factor structure. The model constructs were examined using CFA to determine whether they concur with the researcher's understanding before being examined using SEM to look for casual relationships. Gray (2015) contended that employing SEM methods is becoming more common.

The theoretical model for cyber security is built around the cardinal virtues, and it was put to the test using confirmatory factor analysis and structural equation modeling methods.

The Smart PLS version 2.0 was used for the SEM analyses since it is effective at examining structural correlations among and across latent variables as well as those between latent and observable variables (Ringle et al., 2005). The structural model was subjected to path analysis using SEM to determine how well the proposed model suited the observed data set. In research, path analysis is used to evaluate and test models, especially those that involve chains of effect between several variables (Streiner, 2005).

The Cyber security ethical behavior model was tested using the indices identified after data Analysis. CFA and SEM provided the means to test the validity of the construct indicators, relationships between construct (factor) loadings, determine whether they are correlated or uncorrelated, and evaluate the fit of the hypothesized model to the observed data set thereby providing a basis to confirm or reject the hypotheses of this research. Normality of a variable refers to the level of skewness and kurtosis of the variables (Hair et al., 2010). Skewness refers to a situation where observations are unevenly piled on either the lower or upper side of the arithmetic mean of a variable.

Phase two involves performing the route analysis, analysis of variance, regressions, and zero-order correlations (ANOVA). To determine the independent factors' predictive abilities on the study's dependent variables, multiple regressions were computed.

The presence of mediation and moderating effects, as well as the degree to which independent variables predicted the dependent variable, were established by the hierarchical regressions. The theoretical model-based hypothesis was put to the test in the study using structural equation modeling (SEM).

The two stage method suggested by Anderson & Gerbing (1988) was used to conduct the SEM study. A set of relationships between one or more independent variables, either continuous or discrete, and one or more dependent variables, also either continuous or discrete, can be studied using a variety of statistical techniques known as SEM (Tabachnick & Fidell, 2001). The main goal of SEM, Schumacker & Lomax (1996), is to explain the pattern of a number of concurrent, interrelated dependent connections between a number of latent or unobserved constructs, each of which is measured by one or more observable variables. The entire impact of the mediation variables on the predictor variable was determined using the path analysis.

The data was also analyzed and the hypothesis tested to examine the moderating effects of ethical climate on cardinal virtues using mod graphs.

3.8 Evaluation of measurement model

While establishing the total of construct indicators, Dow et al., (2008) make it clear that models with fewer construct indicators have a better apparent model fit. At least four constructs must be present, and each construct must have three measurement elements. This requirement was met by the ethical behavior model for cyber security in this study. CFA is carried out in the Measurement model to assess whether the indicators are suitable for measuring the relevant latent variables (Field, 2009).

Various tests for model fit, convergent and discriminate validity, normalcy, and reliability approved by the research community were used to evaluate the measurement model in order to assess the overall data fit. The chi-square test is a common way to determine the goodness of a model's fit. It serves as a basis for either accepting or rejecting a model, (Hooper et al. (2008). One of the most explanatory model fit indices is the root mean square error of approximation (RMSEA), which is used for measurement and structural fit analysis to explain model complexity and population covariance (Hooper et al., 2008).

Sun, (2005) suggests utilizing Standardized Root Mean Square Residual (SRMR) for discriminating validity and Root Mean Square Error of Approximation (RMSEA) for convergent validity for evaluating the goodness of fit of the measurement model. The reliability and validity of the indicators used to gauge the various components are the subjects of this assessment. A composite reliability statistic (CR) was developed to evaluate the indicators' reliability, and more specifically, construct reliability. A construct was regarded to have construct reliability if the CR value was 0.6 or greater. The average variance (AVE) explained was used to test dependability, and in this situation, an AVE value of 0.5 or more was regarded as a reliable indicator (Hair, 2010), concerning validity. Discriminant validity and convergent validity can be evaluated using SEM. When indicators of constructs that are supposed to measure different phenomena are actually not strongly associated, this is known as discriminant validity. In this sense, the AVE for each construct in the measurement model should be higher than the squared correlation value for the correlation between the individual constructs. A concept has convergent validity when, first, all of the indicators in the measurement model are significant, and second, when the AVE is larger than or equal to 0.5. Convergent validity occurs when indicators of constructs intended to measure a similar occurrence are significantly correlated.

This study used indices of relative chi-square (X2/df), RMSEA, SRMR, CFI, and NNFI to assess measurement model goodness of fit; AVE, path weights, bootstrap confidence intervals, item to total and squared correlation to assess convergent and discriminate validity; kurtosis and skew for normality; indicatorsessing if the data fits the measurement model. Construct validity, which is a combination of convergent

Structural Model

The route analysis and regression analysis parts of the structural model are crucial. The objectives were addressed using this model, and the standards by which the study's hypotheses were rejected or not were also determined. To estimate causal linkages resulting from behavioral constructs, structural equation modeling is considered appropriate (Babin & Svensson, 2012).

Typically, the structural model is estimated to examine whether there are causal connections between the constructs (Hair et al., 2010). Path coefficients were calculated and their significance was assessed using the Maximum Likelihood (ML) approach.

In contrast to Ordinary Least Squares estimation (OLS), the Maximum Likelihood estimation method was used because it can handle data at levels of measure as low as the ordinal level (Schermelleh-Engel et al., 2003) and because the observed variables (indicators) of the constructs are scaled on an ordinal basis. Depending on whether the various effects are significant or not, the estimated route coefficients were employed to make it easier to address the total impacts, direct effects, and indirect effects that are implied in the study's hypotheses. In addition, for the observed proposed conceptual model, the predictive power of a set of independent variables that together affect a given set of dependent variables was assessed by examining the corresponding squared correlation coefficients.

3.9 Suggestions to the Solution

The study carried out in the previous phase guided the researcher to answer the first research question and achieve the first objective, by establishing the research gap and identifying the requirements for the development of a cyber-security ethical behavior assessment model. drawn from literature review, and using results from the research phase resulted in a tentative design, concept of ECEBA model.

A solution to the existing problem was proposed after the analysis of existing ethical behavior models and there by identifying the weaknesses and challenges with the current ethical behavior assessment models. The tentative design is further developed and implemented in phase development.

3.9.1 A Conceptual Framework of the Proposed Solution

The aim of this study was to enhance cyber security by developing a web-based assessment model to help banks assess cyber security ethical behavior of their employees. This may help banks management pinpoint gaps and then cyber security ethical behavior awareness and training programs be customized to address those gaps. By a review of existing ethical behavior models a conceptual framework for the proposed model was created as shown in fig 2 below. The model was implemented in the following way: questions about cardinal virtue constructs of; Prudence, courage, justice, and temperance that should be possessed by Cyber security employees were created.

Questions about Behavioral intentions and ethical behavior towards Cybersecurity were also created including questions about the general climate in the banks using ethical climate questionnaire. Once a user initiates assessment, the questions are fed to his UI display using an html form.

Questions are on a Likert scale of 5. The user can only choose one answer per question. Once the user completes the assessment and submits the answers, the results are processed using a PHP script in the application controller and the resulting values stored in the same database but in a different table. The analysis is achieved by using a basic JavaScript algorithm to first calculate the percentage from the points earned and then map this percentage onto a chart/graph. After analysis, the user is assigned a percentage score.

3.10 Phase 3: Artifact development

3.10.1. Objective two; Approach to developing an employees' Cyber security ethical behavior assessment model for commercial banks in Uganda.

From the suggested requirements to the developed cyber security ethical behavior assessment model, inputs and outputs of the model were identified, the different necessary sections, software and hardware tools used together with the different sketches/ images of the developed model and their description are also clarified.

A web based cyber security ethical behavior assessment model was developed and the results from objective 1 are the model constructs that are assessed.

XAMPP version 7.2.32 was used to act as the local database server to locally host the MySQL database where the system data is stored. The server also hosted the web application files which were accessed in a client server environment using Google Chrome web browser. MYSQL Workbench 8.0 CE was used to design the database model to illustrate the flow of data between entities. This helped in designing the logical database model which was later converted into a physical database after forward engineering. Sublime Text Editor version 3 32bit was also used as the source code editor for editing the developed web system source code. This was done purposely to create a highly usable and accessible model to support assessing employees' cyber security ethical behavior in the Uganda banking sector. Below is a detailed discussion of how the model was designed.

3.10.2 Requirement gathering and analysis

Requirements Gathering is the process of generating a list of requirements which include functional, non-functional, system, user, and, technical requirements from the stakeholders (customers, users, vendors, IT staff) that will be used as the basis for the formal definition of what the project does. In this phase, the researcher deployed data collection techniques in order to get requirements from the users. Literature was reviewed about the existing cyber security ethical behavior models to identify their strengths and weaknesses and also establish the model requirements. An online questionnaire was sent to commercial banks' employees and their answers are the inputs for the questions in the assessment model

3.10.3 Model design

In the design phase, the researcher used the requirements document from the previous phase to graphically structure how the performance of the model and the flow of data between different entities in the model system. Different tools were used to come up with different designs for example Visual Studio a software tool was used to design the flow chart which diagrammatically represented the workflow of the model. The chart shows how different users will access and use the model since it portrays the functional and non-functional requirements of the system. Another tool is MySQL workbench which was used to come up with the enhanced entity-relationship diagram (EERD) a high-level or conceptual data model incorporating extensions to the original entity-relationship model, used in the design of the system database. The EERD showed all the flow of data amongst entities in the database. It was still this phase where the model user interfaces (UI) were graphically represented. The UIs showed the data input and output forms e., model assessment forms, the structure of reports e.g., assessment completion certificates, and others. Mockup plus was the tool employed to design these interfaces. The designs were subjected to users to make sure they portray the image of the model performance as expected by the user. This phase gave delivered mockups of the model which were used as input in the development phase.

3.10.4 Model Development

In this stage, creating a functional version of the model was the focus. The phase included a variety of designs, including flowchart, database, and user interface designs. Different programming languages and tools were employed during this phase.

Languages utilized include JavaScript for data validations on the clients to prevent users from providing erroneous data inputs, HTML for placing elements like tables, forms, and headings on the model UI, and PHP as a server-side scripting language to connect the user interface and the database server. During the development of, a MySQL database was created and hosted locally on the XAMPP server using MySQL as the database management the model. To interact which the MySQL database, developers used SQL in order to define and run queries on the database. Other technologies used in this phase included Bootstrap a potent front-end framework used to create modern websites and web apps, and jQuery a fast, small, and feature-rich JavaScript library. It makes things like HTML document traversal and manipulation, event handling, animation, and Ajax much simpler with an easy-to-use API that works across a multitude of browsers.

Other tools used included Visual code studio and Sublime Text Editor 3 as source code editors for writing and editing the model source code, Google Chrome, and Microsoft Edge as web browsers for testing the model functionality and performance. This phase produced different working artifacts of the model which were subjected to the users for testing and validation.

Model Testing

Each of the following pages were tested and ascertained to be functioning as intended. login page, , dashboard page, users' management page, create new assessment page, manage assessment page, add assessment questions page, view assessment page, questions management page, edit assessments page, system reports page. The testing of the model was conducted in two sub-phases i.e., Unit testing where each system module was tested separately and internally on the local server. Modules tested include the Users Management Module, Assessment Tools Management Module, Assessment Module, Compilation of Results Module, Reports Module, and others. Then all modules were integrated to come up with a working version of the model which was later hosted on a secure remote server under a sub domain i.e., , in order to allow end-users from different financial institutions to test the functionalities of the system to make sure that it satisfies the requirements that were gathered in the first phase. This was termed Integrated system testing. During this testing, users gave their feedback on each system artifact and this feedback could help the development team produce a better version of the system that incorporated the changes raised by the users in the testing phases. Entire model Testing. All modules were ascertained to be working as intended.

3.11. Ethical Considerations

Seale, (2004), it is necessary to take into account how a study disturbed a person, whether they accepted it or not, and how this worry might be balanced with the goal of improving the world.

This is why several ethical concerns were taken into account during this study. These include: i. Respondents were protected by outlining the study's goals and purpose to them. They have the option of participating or not in the study. iv, the surveys were pre-coded, and no one's names were ever mentioned in connection with the study's findings. iv, in order to produce accurate and verifiable statistics, the integrity of the data analysis was guaranteed by examining the precision with which the survey replies were encoded.

This research was cleared by the Research Ethics Committee at MUST and National Council of Science and Technology.

3.12 Consent from participants to carry out the study on them

Before taking part in the survey, study participants were given a consent form, which they were expected to read and understand (see appendix D). In order to participate in the survey, participants were required to sign a consent form; however, they were allowed to decline if they did not agree with the terms. Additionally, participants in the study gave their consent to participate, and they were allowed to stop filling out the questionnaire at any time. They then signed it to indicate their agreement to participate in the study as participants. They were then given access to an online survey, which they completed and sent using the provided email.

3.13 Confidentiality of the respondents

The participants were aware of the researcher's identity, but they were given the assurance that their particular survey responses would be kept private and that their identities would not be made public even after the completion of the final report. The university's address and the supervisors' contact information were listed in the instrument's introduction remarks. The respondents in this instance were free to inquire of the university or the supervisors as to the validity of this study and were also free to inquire of the university authorities as to this study. A disclaimer indicating that he research is only intended for academic purposes was added in the survey questionnaire. The esearcher indicated in a portion of the data collection tool that the respondents' privacy would lways be protected and that they would not be permitted to write their names.

This indicates that the respondent's privacy was protected. This assertion dispels any respondent's belief that this study may have a purpose beyond what is stated in its objective.

The participants were aware of the researcher's identity, but they were given the assurance that their particular survey responses would be kept private and that their identities would not be made public even after the completion of the final report. The university's address and the supervisors' contact information were listed in the instrument's introduction remarks. The respondents in this instance were free to inquire of the university or the supervisors as to the validity of this study and were also free to inquire of the university authorities as to this study. A disclaimer indicating that the research is only intended for academic purposes was added in the survey questionnaire.

The researcher indicated in a portion of the data collection tool that the respondents' privacy would always be protected and that they would not be permitted to write their names. This indicates that the respondent's privacy was protected. This assertion dispels any respondent's belief that this study may have a purpose beyond what is stated in its objective.

3.14. Permission to carry out the study

Permission to conduct the study was obtained from Mbarara University of Science and Technology via the Research Ethical Committee process, Appendix A, and the participating Banks (appendix B and C) prior to distributing the survey questionnaire. This research also obtained research permission from Uganda National Council for Science and Technology, see appendix D. After obtaining the Research permit, the survey was disseminated using an email to potential participants with an invitation to participate through an Internet link which was provided for participation for ten weeks. Over this time the survey was available and the Banks 'employees being surveyed circulated the survey link to their colleagues. The study participants continued to volunteer to invite and recommend more of their colleagues they considered eligible to take part in the survey. The researcher kept on checking the response numbers during the survey course. When 240 responses were received the results were reviewed for completeness and the main survey was closed.

3.15 Acknowledging information sources and materials

Acknowledgement and references were done all through the study. The researcher made sure all the support given directly or indirectly by various people towards this research was acknowledged in the acknowledgment section. Furthermore, all appropriate citations of works of other authors used in any part of this study was provided.

3.16 Chapter Conclusion

This chapter described the philosophical assumption that were used in respect to this study, which was functionalism paradigm and positivist approach. and presented the research methodology which was used. The use of the survey methodology to gather quantitative data to further develop, validate, and test the reliability of the proposed constructs and the theoretical model through CFA and SEM were described. Issues related to population and sample selection, statistical techniques used, and data collection and analysis were discussed. The procedure for establishing the statistical significance of the results was described. Resources required to conduct the research study and assumptions were offered. Data analysis was done using SEM for descriptive and inferential statistics. Smart-PLS was used for SEM model in the current study. The Smart-PLS is the software of choice and is very relevant for other SEM models (Hair et al., 2010). The challenges encountered and how they were mitigated was also discussed.

CHAPTER FOUR: PRESENTATION AND DISCUSSION OF FINDINGS

Introduction

This chapter contains the results for objective one, that were acquired after the data had been collected, entered and analyzed using the appropriate software. The analysis was done with reference to the research study objectives and the hypothesis in this study. The chapter further presents Descriptive Statistics, Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA) and Structural Equation Modelling (SEM) used in testing for hypotheses. In the first part of the analysis are the attributes of the commercial banks' employees who were the respondents. The statistical models used in this case included percentages, means and the standard deviations. On the other hand, the findings to address the research objectives and hypothesis were examined using exploratory factor analysis (EFA), correlations, and regression as the main models. Finally, the results were discussed.

4.1 Data Analysis

4.1.1 Demographic Data

Data got from the field was analysed to establish the nature of respondents that participated in the study. In this section, the respondents age, gender, level of education, specialty, job titles or categories and experience were examined. The demographic data of the survey participants was analysed in order to establish peripheral validity of the sample results and to be sure that participants are from the commercial banks. This was needed because the sample must be representative of the population in order to provide suitable and accurate answers to the survey questions and to establish confidence in the accuracy of the data that was gathered (Gray, 2015).

4.1.2 Respondents Gender

Data collected about respondent's gender was analyzed using descriptive statistics. This was done in order to understand how female and male employees participated in Cyber security ethical behavior in the banking sector.

This research consists of 240 respondents based on gender, age, education level professional role, and years of employment.

Of the 240 respondents, 129 were male and 111 (46.2%) were female; as shown in the table below.

Table 4. 1 Respondents Gender.

Gender	Frequency (N= 241)	Percent
Female	111	46.2
Male	129	53.8
Total	240	100

Results in table 4.1 above reveal that most respondents were male (freq=129 (53.8%). Female respondents were 111 representing about 46.2%. This outcome clearly indicates that most employees that are in the field of Cyber security in the banking industry in Uganda are male. This distribution can be attributed to the traditionally held view in Uganda among the population that the males are better suited for the public work roles. However, this view has slowly been wrinkled as women are progressively starting up and managing businesses. Women are also these days being regarded as less corrupt than men and hence preferred.

4.1.3 Respondents age group

Data about the respondents age was collected and analyzed using descriptive statistics in order to comprehend the employees' age groups.

Table 4. 2 Respondents age.

Age group	**Frequency**	**Percentage**
20-29 years	60	25
30-39 years	140	58.3
40-49 years	37	15.4
5o and above	3	1.3
Total	**240**	**100**

The results reveal that most of the commercial banks' employees are in the age group 30-39 years (Freq=140, 58.3%), followed by those in age group 20-29 years (Freq=60, 25%) and those in age group 40-49 (Freq=37 15.4%). 3 respondents constituting 1.3% were above 50 years. This finding indicates that most employees in the banking industry in Uganda are youths below the age of 40 years. This distribution truly depicts the average working years of the individuals in Uganda. These are the years full of vigor and individuals are committed to working. But as the years advance from 41 forwards (42 – 49 years), individual employees decline in numbers as some go for other forms of employment or some retire to leave the business to the much younger generation. On the other hand, this is a problematic age. Youth can easily be tricked through social engineering and other forms into committing Cybercrimes. Young people are fascinated with computing technology. They now spend an average of 8.33 hours per day on the internet surfing and visiting prominent social media websites like Facebook, twitter, WhatsApp (Rideout, Roberts, & Foehr, 2005). Rushkoff (2006) has named the younger generation" screenagers" because of their over stay on technology screens.

4.1.4 Respondents' bank

Table 4. 3 Respondents' bank.

	Frequency	Percent
Centenary Bank	147	19.6
ABSA Bank	93	27.1
Total	240	100.0

The study also included the bank from which the employee was coming from. This was important inorder to gauge the representation of the banks that took part in the study since the study focused on commercial banks. The respondent's bank was also crucial to establish the response rate of the employee from the different banks that took part in the study.

4.1.5 Respondents Education level

Table 4. 4 Respondents Education level.

	Frequency	Percent
Diploma	2	.8
Bachelor degree	169	70.4
Master degree	45	18.8
PhD	22	9.2
Others	2	.8
Total	240	100.0

Data gathered about education levels was analyzed using frequencies and percentages as seen in Table 4: above. The results on respondents' highest levels of education reveal that majority of them have Bachelor's degrees, followed by those with Post graduate diplomas, Masters, and those with PhD, then Diploma. The highest levels of education say something about the average literacy levels and the competences that can be examined among the banking sector employees in this study. The greater percentages are either holders of bachelor degrees or masters' degrees. These results indicate that all respondents are educated and could contentedly understand the questions on the questionnaire.

4.1.6 Speciality

Table 4. 5 Speciality.

	Frequency	Percent
Information systems	48	20.0
Information technology	55	22.9
Computer science	16	6.7
Data communication	43	17.9
Others	78	32.5
Total	240	100.0

4.1.7. Current professional role

Table 4. 6 Current professional role.

	Frequency	Percent
Security field	138	57.5
Department head	1	.4
Division Head	27	11.3
IT Specialist	10	4.2
Tellers	108	45.0
Web Designer	9	3.8
Others	80	33.3
Total	240	100.0

The range of the relevant characteristics of professional roles, and specialty, are well represented by this surveys participants and correspond closely with sample populations of other Information system studies; providing confidence about the representativeness of the sample.

Furthermore, the knowledge of the survey participants in the field of information systems security and Cyber security appears to be confirmed and they are considered to be an accurate representation of the population they are intended to represent.

4.2 Data cleaning

After data collection using online questionnaire methods, it was entered into SPSS version 22. The data was cleaned to remove inconsistences and also cater for other aspects that would comprise the quality of the research results. The data cleaning procedures included; missing value analysis and checking for outliers and making the necessary amendments.

4.2.1 Outliers

Outliers are observations that differ from the majority of sample responses (Hair et al., 2010). They might be unique across variables, but they usually cause problems in data analysis because they don't adequately represent the population under study. By skewing the mean results and increasing the standard deviations, this has an effect on the statistical findings. As a result, they affect the consistency of data distribution. So before moving on to parametric testing, it was required to test for them. Results showed that all of the variables had just outliers. see appendix 2,3,4, and 5. The outliers were corrected by entering the correct values in the outlier's data.

4.2.2. Test for Statistical Normality

The Kolmogorov-Smirnov and the Shapiro-Wilkinson's tests, both test the Hypothesis that the Distribution deviates significantly from a normal distribution (sig. >.05). in the results in this study, it was established that the data for all the study variables had statistics that were not statistically significant at all (sig. >. 05).

Table 4. 7 Test for Normality.

	Kolmogorov-Smirnov[a]			Shapiro-Wilk		
	Statistic	df	Sig.	Statistic	df	Sig.
Prudence	.172	240	.000	.943	240	.000
Courage	.234	240	.000	.905	240	.000
Justice	.153	240	.000	.960	240	.000
Temperance	.163	240	.000	.958	240	.000
Ethical Climate	.090	240	.000	.966	240	.000
Behavioral Intentions	.198	240	.000	.918	240	.000
Ethical Behavior	.161	240	.000	.946	240	.000

These results show that the research data were not deviating statistically from a normal distribution and therefore the data could be confirmed to be fairly conforming to a normal distribution.

4.2.3. Test of homogeneity of variance

For this matter, the Levene's Statistic was used to test for whether the variances in the data differ significantly among the data.

Table 4. 8 Test of homogeneity of variance.

	Levene Statistic	df1	df2	Sig.
Prudence	1.575	1	238	.211
Courage	1.967	1	238	.162
Justice	.057	1	238	.812
Temperance	1.808	1	238	.180
Ethical Climate	2.192	1	238	.140
Behavioral Intentions	.276	1	238	.600
Ethical Behavior	2.208	1	238	.139

It was noted that there are no significant differences among the sample variances across the distribution but these were relatively the same for all the study variables (sig. >.05). This means that applying the same data statistic would not be misleading.

The results for the natural logarithm transformed variables are such that, all variables had significance values above 0.05, hence leading to failure to reject the null hypothesis of equal variance. In other words, all the natural logarithm transformed variables did not violate the assumption of homogeneity).

4.2.4. Test for Linearity

A bivariate correlation analysis was used to assess if the independent variables are linearly related to the dependent variable, which establishes whether there was proportionate covariance between the independent and dependent variable. The question of whether there was a meaningful link between the independent and dependent variables was carefully considered.

Table 4. 9 shows bivariate correlation analysis results.

	1	2	3	4	5	6	7
Prudence (1)	1						
Courage (2)	.466**	1					
Justice (3)	.448**	.435**	1				
Temperance (4)	.538**	.383**	.466**	1			
Ethical Climate (5)	.665**	.393**	.486**	.503**	1		
Behavioral Intentions (6)	.357**	.217**	.376**	.432**	.302**	1	
Ethical Behavior (7)	.571**	.522**	.452**	.581**	.633**	.476**	1

**. Correlation is significant at the 0.01 level (2-tailed).

The results in table 5 show that there is a significant positive correlation between the dependent variable, that is; employees ethical behavior towards Cyber security and the independent variables, which are; prudence ($r = .571$, $p<.01$), courage ($r = .522$, $p<.01$), Justice ($r = .452$, $p<.01$), temperence ($r = .581$, $p<.01$), ethical climate ($r = .633$, $p<.01$), behavior intentions ($r=.476$, $p<.01$). This implies that there is a possibility that those six independent variables are linearly related to the dependent variable.

4.2.5 Test for Multicollinearity

Indicator items under the same formative construct were also evaluated for potential multicollinearity. Conceptual overlap is indicated by an excessive degree of correlation between indicators, with high correlation being ≥ 0.90 and moderate being ≥ 0.80. All correlations between items under the same construct were found to be less than 0.6, providing evidence that there are no multicollinearity issues.

Besides the Bi-variate correlations between the independent variables, the Variance Inflation factor (VIF) of the regression model of Cybersecurity ethical behavior were assessed as summarized in Table below.

Table 4. 10 Estimates of the Variance Inflation Factor (VIF).

	Zero order correlation	TV	VIF
(Constant)			
Prudence	.571**	.465	2.149
Courage	.522**	.710	1.409
Justice	.452**	.629	1.590
Temperance	.581**	.586	1.705
Ethical Climate	.633**	.500	2.001
Behavioral Intentions	.476**	.763	1.310

Notes: TV=Tolerance Value; VIF=Variable Inflation Factor

Multicollinearity occurs when the predictor correlated highly when regressed against each other. Multicollinearity in the data was analyzed using the variance inflation factor (VIF) and scrutinizing the correlation coefficients of the study variables. According to Menard (1995), VIF values above 10 indicate multicollinearity, Table above indicate VIF below 10 and the correlations indicated correlation coefficients below .90, therefore implying non multicolliarity among the variables and thus the assumption was met.

4.2.6 The Standardized Root Mean Square Residual (SRMR)

(SRMR) is used to measure the absolute fit of a measurement model. It is a measure of the mean absolute correlation residual, the overall difference between the observed and predicted correlations. It is an extension of the Root Mean Square Residual (RMR), the square root of the discrepancy between the sample covariance matrix and the model covariance matrix, (Hooper et al., 2008).

4.2.7 Path Weight

The path weight or effect size is a sample-based estimation of a population parameter. The amount and direction of the difference between two groups or the strength of the association between two variables are referred to as effect size, the practical or substantive significance (Schumacker & Lomax, 1996). A quantitative study's key finding is the effect magnitude. In regression and SEM, standardized path weights less than 0.10 are regarded as small effects, approximately 0.30 as medium effects, and 0.5 or more as large effects.

The acceptable fit criteria for effect sizes are fairly arbitrary (Kline, 1998). According to Chin (2010), a value of 0.05 is considered minor while a value of 0.10 is considered noteworthy. Inner model parameters in PLS are non-significant at less than 0.10, based on Tenenhaus (2008). Regardless of the value chosen, one or more measures of effect size—not p-values—should be the most significant results of a research study since they quantify the magnitude of the difference or the strength of the association (Chin, 2010; Coe, 2002).

4.2.8 p-value

By comparing the statistical value attained to a crucial value, the p-value, also known as statistical significance, gauges the strength of the evidence or power to support the null hypothesis. Based on the importance of the sample size, the path weight's allowable value is determined. Large samples, defined as 200 to 400, tend to be more significant and are necessary for SEM. Sample sizes are crucial to research since they give precision and confidence in the results (Kline, 1998).

4.3 Exploratory Factor Analysis (EFA) and Confirmatory Factor Analysis (CFA)

Two statistical methods are used to investigate a measure's internal reliability: EFA and CFA. They are used to look into the theoretical elements that might be represented by a collection of objects. Either the factors might be assumed to be orthogonal or unrelated. Both are employed to rate each item's quality individually. Both can be applied to confirmatory or exploratory research.

4.3.1 Exploratory Factor Analysis

Exploratory factor analysis (EFA) is frequently used to identify a measure's factor structure and assess its internal consistency. EFA is characterized by the initial standardization of the observable variables (mean of zero and standard deviation of 1). The correlation matrix between the items is used to run EFA. Latent variables are referred to as factors in EFA, and the relationships between latent and observable variables are referred to as factor loadings. In order to improve the measuring scales for each study variable and ensure the validity and reliability of the indicators and constructs for each variable, an exploratory factor analysis was conducted. EFA was actually used to determine the study variables' factor structures based on correlations among the respective constructs. The number of indicators for the constructs of any factor structure was decreased utilizing the Varimax factor rotation with Kaiser Normalization of the principal component analysis (Hair et al 2006). Indicators with a factor loading more than or equal to 0.5 and factors having an eigen value of larger than one unit were used to extract the factors.

Factor loadings at 0.32 and lower are poor, between 0.32 and 0.45 (fair), 0.45 and 0.55 (good), 0.56 and 0.63 (good) and 0.64 and 0.70 (very good) and 0.71 and above (excellent).

This method was specifically used to keep the indications with sufficient data. The confirmatory factor analysis was conducted after the exploratory factor analysis, in which the initially hypothesized factors were either retained or reduced to only those that were significant in the principal component rotations, and in which the items with a factor loading below 0.5 were deleted from the constructs' factor structure. The CFA was conducted to improve the factor structure of the constructs that had been discovered during the exploratory factor analysis and to further ensure the validity and reliability of the indicators.

4.3.1.1 EFA for Cardinal Virtue Constructs

The cardinal ethical virtues were operationalized using four measurements and 20 indictors. All of the 20 indicators were appended to a 5 – point likert scale.

Table 4. 11 Rotated component matrix for Cardinal Virtue Constructs.

	Prudence	**Justice**	**Courage**	**Temperance**
	Factor loadings			
PR3: An aptitude to make judgments based on professional understanding contributes to Cybersecurity.	0.814			
PR4: Workers awareness of the suitable use of Cybersecurity strategies can affect the Cybersecurity.	0.773			
PR6: Cybersecurity is affected by the workers practical expertise	0.755			
PR5: A person's aptitude to resolve conflicts between organizational policies and goals can impact the security of an information system.	0.696			
PR2: Unbiased decision making by organizational workers can impact their information system security submission	0.628			
JUS1: Public responsibility and community participation are not elements of ethical computer behavior.		0.808		
JUS4: The employees' Ethical use of Cyber assets is not significant to an organization as long as business goals are achieved.		0.766		
JUS5: Being sensitive to loss of information system data is a computer ethics related issue.		0.695		

JUS2: There is no relationship between Cybersecurity ethical behavior and protection of sensitive information.		0.626		
CO3: Making correct judgments contributes to Cyber security strategies compliance.			0.839	
CO2: A focus on one's personal desires over the greater good is an example of good computer ethics.			0.783	
CO4: Regarding Cybersecurity, when employees commit unethical act they will try to justify to themselves that their behavior is acceptable.			0.726	
TEMP2: Employee professionalism promotes Cybersecurity.				0.847
TEMP3: Employees enhance Cybersecurity compliance by making rational decisions.				0.722
TEMP1: Information system security compliance is not affected by a person's attitudes and beliefs.				0.689
Eigen value	**3.465**	**2.883**	**2.639**	**2.461**
Variance (%)	**20.38**	**16.96**	**15.52**	**14.476**
Cummulative Variance (%)	**20.38**	**37.34**	**52.86**	**67.34**

KMO = .888, Bartlett's Test of Sphericity = 1765.027, df = 105, sig. = .000

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. Rotation converged in 6 iterations.

The exploratory factor analysis of ethical virtues as shown in table 5, specifies that all four measurements were retained as significant factors since they have eigen values ranging from 2.4 to 3.4. Furthermore, 5 of the 20 indicators were dropped from measurement scale for either having a factor loading of lower than 0.5 and or cross loading.

The factors that were extracted, in the order of significance include; prudence (Eigen value=3.465, variance=20.38%), followed by **Justice** (Eigen value= 2.883, variance =**16.96** %), **Courage** (Eigen value=2.639, variance = 15.52 %) and Temperance (Eigen value= 2.461, Variance = 14.476 %).

The EFA of cardinal ethical virtues created a Kaiser-Meyer-Olkin (KMO) for sample adequacy of .888, which is above 0.5. Hence the sample was appropriate for factor analysis (Field, 2009). Bartlett s test of sphericity of approximate chi-square = 1765.027, df = 105, sig. = .000 was found

to be significant, which indicates that the factors have significant relationships sufficient to measure cardinal ethical virtues.

4.3.1.2 EFA for ethical climate

Table 4. 12 Rotated component matrix for ethical climate Constructs.

	Team Interest	Organizational Interest	Stakeholder Orientation	Self Interest	Friendship	Public Interest
TI4: A good and broad cooperation among all colleagues is considered to be very important in this bank.	0.760					
TI2: Our major consideration is what is best for all colleagues in this bank	0.737					
TI3: People in this bank view team spirit as important.	0.732					
TI1: The most important concern is the good of all the people in my bank	0.651					
OI2: Organizational members are solemnly concerned with the financial interests and the image of the bank		0.889				

OI3: Decisions here are primarily viewed in terms of the money they generate for this bank	0.886		
OI1: Organizational members are expected to do anything to further the financial interests and the position of this bank.	0.857		
SO3: People in this bank are actively concerned about the citizens they have direct contact with.		0.887	
SO2: People in this bank have a strong sense of responsibility to the citizens they deal with.		0.849	
SO4: The effect of decisions on citizens whom we deal with directly is a primary concern in this organization.		0.764	

SI1: In this company, people are mostly out for themselves.	0.856		
SI2: People in this bank are mostly concerned about what is best for themselves.	0.838		
SI3: Decisions here are primarily viewed in terms of the money they generate for this bank.	0.795		
F2: In this bank our major concern is always what is best for the other person, weather she/he is a colleague or not.		0.787	
F1: Good interpersonal contacts both with colleagues and with outsiders are considered to be very important in our bank.		0.702	
F3: What is best for each individual weather citizen or colleague is the primary concern in this bank.		0.682	

F4: It is expected that each individual both colleague and outsider is cared for when making decisions here.					0.626	
PI2: Everyone is expected to stick to the rules and procedures of the bank.						0.786
PI3: People are expected to comply with the law and public interest over and above other considerations.						0.717
PI5: In this bank public interest is the major consideration.						0.563
PI4: In this bank people are expected to follow legal and professional standards.						0.529
Eigen value	3.028	2.919	2.456	2.240	2.320	1.899
Variance (%)	16.713	14.419	13.901	11.523	11.047	9.043
Cummulative Variance (%)	16.713	31.132	45.033	56.556	67.603	76.646

KMO = .861, Bartlett's Test of Sphericity = 2880.125, df = 253, sig. = .000

Extraction Method: Principal Component Analysis. Rotation Method: Varimax with Kaiser Normalization. Rotation converged in 6 iterations.

The exploratory factor analysis of ethical climate as shown in table 6, specifies that 5 measurements were retained as significant factors since they have eigenvalues ranging from 2.4 to 3.4. and one was dropped since it had the small eigenvalue of 1.899. Furthermore, 21 of the 32 indicators were dropped from measurement scale for either having a factor loading of lower than 0.5 and or cross loading.

The factors that were extracted, in the order of significance include; i) Team Interest (Eigen value=3.208, variance=16.713%), ii) Organizational Interest (Eigen value= 2.919, variance =14.419 %), iii) **Stake Holder Oriantation** (Eigen value=2.456, variance = 13.901, %), iv) **Self Interest** (Eigen value= 2.240, Variance = 11.523%), v) Friendship (Eigenvalue =2.320, variance =11.047%), vi) Public Interest (Eigenvalue =1.899, variance=9.043%).

The EFA of ethical climate created a Kaiser-Meyer-Olkin (KMO) for sample adequacy = .861 which is above 0.5. Hence the sample was appropriate for factor analysis (Field, 2009). Bartlett s test of sphericity of approximate chi-square = KMO, Bartlett's Test of Sphericity = 2880.125, df = 253, sig. = .000 was found to be significant, which indicates that the factors have significant relationships sufficient to measure ethical climate.

4.3.1.3 EFA of Behavioral Intentions

Table 4. 13 The exploratory factor analysis of ethical Behavioral Intentions constructs.

	Behavioral Intentions
BI2: I will take precautions against Cyber security violations	0.917
BI3: I intend to actively use Cyber security technologies.	0.861
BI1: I will take measures to protect information and computer assets from Cyber security violations	0.851
Eigen value	**2.306**
Variance (%)	**76.881**
KMO = .696, Bartlett's Test of Sphericity = 323.125, df = 3, sig. = .000	
Extraction Method: Principal Component Analysis. 1 component extracted.	

The exploratory factor analysis of ethical **Behavioral Intentions** as shown in table 7, specifies that all the 3 indicators having a factor loading of higher than 0.5 were measured.

The EFA of ethical behavior intentions created a Kaiser-Meyer-Olkin (KMO) for sample adequacy =. KMO = .696, which is above 0.5. Hence the sample was appropriate for factor analysis (Field, 2009). Bartlett s test of sphericity of approximate chi-square = KMO, Bartlett's Test of Sphericity = Bartlett's Test of Sphericity = 323.125, df = 3, sig. = .000 was found to be significant, which indicates that the factors have significant relationships sufficient to measure ethical **Behavioral Intentions**.

4.3.1.4 The exploratory factor analysis of Ethical Behavior

Table 4. 14 The exploratory factor analysis of ethical Behavioral Intentions constructs.

Indicators	**Ethical Behavior**
CEB3: An organization experiencing a reduction in the number of events involving loss or compromise of information is an indicator of employee ethical behavior.	0.859
CEB4: An example of ethical behavior is when employees feel uncomfortable in disclosing security issues if they believe that other employees or the organization may disagree with them.	0.835
CEB5: In the absence of specific organizational guidance employees may deviate from information system security best practices.	0.834
CEB1: Employees follow organizational policies and rules when making decisions regarding Cyber security.	0.827
CEB2: Employees exhibit concern with the well-being of the organization by protecting organizational Cyber information and other Cyber assets	0.815
Eigen value	**3.477**
Variance (%)	**69.542**

KMO = .874, Bartlett's Test of Sphericity = 634.659, df = 10, sig. = .000

Extraction Method: Principal Component Analysis, components extracted.

The exploratory factor analysis of Ethical Behavior as shown in table 6, specifies that all the 5 indicators were retained in the measurement scale and all hard a high factor loading of above 0.5.

The EFA of ethical behavior created a Kaiser-Meyer-Olkin (KMO) for sample adequacy = .861 which is above 0.5. Hence the sample was appropriate for factor analysis (Field, 2009). Bartlett s test of sphericity of approximate chi-square = KMO, Bartlett's Test of Sphericity = 2880.125, df = 253, sig. = .000 was found to be significant, which indicates that the factors have significant relationships sufficient to measure ethical Behavior.

4.3.2 Confirmatory Factor Analysis (CFA)

CFA is a unique type of factor analysis that is beneficial in social science. It is used to determine whether measurements of a construct comply with the definition of that construct as understood by the researcher. CFA is the application of a multivariate modus operandi to validate a pre-specified association, according to Hair et al. (2010). CFA is a technique for evaluating how well measured variables represent fewer constructs. Contrary to exploratory factor analysis, which computes factor scores, CFA offers a variety of goodness-of-fit measures to evaluate the model. According to Hair et al. (2010), CFA is concerned with the strength of the regression lines from the Factor loadings and how much the observed variables are created by the underlying latent components.

4.3.2.1 Goodness of Fit

How well a model fits a set of observations is referred to as the "goodness of fit." To assess how well the employees' ethical behavior model regarding Cyber security reflective constructs fit the data gathered, a number of goodness of fit statistical tests were used.

The model used in this study underwent tests for parsimony, normality of the data set, and quality of fit. The outcomes are as follows:

To assess for overidentified models and models that do not fit the observable data, relative Chi-square X2/df was utilized. The range of a suitable fit value is 1.0 to 5.0. The absolute fit of a measurement model was measured using the RMSEA formula; acceptable fit values are less than 0.06 for good fit and between 0.06 and 0.08 for fair fit. The use of SRMR to evaluate absolute fit.

The mean absolute correlation residual, or the overall difference between the observed and anticipated correlations, is a measure of fit. Less than 0.05 is considered a good fit, with fit values up to 0.08 commonly accepted. Less than 0.05 is considered a good fit, with fit values up to 0.08 commonly accepted.

The study SEM models were chosen to use the Smart-PLS program because of its high relevance (Hair et al., 2010). The Smart-PLS software was used to conduct a confirmatory factor analysis model for each variable in this study, and the findings are provided in the following sections. CFA is carried out as a measurement modeling analysis. The measurement model's fundamental goal is to evaluate the validity and dependability of the indicators.

ReliabilityThe scale's internal homogeneity is measured, and the degree to which the items on it are representative of the measurement's domain is estimated. It is regarded as being the first explanation and measures the internal consistency of a group of things. The Composite Reliability statistic is used to measure it, and a threshold value of 0.6 is used.

Validity; is the extent to which an indicator that has been suggested to measure a particular concept actually does so. Convergent validity and discriminant validity are the two types of validity.

Convergent validity; refers to the degree to which two indicators of constructs that theoretically should be related, are in fact related.

Gerring, 2012 describe Convergent validity as the degree to which scores on a test relate with scores on other tests that are designed to assess the same construct. Convergent validity is assured by the Average Variance Explained value of over 0.5.

Convergent validity was evaluated using average variance extracted (AVE) to determine inter-item correlation. AVE was assessed for each reflective construct with 0.50 used as the acceptable fit value. correlation value of less than 0.2 or 0.3 indicates that the corresponding item does not

Discriminant validity;

It examines whether indications that aren't meant to be related are, in fact, unrelated (also known as divergent validity). This is determined by comparing the correlation coefficients between the square root of the AVE of one latent variable and those of other latent variables. In essence, all of

the correlation coefficients should be smaller than the square root of the AVE. The Fornel-Larcker criterion table summarizes these comparable statistics. In addition to evaluating the indicators' dependability and validity, the measurement model is also assessed for model fit. To do this, one looks at the Standardized Root Mean Square Residual (SRMR), which should be under the cutoff of 0.8.

4.3.2.2 CFA for Ethical virtues

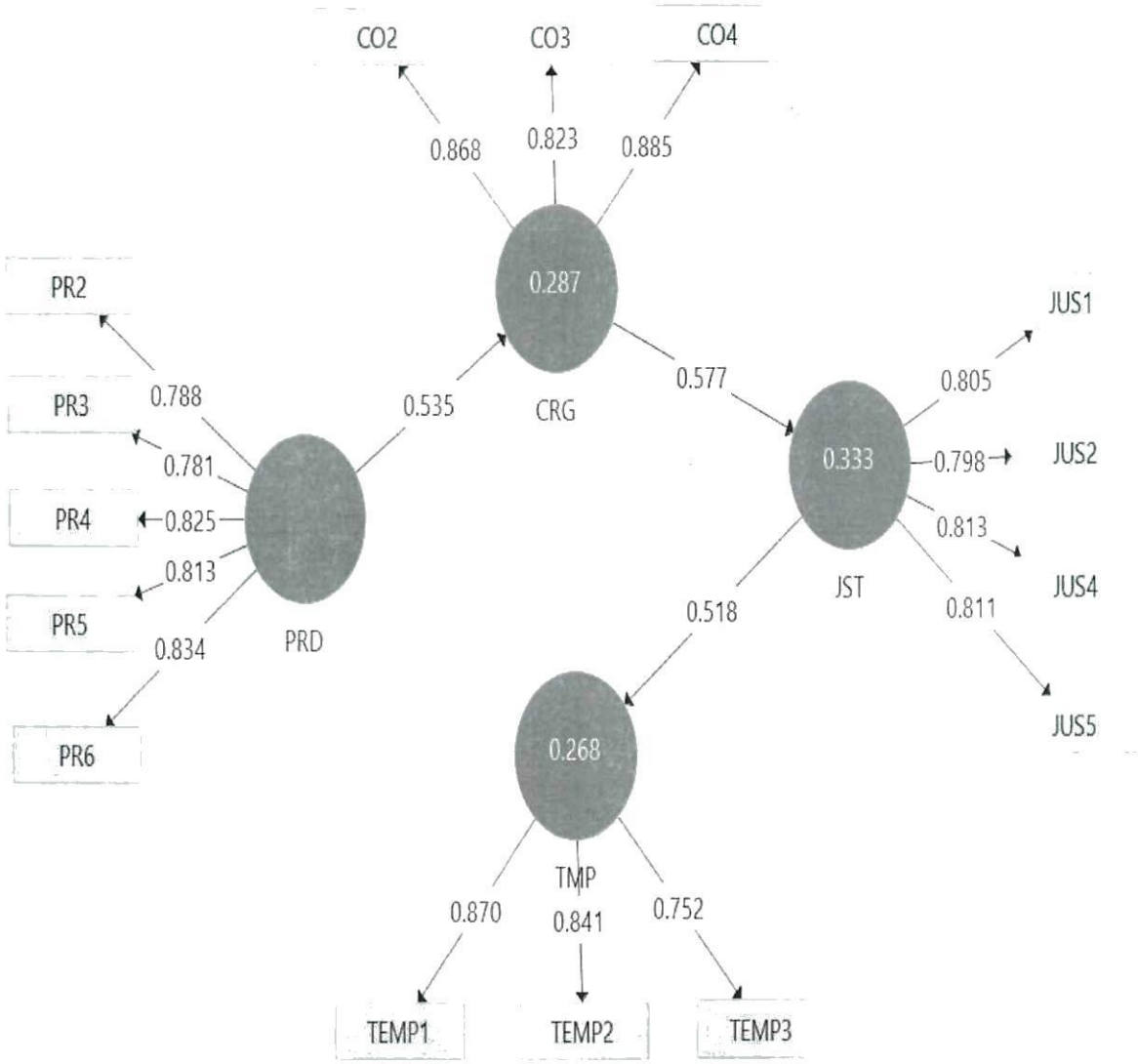


Figure 4. 1 Ethical virtues.

4.3.2.3 Indicator validity

Table 4. 15 Indicator validity.

Latent variable	Indicator	Sample Mean	Standard Deviation	T Statistics	P Values
Courage	CO2	0.869	0.019	45.089	0.000
	CO3	0.82	0.034	23.952	0.000
	CO4	0.884	0.015	59.407	0.000
Justice	JUS1	0.804	0.034	23.75	0.000
	JUS2	0.796	0.027	29.336	0.000
	JUS4	0.809	0.047	17.227	0.000
	JUS5	0.807	0.03	26.877	0.000
Prudence	PR2	0.789	0.029	27.065	0.000
	PR3	0.776	0.036	21.963	0.000
	PR4	0.821	0.029	28.606	0.000
	PR5	0.813	0.025	32.083	0.000
	PR6	0.832	0.029	28.856	0.000
Temperance	TEMP1	0.87	0.021	41.407	0.000
	TEMP2	0.839	0.027	31.668	0.000
	TEMP3	0.748	0.041	18.505	0.000

The table 4.15 above shows the factors that were retained after the deletion of some indicators of the ethical virtue constructs. These indicators were erased because they were insignificant, and or they had squared regression weights (L2) that were below 0.2. Moreover, on removing them, the measurement model fit improved. Thus presented here is the summary of the CFA in the measurement model of ethical virtues and clearly indicates that of all the indicators that were retained in the EFA, the following indicators were found to be significant; for Courage CO2 CO3, CO4, for Justice; JUS1, JUS2, JUS4, JUS5., for Prudence; PR2, PR3, PR4, PR5, PR6., for Temperance TEMP1, TEMP2, TEMP3. These indicators were then used in the computation of the scores for ethical virtues used in the estimation of the structural model.

Table 4. 16 Construct reliability and validity.

Latent variable	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Courage	0.823	0.839	0.894	0.738
Justice	0.821	0.822	0.882	0.651
Prudence	0.868	0.872	0.904	0.653
Temperance	0.764	0.799	0.862	0.677

Table 4. 17 Fornell-Larcker Criterion/Test for discriminant validity.

	Courage	Justice	Prudence	Temperance
Courage	**0.859**			
Justice	0.577	**0.807**		
Prudence	0.535	0.575	**0.808**	
Temperance	0.423	0.518	0.553	**0.823**

Note: Values in bold are the square roots of the AVEs for the reflective constructs

The results in table 4.16 show that the indictors retained in the summary of the measurement model of ethical virtues warranty both reliability and validity. The composite reliability statistics of over 0.60 implies that there is internal consistency. Furthermore, both convergent validity and discriminant validity were assured since the AVE for all factors is over 0.5 and the square root of the AVE for each construct is above the correlation coefficients with other factors.

The results in table 4.17 show that the indictors retained in the summary of the measurement model cardinal virtue constructs guarantee both reliability and validity. The composite reliability statistics of over 0.60 implies that there is internal consistency. Furthermore, both convergent validity and discriminant validity were assured since the AVE for all factors is over 0.5 and the square root of the AVE for each construct is above the correlation coefficients with other factors. The SRMR of 0.062 also indicates good model fit for the measurement model.

4.3.2.4 CFA for Ethical Climate

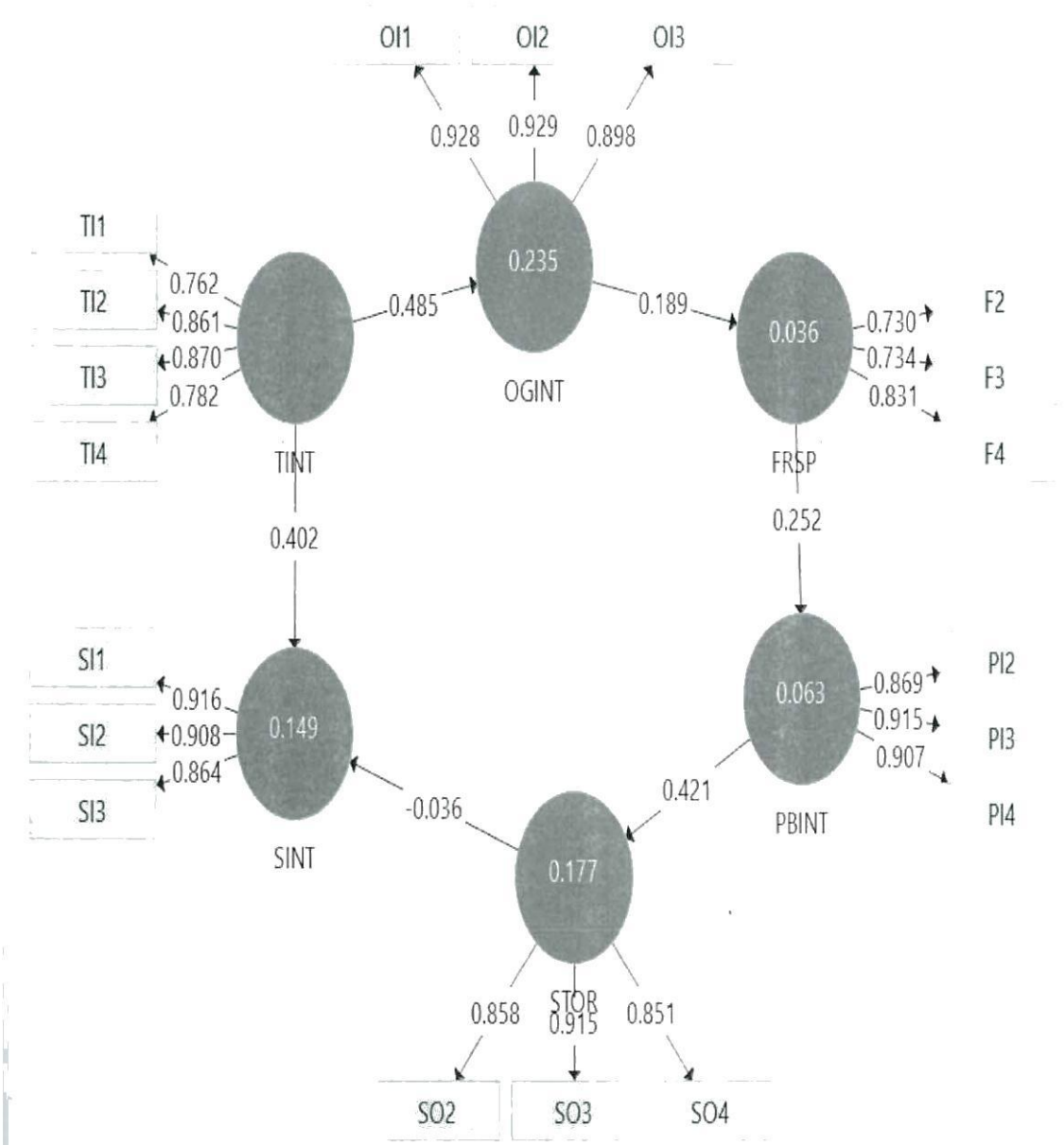


Figure 4. 2 Ethical Climate.

'able 4. 18 Indicator validity.

Latent variable	Indicator	Original Sample	Sample Mean	Standard Deviation	T Statistics	P Values
Friendship	F2	0.73	0.709	0.098	7.434	0.000
	F3	0.734	0.718	0.097	7.593	0.000
	F4	0.831	0.831	0.059	14.115	0.000
Organizational Interest	OI1	0.928	0.928	0.014	67.951	0.000
	OI2	0.929	0.929	0.01	89.424	0.000
	OI3	0.898	0.898	0.014	62.906	0.000
Public interest	PI2	0.869	0.864	0.035	25.076	0.000
	PI3	0.915	0.912	0.019	47.665	0.000
	PI4	0.907	0.908	0.016	58.445	0.000
Self interest	SI1	0.916	0.917	0.018	51.19	0.000
	SI2	0.908	0.907	0.019	48.942	0.000
	SI3	0.864	0.861	0.027	32.32	0.000
Stakeholder Orientation	SO2	0.858	0.858	0.024	35.616	0.000
	SO3	0.915	0.914	0.015	60.314	0.000
	SO4	0.851	0.849	0.029	29.817	0.000
Team Interest	TI1	0.762	0.758	0.048	15.95	0.000
	TI2	0.861	0.86	0.022	39.498	0.000
	TI3	0.87	0.872	0.018	48.699	0.000
	TI4	0.782	0.779	0.035	22.551	0.000

The table above shows the factors that were retained after the deletion of some indicators of the ethical climate constructs. The following indicators were found to be significant; Friendship; F2, F3, F4, for organizational interest; OI1, OI2,OI3, for Public interest; PI2, PI3, PI4 Self-interest; SI1, SI2, SI3, for Stakeholder Orientation, SO2, SO3, SO4, for Team Interest; TI1, TI2, TI4. These indicators were successively used in the working out of the scores for the variable of ethical climate and also applied in the estimation of the structural model.

Table 4. 19 Construct Reliability and validity.

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Friendship	0.661	0.7	0.81	0.588
Organizational Interest	0.908	0.921	0.942	0.844
Public Interest	0.883	0.941	0.925	0.805
Self Interest	0.878	0.889	0.924	0.803
Stakeholder Orientation	0.846	0.846	0.907	0.766
Team Interest	0.837	0.85	0.891	0.673

The results in table 4.20. show that the indictors retained in the summary of the measurement model of ethical climate warranty both reliability and validity. The composite reliability statistics of over 0.60 implies that there is internal consistency. Furthermore, both convergent validity and discriminant validity were assured since the AVE for all factors is over 0.5 and the square root of the AVE for each construct is above the correlation coefficients with other factors.

Considering the Composite Reliability (CR) values in table 4.20 of over 0.6 shows that the indicators retained in the CFA of ethical climate, it is evident that all items guarantee internal consistency reliability. Furthermore, both convergent validity and discriminant validity were assured since the AVE for both factors is o0.5 or over and the square root of the AVE for each construct is above the correlation coefficients with other factors. The SRMR of 0.06 also indicates good model fit for the measurement model.

Table 4. 20 Fornell-Larcker Criterion/Test for discriminant validity.

	Friendship	Organizational Interest	Public Interst	Self Interest	Stakeholder Orientation	Team Interest
Friendship	**0.767**					
Organizational Interest	0.189	**0.919**				
Public Interst	0.252	0.498	**0.897**			
Self Interest	0.494	0.169	0.281	**0.896**		
Stakeholder Orientation	0.206	0.304	0.421	0.161	**0.875**	
Team Interest	0.357	0.485	0.573	0.385	0.489	**0.82**

Note: Values in bold are the square roots of the AVEs for the reflective constructs

The results in table 4.21 show that the indictors retained in the summary of the measurement model of ethical climate guarantee both reliability and validity. The composite reliability statistics of over 0.60 implies that there is internal consistency. Furthermore, both convergent validity and discriminant validity were assured since the AVE for all factors is over 0.5 and the square root of the AVE for each construct is above the correlation coefficients with other factors. The SRMR of 0.062 also indicates good model fit for the measurement model.

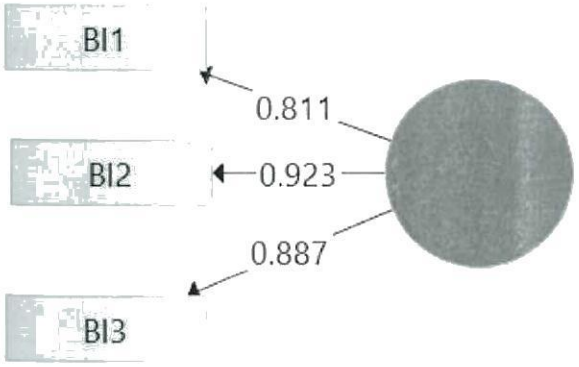


Figure 4. 3 Behavioral intentions and Actual Ethical Behavior.

Table 4. 21 Indicator validity.

Latent variable	Indicator	Original Sample	Sample Mean	Standard Deviation	T Statistics	P Values
Behavioral Intentions	BI1	0.811	0.808	0.033	24.79	0.000
	BI2	0.923	0.921	0.013	72.554	0.000
	BI3	0.887	0.885	0.019	46.886	0.000

The table above shows the elements considered of Behavioral intentions construct. The following indicators were found to be significant; BI1, BI2, BI3; These indicators were successively used in the working out of the scores for the variable of Behavioral intentions and also applied in the estimation of the structural model.

Table 4. 22 Construct Reliability and validity.

	Cronbach's Alpha	rho_A	Composite Reliability	Average Variance Extracted (AVE)
Friendship	0.661	0.7	0.81	0.588
Organizational Interest	0.908	0.921	0.942	0.844
Public Interst	0.883	0.941	0.925	0.805
Self Interest	0.878	0.889	0.924	0.803
Stakeholder Orientation	0.846	0.846	0.907	0.766
Team Interest	0.837	0.85	0.891	0.673

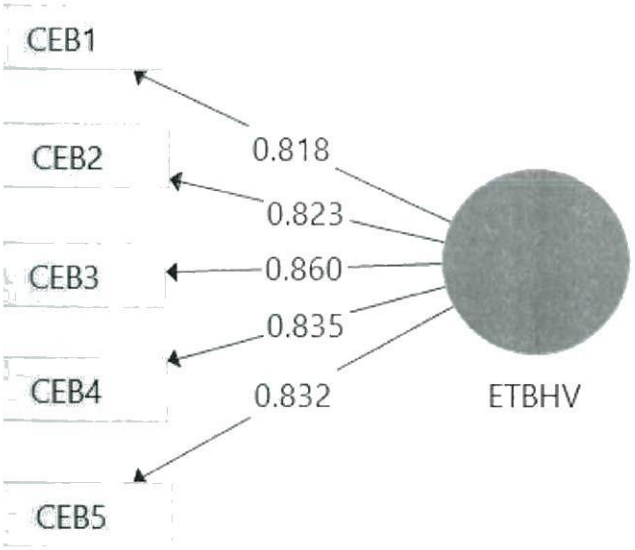


Figure 4. 4 Ethical Behaviour.

Table 4. 23 Indicator validity.

Latent variable	Indicator	Original Sample	Sample Mean	Standard Deviation	T Statistics	P Values
Ethical behavior	CEB1	0.818	0.815	0.026	30.927	0.000
	CEB2	0.823	0.821	0.025	33.48	0.000
	CEB3	0.86	0.858	0.02	43.399	0.000
	CEB4	0.835	0.834	0.028	30.12	0.000
	CEB5	0.832	0.832	0.019	44.024	0.000

The table above shows the elements considered of Cyber security ethical behavior construct. The following indicators were found to be significant; CEB1, CEB2, CEB3, CEB4, CEB5; These indicators were successively used in the working out of the scores for the variable of Cyber security ethical behavior construct and also applied in the estimation of the structural model.

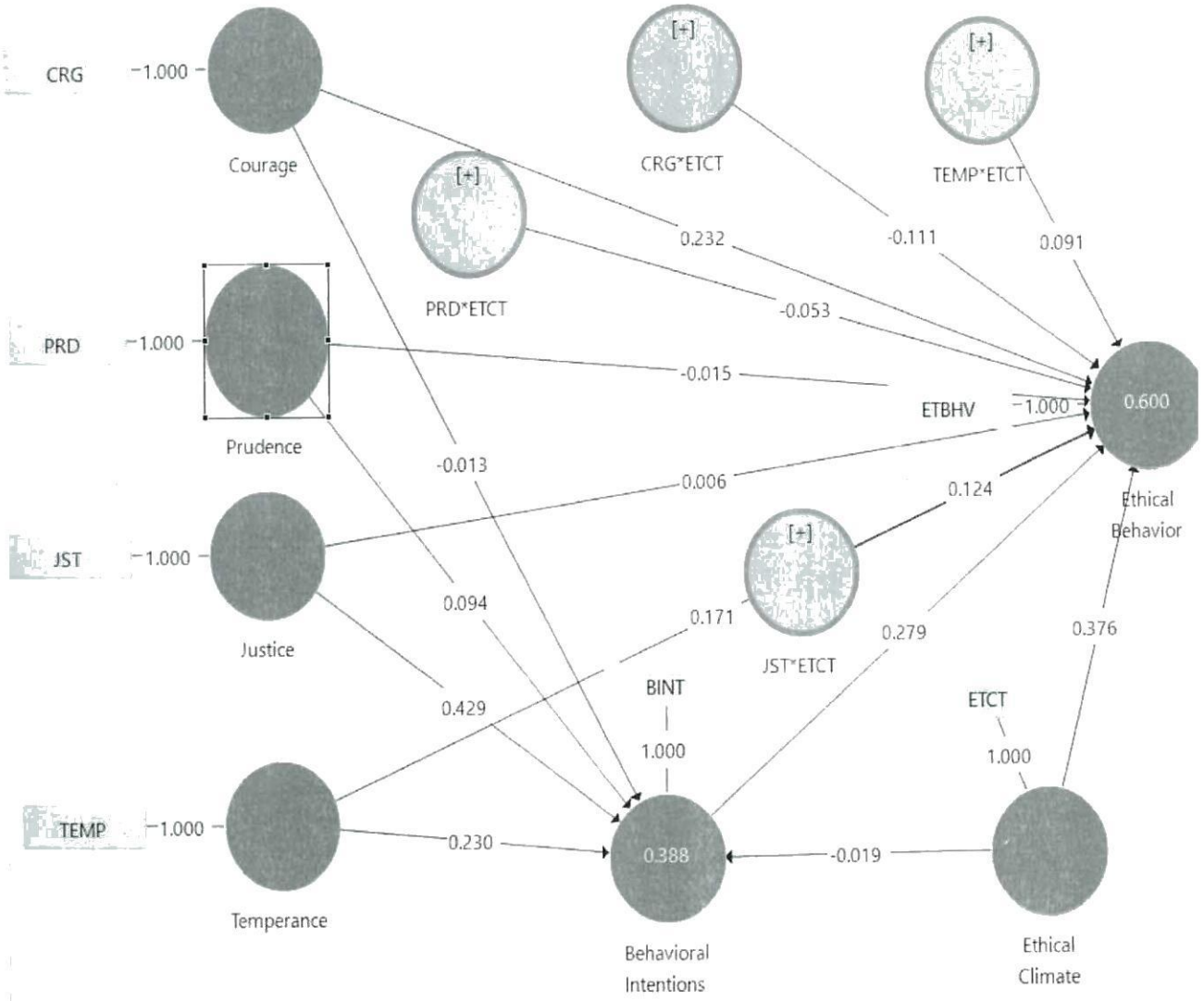


Figure 4. 5 The Original Structural Equation Model.

With prudence Beta= -0.015 P= -1.000 in this model it was knocked out because it was not significant in ethical behaviour.

Ethical climate did not moderate the virtue ethical constructs of courage, prudence, temperance, and justice.

4.3.3 Estimation of Total Effects: The Original Structural Equation Model

Table 4. 24 Estimation of Total Effects: The Original Structural Equation Model.

	Beta	Mean	SD	T Statistics	P Values	R Square
CRG -> BINT	-0.013	-0.012	0.076	0.167	0.868	
JST -> BINT	0.429	0.424	0.077	5.553	0.000	
PRD -> BINT	0.094	0.1	0.087	1.089	0.277	0.388
TEMP -> BINT	0.23	0.227	0.067	3.411	0.001	
ETCT -> BINT	-0.019	-0.021	0.087	0.22	0.826	
CRG*ETCT -> BINT	-0.111	-0.11	0.071	1.576	0.116	
CRG -> ETBHV	0.228	0.224	0.072	3.161	0.002	
ETCT -> ETBHV	0.371	0.376	0.078	4.738	0.000	
JST*ETCT -> BINT	0.124	0.117	0.053	2.342	0.020	
JST -> ETBHV	0.125	0.119	0.077	1.634	0.103	0.600
PRD*ETCT ->BINT	-0.053	-0.047	0.064	0.825	0.410	
PRD -> ETBHV	0.011	0.018	0.083	0.133	0.894	
TEMP*ETCT -> BINT	0.091	0.084	0.055	1.646	0.100	
TEMP -> ETBHV	0.236	0.241	0.054	4.335	0.000	
BINT -> ETBHV	0.279	0.275	0.08	3.48	0.001	

The structural model was estimated for predictive potential on the variables using the R Square values as seen in Table 4.24 above. The results show that Behavioral Intentions had a multiple squared correlation of .388. This implies that the joint effect of courage, Justice, Temperance, Prudence and ethical climate on behavior intentions was 39%. This further indicates that the variation in behavior intentions due to other factors apart from the variables in the model was 61.%. Ethical climate did not moderate the virtue ethical constructs of courage, prudence, temperance, and justice. Also ethical behaviour was found to have a multiple coefficient of determination of. 0.600 inferring that the variation in ethical behavior due to variations in courage, Justice, Temperance, Prudence and ethical climate on ethical behavior was 60%. Thus other variables not in the model predict 40% of ethical behaviour.

4.3.4 Estimation of mediation effect (Indirect Effects) for the Original Structural Equation Model

Table 4. 25 Estimation of mediation effect (Indirect Effects) for the Original Structural Equation Model.

	Beta	Mean	SD	T Statistics	P Values
CRG -> BINT -> ETBHV	-0.004	-0.002	0.023	0.157	0.875
ETCT -> BINT -> ETBHV	-0.005	-0.005	0.024	0.219	0.827
JST -> BINT -> ETBHV	0.12	0.117	0.041	2.907	0.004
PRD -> BINT -> ETBHV	0.026	0.027	0.026	1.004	0.316
TEMP -> BINT -> ETBHV	0.064	0.061	0.023	2.794	0.005

The path weights of the formative constructs of courage Beta = -0.004, P= 0.875 signify a negative influence on ethical behaviour intentions. Behaviour intentions did not mediate the effects of courage on ethical behaviour. Thus the effect was insignificant. Behavior intentions did not mediate the effect of Ethical Climate Beta=-0.005, P=0.827, thus there is a negative and insignificant mediation effect between behavior intentions and ethical behavior. Justice, Beta = 0.12, p = .004; Prudence Beta=0.026, P=0.316, Temperance, Beta = 0. 0.64, p = 0.005; did signify a positive influence on ethical behaviour intention.

4.4 Hypotheses Testing

A PLS model was fitted to the data to test the following seven hypotheses offered in this study.

H1. Increased Prudence positively influences employees 'cyber security ethical behavioral intention

Results in Table 4.24 reveal that there is an insignificant effect of prudence Beta 0.094. p = 0.277 on Behavioral Intentions. This means that a positive change in prudence leads to a negative change in the Behavior intention of organizational employees. However, there is no significant direct effect of prudence on ethical behavior towards Cyber security. Therefore, H1 was not supported by the data. Thus increased prudence has a negative influence on the behavioral intentions of organizational employees 'ethical behavior towards Cyber security

H2: Increased temperance positively influences employees 'cyber security ethical behavioral intention

Results in Table 4.24 reveal that there is a positive and significant influence of Temperance; Beta 0.255, p = .000; on Behavioral Intentions. This means that a positive change in Temperance leads to a positive change in the Behavior intention of organizational employees 'ethical behavior towards Cyber security. Therefore, H2 was supported by the data. Thus increased Temperance has a positive influence on the behavioral intentions of organizational employees 'ethical behavior towards Cyber security

H3: Increased courage positively influences employees 'cyber security ethical behavioral intention. When data was fitted to the PLS model to test the courage hypothesis it was disclosed that courage has an indirect influence on behavior intentions. The results disclose that there is a positive and significant influence of courage; Beta 0.247, p = .001; on ethical Behavior. This means that a positive change in courage leads to a positive change in the ethical behaviour and not through influence on Behavior intentions of organizational employees 'ethical behavior towards Cyber security. Therefore, H3 was not supported by the data. Thus increased courage has a negative influence on employees 'ethical behavior intentions towards Cyber security

H4: Increased Justice positively influences employees 'cyber security ethical behavioral intention

Results in Table 4.23 reveal that there is a positive and significant influence of Justice; Beta 0.452, p = .000; on Behavioral Intentions. This means that a positive change in justice leads to a positive change in the Behavior intentions of organizational employees 'ethical behavior towards Cyber security. Therefore, H4 was supported by the data.

H5: The presence of strong ethical climate moderates the influence of virtue ethics on employees' ethical behavior towards Cyber security.

4.4.1 Moderation test results; Modgraphs

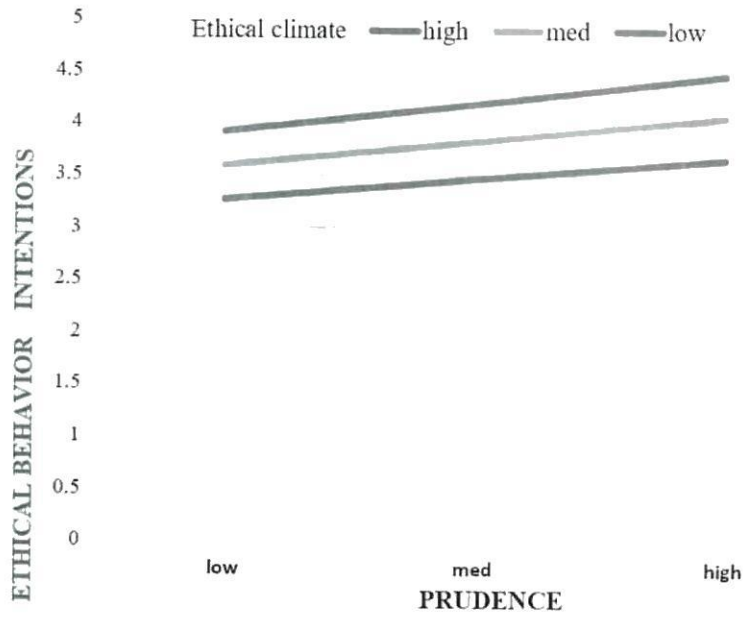
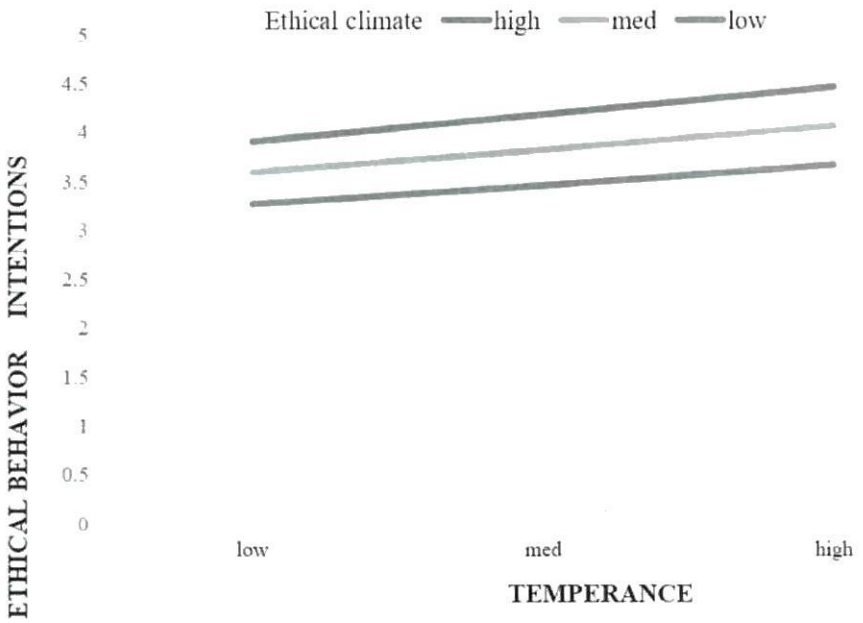


Figure 4. 6 Moderation Effect of ethical climate on cardinal virtue constructs and ethical behaviour.


Ethical climate
high
med
low
ETHICAL BEHAVIOR INTENTIONS
5
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
low
med
high
COURAGE


Ethical climate
high
med
low
ETHICAL BEHAVIOR INTENTIONS
5
4.5
4
3.5
3
2.5
2
1.5
1
0.5
0
low
med
high
JUSTICE



According to the modgraphs above, lines of the Mod graph for Prudence, courage, Justice, and temperance by ethical climate are parallel meaning that there is no moderation effect of ethical climate on the influence of the four cardinal virtues, (prudence, courage, temperance, justice), on employes'ethical behavior towards Cyber security.

Moderation test results

After the CFA, the study estimated the structural equation model. Some of the model estimations were the test for moderation of ethical climate on the effect of the four virtue constructs and the banking sector employee's ethical behavior intentions towards Cyber security in Uganda. The mod graph lines show that the slope for the regression lines for ethical behavior intention on cardinal virtues is lower at higher levels of ethical climate than at lower levels of ethical climate.

All the lines of the modgraphs are parallel meaning that the slope and the influence of cardinal virtues on ethical behavior intention towards Cyber security ethical behavior intention is the same at all levels of the ethical climate. Inferring that Ethical climate does not moderate the influence of cardinal virtues and ethical behavior intention towards Cyber security.

According to the modgraphs above, lines of the Mod graph for Prudence, courage, Justice, and temperance by ethical climate are parallel meaning that there is no moderation effect of ethical climate on the influence of the four cardinal virtues, (prudence, courage, temperance, justice), on employees' ethical behavior intentions towards Cyber security. The mod graph lines show that the slope for the regression lines for ethical behavior intentions on cardinal virtues is lower at higher levels of ethical climate than at lower levels of ethical climate. All the lines of the model graphs are parallel meaning that the slope and the influence of cardinal virtues on Cyber security ethical behavior intentions is the same at all levels of the ethical climate. Inferring that Ethical climate does not moderate the influence of cardinal virtues and Cyber security ethical behavior intentions.

H6; Cyber security ethical Behavior intention has a mediation effect on the influence of cardinal virtue ethics and Cyber security ethical behavior.

The results in table 4.24 reveal that there is a negative mediation effect of behaviour intentions on courage, Beta = -0.004 P= 0.875. It was unveiled that there is negative mediation effect of behaviour intentions on courage and that behaviour intentions does not mediate the effect of courage on organizational employees 'ethical behavior towards Cyber security. and prudence towards ethical Behavior.

It was disclosed that there is negative mediation effect of behaviour intentions on prudence, Beta = -0.026 P= 0.316 and that behaviour intentions does not mediate the effect of prudence on organizational employees 'ethical behavior towards Cyber security.

H6c. Behavior intention of organisational employees has a mediation effect on the influence of Justice Beta= 0.12, P= 0.004 and ethical behavior towards Cyber security. It was also disclosed that there is a positive mediation effect of behaviour intentions on justice and that a positive change in justice leads to a positive and significant change on Behavior intentions of organizational employees 'ethical behavior towards Cyber security. Thus H6c was supported by data. H6d Behavior intention of organisational employees has a mediation effect on the influence of Temperence and ethical behavior towards Cyber security was supported.

It was also unveiled that there is a positive mediation effect of behaviour intentions on temperance, Beta = 0.064 P = P= 0.005 and that a positive change in temperance leads to a positive and significant change on Behavior intentions of organizational employees 'ethical behavior towards Cyber security. Thus H6d was supported by data.

Behavior intention of organisational employees has a mediation effect on the influence of Justice and ethical behavior towards Cyber security. It was disclosed that there is a positive mediation effect of behaviour intentions on Justice and that a positive change in justice leads to a positive and significant change on Behavior intentions of organizational employees 'ethical behavior towards Cyber security. Thus H6c was supported by data.

It was also unveiled that there is a positive mediation effect of behaviour intentions on temperance. A positive change in temperance leads to a positive and significant change on Behavior intentions of organizational employees 'ethical behavior towards Cyber security.

Further still the results of this study according to table 4 26, indicate that there is a negative mediation effect of behaviour intentions on ethical climate, Beta = -0.005 P= 0.827, therefore a positive change in ethical climate leads to a negative and insignificant change on Behavior intentions of organizational employees 'ethical behavior towards Cyber security.

H7: organizational employees' ethical behavioral intention leads to improved ethical behavior towards Cyber security. The results from this research indicate that the influences of behaviour intentions on ethical behaviour were positive and significant, Beta = 0.257 p = 0.000. thus a positive change in behavior intentions leads to a positive change in ethical behavior towards Cyber security. Thus H7 was supported by the data.

4.5 Summary of Findings

A number of goodness of fit tests were done on the measurement model and the fit was evaluated as good, with the indices of $\chi 2$/df, RMSEA, SRMR, and CFI being acceptable. Convergent validity and discriminant validity were guaranteed since the AVE for all factors was over 0.5 and the square root of the AVE for each construct was above the correlation coefficients with other factors.

)iscriminant validity for the reflective constructs was evaluated by comparing AVE correlations etween latent variables and all were found to be acceptable. Formative construct discriminant alidity was evaluated using indicator path weights and loadings.

he indictors retained in the summary of the measurement model of ethical virtues warranted both :liability and validity. The composite reliability statistics of over 0.60 implied that there was ıternal consistency. Both convergent validity and discriminant validity were assured since the .VE for most factors was over 0.5 and the square root of the AVE for each construct was above ıe correlation coefficients with other factors. The SRMR of 0.072 which was below the cut-off f 0.8 also indicated good model fit for the measurement model.

he ethical climate indictors that were retained also warranted both reliability and validity. The ɔmposite reliability statistics of over 0.60 implies that there is internal consistency. Furthermore, ɔth convergent validity and discriminant validity were assured since the AVE for all factors is ver 0.5 and the square root of the AVE for each construct was above the correlation coefficients ith other factors.

ehavior intentions and ethical behavior indicators that were retained justified reliability and ılidity. All items guaranteed internal consistency reliability. Furthermore, both convergent ılidity and discriminant validity were assured since the AVE for both factors is 0.5 or over and e square root of the AVE for each construct is above the correlation coefficients with other ctors. The SRMR of 0.06 also indicates good model fit for the measurement model.

he evaluation of the structural model's validity and interactions indicated that the influence :tween the constructs of justice, Temperance, signify a positive influence on ethical behavior tentions, and the constructs and the path weight of courage had no significant effect on behavior tentions but positive and direct effect on Ethical Behavior.

n evaluation of the moderating effects discloses that ethical climate construct did not gnificantly moderate the effects of virtue constructs on behavior intentions. Its effect on courage, emperance, and Justice was insignificant. However, it had a direct influence on ethical behavior. rong ethical climate gave rise to a positive influence on Ethical Behavior. The influences of ehavior intentions on ethical behavior were strong and significant.

Table 4. 26 Hypothesis influence Results.

Hypothesis	*Link*	*Influence*	*P-Value*	*Result*
H1	PRD -> BINT	negative	0.277	Not significant
H2	CRG -> BINT	Negative	0.875	Not significant
H3	JST -> BINT	positive	0.000	significant
H4	TEMP -> BINT	positive	0.000	significant
H5	ETCT -> BINT	negative	0.087	Not significant
H5a	PRD*ETCT > BINT	Negative	0.410	Not significant
H5b	CRG*ETCT-> BINT	negative	0.116	Nott significant
H5c	JST*ETCT -> BINT	negative	0.020	insignificant
H5d	TEMP*ETCT -> BINT	negative	0.100	insignificant
H6a	PRD -> BINT -> ETBHV	positive	0.316,	significant
H6b	CRG -> BINT -> ETBHV	Negative	0.875	Not significant
H6c	JST -> BINT -> ETBHV	positive	p = .004	significant
H6d	TEMP -> BINT -> ETBHV	positive	0.005	significant

H6e	ETCT -> BINT -> ETBHV	Negative	P=0.827,	insignificant
H7	BINT -> ETBHV	positive	0.001	significant
	Courage -> Ethical Behavior	***positive***	***0.001***	***significant***
	Justice -> Ethical Behavior	***Positive***	***0.005***	***significant***
	Temperance -> Ethical Behavior	***Positive***	***0.001***	***significant***
	Ethical Climate -> Ethical Behavior	***Positive***	***0.000***	***significant***

CHAPTER FIVE: DISCUSSION OF FINDINGS

Introduction

This chapter presents the results obtained in Chapter Four. This research aimed at enhancing Cyber security by proposing a model and a means of addressing the employees' ethical behavior towards Cyber security. These results are accordingly discussed in relation to the research questions and hypotheses. The discussion further emphasizes the underlying theoretical and empirical explanations and justifications for the findings. The chapter also comes up with some Implications and recommendations to practice, plus the limitations of this study and finally proposes areas of future research.

5.1 Findings for objective 1

The hypothesized influences of the cardinal virtue ethical constructs were studied using p-values.

The study identified Justice, Courage, temperance and ethical climate as significant drivers of Cyber security ethical behavior in Ugandan commercial banks. Findings reveal that creating an ethical working climate improves Cyber security

H1. ***Increased Prudence has a positive influence on employees' cyber security ethical behavior intentions.***

This hypothesis was not supported by the data, which means that a positive change in prudence leads to a negative change in the Cyber security ethical Behavior intentions. This meant that the causal effect of Prudence on ethical behavior had no role in the model explaining Cyber security ethical behavior in the commercial banks in Uganda. This finding is not in agreement with literature which argued that Prudence is the aptitude to make a decision on the correct thing to do building on experience. Aristotle, (2005) contends that discovering this ethical element is not just an ability, but a kind of understanding, or a learning process. literature indicates that high prudence scores are associated with people who are reliable, are detail oriented, and follow organizational procedures, whereas low prudence scores are associated with behaving impulsively, irresponsibly, and carelessly (Hogan & Hogan, 1995). Aquinas continues to explain that the mental act of seeking good counsel needs that the prudent individual devotes time and verve ascertaining which act in a particular setting attains the best end. Aristotle vies that a prudent person recognizes and relates his decisions to righteousness.

H2: Increased Temperance has a positive influence on employees' cyber security ethical behavioral intentions. This hypothesis was supported. This finding is in agreement with literature Tangen, (2015), posits that Temperance is agreed as sound thinking, personified self-discipline and dynamic patience when dealing with other members that share the same ethical vision. Temperance enables individuals' honesty and defends their '*internal being* 'from turmoil and devastation. Temperance can enable employees to treat each other with deference and understanding and grip change and conflict with consideration. Temperance is the aptitude of individuals to uphold control and to desist from acting in excess on their security responsibilities, regulate their yearnings, activities, and conducts particularly in their security dealings, (Chatterjee *et al.,* 2015). This can have a big contribution in Cyber security practices adherence. Papouli, (2018) affirms that temperance consist of self-discipline such that an individual can evade doing things that are injurious to him and others. The banking sector workers' temperance may encourage moral behavior towards enhancing Cyber security. employees in the banking sector who implement Cyber security act falsely or pretend to be meek by abandoning themselves and their suitable desires, and also end up showing untrue humbleness are intemperate workers. Therefore, where temperance is present the employees' ethics are clearly impacted on by enhancing their moralities and competence and this can help to improve the banks' Cyber security.

H3: Increased courage has a positive influence on employees' cyber security ethical behavioral intentions. The findings revealed that courage had an indirect influence on behavior intentions. Instead courage has a positive and significant influence on ethical Behavior. This means that a positive change in courage leads to a positive change in the ethical behaviour and not through the influence on Behavior intentions. Therefore, H3 was not supported by the data. But results agreed with literature Aquinas, (2005) that courage is the will power of spirit, steadiness of will in undertaking moral acts regardless of impediments in carrying out of our day-to-day obligation. Banking sector employees should learn to respect true values and work hard to produce results for the good and welfare of others. Even if it means sacrificing their own safety and welfare. Volkman asserts that courage is a virtue of the respectable computer professional. Success requires real courage. Hawking, 2017 confer virtues as characters required to face the challenges of life. Thus, courageous employees are willing to embrace innovation and change which is not a characteristic of the coward especially when implementing Cyber security strategies.

H4: Increased Justice has a positive influence on the cyber security ethical behavioral intentions. H4 was supported by the data. This finding is in agreement with literature. According to Weber, (2015), each person has an unchallengeable dignity and is eligible to equal privileges; profound admiration for one other promotes justice; fair and equal access to information enables members of civil society to reach for mutual understanding.

According to Aquinas, (2005) justice considers relationships between others. The continuous willingness to provide to each individual what they rightly deserve; just or fair acts. Justice is restricted to the fair distribution of goods and services according to merit, virtue, or need. Thus justice is without doubt a motivational virtue.

According to Willison et al., (2018) the procedural injustice causes employees to engage in abusive behaviors. Employees become more upset when they perceive that a procedure is unfair than when they perceive an injustice in rewards and compensations. The moral method to making use of information systems is considering all stakeholders including colleagues, clienteles, and the administration. Cyber security professionals should also take morally fair rulings and decisions concerning Cyber security and safety policies.

H5: *The presence of strong ethical climate moderates the influence of cardinal virtues on employees' cyber security ethical behavior intention.*

H5 was not supported by data, all the 4 cardinal virtues of Prudence, courage, justice and temperance were not moderated by ethical climate. This implies that a virtuous employee should come with a strong character and personality, caring, good listener, should have positive values, a team player, and constantly guiding and mentoring others on the team. An ethical employee should be ready to endure when dealing with office politics and be ready to swim with the current in the technological implementation of Cyber security.

The findings further uncovered that Ethical climates have a direct effect on cyber security ethical behaviour. This finding is consistent with some previous research for instance, in a systematic literature review carried out by Ali et al, (2021) it was maintained that workplace-related factors also affect security behavior. VanSandt et al., (2006) established that there is relationship between ethical climate and moral awareness.

Shafer, (2008) found that those high in relativism were significantly influenced by the ethical climate in terms of reduced intentions to commit unethical acts. Thus the moderation hypothesis Ethical Climate on the link between cardinal virtues and ethical behavior intentions emphasized the value of ethical climate in improving Cyber security. Evidence from this study suggests that organizations should develop strong EC in order to achieve improved cyber security.

H6 Behavior intentions has a positive mediation effect on the influence of cardinal virtue ethics and ethical behavior towards Cyber security.

This hypothesis had 4 components and 2 of them were supported. Thus it was patially supported.

H7: organizational employees' ethical behavioral intentions lead to improved Cyber security ethical behavior. This hypothesis was supported by data. This finding is consistent with other schoolars, for instance the Theory of Planned Behavior Ajzen, 1991 asserts that actual behavior is most associated with the intention to carry out that behavior. Understanding the behavior of banks employees is important. Several studies suggest that while systems are increasingly well protected, human behavior is the most vulnerable link in an information security system (Ameen *et al*, 2020). Whereas ethical intentions refer to how individuals intend to deal with ethical issues they face, ethical behavior refers to whether individuals are acting in ways consistent with what others in society believe is morally appropriate.

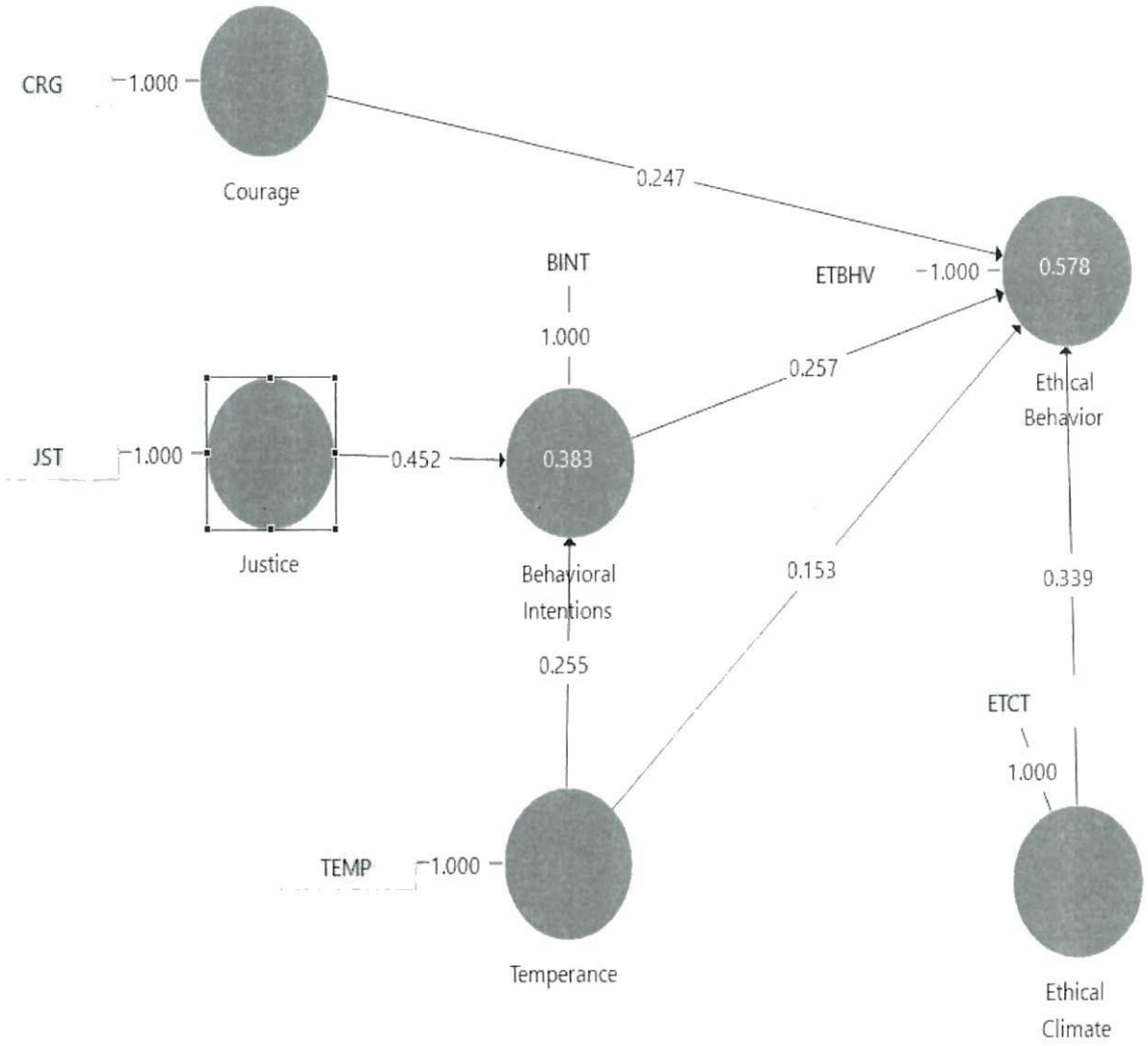


Figure 5. 1 Final model.

The path weights of the formative constructs of justice, Beta = 0.452, p = .000; Temperance, Beta = 0.255, p = 0.000; did signify a positive influence on ethical behavior intentions. And the path weight of courage, Beta =. 0.247, p = 0.001; indicates a direct significant influence on ethical behaviour. The ethical climate construct Beta 0.339; p = 0.000 did not significantly moderate the effects of behaviour intentions Beta = 0.257 p = 0.000 it instead had a direct influence on ethical behaviour. Strong ethical climate gave rise to a positive influence on Ethical Behavior. The influences of behaviour intentions on ethical behaviour were significant, Beta = 0.257 p = 0.000.

The path weights of the formative constructs of justice, Beta = 0.452, p = .000; Temperance, Beta = 0.255, p = 0.000; did signify a positive influence on ethical behaviour intentions. And the path weitht of courage, Beta =. 0.247, p = 0.001; indicates a direct significant influence on ethical behaviour. The ethical climate construct Beta 0.339; p = 0.000 did not significantly moderate the effects of behaviour intentions Beta = 0.257 p = 0.000 it instead had a direct influence on ethical behaviour. Strong ethical climate gave rise to a positive influence on Ethical Behavior. The influences of behaviour intentions on ethical behaviour were significant, Beta = 0.257 p = 0.000

Table 5. 1 Estimation results for the Structural Equation Model for Ethical Behavior.

	Beta	Mean	SD	T Value	P Value	R Square
Justice -> Behavioral Intentions	0.452	0.451	0.069	6.596	0.000	
Temperance -> Behavioral Intentions	0.255	0.256	0.061	4.183	0.000	0.383
Behavioral Intentions -> Ethical Behavior	0.257	0.26	0.072	3.559	0.000	
Courage -> Ethical Behavior	0.247	0.235	0.074	3.319	0.001	
Ethical Climate -> Ethical Behavior	0.339	0.342	0.055	6.207	0.000	0.578
Justice -> Ethical Behavior	0.116	0.118	0.041	2.828	0.005	
Temperance -> Ethical Behavior	0.218	0.226	0.065	3.362	0.001	

Table 5. 2 Estimation results for the regression of factors on ethical behavior.

	Beta	Mean	SD	T Statistics	P Values
Behavioral Intentions -> Ethical Behavior	0.257	0.26	0.072	3.559	0.000
Courage -> Ethical Behavior	0.247	0.235	0.074	3.319	0.001
Ethical Climate -> Ethical Behavior	0.339	0.342	0.055	6.207	0.000
Justice -> Behavioral Intentions	0.452	0.451	0.069	6.596	0.000
Justice -> Ethical Behavior	0.116	0.118	0.041	2.828	0.005
Temperance -> Behavioral Intentions	0.255	0.256	0.061	4.183	0.000
Temperance -> Ethical Behavior	0.218	0.226	0.065	3.362	0.001

Predictive power of the model

The structural model was estimated for predictive potential on the variables using the R Square values as seen in Table 4.23 above. The results show that Behavioral Intentions had a multiple squared correlation of .383. This implies that the joint effect of Justice and Temperance on behavior intentions was 38.3%. This further indicates that the variation in behavior intentions due to other factors apart from the variables in the model was 61.7%. Similarly, ethical behaviour was found to have a multiple coefficient of determination of. 0.578 inferring that the variation in ethical behavior due to variations in courage, temperance and justice on ethical behavior was 57.8%. Thus other variables not in the model predict 42.2% of ethical behaviour.

5.2 Estimation of mediation relationships (Indirect Effects) for the final Structural Equation Model

Table 5. 3 Estimation of mediation relationships (Indirect Effects) for the final Structural Equation Model.

	Beta	Mean	SD	T Statistics
Justice -> Behavioral Intentions -> Ethical Behavior	0.116	0.118	0.041	2.828
Temperance -> Behavioral Intentions -> Ethical Behavior	0.066	0.066	0.022	3.024

Table 5. 4 Model fit for Final Structural Model for Ethical Behavior.

	Saturated Model	Estimated Model
SRMR	0.04	0.072
d_ULS	0.492	0.599
d_G	0.265	0.385
Chi-Square	842.395	949.686
NFI	0.981	0.972

*SRMR = .072

The model fit statistics and indices for the hypothesized model summarized in figure 4.4 above how that the model fitted the data well. This is so because fit statistics and indices were found to e in commendable ranges. The SRMR of 0.072 also indicates good model fit for the measurement iodel.

5.3 Discussion for objective 2

To develop a model for guiding the design of a web based application that analyses Employees' character traits which may influence Cyber security ethical behavior.

In this thesis, the concept of the ECEBA model for assessing the banks employees' ethical behavior towards cyber security is presented. The model is composed of six modules responsible for the functionality of the developed application. These include; i. Application module: (front-end) accessible via web browser for user interaction. ii. Network connection: for connectivity of the developed app to function, iii. Data storage: a web server with cloud database & MySQL database management system, iv. Question engine: Generation and Storage of questions, v. Scoring Engine: Marking and computing of Scores, vi. Data analytic module: for analysis & report generation.

Requirements for the ECEBA model

- Provision of data storage, access & retrieval about cyber security ethical situations and decisions
- Map these elements to mitigate unethical behavior towards Cyber security
- The ECEBA model should serve as a web-based tool that supports banks in assessing their current and potential employees' cyber security ethical behavior

The ECEBA model introduces a new perspective on how web based assessments can be developed to assess the employees' ethical behavior thus offering an opportunity for employees' self-assessments to ensure improvement in cyber security ethical behavior in the banks.

In this thesis, a web based application called Ethica was developed based on the modules of the ECEBA model to test its validity and reliability and to enhance the cyber security ethical behavior in Ugandan commercial banks. Thakur et al., (2016) state that running anti-virus software, installing software updates, preventing identity theft, turning on personal firewalls, avoiding adware/spyware, protecting passwords, using spam filtering techniques, and backing up important files are all important cyber-safety measures to take. In a review by Veksler et al., (2018), technical solutions to cyber-security are crucial for a successful security endeavor. Utilizing access control methods, using encryption for communication, and using monitoring and auditing models are all effective countermeasures. However, Siponen et al., (2010) state that policies alone are not a deterrent against internal threats.

The Eceba Model was developed which guided the design of Ethica Application, a web based application that analyses Employees' character traits which may influence Cyber security ethical behavior. The app. Encourages the commercial banks to carry out continuous assessment of Banks 'employees & potential new hires Ethical behavior towards Cyber security.

After assessment

- Continuous ethical behavior assessment encourages bank employees to make ethical decisions
- Commercial banks can organize efforts to comprehend, encourage, and support the moral values and behavioral objectives of employees with those of the banks.
- Banks can also tailor Cyber security ethical based awareness, and training programs to meet employees' cyber security ethical behavioral needs.
- Continuous assessments also help the recruitment panel to know that the person is a good fit for the bank into Cyber security related positions

Hiring and keeping more moral people leads to a more moral workplace atmosphere. Which may lead to cyber security incident reduction.

5.4 Discussion for objective 3

ECEBA model was tested using the ETHICA App. The units were independently tested, then tested as a whole Application.

Deployed via the web to allow employees of ABSA to test its usability. During usability testing, feedback was analyzed to demonstrate that the solution fulfils its intended purpose.

This system was tested to confirm its accuracy and see if it completely fulfils the requirements. Separate components of the employees' Cyber security ethical behavior assessment model were individually tested, before testing the whole system. There after the model was set up via the web to allow employees of Absa and centenary banks test its usability. This was done with the help and consultation with bank branch managers who helped identify departments and staff who could participate in the testing.

5.5 Conclusions

In order to determine the possible required changes to improve Cyber security in the banking industry, it's essential to study the factors that affect ethical behavior.

The hypotheses that were not significant in this research findings are not excluded completely but they have to be subjected to refinement and further study together with the whole model. The current conclusion by this scholar is that it is a good model and most components are significant. Three out of the four cardinal virtues made an impact on ethical behavior, but the effects are not moderated by ethical climate.

The current research outcomes provide understanding of virtue elements and their influences on the employees' cyber security ethical behavior in the commercial in Uganda.

This research aimed at enhancing Cyber security by proposing and developing a model and a means of addressing the employees' ethical behavior towards Cyber security. The research also analyzed the moderation effect of ethical climate on the influence of cardinal virtues on behavior intentions of employees' Cyber security. The study further developed a model which banks can use to generate ethical Cyber security behavior assessments for their employees.

H1 stating that Increased Prudence has a positive influence on the behavioral intention of organizational employees' ethical behavior towards Cyber security was not supported as it was not significant and there was no significant direct effect of prudence on ethical behavior towards Cyber security. H2: Increased temperance has a positive influence on the behavioral intention of organizational employees 'ethical behavior towards Cyber security was supported because it was significant. H3: Increased courage has a positive influence on the behavioral intention of organizational employees 'ethical behavior towards Cyber security was not supported at 0.875 level. H4: Increased justice has a positive influence on the behavioral intention of organizational employees' ethical behavior towards Cyber security was supported.

H5. The presence of strong ethical climate moderates the influence of virtue ethics on behavior intentions of organizational employees' Cyber security ethical behavior was not supported.

H6. Behaviour intention has a positive mediation effect on the influence of prudence on organizational employees' ethical behavior towards Cyber security was not supported.

Behaviour intentions has a positive mediation effect on the influence of courage on organizational employees' ethical behavior towards Cyber security was not supported. Behaviour intention has a positive mediation effect on the influence of Justice on organizational employees' ethical

behavior towards Cyber security was supported. Behaviour intention has a positive mediation effect on the influence of Temperance on organizational employees' ethical behavior towards Cyber security was supported as it was significant. Behaviour intention has a positive mediation effect on the influence of Justice on organizational employees' ethical behavior towards Cyber security was supported as it was significant.

Behavior intentions did not mediate the effect of Ethical climate thus there is a negative and insignificant mediation effect between behavior intentions and ethical climate.
Hypothesized relationships of the Cyber security ethical behavior model were studied based on *p*-values.
H7: organizational employees' ethical behavioral intention leads to improved ethical behavior towards Cyber security. H7 was supported by the data and was significant.

H7. The influences of behaviour intentions on ethical behaviour were significant. This lead to the conclusion that ethical behavior towards Cyber security in the banking sector is mediated by behavior intentions.

CHAPTER SIX: DEVELOPMENT OF THE MODEL

Introduction

This chapter explicates the tasks and activities that were instrumental to the development and implementation of an employees' Cyber security ethical behavior assessment model in commercial banks in Uganda. This chapter covers objectives three and four.

Objective two: To develop an Employees' Cyber Security Ethical Behavior Assessment Model for Ugandan Commercial Banks (ECEBA).

The chapter explains the different requirements that were used in the development of the system. Software and hardware models used together with the different sketches/images of the developed system and their description are also clarified.

Safa et al., (2016) posit that technology measures alone cannot guarantee protection to critical information and Cyber security and other assets in the Cyber space. Therefore, this research provides practitioners with alternatives to technical controls, checklists, and formal procedures; which are known to have been ineffective against human being who are recognized as the weakest link to Cyber security. Virtue ethical theory, Ethical climate theory and the theory of planned behavior provided the construct questions to be assessed using the web based model.

The virtue theory, the ethical climate theory, and the theory of planned behavior provided the constructs that the model assesses. Harrison, (2014), contends that Virtues are moral excellence. Virtues are inherently good and they guide conduct and are the foundations of good character. Individuals should actively choose to show their virtues because it's helpful to them and the entire community in which they are living. Ethical behavior starts with employees and the ethical climate theory proves to be a suitable basis to explore Cyber security ethical behaviors and compliance. Brennan and Richardson, (2017); Pham et al., (2017) contends that the TPB is one of the most powerful models for studying human behavior since it explains behavioral antecedents.

6.1 Description of the ECEBA model

The model was used as an experimentation instrument for the development of a web-based application for assessing cyber security ethical behavior in Ugandan commercial banks.

The model was designed using the Unified Modelling Language (UML). UML is a standardized modeling language made up of an integrated set of diagrams for assisting software developers in specifying, visualizing, constructing, and documenting the artifacts of software systems (Tumuhimbise et al., 2022). UML uses notations to explicitly represent the variation points in the structure of the model thus allowing partial automation of the development and implementation. To avoid re-inventing the wheel, The ECEBA model followed the reuse concept by customizing the 3-tier architecture of the web application development. Three-tier architecture is a well-established software application architecture that organizes applications into three logical and physical computing tiers: the presentation tier, or user interface; the application tier, where data is processed; and the data tier, where the data associated with the application is stored. The web-based model focusing on specific modules tailored for assessing banks' employees' cyber security ethical behavior was designed and developed. The web-based customization was done by the researcher by aligning modules specific to this research.

Based on the results and the correlations from the study variables the researcher developed a model called an Employee Cyber security ethical behavior assessment model that might enable a bank to assess its employees' Cyber security ethical behavior intention. The Cyber security ethical behavior questions covering the cardinal virtues and ethical climate, are created by the system administrator. These are then stored in a database.

Part one covers demographic data and professional characteristics of employees. Section two fences the cardinal virtue questions and surveyed the extent to which cardinal virtues can influence the employees' Cybersecurity ethical behavior intention in the commercial banks in Uganda. This section considers the cardinal virtue constructs of; Prudence, courage, justice, and temperance that should be possessed by the banks' employees. Cyber security ethical behavioral intentions, actual ethical behavior and the Ethical Climate are also examined.

The model recommends that banks should give employees opportunity to assess themselves by responding to questions that help them improve ethical behavior and ensure employees are motivated by appreciating their opinions towards Cyber security ethics.

6.1.1 Requirements for the ECEBA model

Following the results from objective1 and correlation from study variables an Eceba model was proposed and the following are its requirements.

- Provision of data storage, access & retrieval about cyber security ethical situations and decisions.
- Map these elements to mitigate unethical behavior towards Cyber security
- The ECEBA model should serve as a web-based tool that supports banks in assessing their current and potential employees' cyber security ethical behavior
- Provide a mechanism of transferring and sharing knowledge about Cyber security ethical behavior within the bank.

6.1.2. The ECEBA Modules (Architecture)

- Application module: (front-end) accessible via web browser for user interaction (backbone 4 all other modules
- Network connection: for connectivity of the developed app to function
- Data storage: a web server with cloud database & MySQL database management system
- Question engine: Generation and Storage of questions, Assessments
- Scoring Engine: Marking and computing of Scores
- Data analytic module: for analysis & report generation

6.2 The ECEBA Model Architecture

The Application layer module

This module offers a platform that enables Ethica web-based application to perform with ease on the web platform. This layer, also called Business Logic or Domain Logic or Application Layer, accepts user requests from the browser, processes them, and determines the routes through which the data will be accessed. The workflows by which the data and requests travel through the back end are encoded in a business layer. Using the web browser, the module enables users to view, interact with, and access web content. It sends an HTTP request to the web server and displays the results for the user. The module offers an interface where employees enter their details and access the assessment Details. It also enables the application manager to edit the assessments. This module offers a backbone for the connection of all other modules of the ECEBA model.

Network connection module

This module is responsible for ensuring the connectivity of the developed application to ensure that it functions. The Ethica web-based app is an internet-based application which requires the internet to function, thus the network module ensures that the application connects to the internet to run efficiently.

Storage Module

This module offers storage and access to the patients' data. The module enhances the connection of the app and is responsible for ensuring that data is accessed and retrieved. Data is stored on the **Web Server:** This is a back-end component that receives requests from the client side and processes them using business logic. It retrieves data from the database and transfers it to the web browser for display. The module is responsible for the local and cloud database management and a central repository for ensuring that all data regarding employee's assessments are stored.

ECEBA Analytics Back-end

Question engine, Scoring Engine, and Data analytic module are in the application back end. **Question engine:** Questions are generated from normal text data input into an html form in the application. When employees are logged in, they can only view their respective profiles and attempt the assessments available. There are three sections of assessments; **Section 1;** Background Information that includes Demographic data and professional characteristics of employees. Section Two: Cardinal Virtue Constructs that assesses list of items related to Cyber security i. virtue of courage, which is defined as; Personal honesty and determination to make ethically correct or unpopular decisions regarding Cyber security that affect decisions concerning adherence ii. list of items associated to the virtue of **Temperance** that is explained as; individual modesty, self-control, and the ability to regulate sentiments and actions that affect decisions regarding Cybersecurity. iii. items connected to **justice** which is defined as; Being sensitive to the rights of others and acting fairly and responsibly towards individuals, organizations, and communities.

Behavioral intentions towards Cyber security; (defined as the desire and likelihood of the individual to perform Cyber security ethical behavior), Ethical Behavior towards Cybersecurity and Ethical Climate Questionnaire.

Scoring Engine does the marking and computing of scores. When an employee logs into the App. She/he can continue to answer the questions by selecting and responding to the answer options and ticking the most appropriate option. The system analyses the answer provided by the user and marks them depending on whether they tally with preset options stored in the database. Scores are calculated by a script in the 'Assessments Controller'. This script computes all total questions attempted, and answered in a Likert scale, correctly answered questions, missed questions, time taken to complete assessment.

Marking and Scoring

depending on the department of the specific employee, questions are pulled from the database and supplied to his UI. The employee is given the opportunity to respond to each question by choosing what he believes to be the appropriate response. Depending on whether the user's response is correct or incorrect after analysis by the system they add up to a specified, database-stored accurate response. A script in the "Assessments Controller" determines the user's scores. script calculates the total number of questions attempted, the proportion of questions that were answered correctly, incorrectly, and in the allotted time for the assessment.

Reporting

For reporting and analytical visualizations, the generated data is then attached to JavaScript charts and graphs. These are then read by the different policy makers for further recommendations including cyber security ethical trainings.

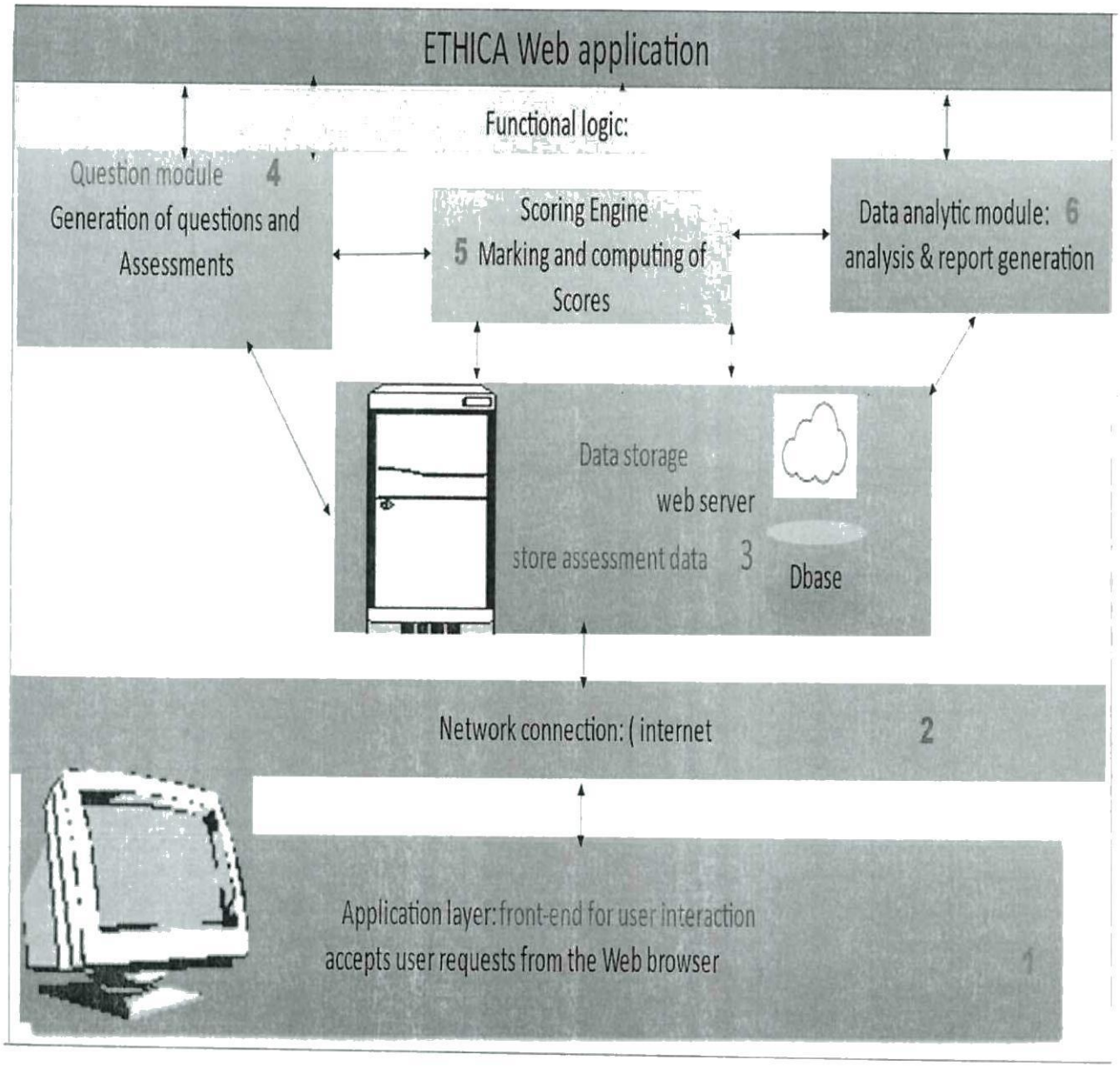


Figure 6. 1 The ECEBA model architecture.

6.3 ECEBA Model design tools

6.3.1The ECEBA Use Case Diagram

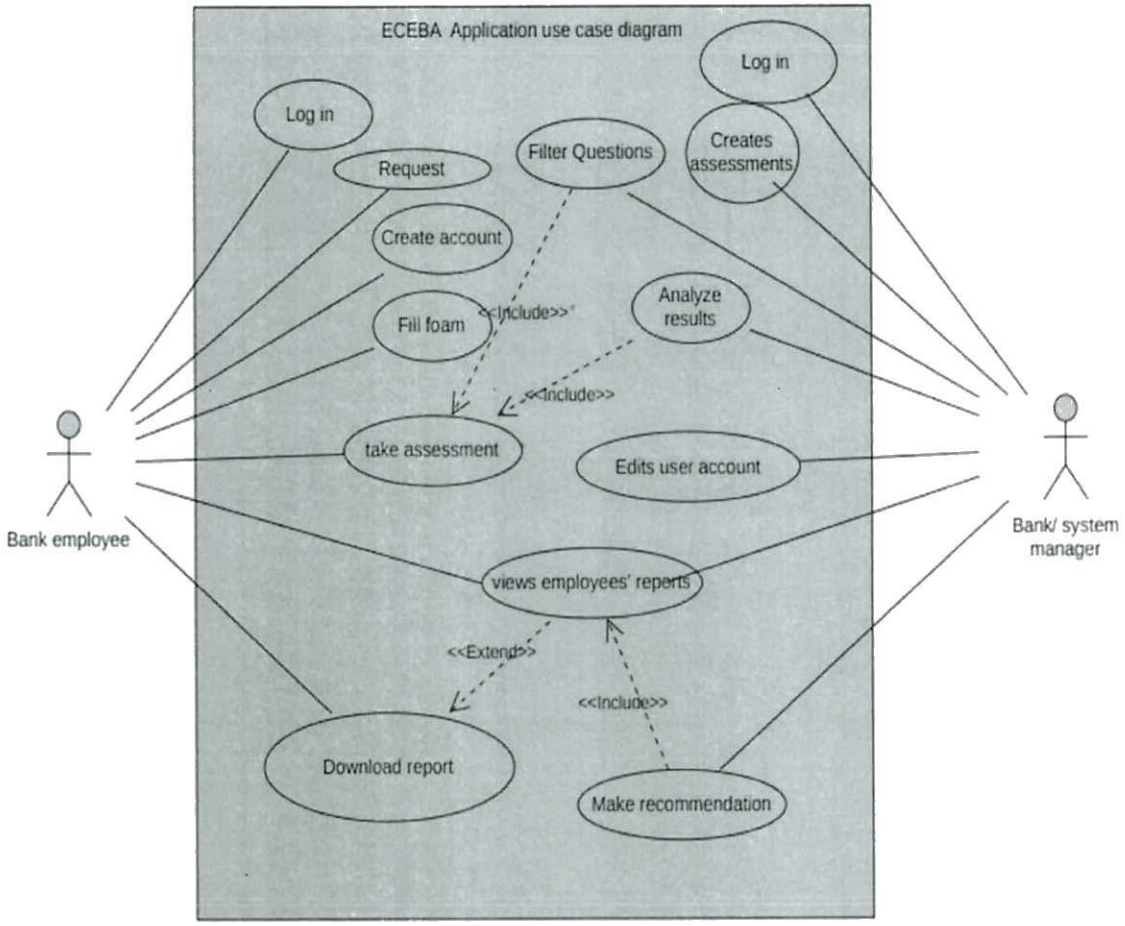


Figure 6. 2 The ECEBA Use Case Diagram.

The Use Case diagram illustrates the major interactions that take place between the various subsystems and actors in the developed Eceba model.

Eceba Model reaction to the Use Case

Eceba model is built on a 3 tier web architecture to provide an ethical behavior assessment ground that brings together technical employees in the bank to effectively manage cyber security ethical behavior in Ugandan commercial banks.

Existing and potential new employees are continuously assessed to identify any misconduct in decision making especially when they are presented with cyber security ethical dilemmas.

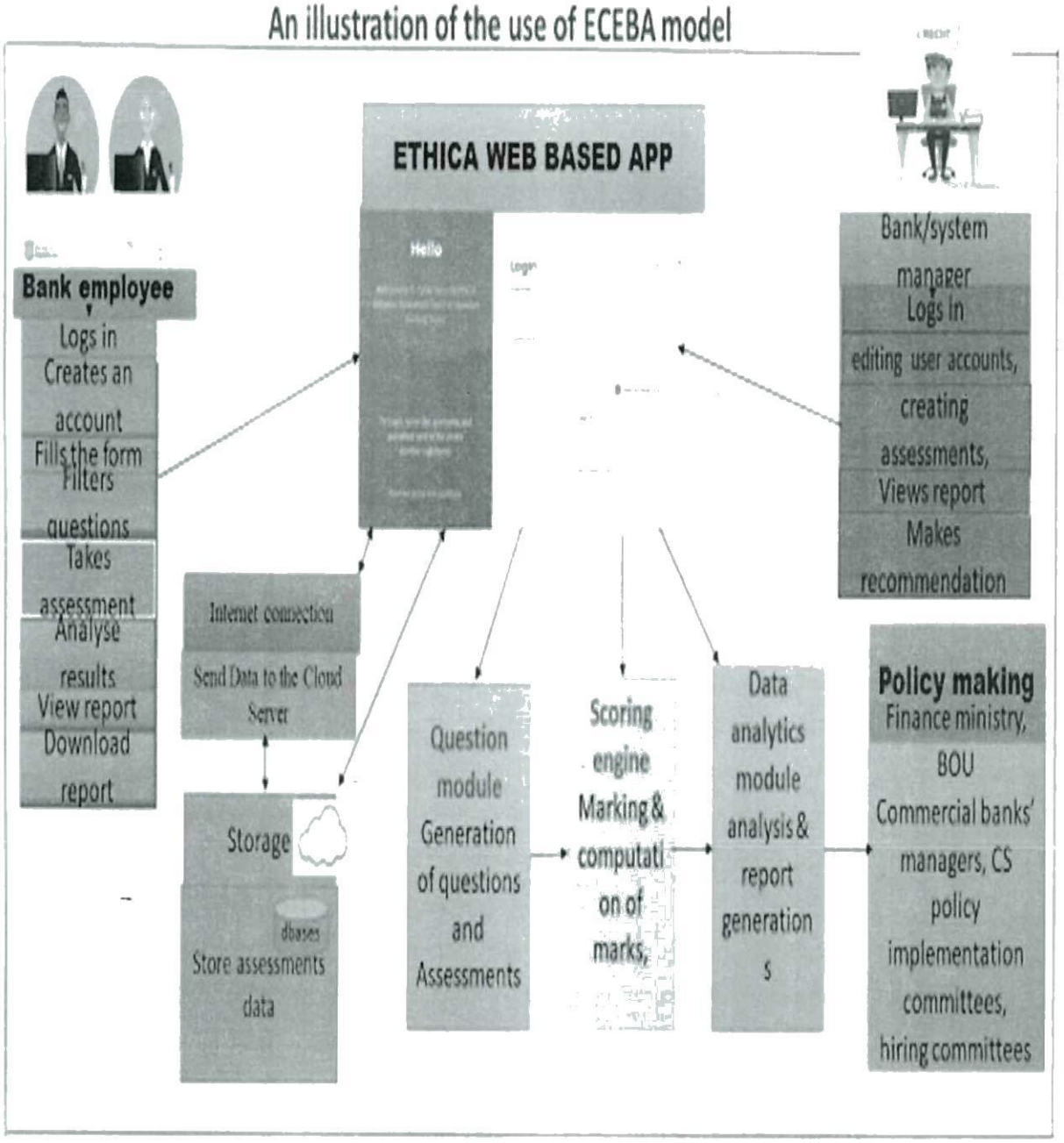


Figure 6. 3 illustrates how Eceba model is used during employees' cyber security ethical behavior assessment.

a. The Ethica App has an administrator, who is responsible for configuring and managing the developed Web based Application. He/she is answerable for administration, management, and support activities associated with the system.

b. The system administrator further drafts and issues system terms and conditions, views registered users in the system, notices registered banks in the system,

c. observes and updates the assessment questions these include; (constructs of Justice, courage, Temperance, ethical climate, ethical behavior intentions and ethical behavior elements). From the results of this research objective one

d. the administrator is entitled to freezing/ blocking accounts for banks and users in case they fail to abide by the system rules and regulation or using the system for a different purpose he can unblock them when issues are resolved.

e. Information managed and administered by a App administrator include assessment model sections, subsections, questions, assessment results, and bank staff information. They register their respective bank employees in the system, create and manage their accounts. an App administrator is privileged to register bank departments in the system which are used to group users under their designated departments. This helps in data visualization where it's easy to know how many staff belong to a certain department. He describes the role of the App to users. She/he is also responsible for creating and adding questions to the assessment model. These questions are placed under subsections of the Ethica App. Creating a question involves selecting its level of evaluation. Manages the visibility status of the assessment model after adding questions. After staff performing assessment on the model, it cannot be accessed or edited.

f. The administrator views assessment results Note: the system calculates the assessment results basing on the staff response and given a recommendation based on the staff score. Then the administrator after accessing the results can provide their responses basing on the degree of assessment on a given question. Generate reports, the administrator is also able to generate reports from the system. These include staff who have passed or failed the assessment, those who have partially or fully completed the assessment. They are also entitled to viewing statistics generated from the system.

c) Bank Staff Performing assessment, a bank staff registered in the system is able to perform assessment simply by selecting any open model and answer the questions. Note: (ii) Viewing the certificate after assessment, once the staff has completed assessment under a given model, the system automatically generates a certificate for the user showing assessment completion.

6.4 Non-Functional requirements for Ethica Application

These are requirements that explain the operation state and attributes of the developed system. They include: (i) Security, this is enforced in the way that only authorized users with correct login credentials are allowed to access the system. ii) access control only authorized users' access what they are supposed to access. For example, a bank staff cannot perform what is privately delegated to administrators. (iii) Lean-ability, the developed web system provides clear and user friendly interfaces which can be easily remembered by the users. For instance, when a user is attempting the questionnaire, only one question displays at a time to keep user focused. (iv) Usability, the developed system provides properly labelled modules which are easy for a user.

6.4.2 Sequence diagram

This diagram shows the interactions and communications between the Model actors. It helps in logical understandings of the model development. The purpose of a sequence diagram is to illustrate the sequential flow of information passing through the key entities of the system.

Figure 6.3. shows Eceba sequence diagram showing how a user is authenticated into the system to allow access to the assessment.

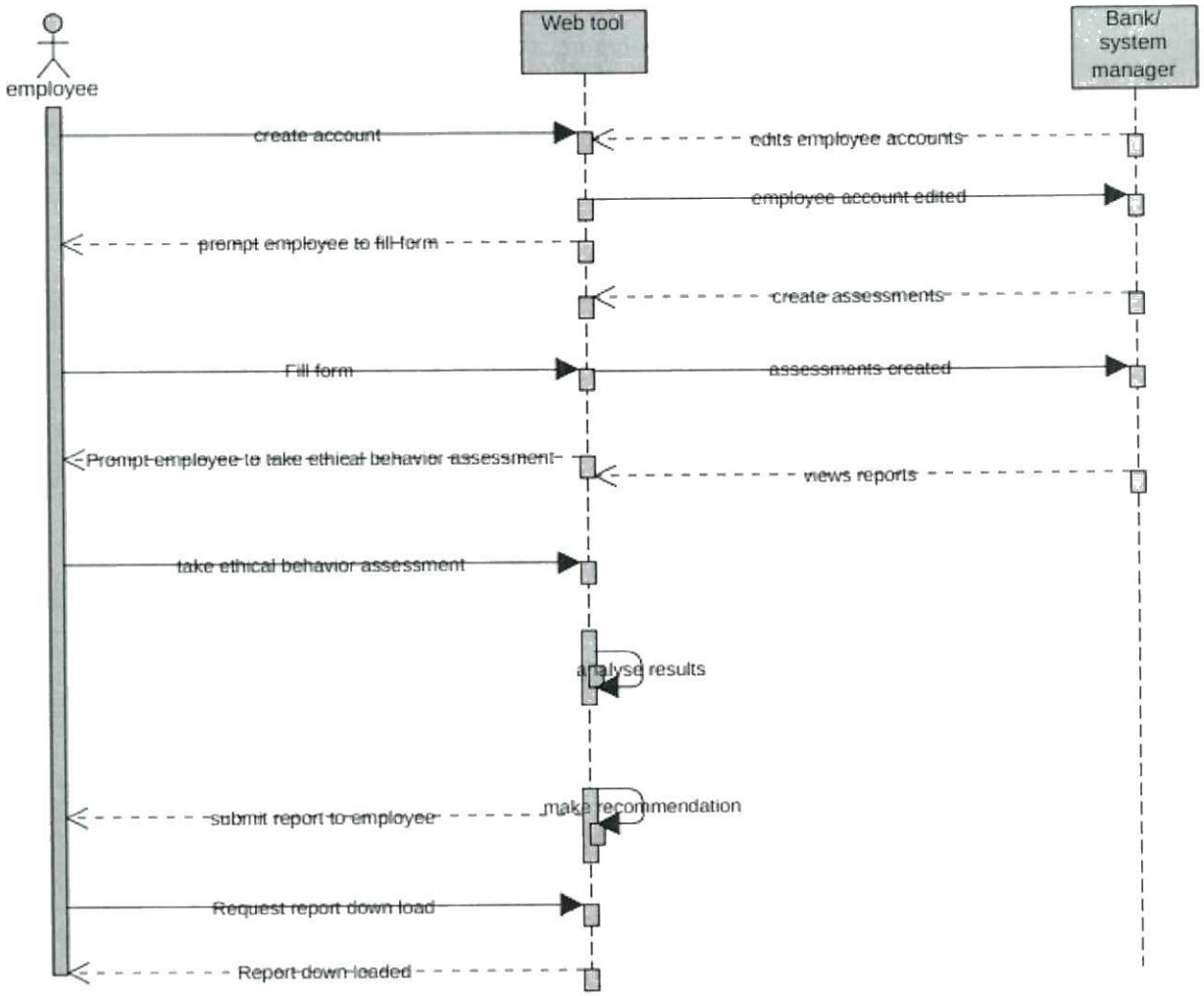


Figure 6. 4 The Ethica web based Application Development to test ECEBA model.

ETHICA app was developed to illustrate the potential of the Eceba model, to prove its reliability (internal consistency and stability), validity (construct and concurrency), and accuracy in improving cyber security ethical behavior. The key features of the Eceba model have been employed in the implementation of the Ethica web based App. The word Ethica was derived from ethical implying employees should possess good morals. The app was implemented among commercial banks employees and Absa bank Mbarara consented to test our App. The app enables bank employees to log in at their convenient time and take assessment and the banks can also carry out their employees' ethical behavior assessment.

6.5 The Ethica Web based System's Requirements

6.5.1 Software requirements

Table 6. 1 Software requirements of the developed model.

Requirement	Description	Usage
A source code editor	A text editor program designed specifically for editing source code of computer programs by system developers.	In this case Sublime text editor 3 was used to write codes during the process of system development.
Data Store	A repository for persistently storing and managing collections of data.	MySQL database management system was used to store and manage the system data.
Database Server	A software application typically for hosting application databases.	XAMP a local MySQL server was used to locally host the database that stores the system database and host the system files so that it was able to be accessed in a client server environment using a web browser.
Database Modelling Model	A software application for creating and manipulating database models and physical databases.	MYSQL Workbench was used to design the logical database model so as to graphically represent the different database entities and their relationship and also show how data flows in the system.
Operating System	A system software that manages computer hardware and hardware resources and support basic computer functions	Only Windows 10 was used to provide a platform for installing other software in order to design and develop the system.

6.5.2 Software Specifications

XAMPP version 7.2.32 was used to act as the local database server to locally host the MYSQL database where the system data is stored. The server also hosted the web application files which were accessed in a client server environment using a web browser i.e, Google Chrome. MYSQL Workbench 8.0 CE was used to design the database model purposely to illustrate the flow of data between entities. This helped in designing the logical database model which was later converted into a physical database after forward engineering. Sublime Text Editor version 3 32bit was also used as the source code editor for editing the developed web system source code.

6.6 Architectural design

6.6.1 Account of the Designed System

The Ethica Web based App provides a platform for assessing the staff Cybersecurity ethical behavior intention in commercial banks in Uganda. In developing the system, a number of programming languages and platforms were used. The front end interface was done using HTML5 to design the web interfaces of the system. To style the interfaces, CSS3 was used since it provides styling attributes for the HTML5 Components like headings, Paragraphs, Forms and Others. Then JavaScript was used as a client side script to validate the data before submitting it to the server. To achieve submission of data asynchronously, AJAX a JavaScript library was used to allow submission and loading of data without loading the 7 entire page. This was done to limit the amount of data bundles required by the users while using the system. In order to achieve responsiveness of the user interfaces Bootstrap was used. Bootstrap is a free and open-source CSS framework directed at responsive, MobileFirst front-end web development. It contains CSS- and JavaScript-based design templates for typography, forms, buttons, navigation, and other interface components. When it comes to processing system data to and from the database, XAMPP a local MySQL server was used to host the database and also the system files and Object Oriented PHP was used to act as a GCI to manage data communication between the server and interfaces (connecting front end to back end). PDO (PHP Data Object) driver class was used to achieve this simply because PDO involves use of prepared statements which makes execution faster than running direct queries. In order to interact with the MySQL server using PHP, SQL was used to write the queries purposely to perform data processing on the server.

6.7 System Flow

6.7.1 System Flow Chart

The system flow chart below shows how the different system users access the system and what they are entitled to execute in the system.

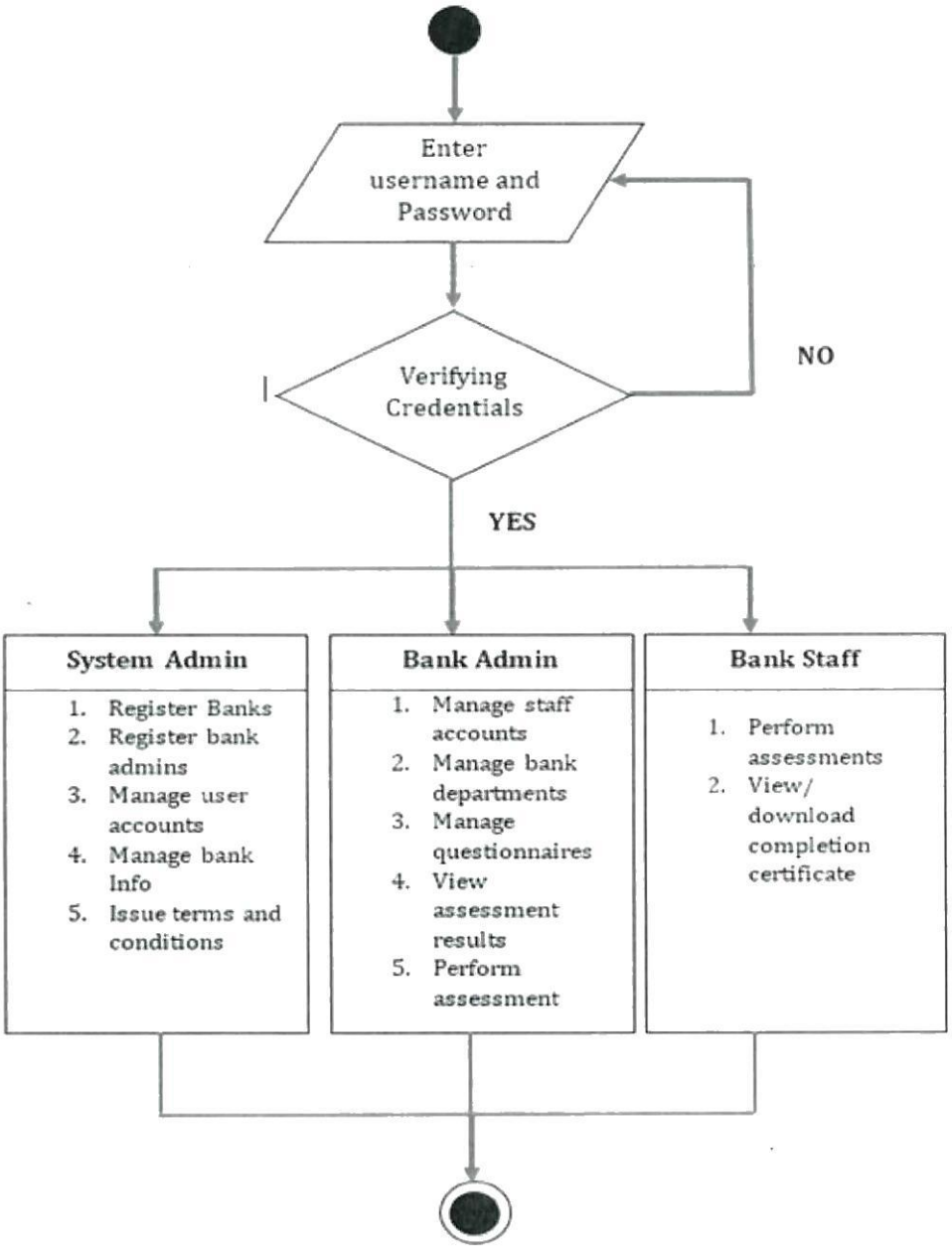


Figure 6. 5 Showing the Flow of the system, system users and their designated tasks.

6.8. Database Design

6.8.1. Entity Relationship Diagram (EERD)

Enhanced entity-relationship diagrams, or EERDs, are specialized Entity Relationship Diagrams that can be extremely useful for modeling the databases. EERDs use several concepts that are closely related to object-oriented design and programming. The EERD below shows the logical database design of the developed system. It portrays different entities/ tables and the relationships among them. It shows how data flows in the system database. The database uses a number of entities to collect, save and retrieve data. These entities are represented in Figure 6.5. An Entity Relationship Diagram is a type of flowchart that shows how "entities" such as people, objects or concepts communicate with each other within a system. In this system, a basic user can only take the assessment appropriate for his department. A user can attempt only one assessment at a time. A basic user can edit his own profile, change his password, view his own assessment report, and print his own certificate of completion. The system administrator can create user accounts, create new categories of assessment, and populate an assessment with questions, view individual users' reports, and view aggregate reports.

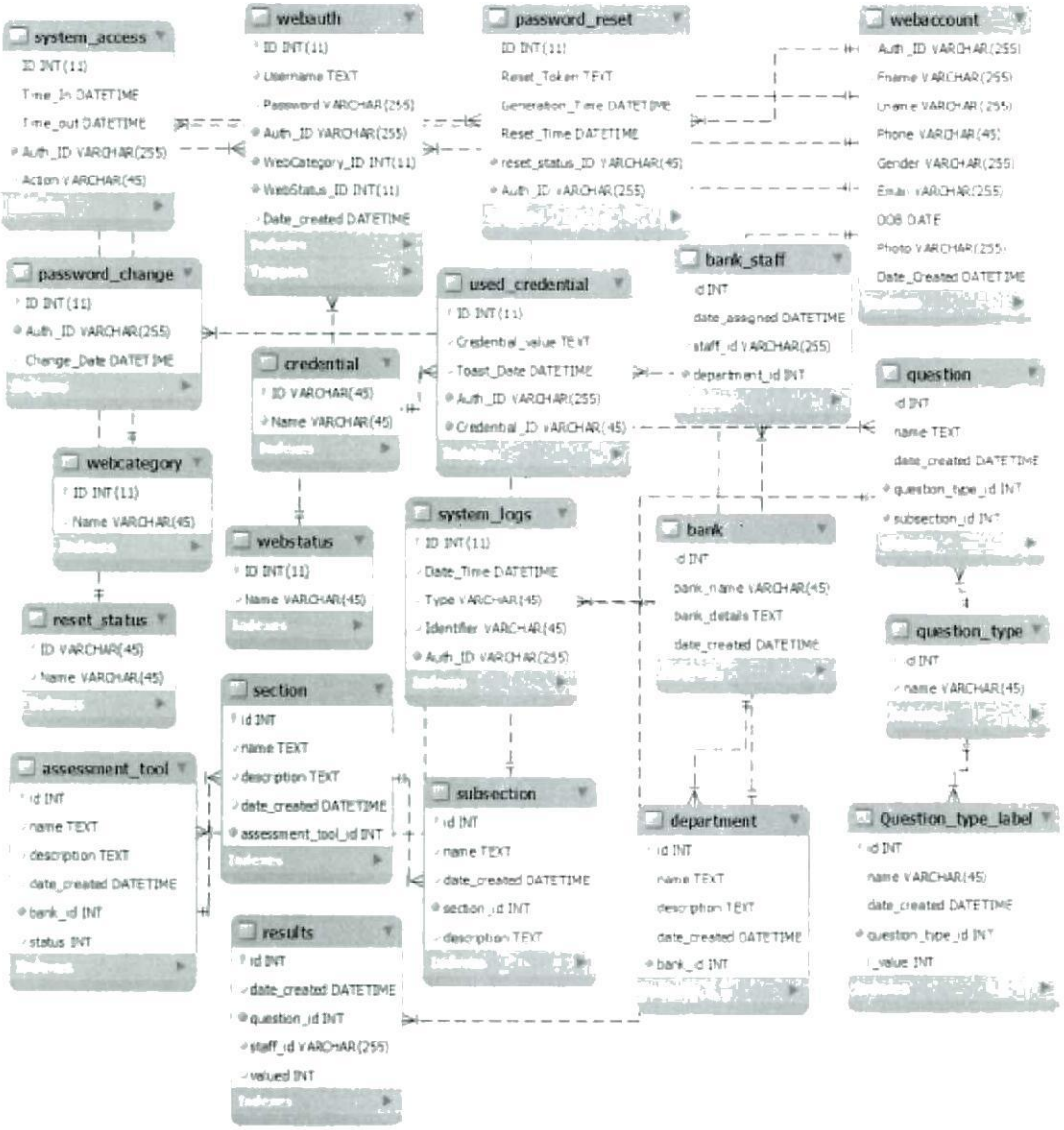


Figure 6. 6 An Enhanced Entity-relationship diagram showing database entities and their relationships.

6.9 Graphical User Interface

6.9.1 User Login Interface

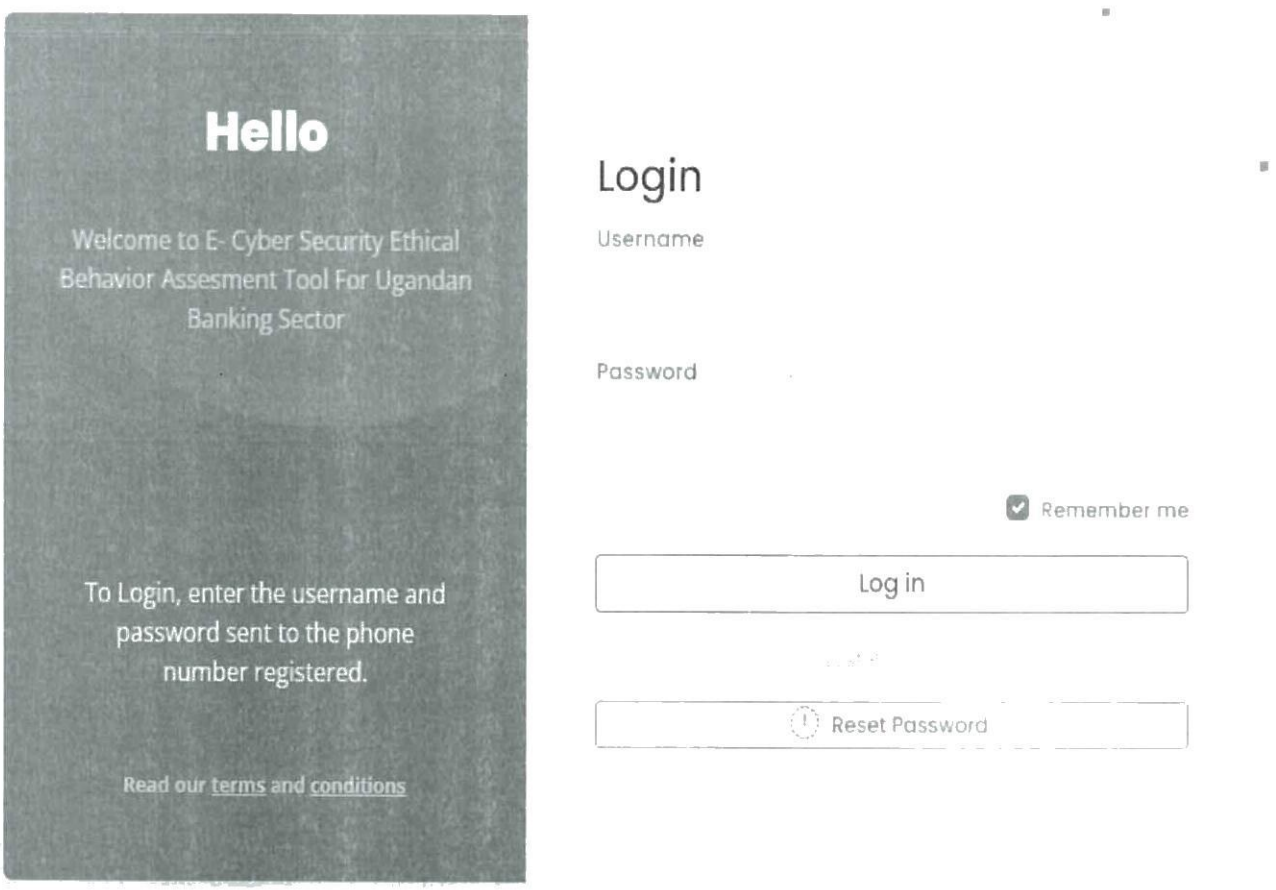


Figure 6. 7 System Login Interface.

The figure above portrays the login interface used to authenticate users at different levels into the system. On login, a user is required to provide a pair of matching credentials i.e., user name and password which are used to prove the user's identity. Once the user has provided the correct and valid credentials, authorization to the system is granted and a new session is started holding the ID of the user which is used to determine the level at which the user has accessed the system in order to prepare the right modules corresponding to the level of access. The system uses the same session ID to determine the bank where the user is registered so that all actions executed are tracked and stored under that bank.

When the users forget their password, the login interface provides a reset password button where user can click and get directed to the reset password interface. On this interface, a user is requested to enter their phone number or email address registered during account creation. If the phone number or email address exists, a six-digit OTP (One Time Passcode) is sent to the phone number or email address provided and thereafter a user is given an input field to confirm the sent code. The OTP is given a lifetime of 60 minutes valid. True confirmation of the OTP directs a user to where they can enter a new password and also confirm.

6.9.2 New Staff/Employee registration form

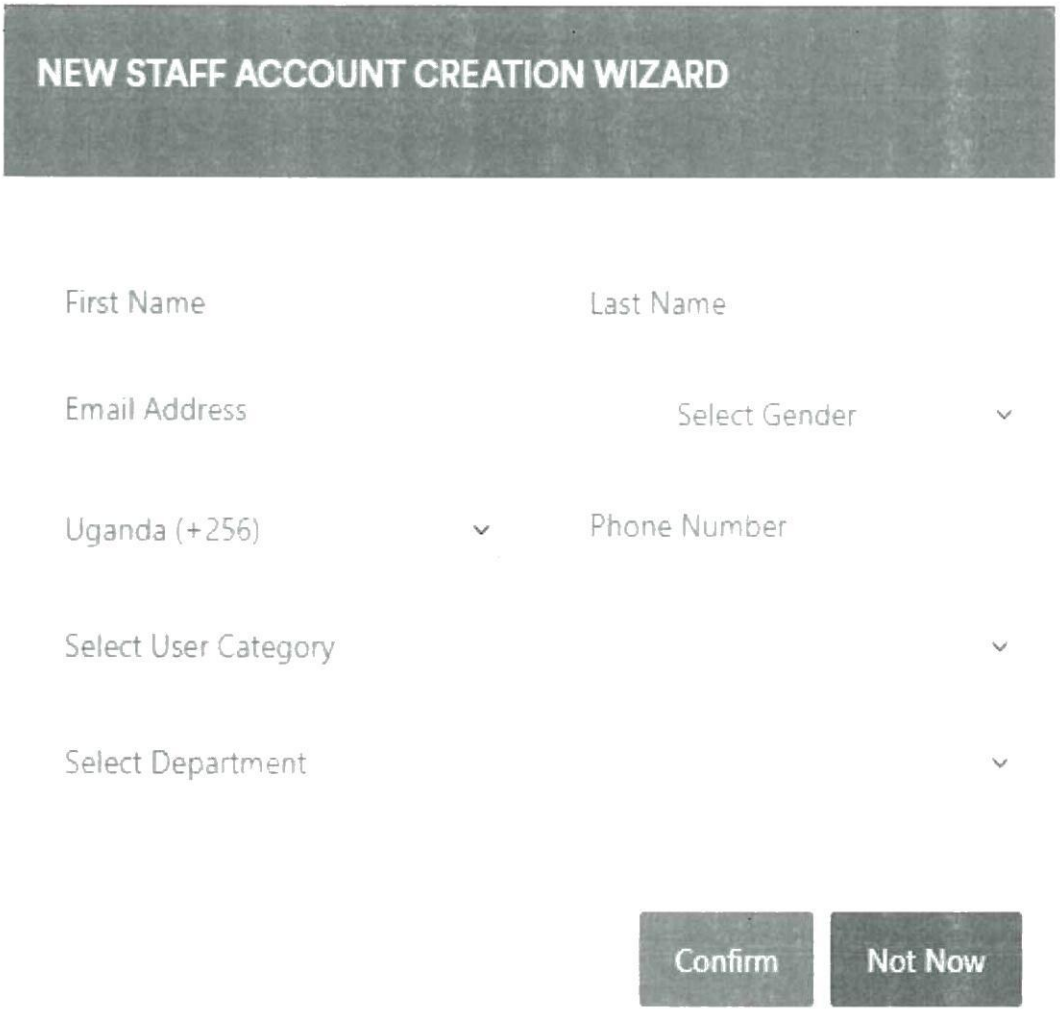


Figure 6. 8 New User Account Creation Interface.

The figure above shows new user account creation interface. On this interface, a bank administrator is able to provide basic information about a user which is used to set up an account for them as well labelled in the form placeholders above. After validating that the email or phone number is not already in use, the system concatenates the selected country code and the provided phone number to generate a full number with a plus which together with the email address acts as the address to which the system generated authentication credentials for that account are sent i.e., username and password. After sending a copy, the system goes ahead and encrypts them before being inserted in the authentication table. Encryption is done using a PHP encryption method which takes in two argument i.e., the encryption algorithm **sha256** and the string to be encrypted i.e., username or password to form a ciphertext(encrypted). Formula below clearly explains the process of encryption in the developed model.

Where x represents the encrypted string to be obtained(ciphertext), ***hash*** is the predefined PHP function used to encrypt, y is passed as ***sha256*** which is the encryption alogorithm and z is the text to be encrypted in plain text i.e., username or password in plain text. Once this step is completed, the system sends a POST request to the MySQL in order to store the user information in the database. The posted information includes an ID which is automatically generated. The ID is used as a primary attribute to uniquely represent and track user actions in the system.

6.9.3 Attempting a questionnaire

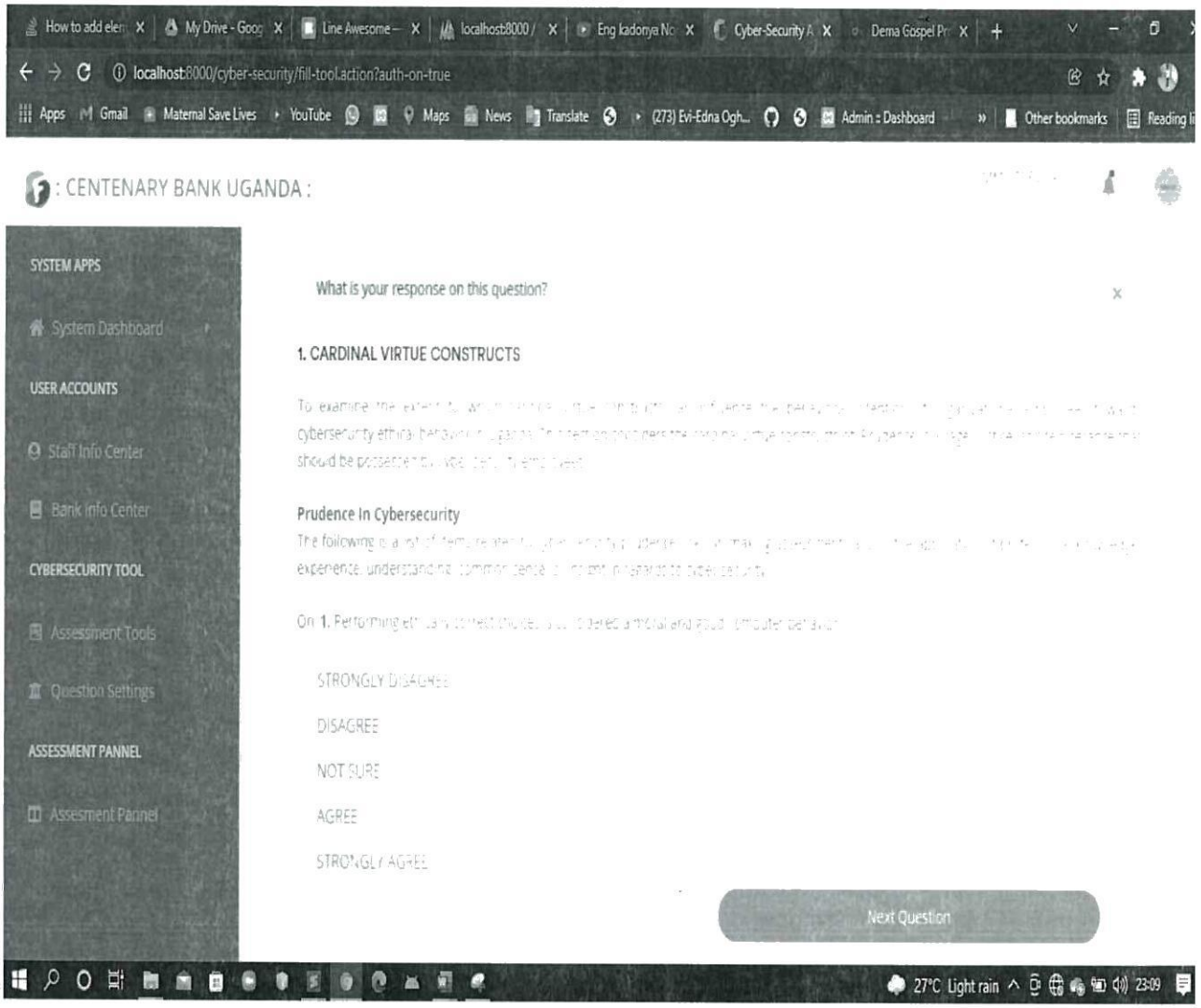


Figure 6. 9 Attempting the questionnaire.

The figure above provides a clear view of how the assessment is conducted in the system. On this interface, a user is able to interact with the system by providing their view or level of satistication based on the question displayed. During the question setting, each question is given a response type which is used to determine the degree of user's statisfation towards that question. Each response type is allocated different levels where a user selects basing on their statisfation toward the question. Majorly, two response types are used in the model.

These include **True/False Type** with level of ***mostly false, somewhat false, somewhat true, mostly true, completely true and agree/disagree type with levels of strongly disagree, diagree, not sure, agree, and strongly agree. each response type level is assigned a mark/ numeric value which is based on to assess user's performace. 1- mostly false, 2- somewhat false, 3- somewhat true, 4-mostly true, 5-completely true.***

After a user providing their response, the system sends a POST request to the server containing the reponse Value/Mark, Question ID, User ID and store the information in the result entity in the database which awaits for atleast 85% of the attempt to mathematically compute the results.

6.10 Marking and tot up

To the employees assessed, the system bases on the number of questions a model contains to determine the response progress as given in the formula below;

To the employees assessed, the system bases on the number of questions a model contains to determine the response progress as given in the formula below;

$$\boldsymbol{Res = (NoQ/TnQ) * 100}$$

Where $\boldsymbol{Res}$ respresent the Assessment progress result in percentages, $\boldsymbol{NoQ}$ represents the Number of Question Attempted and $\boldsymbol{TnQ}$ is the Total number of questions in a given cybersecurity ethical behavior assessment model. ***Note***: For an employee to be assessed, the $\boldsymbol{Res}$ must be above **85%.**

6.10.1 Computing the Employee Assessment Score (EAS)

The computation is based on the Employee response on a given Question. The system adds the reponse values/marks of all questions divides it with the maximum score possible and multiplies the result by 100 to convert it to percentage.

6.10.2 Computing the Maximum Score Possible (MsP)

The MsP is given by the fomular below;

$$\boldsymbol{MsP = (TnP * 5)}$$

Where the TnP is the Total number of Questions in the given assessment model. The value Five (5) is considered to be the maximum response type value based on the range. This means response values ranges from $1 - 5$.

6.10.3 Computing the Total Response Score (TrS)

The TrS is given by the fomular below;

$$\boldsymbol{TrS} \mathbf{+=} \boldsymbol{SqV} \quad \textbf{OR} \quad \boldsymbol{TrS} = \boldsymbol{TrS} + \boldsymbol{SqV}$$

Where the $\boldsymbol{TrS}$ is given an intial numeric value Zero (0) and then subjected to the loop counted basing on all the questions attempted. As loop counter traversers through the attempts, it add the $\boldsymbol{SqV}$ which is the Single Question value to the $\boldsymbol{TrS}$ basing on the given creteria/ condition which looks at traversing through all the question attempts of a given user. When the loop counter terminates, the last incremented $\boldsymbol{TrS}$ value is recorded.

6.10.4 Computing the Final Assessment Results (FaR)

The $\boldsymbol{FaR}$ is given by the formula below;

$$\boldsymbol{FaS} = (\boldsymbol{TrS}/\ \boldsymbol{MsP}) * \mathbf{100}$$

Where the $\boldsymbol{Trs}$ is the Total response score and $\boldsymbol{MsP}$ is the Maximum Score Possible.

6.10.5 Determining the Employee Recommendation

The employee recommendation is determine by the Final Assessment Results **($\boldsymbol{FaR}$).** The FaR is subjected to a condition statement i.e. , **IF Statement** to make decision regarding employee performance. This determination was done using the formula below;

$$if(\boldsymbol{intval}(FaR) \geq 50):$$

Cybersecurity ethical behavior Assessment Passed

$$else:$$

Cybersecurity ethical behavior Training Needed

Where $intval()$ is the function used to convert the result of FaR to an integer value.

6.10.6 Assessment Results

Assessment Results

Show 10 entries Search:

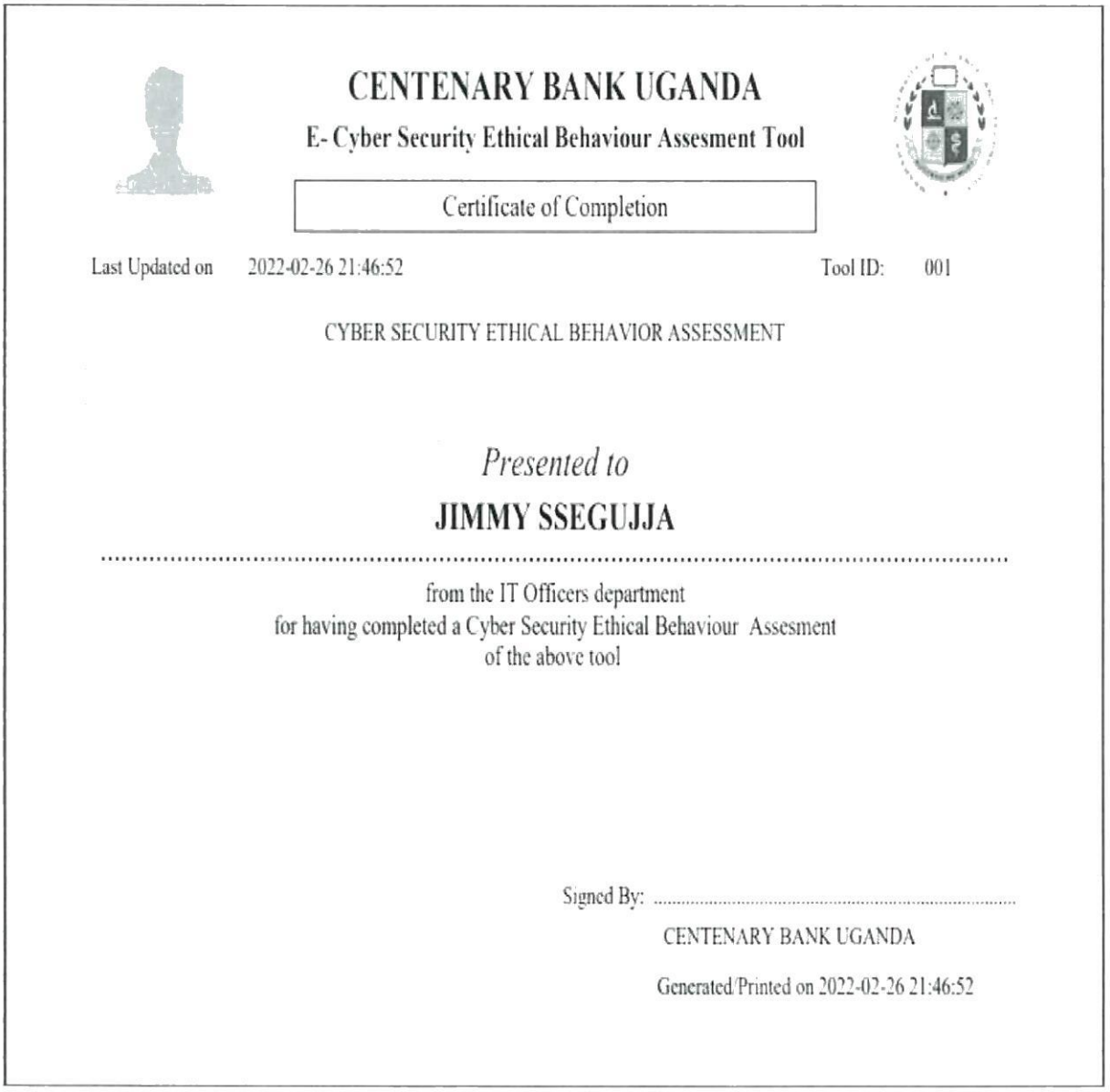
ID	Staff Name	Phone	Attempts	Tool Qns	Score	% Score	Recomendation
1	Jimmy Sseguja	+256774165087	60 100%	60	163	39%	CyberSec Ethics Training Needed
2	Emma Muheerza	+256756254760	60 100%	60	227	27%	CyberSec Ethics Training Needed
3	Chris Trevor	+256752453465	59 98%	60	129	57%	CyberSec Ethics Assessment Passed
4	Tony Engwa	+256751656252	51 85%	60	121	58%	CyberSec Ethics Assessment Passed
5	Ruth Nakato	+256701501880	10 16%	60	28	85 of Tool Attempt not reached	of Tool Attempts reached

Showing 1 to 5 of 5 entries Previous 1 Next

Figure 6. 10 Assessment Results.

The figure below shows a report generated by the system displaying the assessment progress of each staff on a given cybersecurity ethical behavior assessment model. The report only shows those employees who have made any progress towards attempting the assessment model. The reversed result set of this report is a list of employees who are registered in the system but have not attempted any assessment question under the selected model.

6.10.7 Complete assessment Certificate



CENTENARY BANK UGANDA

E- Cyber Security Ethical Behaviour Assesment Tool

Certificate of Completion

Last Updated on 2022-02-26 21:46:52 Tool ID: 001

CYBER SECURITY ETHICAL BEHAVIOR ASSESSMENT

Presented to

JIMMY SSEGUJJA

from the IT Officers department
for having completed a Cyber Security Ethical Behaviour Assesment
of the above tool

Signed By: .....

CENTENARY BANK UGANDA

Generated/Printed on 2022-02-26 21:46:52

Figure 6. 11 Complete assessment Certificate.

Figure above a sample certificate generated by the system when an employee completes the assessment excersie for a given cybersecurity assessement model. An employee who has completed the assessment can download the certificate and take it to the bank administrators to attach a signature and a bank stamp in order to brand its authenticity.

6.11 Ethica Application Testing

This system was tested to confirm its accuracy and see if it completely fulfils the requirements. Separate components of the Ethica App. were individually tested, before testing the whole system. There after the App was set up via the web to allow employees of Absa Mbarara branch test its usability. This was done with the help and consultation with bank branch managers who helped identify departments and staff who could participate in the testing.

6.11.1 Individual Component Testing

The main pages of a Cyber security ethical behavior intention assessment model are login page, dashboard page, users' management page, create new assessment page, manage assessment page, add assessment questions page, view assessment page, questions management page, edit assessments page, system reports page. Each of these were tested and ascertained to be functioning as intended.

6.11.2 Entire model Testing

After testing the individual components, the entire system was subjected to testing too. This was to check on functionality, robustness, performance speed and security. All pages and reports loaded in less than 3 seconds. All modules were ascertained to be working as intended. As shown in the sample screenshots above.

6.11.3 Usability Testing

All study participants received the testing version of the Ethica application by following the link on https://cybersecurity.groxels.com. Of the 24 participants who received the application, two reported failures to download the application from the shared link. After one week of receiving the application, downloading, and installing the app, participants were contacted for a phone interview, and the interviewer-administered questionnaire to assess their overall experience with using the application. Once the above testing was completed, the application was deployed to the internet via URL **https://cybersecurity. groxels.com.** Employees of Absa and centenary banks were invited to test the application. The researcher selected some key departments with consultation with bank branch managers who helped to find staff who could participate in the testing. The feedback was generally positive. Appendix D shows a questionnaire that was used to collect feedback from users.

6.12 Usability Testing Results

Questionnaires were used to collect feedback from 10 respondents who volunteered to test the application. This feedback is shown in Appendix and is further discussed below.

Table 6. 2 Usability Testing Results.

US Score	Grade	Adjective Rating
> 80.3	A	Excellent
68 – 80.3	B	Good
68	C	Okay
51 – 68	D	Poor
< 51	F	Awful

6.12.1 User Friendliness

By use of the usability testing questionnaire, **appendix F**, 100% of respondents were able to login to the model. 15% however indicated that they had trouble logging in at the start. They however indicated incorrectly typed password and poor internet connectivity as the cause. Out of the 10 respondents who tested the application, 60% rated ease of navigation and clarity of questions good while 40% rated it excellent. Clarity of assessment reports was rated good by 50% of respondents and excellent by the other 50%. Usefulness of assessment report was rated excellent by 90% of respondents. 50% respondents strongly agreed that the system was easy to use. 70% of respondents strongly disagreed with the statement that they would need support of a technical person to be able to use the system, 20% disagreed and 10% were neutral.

6.12.2 Usefulness of the System

90% respondents strongly agreed that the system was useful and 80% respondents strongly agreed that they would recommend it to their friends. When asked what they liked most about the application, many respondents responded that they did not know that ethical behavior could be assessed and that the application was a unique and very important idea.

CHAPTER SEVEN: STUDY CONCLUSIONS, RECOMMENDATIONS AND IMPLICATIONS

Introduction

This chapter presents conclusion, implications and recommendations of the study.

7.1 Study Conclusion

This research aimed at enhancing Cyber security by confirming through statistical analysis the applicability of cardinal virtues related to Cyber security ethical behavior. This study confirmed through statistical analysis the applicability of cardinal virtue constructs as they relate to Cyber security by validating each construct's indicators and factors which influence the ethical behavior of banking sector employees in Uganda. This was done through assessing those components and their interactions in an ethical behavior model. The research methodology used was the survey method, utilizing an online questionnaire. The survey population consisted of commercial banks'employees in Uganda. The study was carried out among the employees of the Centenary and ABSA banks' branches located in Kampala capital city of Uganda. Confirmatory factor analysis was used to determine causal patterns in the variables and assess them for validity and reliability in the proposed theoretical model. Structural equation modeling was then used to test for casual relations between the model's constructs.

This research presents the creation of a Cyber security ethical behavior assessment model and presents its applicability among the banking sector employees in Uganda. The Cyber security ethical behavior questions covering the cardinal virtues and ethical climate, are created by the system administrator and stored in a database. XAMPP version 7.2.32 was used to act as the local database server to locally host the MYSQL database where the system data is stored. The server also hosted the web application files which were accessed in a client server environment using Google Chrome web browser. MYSQL Workbench 8.0 CE was used to design the database model to illustrate the flow of data between entities. This helped in designing the logical database model which was later converted into a physical database after forward engineering. Sublime Text Editor version 3 32bit was also used as the source code editor for editing the developed web system source code.

Employees can then log into the model at their appropriate time and take the assessment. Depending on the employees' assessment answers, the weak areas can be used to recognize openings and this data be used to tailor Cyber security virtue ethical based awareness, and training programs to meet employees' ethical behavioral needs.

The findings of this study provide a concrete preliminary explanation of virtue elements and their influences on employees' Cyber security ethical behavior intention in the banking sector in Uganda. The results also provide a foundation on which to guide further research and analysis of the developed Cyber security ethical behavior assessment model.

Practitioners may use the model to develop a comprehensive awareness of the impact that virtue ethics may have on employees' behavior; develop employees' ethics education and training programs, standards of conduct, and guidelines for ethical responsibilities and behavior.

Researchers can use the model to reflect on the applicability of the virtues to Cyber security and to search for their relations and influences on employees' ethical behavior.

The critical objective of including an ethics approach based on the employees' ethical behavior model is for Cyber security professionals to exercise more ethical behavior resulting from their own inner inspirations. Founded on the results of this research, a virtue ethics based methodology that encourages employees to make ethical decisions especially as experts and for the employing organizations appears to be an effective approach to reducing employee Cyber security violations. Bright et al., (2014) stresses that the things that create organizational virtue should be explored.

Morris and Morris (2016), contend that Virtue ethics, focuses on the development of the character of the individual who must confront ethical dilemmas. Virtue ethics recognizes that making a decision about difficult problems depends on the character of the people making decisions. Therefore, a person's decisions about what to do reflect who they are as a person.

The results also imply that it may be possible to identify an employee's ethical conduct in relation to cyber security through a background check or personnel screening procedure that analyzes how they respond to ethical dilemmas. The development of this model aids in identifying the ethical virtue characteristics of a potential new hire's and current employee's backgrounds. This could reveal whether or not the person has a strong sense of morality and ethics. This can make it clear to the hiring committee that the applicant is a suitable fit for employment connected to cyber security within the company.

The banks are urged to use the methods from this methodology to figure out how each employee makes ethical decisions. Hiring and keeping more moral people could lead to a more moral workplace atmosphere. There might be fewer cyber security violations as a result in the future. This may depend on a person's ethical conduct, which may then be affected by the ethical climate of the company they work for.

7.2 Implications

7.2.1 implications to theory

Despite the fact that there is study and literature on information and cyber security ethics, there is still much that we do not know, particularly about its impact on people and societies as a whole (Harrison, 2014). In order to advance virtue ethics as a framework for moral inquiries into cyber security, it is intended that this thesis provides a unique and noteworthy theoretical addition to the subject. The research implemented the Philosophical Virtue theory Aristotle (2005) and Aquinas (2005) the theory of Planned Behavior (TPB) (Ajzen, 1991) together with Ethical climate theory by Victor and Cullen (1987, 1988), as the pillars of the employees' Cyber security ethical behavior assessment model. It is important to note that very few studies have applied virtue ethics theories in combination with TPB variables in Cyber security. Previous studies did not examine the influence of these variables towards Cyber security nor map these relationships. Also the Theory of Planned behavior (TPB) is one of the most well-established theories used in the field of Information systems (IS) regarding social behavior (Papouli, 2018). Ajzen suggested there may be a need to investigate "personal feelings of moral obligation or responsibility to perform" though it was not specifically incorporated into the TPB (Ajzen,1991). This research borrowed behavior intentions and ethical behavior constructs from TPB. These theories were used in assessing the banking sector employees' ethical behavior towards Cyber security. This was essential because these theories independently could not elucidate employees' ethical behavior towards Cyber security. The virtue ethics theory Aristotle (2005) helped to ascertain the cardinal concepts of prudence, justice, courage, and temperance for the ethical behavior towards Cyber security by the banks' employees in Uganda. However, the theory fails to explicate behavior intentions and actual behavior towards Cyber security. The virtue ethical theory lacks the behavior intention and ethical behavior. TPB is suitable at explaining behavior antecedents but it does not explain how ethical behavior comes about. The theory of planned behavior fails to indicate how the ethical behavior could be attained and would not be used alone to explain behavior.

Therefore, combining these two theories went a long way in checking and eliminating the weaknesses presented by either one of the theories.

Furthermore, these two theories did not address the ethical climate and yet it institutes the right behavior and acceptable conduct among organizational members Martin and (Cullen, 2006). The cardinal virtue constructs could not directly affect employee's ethical behavior; they are always filtered through ethical climate which moderate their effect. Hence, from this perspective, it is argued that this model makes a significant contribution to the ethical theories of behavior for improved Cyber security. There is no existent research previously that has applied these theories in assessing the banking sector employees' ethical behavior towards Cyber security in Uganda.

7.2.2. Practitioner Implications

This research is in agreement with other schoolars (Gray, 2015) who contend that an increased emphasis on the recruitement, induction, sensitization, inspiration and behavioral processes founded in virtue ethics approach might be effective in improving Cyber security. Results can be utilized in improving methods, instruments, and models to evaluate the employees' Cyber ssecurity ethical behavior.

Progressing research on ethical climates that endorse confidence in commercial banks certainly affects banks' aptitudes to improve their reputations. Providing the banks' policy makers with a model on how to assess ethical behavior within the organizational climate increases the practical value of this study. Banking managers may use the results of this research to regulate the ethical climate to promote ethical behaviour.

This research also establishes practitioner consensus on virtue constructs that can be explored, expanded upon, and validated by both the researcher and practitioner communities (Gray, 2015). After undergoing validation and reliability testing in this study, these constructs were potentially operationalized to predict a worker's future ethical behavior using the developed model thereby improving Cyber security.

Cyber-attacks on banks continue finding a way despite improved Cybersecurity infrastructures. Malik et al., (2018), Kuepper (2019) advice that there is an agent need for banks to assess the efficiency of application and implementation aspects of the numerous interior controls, and also be cautious of their employees' behavior.

Shoemaker et al., (2019) argue that the extent to which an organization is secure depends on the readiness of its workers' applied ethical behavior. Thus the banks' management can make use of this research findings to improve employees 'ethical behavior towards Cyber security. The results got from this study are a platform to the government of Uganda through the Ministry of Information and Communication Technology (ICT) and Uganda Bankers' Association in generating appropriate national policies implementing issues, methods and strategies related to Cyber security ethics as one of the strategy aimed at improving Cyber security and particularly in the banking sector.

The insinuations of current research are that it provides researchers with the evidence that virtue ethics has potential application in the field of Cyber security, assuming that any concerns that practitioners may have can be addressed.

Furthermore, the empirical evidences of this study are an attempt to provide an insight into virtue character traits moderated by ethical climate as self-regulatory factors influencing Cyber security ethical behavior. More specifically, the study identified Justice, Courage and temperance and ethical climate as significant drivers of Cyber security ethical behavior in the banking industry. In this regard, policy makers should develop virtue ethical based training programs with dedicated, continueuos learning and teaching undertakings geared towards monitoring and enhancing the overall ethical behavior towards Cyber security in the banking industry. Employees could be allocated a mentor and participate in virtue ethics focused on-the-job training which facilitates the continuous inculcation of virtuous practices in order to promote acquisition and development of desired decision making habits. This is in line with Morris and Morris (2016), posit that Virtue ethics intensely stresses that individuals should be trained in the virtues so that they develop excellent habits of mind. Such habits best prepare employees to choose optimally in any given situation.

Safa et al., (2016) posit that technology measures alone cannot guarantee protection to critical information and Cyber security and other assets in the Cyber space. Therefore, this research provides practitioners with alternatives to technical controls, checklists, and formal procedures; which are known to have been ineffective against human being who are recognized as the weakest link to Cyber security. Harrison (2014), contends that Virtues are moral excellence. Virtues are inherently good and they guide conduct and are the foundations of good character.

Individuals should actively choose to show their virtues because they are helpful to them and the entire community in which they are living. 169

7.2.3. Researcher Implications

This research is a stepping stone for further research into virtue ethics for addressing behavioral issues linked to upholding Cyber security. It offers the interfaces of the components and indicators of an employee ethical behavior model and provides a structure for future research.

7.2.4 Research contributions

This research contributes to the emerging knowledge on Cyber Security ethics through the following ways;-

To Theory.

This study provides a theoretical contribution by investigating the applicability of virtue constructs and ethical behavior intentions in understanding how employees' Cyber security ethical behavior could be improved in Uganda. No study has approached improvement of Cyber security performance from this viewpoint where the virtue ethical theories in combination with theory of planned behavior and ethical climate are used in regard to attaining improved Cyber security. Drawing on virtue ethical theory, ethical climate theory, and the theory of planned behavior, this study developed a web-based cyber security ethical behavior assessment model. This model is a platform for managers in assessing those individuals who may present Cyber security unethical behavior intentions (Papouli, 2018). Hackett, and Wang (2012), assert that the management selection and recruitment writings concentrate on valuations of facts, talents, aptitudes, skills, persona and capability minus consideration on examining character of the selected candidates.

To the Banks Employees.

This study targeted the commercial banks employees. By concentrating on organizational personnel, the results of this study could be useful when developing strategies to prevent Cyber security violations aided by these workers. The study paid a lot of attention on statistical verification of instruments and the study results was used to build Cyber security ethical behavior assessment model in order to be able to make recommendations to the banks management, Cyber users and entire Cyber society.

To the Banks Policy Makers

The study is relevant to the banking sector and the banks policy makers who could be aided to make informed decisions by incorporating Cyber security ethics trainings in the banks such that ethical personnel with the right knowledge and skills are recruited and retained. The incorporation of Cyber security ethics in the recruitment and selection process can further enhance the ethical use and implementation of Cyber security strategies among these employees. Banking institutions need to use the recommendations given in this study in developing relevant policies and guidelines on matters pertaining to cyber security employees ethical conduct.

The model further helps when unethical persons are identified, they would be allowed to be educated or trained further through Cyber security ethics education. Using the Cyber security ethical behavior assessment model, employees who may have diverse indigenous, cultural and religious upbringings could be helped to engage in the art of virtuous living in the Cyber space social environments Papouli (2018).

To the Researchers

This study is part of the pool of knowledge on Cyber-security ethics where other scholars and researchers refer to the contents of the study for any future related studies and debate. The study tested the virtue theory on Cyber security in Uganda and made recommendations for further studies.

7.2.5 Limitations of the study

This research employed a cross sectional survey and thus the study is limited to a particular time of measurement. Given that behaviors change over time, there is need for a longitudinal study. This will provide a more complete depiction to researchers and practitioners to understand when virtues and ethical climate have the robust influence on ethical behavior, and to prove that managerial interventions are continueous in order to improve Cyber security.

In addition, the approach did not allow making clear causal attributions for the observed relationships and influences. Therefore, directional influences posited within the hypothesis models must be interpreted with caution.

This study involved a sample of commercial banks in Uganda Though, given that there may be characteristics of banks' employees unique to particular commercial banks; by quality of their organizational cultures, inclination or mandate of the bank or national interest, divergent views could have been left out which could have enriched the findings of the study. This short coming of the study could be overcome by involving all commercial banks in the country.

On the same note the target population for this study was members of only the commercial banks picked from the banking sector. While a large enough sample might be generalizable, the findings are specific to that sector. If this study was carried out in a different other financial sectors like micro finance may be the results would be different. There is a likelihood that the data gathered in this study is not representative of the financial industry employees. Further studies should be conducted with users from other institutions to more confidently generalize the findings.

The study focused on commercial banks in Kampala city which is an urban setting rather than rural setting. Due to different business environments, the findings may not entirely apply to small commercial banks in rural places. Businesses in the urban areas have access to training and other advisory services. The model should be tested in a rural setting for reliability and validity.

Another limitation is that due to Covid 19 pandemic physical contact was limited. Thus, the invitations to participate in the study were sent via e-mail. This raises the possibility that users may not have received the invitations; or that they were ignored, forgotten, or identified as spam, thereby lowering the response rate. So reminders were constantly sent to remind them fill the surveys. 3.15 Research Challenges Encountered

There were a number of challenges encountered by the researcher particularly during the data collection process.

Financial Challenges

To mitigate the financial challenge, the researcher obtained a scholarship from ADB- HEST

I thankfully own up the funding received towards this research from the AfDB- HEST project academic staff scholarship.

Sampling Challenges

In the sample screening process, the researcher noted that most commercial banks had their headquarters in Kampala and their branches concentrated in the central region, where also the capital city of Uganda, Kampala is located.

Thus, Kampala is the business center and most people would want the bank services. Since majority of business come from city dwellers because of close proximity with the capital city, therefore banks' branches in the central region had a higher propensity to use e- banking and Cyber security strategies than their other counter parts in up country bank branches in Uganda. This state of affairs caused disparities in the sample proportions.

7.2.6 Data collection Challenges

There were a number of limitations of the study like banking employees' time availability being limited.

Impacts of the closure of economic activities due to covid 19 pandemic was a big challenge. We could not send research assistants to the field, to ride on public transportation and go in and out of banking halls. The problem was the traditional way of delivering physical questionnaires could not be utilized for fear of physical contacts to spread and contract the covid 19 diseases. But there was still a need to get the information the survey was supposed to provide anyway. Thus, the study utilized and collected data using online questionnaires. This approach was extremely successful and ensured that majority of respondents who had to answer online questionnaires actually filled them.

Missing Data

Many times, surveys had blanks or unanswered questions. The majority of the missing responses were unintentional, but some were due to respondents misinterpreting the statement, believing it did not apply to them, or simply being too busy with other tasks to give the questionnaire enough time. The researcher had to follow up by phone to clarify these cases. As a result, respondents received enough justifications, particularly regarding the necessity for them to complete the entire questionnaire and why; but, in some instances, missing values were still included. Many respondents claimed to be busy but failed to complete the questionnaire in a timely manner, which caused delays in getting the completed forms back.

Non-Responsiveness

In some cases, respondents had doubts about the purpose of the study; some believed it was a scheme by the Bank of Uganda to gather private information about them. Additionally, a lot of employees don't appear to recognize the importance of research.

They think that research gives their rivals access to information about their business operations, which they would then use to undercut them. This justification led to a lot of non-responses and uncooperativeness. However, it must be noted that there was also a voluntary clause in filling out the questionnaire. In these circumstances, non-responses were minimized by assurances, particularly using the recommendation letter (see Appendix 3) and secrecy clause placed at commencement of the questionnaire.

The contextual of the respondents was that of banks' employees with knowledge of IT/IS and Cyber security professionals, they may not have had the advantage of being acquainted with knowledge of virtue ethics. Also, predominate mindset of the participants for addressing Cyber security issues was likely through the use of technical controls, which may have affected their consideration or acceptance of ethical concepts and solutions.

The study was intended for Cyber security professionals but it became difficult to target them specifically, thus their participation may have been under or over represented. this could have tilted the outcomes in a particular direction based on the viewpoint of the participants and not accurately representing the opinions of the entire information and Cyber security professionals' community. Despite some limitations, this study dependably makes important contributions, to theory, policy, as stated before.

7.3 Recommendations and Future Research

H1. This study found that virtue ethics were partially significant, and even the link between prudence and ethical behavior was insignificant. Yet the existing empirical literature proves that prudence are excellences of character, which involve getting things right, Harrison (2014). Thus Further studies on the direct influence of prudence on ethical behavior should be done to confirm the results.

H2. Was positively supported in the research model. The banking sector workers' temperence may encourage Cyber security moral behavior. Therefore, this research recommends that the banks should have a continuous assessment of their employees' temperance traits. Because where temperance is present the employees' ethics are clearly impacted on by enhancing their moralities and competence and this can help to improve the banks' Cyber security.

A web based Cyber security ethical behavior assessment model is of great prominence to banks' employees. However, the banks' employees' awareness of the existence of the system is required to help increase acceptance and execution of this model. This web based model can progressively be made known to the entire bank by the systems' administrator cooperating with all bank branch managers and heads of departments so as to create more awareness about its existence. In so doing Cyber security ethical behavior intention assessments could be a continuous process and be used to identify and address employees' unethical behavior towards Cyber security.

The developed model might be of help in identifying ethical virtue traits of a prospective new employee's background. This can provide insight as to whether the individual is ethically and morally well-grounded. This helps the recruitment panel to know that the person is a good fit for the bank into Cyber security related situations.

The banks are encouraged to implement this model and use it as a methodology to identify an employee's style of ethical decision making towards Cyber security.

The study's findings reveal that not only can employees' ethical behavior improve Cyber security but also creating an ethical working climate is another important way to improve Cyber security. The study recommends that the banks need to establish strong ethical climate to allow employees to continue observing ethical conduct among themselves. When the ethical climate is strong, employees experience a lesser amount of force to breach the banks' ethical principles.

The results of this study are of help to the managers, administrators, policy makers/stakeholders and Cyber security policy implementation committees in Ugandan banks, micro finance organizations, and finance ministry. The above leaders are encouraged to ensure proper and adequate assessment of employees with quick response that can create ethical behavior that enhances better Cyber security ethical decision making.

The banks are encouraged to apply procedures from this methodology to identify an employee's style of ethical decision making. Employing and maintaining more ethical employees may bring about a more ethical organizational environment. An individual's ethical behavior intentions and actual ethical behavior can result in a reduction in the likelihood of Cyber security violations.

Since this research investigated the influence of cardinal virtues upon employees' ethical behavior towards Cyber security, exploring the influence of other types of ethical theories upon the effectiveness of Cyber security may help banks understand better the relationship between ethics and Cyber security.

This research utilized cross sectional data to study the antecedents and influence of cardinal virtues, behavior intentions on Cyber security ethical behavior. Cross-sectional designs do not provide robust support for underlying effects between variables. Future studies should consider an investigation and assessment of the employees' ethical behavior towards Cybersecurity using longitudinal/ qualitative methods so as to verify the findings of the current study and extend the results.

Since the current study involved only commercial banks, a similar study should be extended to other financial businesses like microfinances. That study once undertaken would inform the regulating body of financial institutions how virtue ethical behavior varies between commercial banks and micro finances.

7.3.1 List of papers

7.3.1.1 The following papers were published from this work

1. Nakato, R., Kituyi, M. G., & Kaggwa, F. (2022). Ethical Climate: Analyzing the Moderation Effect on Cardinal Virtues and Employees' Cyber Security Ethical Behavior Intention in Ugandan Commercial Banks. *European Journal of Technology*, *6*(2), 49 - 61. https://doi.org/10.47672/ejt.1112
2. Nakato, R., Kituyi, M. G., & Kaggwa, F. (2022). Establishing the Influences of Cardinal Virtues on Employees' Cyber Security Ethical Behavior in the Banking Sector in Uganda. European Journal of Technology, 6(1), 1 - 13. https://doi.org/10.47672/ejt.896

REFERENCES

Abdelhamid A. (2008). Ontological, Epistemological and Methodological Assumptions: Qualitative Versus Quantitative 10 - 11May 2018 – Bosnia and Hercegovina / Sarajevo

Ait Maalem . R. L., et al. (2020), Review and insight on the behavioral aspects of Cybersecurity

Cybersecurity (2020) 3:10

Ameen. N., Tarhini. A. Mahmood. H. et al (2020), Employees' behavior intention to smartphone security: A gender based, cross national study. Computers in human behavior. Volume 104.

Ajzen, I. (1991). The theory of planned behavior, Organizational Behavior and Human Decision Processes, vol. 50, no. 2, pp. 179-211.

Ajzen, I. (1991). Theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179– 211.

Ajzen, I. (2001). Nature and operation of attitudes. Annual Review of Psychology, 52(1), 27-58.

Ajzen, I. (2002). Perceived behavioral control, self-efficacy, locus of control, and the theory of planned behavior. Journal of Applied Social Psychology, 32(4), 665-683.

Alexander N., Heather R., Bhattacharya, S., Achinto R. (2017). Ethical Climates in Organizations: A Review and Research Agenda. Business Ethics Quarterly vol. 27, issue 4, 475-512

Internet Governance Forum: 9 Nov 2019|Featured, Goal 9: industry, Innovation and Infrastructure, New technologies, Press material; We must act now to tackle the threats of cyberspace.

Ali, R.F.; Dominic, P.D.D.; Ali, S.E.A.; Rehman, M.; Sohail, A. (2021), Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. Appl. Sci. 11, 3383.

Al-Saadi, H. (2014). Demystifying Ontology and Epistemology in Research Methods, Health Care Chaplaincy, 20:4, 161-170.

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' Cybersecurity behaviors. Computers in Human Behavior, 69, 437-443.

Apvera (2018) The Essential Guide to Risk Management & Compliance (GRC). 2018, Tech. rep. Apvera

Aquinas.T.; (2005) The Cardinal Virtunes:Prudance,Justice,Fortitude,and Temperance;2005;Pg.159

Aristoles; Nicomachean Ethics;2011; Library of Congress; pg.29

Balarabe K. S. Y. (2012). Qualitative and Quantitative Approaches to the Study of Poverty: Taming the Tensions and Appreciating the Complementarities. The Qualitative Report, 17(20), 1-19. Retrieved from 18 April 2019

Banerjee, T. P. Cronan and Jones T. W. (1998) Modeling IT Ethics: A Study in Situational Ethics MIS Quarterly, Vol. 22, No. 1 pp. 31-60. M1anagement Information Systems Research Center, University of Minnesota

Bank of Uganda (31 March 2017). "List of Licensed Commercial Banks as At 31 March 2017" (PDF). Kampala: Bank of Uganda. Archived from the original (PDF) on 30 July 2017. Retrieved October 17, 2020.

Baron R.M. and Kenny, D.A. (1986). "The moderator–mediator variable distinction in social psychological research: conceptual, strategic, and statistical considerations", Journal of Behavior in an Information Technology

Bartunek J.M. and Jordi T. (2007). Individual ethics, The Virtue of Prudence; A Hand Book of Organizational and Managerial wisdom; Sage publications.

Bentham, J. (1907) An Introduction to the Principles of Morals and Legislation. Oxford: Clarendon Press.

Beyer, E. and Bradley J. B. (2015). Implementing Effective Cyber Security Training for End Users of Computer Networks SHRM-SIOP Science of HR Series.

Bhatt, C. and Pant, D. (2011). Study of Indian Banks Websites for Cyber Crime Safety Mechanism‖, International Journal of Advanced Computer Science and Applications, vol. 2, no.10, pp. 87-90.

Bhattacherjee. A. (2012) "Social Science Research: Principles, Methods, and Practices" Textbooks Collection.

Birtch, A. and Chiang, F. F. T. (2016). The Influence of Business School's Ethical Climate on Students' Unethical Behavior; J Bus Ethics 123:283–294

Bommer, M. G. C., Gravander, J., and Tuttle, M. (1987). A Behavioral Model of Ethical an Unethical Decision Making. Journal of Business Ethics, 6, 265-280.

Brennan (2017). Cybercrime and the 'Peelian Model' of Policing: A Literature Review

Brenner, J.M.W. (2017). (Hrsg.): Proceedings der 13. Internationalen Tagung Wirtschaftsinformatik St. Gallen, S. 1111-1125

Bryan (2016). An Empirical Investigation of Factors that Influence Individual Behavior Toward Changing Social Networking Security Settings; Journal of theoretical and applied electronic commerce research vol.11 no.2 Talca mayo 2016

Caldwell, Z. S., Smith H, (2015), Virtuous leadership – insights for the 21st century

Carter, A. and Crumpler, W D. (2019). Financial Sector Cyber Security Requirements in the Asia-Pacific Region; A Report of the CSIS Technology Policy Program

Centenary Bank (27 April 2019). "Annual Report for the Twelve Months Ended 31 December 2018" (PDF). Kampala: Centenary Bank. Retrieved 17 October 2020.

Chatterjee, S. Moody, G., P.B. Lowry, et al., Chatterjee, S. Gregory, M., Lowry, P. B. Suranjan C., & Andrew Hardin (2015). (2015) Strategic Relevance of Organizational Virtues Enabled by Information Technology in Organizational Innovation, Journal of Management Information Systems, 32:3, 158-196,

Chilisa B. and B. Kawulich (2009), CHAPTER 3 Selecting a research approach: paradigm, methodology and methods.

Cronan T. P., and Douglas D. E., Information Technology Ethical Behavior: Toward a Comprehensive Ethical Behavior Model EDITORIAL PREFACEd

Cronan, T.P., Foltz, C. and Jones, T.W. (2006). Piracy, computer crime, and IS misuse at the university, Communications of the ACM, vol. 49, no. 6, pp 84-90.

Crotty, M. (2003): The Foundations of Social Research: Meaning and Perspectives in the Research Process, London: Sage Publications, 3rd edition, 10.

Cullen, B., Victor, B. and Bronson J. W. (1993). The Ethical Climate Questionnaire: An Assessment of its development and validity. Psychological Reports, 73, 667-674.

D. Langston (2014), What's Justice got to do with it? International Journal of Philosophy and Theology, Vol. 2, No. 4, pp. 45-59

Dark, D. L. & Rix, M. (2015). Back to the future: using the ethical climate questionnaire to understand ethical behaviour in not for profits. Asia Pacific Journal of Health Management, 10 (3), S122-S131.

Dawson J and Thomson R (2018), The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance. Front. Psychol. 9:744.

Dieronitou, I. (2014). The Ontological and Epistemological Foundations of Qualitative and Quantitative Approaches to Research with Particular Reference to Content and Discourse Analysis of Textbooks, International Journal of Economics, Commerce and Management United Kingdom Vol. II, Issue 10.

Dinc, S. (2018). Linking Ethical Climate to Employee Behaviors: An Empirical Study in Banking Sector.

Dow, K. E., Wong, J., Jackson, C., & Leitch, R. A. (2008). A comparison of structural equation modeling approaches: The case of user acceptance of information systems. *Journal of Computer Information Systems, 48*(4), 106-114.

Alaney J. Mc (2018). Behavior Change: Cyber security; The British Psychological Society Promoting excellence in psychology.

Burney S. M. A. (2008) INDUCTIVE & DEDUCTIVE RESEARCH APPROACH

Manisha, M. M., Meenakshi P.J. & K.M. Nalawade. (2015) Online Banking and Cyber-attacks: The current Scenario‖, International Journal of Advanced Research in Computer Science and Software Engineering, vol. 5, no. 12, pp. 743-749.

Dupont, B. (2019). The Cyber-resilience of financial institutions significance and applicability Journal of Cyber security, 2019, Vol. 5, No. 1

Ebede, O. Shaffakat, S., Scott, F. (2019). A Multilevel Model Examining the Relationships Between Workplace Spirituality, Ethical Climate and Outcomes: A Social Cognitive Theory Perspective

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Publisher: Todd Green

Edirisingha P. (2012), Research Paradigms and Approaches; Interpretivism and Positivism (Ontological and Epistemological Perspectives).

ENISA European Union Agency for Network and Information Security (2018) Cyber security Culture Guidelines: Behavioral Aspects of Cyber security; field study in banking sector in the city of Tokat. Turkish Journal of Business Ethics, 9, 131–152.

Floridi L. (2006) "Information ethics, its nature and scope," in Moral Philosophy and Information Technology, J. van den Hoven and J. Weckert, Eds. Cambridge: Cambridge University Press.

FinScope (2018) Report on banking and the status of financial inclusion in Uganda: Insights from FinScope 2018 Survey

Friedrich, T., Schlauderer, S., Weidinger, J. Raab, M. (2017). On the Research Paradigms and Research Methods Employed in the BISE Journal - A Ten-Year Update, in Leimeister,

Gana, N., Abdulhamid, S. M. and Ojeniyi J. A. (2019). security Risk Analysis and Management in Banking Sector: A Case Study of a Selected Commercial Bank in NigeriaI.J. Information Engineering and Electronic Business, 2, 35-43

Garretta B.M and Cutting R. L (2015). Ways of knowing: realism, non-realism, nominalism and a typology revisited with a counter perspective for nursing science Nursing Inquiry 22(2): 95–105

Ghosh, K. 2015. Benevolent leadership in not-for-profit organizations. ***Leadership & Organization Development Journal***, 36(5): 592–611.

Gray, J. .M (2015). Virtue Ethics: Examining Influences on the Ethical Commitment of Information System Workers in Trusted Positions. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (364)

Gray, J. M., and Tejay. G. (2014). Development of virtue ethics based security constructs for information systems trusted workers. Proceedings of the 9th International Conference on Cyber Warfare and Security (ICCWS-2014), West Lafayette, IN, USA, 256-264.

Gray, J.M. and Tejay, G.P.S. (2020) 'Introducing virtue ethics concepts into the decision processes of information systems trusted workers: a Delphi study', Int. J. Information and Computer Security, Vol. 12, No. 1, pp.1–19.

Guba, E. G., & Lincoln, Y. S. (1982). Epistemological and methodological bases of naturalistic inquiry. ECTJ, 30(4), 233–252.

Habibi, A. Sarafrazi, S. I (2014). Delphi Technique Theoretical Framework in Qualitative Research the International Journal of Engineering and Science (IJES) Volume 3 Issue 4 |Pages 08-13

Hackett, R. D., G. Wang, (2012),"Virtues and leadership: An integrating conceptual framework founded in Aristotelian and Confucian perspectives on virtues", Management Decision, Vol. 50 Iss: 5 pp. 868 – 899

Hadlington, L. (2017). Human factors in Cyber security; examining the link between Internet addiction, impulsivity, attitudes towards Cyber security, and risky Cyber security behaviours. Heliyon 3 e00346.

Hamburg, I., & Grosch, K. R. (2017). Ethical Aspects in Cyber Security. Archives of Business Research, 5(10), 199-206

Hair, J. F. J., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). Multivariate Data Analysis: A global perspective. Upper Saddle River, NJ: Pearson Prentice-Hall.

Harrison, T. J. (2014). Does the Internet Influence the Character Virtues of 11 to 14 year olds in England? A mixed method study with particular regard to Cyber-bullying; dissertation PhD level. University of Birmingham

Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. computers & security 83 354-366.

Basel. H., (2019). A Conceptual Framework for Mobile Security Supporting Enterprises in Adopting Mobility. PhD thesis. Doktors der Ingenieurwissenschaften (Dr.-Ing.) Carl von Ossietzky Universität Oldenburg

Hatfield. M. (2018) "Cybersecurity and Tax Reform," *Indiana Law Journal: Vol. 93*: Iss. 4, Article 6.

Hatfield J. (2018) Social Engineering in Cybersecurity: The Evolution of a Concept of social engineering in Cybersecurity. *Computers and Security* 73:102-113

Hawking, M. Curlin, F. A., and Yoon J. D. (2017). Courage and Compassion: Virtues in Caring for So-Called "Difficult" Patients Journal of Ethics Volume 19, Number 4: 357-363 AMA.

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design Science in Information Systems Research. *MIS Quarterly, 28, 75–105.*

Hevner, A. R., & Chatterjee, S. (2010). Design Research in Information Systems (Vol. 22). Boston, MA: Springer US.

Hooper, D., Coughlan, J., & Mullen, M. R. (2008). Structural equation modelling: Guidelines for determining model fit. *Electronic Journal of Business Research Methods, 6* (1), 53-60.

Ifinedo, I. (2012). Effects of organization insiders' self-control and relevant knowledge on participation in information systems security deviant behavior.

Jafarkarimi, H., Saadatdoost, R., A T. H. Sim, J. Mei. (2015). Determinant Factors of Cyberbullying: An Application of Theory of Planned Behavior Information and Computer Security; Journal of Theoretical & Applied Information Technology 95 (23), ISSN: 2056-4961.

Jarvis, C. B., MacKenzie, S. B., & Podsakoff, P. M. (2003). A critical review of construct, Journal of Internet Banking and Commerce, June 2018, vol. 23, no. 2

Kauthamy, K., Ashrafi, N. and Kuilboer, J.P. (2017). Mobile Devices and Cyber Security - An Exploratory Study on User's Response to Cyber Security Challenges. In Proceedings of the 13th International Conference on Web Information Systems and Technologies (WEBIST 2017), pages 306-311

Kazmi, J., Alghazo M., Latif G. (2017). Cyber Security Analysis of Internet Banking in Emerging Countries: User and Bank perspectives

Kearney, W.D. and Kruger, H.A. (2016). Can perceptual differences account for enigmatic information security behaviour in an organisation? Computers & Security 61, 46–58.

Ki, S. and Ahn, S. (2006). A study on the methodology of information ethics in youth. International journal of computer science and network security, vol 6 No 6 Kivunja, C. and A. B. Kuyini, (2017). Understanding and Applying Research Paradigms in Educational Contexts. International Journal of Higher Education Vol. 6, No.

Klima G. (2013). The medieval problem of universals. In The Stanford encyclopedia of philosophy (Fall 2013 edn) ed.

Khan, N.F., Ikram, N., Saleem, S. *et al.* Cyber-security and risky behaviors in a developing country context: a Pakistani perspective. *Secur J* (2022). https://doi.org/10.1057/s41284-022-00343-4

Korovessis, P., Furnell, S., Papadaki, M. Haskell-Dowland, P. (2017)."A modelkit approach to information security awareness and education," Journal of Cyber Security Education, Research and Practice: No. 2, Article 5.

Kost. E. (2022) 10 Biggest Data Breaches in Finance, UpGuard's weekly data breach and cybersecurity newsletter.

Krauss, S. E. (2005). Research Paradigms and Meaning Making: A Primer. The Qualitative Report, 10(4), 758-770.

Krejcie, R.V., & Morgan, D.W., (1970). Determining Sample Size for Research Activities. Educational and Psychological Measurement. 30, 607-610.

Kuenzi, et al., (2019) Creating an ethical organizational environment: The relationship between ethical leadership, ethical organizational climate, and unethical behavior; Personnel Psychology. 1–29. Wiley Periodicals, Inc.

Kuepper, (2019) Bank Fraud effects on the banking industry, customers and the economy Cyberattacks and Bank Failures

Lau, V. P., & Wong, Y. Y. 2009. Direct and multiplicative effects of ethical dispositions and ethical climates on personal justice norms: A virtue ethics perspective. ***Journal of Business Ethics***, 90(2): 279–294.

Leung, (2018) Cyber security regulation in the banking sector: global emerging themes. The London School of Economics and Political Science. Research gate.

Linstone, H.A. and Turoff, M. (eds.) (1975) the Delphi Method Techniques and Applications, Massachusetts, Reading: AddisonWesley.

"List of Branches of Barclays Bank Uganda". Barclays Bank Uganda. Retrieved 17 october 2020

Loch, K. D., Conger S., (1996), Evaluating ethical decision making and computer use, Communications of the ACM 39 (7), pp. 74–83.

Löfquist, L. (2018). Virtue Ethics and Disasters. In: O'Mathúna D., Dranseika V., Gordijn B. (eds) Disasters: Core Concepts and Ethical Theories. Advancing Global Bioethics, vol 11. Springer, Cham

Lori N.K. Leonarda., Timothy. P. C., Kreiec. J,. (2004). What influences IT ethical behavior intentions—planned behavior, reasoned action, perceived importance, or individual characteristics? Information & Management 42 (2004) 143–158

Lori,N.K., Timothy, L., and Cronan P. (2005). Attitude toward ethical behavior in computer use: a shifting model. Industrial Management & Data Systems Vol. 105 No. 9, pp. 1150-1171

Loukaka, S. and Rahman S. M., (2017). Discovering New Cyber Protection Approaches from a Security Professional Prospective. International Journal of Computer Networks & Communications (IJCNC) Vol.9, No.4,

Lowry, B., Posey, C., Roberts, T. L. Rebecca, J. B. (2013). "Is your banker leaking your personal information? The roles of ethics and individual-level cultural characteristics in predicting organizational computer abuse," Journal of Business Ethics pp. 302-27.

Moses Owiny, (2023) Technical Advisor, Digitalisation. GIZ Uganda

D. Ochieng Otieno (2020), Cyber security challenges: The Case of Developing Countries

Enhancing Cybersecurity in Least Developed Countries. Master's thesis, School of Informatics and Innovative Systems, Jaramogi Oginga Odinga University of Science and Technology

M. Cacacho (2021), Cyber security policy in developing countries: Rowing in an unfamiliar world without a paddle; Senior Security Engineer, 15 October 2021

Maalem Lahcen, R.A., Caulkins, B., Mohapatra, R. *et al.* Review and insight on the behavioral aspects of cybersecurity. *Cybersecur* **3,** 10 (2020). https://doi.org/10.1186/s42400-020-00050-w

MacKenzie, S. B., Podsakoff P. M., Podsakoff N. P. (2011). Construct Measurement and Validation Procedures in MIS and Behavioral Research: Integrating New and Existing Techniques June MIS Quarterly 35(2):293-334

Malaba, T. (2018). When BoU officials connived with criminal to defraud bank. daily monitor newspaper of Sunday April 15 2018.

Malik, S., Shazia, N., Awan, A. G. (2018), The Impact of Cybercrimes on the Efficiency of Banking Sector of Pakistan Global journal of management, social sciences and humanities Vol 4 (4), pp. 821-842.

Manishimwe, (2018) Cyber-crimes on the rise, experts call for skilling; the new vision Uganda's popular newspaper 25th April 2018.Written by URN

Marilyn C Morris and Jason Z Morris (2016), The importance of virtue ethics in the IRB Research Ethics Vol. 12(4) 201–216

Matovu, A. (2018). Electronic Fraud and performance of Retail Banking in Uganda: A Case Study of Centenary Bank limited Mapeera House. Masters level. Nkumba University

McQueen, P. and McQueen, H. (2010) Key Concepts in Philosophy Basingstoke: Palgrave MacMillan

Mihaela.M., Rodica-Doina. D., Luminiţa. H. (2022). The 8th International Conference on Information Technology and Quantitative Management (ITQM 2020 & 2021). Applying Design Science Research for Developing Business artifacts. *Procedia Computer Science 199 (2022) 637–642.*

Morgan G. and Gordijn B. (2019). A Care-Based Stakeholder Approach to Ethics of Cyber security in Business. Chapter 6; Institute of Ethics, Dublin City University, Dublin, Ireland. G.J. C.M.P., Vol. 2(3) 2013:132-135 ISSN: 2319 – 7285

Mulki, J. P., Jaramillo, F., & Locander, W. B. 2006. Effects of ethical climate and supervisory trust on salesperson's job attitudes and intentions to quit. ***Journal of Personal Selling & Sales,*** 26: 19–26.

Mugisa M. B. (2019), Towards a Cyber-secure Uganda's banking industry – a presentation to CEOs of financial institutions in Uganda, at an event organized by the Uganda Bankers Association.

Mumcu, A., and Döven, M. S. (2016). Ethical climate and its relationship with perceived organizational justice: A field study in banking sector in the city of Tokat. Turkish Journal of Business Ethics, 9, 131–152.

Muncaster, P. (2015). Finance Hit by 300 Times More Attacks Than Other Industries.

Niehaves, B. (2007). On Epistemological Diversity In Design Science – New Vistas For A Design-Oriented IS Research.

Newman. A., Heather R., S. Bhattacharya., Achinto R. (2017) Ethical Climates in Organizations: A Review and Research Agenda; Business Ethics Quarterly 27:4 (October 2017) pp. 475–512.

Norshima, H. and Balakrishnan, V. (2017). Indirect effect of management support on users' compliance behavior towards information security policies. Health Information Management Journal. Vol. 47(1) 17–27

Nussbaum M, Sen A. (1993) eds. The Quality of Life. Oxford, England: Clarendon Press.

O'Mathúna, D. P., Dranseika, V., Gordijn, B. (Eds.), (2018). Disasters: Core Concepts and Ethical Theories, Advancing Global Bioethics 11,

Ocholla, D. (2008) Information Ethics Education in Africa. Where do we stand? for the CIPR/SOIS "Thinking Critically: Alternative Perspectives and Methods in Library and Information Studies" conference in Milwaukee, Wisconsin. USA.

Ojeka, Ojeka, S. Ojeka, A., Egbide, B-C., Edara-Obong I. E., (2017) Cyber Security in the Nigerian Banking Sector: An Appraisal of Audit Committee. Effectiveness International Review of Management and Marketing | Vol 7 Issue 2

Oliveira, S. D. and Stickings, A. (2016). Financial Institutions and Cybercrime: Threats, Challenges and Opportunities RUSI News brief Cybercrime Vol. 36, No. 4

Park, Y., Konge, L., & Artino, A. R. (2020). The Positivism Paradigm of Research. Academic medicine: journal of the Association of American Medical Colleges, 95 (5). http://dx.doi.org/10.1097/ ACM.0000000000003093

Paulinus W. I, D. Eaton (2013). The Pragmatic Research Approach: A Framework for Sustainable Management of Public Housing Estates in Nigeria. Journal of US-China Public Administration, ISSN 1548-6591 October 2013, Vol. 10, No. 10, 933-944

Papouli, E. (2018). Aristotle's virtue ethics as a conceptual framework for EN Zalta. for EN Zalta. http://plato.stanford.edu/archives/fall2013/

Peffers K., Tuure T., Rothenberger M.A, and Chatterjee S., (2007). A design science research methodology for information systems research. *Journal of management information systems,* 24(3):45–77, 2007.

Perera, S. (2018). Research Paradigms Workshop on Research Methodology. Department of Demography, University of Colombo

Pham, H-C., Brennan, L., & Richardson. J. (2017). Review of behavioral theories in security compliance and research challenges. Proceedings of the Informing Science and Information Technology Education Conference, Vietnam, pp. 65-76. Santa Rosa, CA: Informing Science Institute.

Ping A. W. (2013). Assessment of Cyber Security Knowledge and Behavior: An Anti-Phishing Scenario: The Eighth International Conference on Internet Monitoring and Protection ICIMP

Pisk J. (2017). The role of cardinal virtues in sport; Philosophic Reflections in Sport; A Collection of Essays E-book published by: SPOLINT Institute, International Institute for Sustainable Development, Policy, and Diplomacy in Sport Slovenia

Pollet T. V. & van der Meij, L. (2017), To Remove or not to Remove: the Impact of Outlier Handling on Significance Testing in Testosterone Data Adaptive Human Behaviour and Psychology. 3(1), 43-60.

Ponelis, S. R. (2015). Using interpretive qualitative case studies for exploratory research in doctoral studies: A case of Information Systems research in small and medium enterprises. International Journal of Doctoral Studies, 10, 535-550.

Pring, R., (2004), Philosophy of Educational Research, 2nd ed. London: Continuum, p.40.

Ralf S. (2012). Personality, human development, and culture: international perspectives on psychological science. Hove: Psychology. pp. 127–129. ISBN 978-0-415-65080-9.

Rao, S. (2019). "CYBER CRIME IN BANKING SECTOR." International Journal of Research - Granthaalayah, 7(1), 148-161.

Reddy, L., Bhargavi V. (2018). Cyber security attacks in banking sector: Emerging security challenges and threatsAmerican International Journal of Research in Humanities, Arts and Social Sciences21(1) pp. 65-71

Rehman, A., and Alharthi, K. (2016). An Introduction to Research Paradigms; International Journal of Educational Investigations

Riggio, R. E., Zhu, W., Reina, C., Maroosis, J. A. (2010). Virtue-Based Measurement of Ethical Leadership: The Leadership Virtues Questionnaire, Consulting Psychology Journal: Practice and Research American Psychological Association, Vol. 62, No. 4, 235–250

Russu, C. (2022), The impact of low cyber security on the development of poor nations | Experts' Opinions. DevelopmentAid

Sabiu, M. S., Mei T. S. and Joarder H. R. (2016). Moderating Role of Ethical Climates on HRM Practices and Organizational Performance: A Proposed Conceptual Model Mediterranean Journal of Social Sciences Vol 7 No 1. MCSER Publishing, Rome-Italy

Sabiu, M., Ringim, K., Mei, T. and Joarder, M. (2019), "Relationship between human resource management practices, ethical climates and organizational performance, the missing link: An empirical analysis", PSU Research Review, Vol. 3 No. 1, pp. 50-6

Safa, N. S., Safa, S., Rossouw, V. S., Sookhak, M., Ghani, N., Tutut, H., Furnell, S. (2015). Information security conscious care behavior formation in organizations; computers & security 53: 65-78

Sang, H. K., Kyung H. Y., and Sunyoung, P. (2014). An Integrative Behavioral Model of Information Security Policy Compliance Hindawi Publishing Corporation. ***Scientific World Journal*** Volume 2014, Article ID 463870, 12 pages.

Shafer, W. E., Poon, M. C. C., & Tjosvold, D. 2013a. An investigation of ethical climate in a Singaporean accounting firm. ***Accounting, Auditing & Accountability Journal***, 26(2): 312–343.

Shamsudin, N. N. A., Yatin, S. F. M., Nazim, N. F. M., Talib, A. W., Sopiee, M. A. M., & Shaari, F. N. (2019). Information Security Behaviors among Employees. International Journal of Academic Research in Business and Social Sciences, 9(6), 560–571.

Shah, S. R., and Al-Bargi, A. (2013), Research Paradigms: Researchers' Worldviews, Theoretical Frameworks and Study Designs; AWEJ Volume.4 Number.4, 2013 ; Pp. 252 -264

Sheikh, A. A. (2017). Cyber Security Framework, Saudi Arabian Monetary Authority Version 1.0 and Compatible Methods ("All but Dissertation" (ABD) Doctoral Candidate in Tesol)

Smith, B. and Ceusters W. (2010). Ontological realism: A methodology for coordinated evolution of scientific ontologies; Appl Ontol. 15; 5(3-4): 139–188,

Sniehotta, F.F., Scholz, U., Schwarzer, R., 2005. Bridging the intention–behaviour gap: planning, self-efficacy, and action control in the adoption and maintenance of physical exercise. Psychol. Health 20 (2), 143–160.

Stückelberger, c., and Duggal, P. (2018). Cyber Ethics 4.0: Serving Humanity with Values, Geneva: Globethics.net.

Sutirtha, C., Valacich, J. S., Suprateek, S. (2012), Unethical Use of Information Technology: A Two-Country Study the study and practice of social work in modern times, European Journal of Social Work.

T. J. Harrison (2014), Does the Internet Influence the Character Virtues of 11 to 14 year olds in England? A mixed method study with particular regard to Cyber-bullying. PhD thesis. University of Birming

Tanner, E. C., Tanner, J. F., & Wakefield, K. 2015. Panacea or paradox? The moderating role of ethical climate. ***Journal of Personal Selling & Sales Management***, 35(2): 175–190

Tangen. K. I. (2015), The Need for Temperance On Organizational Leadership and Temperance SJLT 2.

Tariq, N. (2018). Impact of Cyber-attacks on Financial Institutions; Journal of Internet Banking and Commerce vol. 23, no.

Terlizzi, M. A,. Meirelle. F. de S., and Cortez da Cunha. M. A. V., (2017). Behavior of Brazilian Banks Employees on Facebook and the Cybersecurity Governance. JOURNAL OF APPLIED SECURITY RESEARCH 2017, VOL. 12, NO. 2, 224–252

Tommasetti, P. Singer, Orlando T. et al., (2018). Extended Theory of Planned Behavior (ETPB): Investigating Customers' Perception of Restaurants Sustainability by Testing a Structural Equation Model Sustainability, 10, 2580;

Tumuhimbise, W., Atwine, D., Kaggwa, F. et al. Enhancing Tuberculosis Care in Southwestern

Uganda: Facilitators and Barriers to Utilizing Mobile Health Technologies. Glob Implement Res Appl (2022). https://doi.org/10.1007/s43477-022-00056-1.

Tushabe, F. and Baryamureeba, V. (2007). Cyber Crime in Uganda: Myth or Reality? (Version 5247).

Uffen. J. and Breitner M.H (2013). Management of technical security measures: an empirical examination of personality traits and behavioral intentions. System Sciences (HICSS), 2013 46th Hawaii International Conference on. IEEE

Uppström,E. (2014). The Promise of Public Value CoCreation in Open Government Designing IT Services for Open Government and Public Value Co-Creation

Vaishnavi, V., Kuechler, W., and Petter, S. (Eds.) (2004/19). "Design Science Research in Information Systems" January 20, 2004 (created in 2004 and updated until 2015 by Vaishnavi, V. and Kuechler, W.); last updated (by Vaishnavi, V. and Petter, S.), June 30, 2019.

VanSandt, C. V., Shepard, J. M., &. Zappe, S. M. 2006. An examination of the relationship between ethical work climate and moral awareness. ***Journal of Business Ethics***, 68(4): 409–432.

Veksler VD, Buchler N, Hoffman BE, Cassenti DN, Sample C and Sugrim S (2018) Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users. Front. Psychol. 9:691.

Wahyuni, D. (2012). The research design maze: understanding paradigms, cases, methods and methodologies, Journal of applied management accounting research, vol. 10, no. 1, Winter 2012, pp. 69-80.

Waithaka, S. (2016), Factors Affecting Cyber Security in National Government Ministries in Kenya. Masters level. University of Nairobi.

WaterISAC (2015). 10 Basic Cyber security Measures Best Practices to Reduce Exploitable Weaknesses and Attacks.

Weber. Rolf H. (2016) ETHICS IN THE INTERNET ENVIRONMENT ***Global Commission on Internet Governance***, PAPER SERIES: NO. 39 — JULY 2016

Wieringa, R. J. (2014), Design science methodology for information systems and software engineering, Springer.

Williams, A., Billington, T., & Goodley, D. (2015). Critical Educational psychology. London: Wiley Blackwell.

Willison, R. (2006). Understanding the Perpetration of Employee Computer Crime in the Organizational Context Working paper no. 04 – 2006

Willison, R.; Warkentin, M.; Johnston, A.C. (2018) Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. Inf. Syst. J., 28, 266–293.

Yoon, C. and Kim, H. (2013). "Understanding computer security behavioral intention in the workplace: An empirical study of Korean firms", Information Technology & People, Vol. 26 No. 4, pp. 401-419.

Zahoor, Z., Ud-din, Moin., Sunami, K. (2016). Challenges in Privacy and Security in Banking Sector and Related Countermeasures. International Journal of Computer Applications (0975 – 8887) Volume 144 – No.3.

Zhou, T. T. and M. J. Noyes. (2016). Teachers and technology: Development of an extended theory of planned behavior. Educ. Technol. Res. Dev. 64, 1033–1052

Ononye T. G. (2017). An Appraisal of the Legal Framework on Cyber Fraud in Uganda. Kampala International University Kampala, Uganda

ETUKURI . C SATURDAY VISION February 4, 2017. SPECIAL REPORT; Banks lose sh20b to fraud annually STAFF COLLUDE WITH CRIMINALS TO STEAL AND KILL THE UNSUSPECTING CLIENTS

7.5 Appendices

7.5.1 Appendix A

Table 7. 1 Determining Sample Size from a Given Population.

N	S	N	S	N	S
10	10	220	140	1200	291
15	14	230	144	1300	297
20	19	240	148	1400	302
25	24	250	152	1500	306
30	28	260	155	1600	310
35	32	270	159	1700	313
40	36	280	162	1800	317
45	40	290	165	1900	320
50	44	300	169	2000	322
55	48	320	175	2200	327
60	52	340	181	2400	331
65	56	360	186	2600	335
70	59	380	191	2800	338
75	63	400	196	3000	341
80	66	420	201	3500	346
85	70	440	205	4000	351
90	73	460	210	4500	354
95	76	480	214	5000	357
110	86	550	226	7000	364
120	92	600	234	8000	367
130	97	650	242	9000	368
140	103	700	248	10000	370
150	108	750	254	15000	375
160	113	800	260	20000	377
170	118	850	265	30000	379

180	123	900	269	40000	380
190	127	950	274	50000	381
200	132	1000	278	75000	382
210	136	1100	285	1000000	384

N is population size. S is sample size.

Adopted from Krejcie, R.V., & Morgan, D.W., (1970)

7.5.2 Appendix B

Table 7. 2 Study population.

No	**Bank**	**Number of employees**	**Headquarters:**	**reference**
1	Stan Bic bank	1,667	Kampala	Stanbic Uganda Holdings Limited Annual Report (2019)
	DFCU bank	1,200 (2018)	Kampala	Website,www.dfcugroup.com.
	Centenary bank,	2,792 (2018)	Mapeera House in Kampala City	www.centenarybank.co.ug
	Standard chattered bank,	600+ (2018)	5 Speke Road, Kampala, Uganda	www.sc.com/ug
	ABSA bank,	850 (2014)		www.absa.co.ug/
	Bank of Baroda	188 (2011)	18 Kampala Road Kampala, Uganda	www.bankofbaroda.ug
	Citi bank Uganda	400 (2020)	Nakasero Kampala	www.citigroup.com/
	Equity bank,	700 (2020)		equitygroupholdings.com/ug/

			Janani Luwum Church House, at 34 Kampala Road,	
	Bank of Africa-Uganda LTD.	448 (2018)	45 Jinja Road, Kampala	website boauganda.com
	Total	**8385**		

7.5.3 Appendix C; Survey Instrument

An Employees' Cyber Security Ethical Behavior, ethical Climate and Influences Survey.



Dear Respondent,

I am a doctoral student at Mbarara University of science and Technology. I am conducting a study about "***Assessing the Employees' Ethical Behavior Towards Cyber security.***"

Cyber security are all the technologies, processes and practices designed to protect networks, computers, programs, people and data from attack, damage, injury or unauthorized access.

The aim of this study is to enhance Cyber security performance by developing a model that will guide managers to comprehend well the problem of Cyber security violations in order to prevent employees' unethical behavior towards Cyber security.

The purpose of this questionnaire is to solicit your input on cardinal virtue constructs, and ethical climate for Banks employees. You have been carefully chosen to voluntarily participate in this survey by filling in the survey form. Your responses will be treated with utmost confidentiality and shall be used for academic purposes only. I shall be so glad to share our findings with interested participants. Please let us know by sending an e-mail to rnakato@must.ac.ug.

Kindly complete and submit the survey to the researcher as soon as possible.

Thank you for accepting to participate in this survey.

7.5.3.3 SECTION A: BACKGROUND INFORMATION

7.5.3.4 Part I: Demographic data and professional characteristics of participants

Please tick your gender.

Female	Male

Select your age group?

Below 20 years	
20-29 years	
30-39 years	
40-39 years	
5o and above	

What bank in Kampala or Mbarara are you working from?

Stanbic bank	
Centenary bank	
DFCU bank	
Post bank	
Equity bank	
ABSA bank	

What is your highest level of education?

Certificate	
Diploma	
Bachelors	
Post graduate diploma	
masters	
PhD	
Others specify	

Please tick your area of specialty.

Software engineering	
information systems	
information technology	
Computer science	
Data communication	
Other specify	

Are you presently working directly in the information system security field?

Yes	No

Which of the following job titles or categories best describes your current professional role?

IT Department Head,	
IT Division Head, or IT Manager	
Information Security Specialist	
IT Specialist	
Information Systems, or Systems administrator	
Web designer	
Computer science, software engineering or IT Student	
Others specify	

How many years of information system security experience do you have?

1-5	
6-10	
11-15	
16-20	
21 and above	

7.5.3.5 Section Two: Cardinal Virtue Constructs

1.To examine the extent to which cardinal virtue constructs can influence the behavioral intention of organizational employees towards Cybersecurity ethical behavior in Uganda.

This section considers the cardinal virtue constructs of; Prudence, courage, justice, and temperance that should be possessed by Cyber security employees.

A. The following is a list of items related to Cyber security prudence ("skill in making assessments and in the application of professional knowledge, experience, understanding, common sense, or insight in regards to Cyber security."

Please indicate your level of agreement that the following items or statements are applicable elements of Cyber security prudence:

Strongly Disagree (1); Disagree (2), Not Sure (3); Agree (4); Strongly Agree (5)						
No	**Prudence in Cybersecurity**	**1**	**2**	**3**	**4**	**5**
PR1	Performing ethically correct choices is considered a moral and good computer behavior.					
PR2	Unbiased decision making by organizational workers can impact their information system security submission					
PR3	An aptitude to make judgments based on professional understanding contributes to Cybersecurity.					
PR4	Workers awareness of the suitable use of Cybersecurity strategies can affect the Cybersecurity.					
PR5	A person's aptitude to resolve conflicts between organizational policies and goals can impact the security of an information system.					
PR6	Cybersecurity is affected by the workers practical expertise					
PR7	Dependable conduct is a requirement when a worker performs safety actions in Cybersecurity.					
PR8	Being able to recognize ethical issues has no effect on information system security. (R)					

B. Below is a list of items associated to the virtue of temperance that is explained as; individual modesty, self-control, and the ability to regulate sentiments and actions that affect decisions regarding Cybersecurity.

Please indicate how much you agree or disagree with the following responses about the virtue of temperance:

Strongly Disagree (1); Disagree (2), Not Sure (3); Agree (4); Strongly Agree (5)						
NO	**Temperance in Cybersecurity**	**1**	**2**	**3**	**4**	**5**
TEMP1	Information system security compliance is not affected by a person's attitudes and beliefs. (R)					
Temp2	Employee professionalism promotes Cybersecurity.					
TEMP3	Employees enhance Cybersecurity compliance by making rational decisions.					

C. The presented items are connected to justice which is defined as;

Being sensitive to the rights of others and acting fairly and responsibly towards individuals, organizations, and communities.

Please indicate how much you agree or disagree with the following responses about the virtue of Justice:

Strongly Disagree (1); Disagree (2), Not Sure (3); Agree (4); Strongly Agree (5)						
No	**Justice**	**1**	**2**	**3**	**4**	**5**
JUS1	Public responsibility and community participation are not elements of ethical computer behavior. (R)					
JUS2	There is no relationship between Cybersecurity ethical behavior and protection of sensitive information. (R)					
JUS3	Cybersecurity ethical behavior involves making decisions that may affect society.					
JUS4	The employees' Ethical use of Cyber assets is not significant to an organization as long as business goals are achieved. (R)					
JUS5	Being sensitive to loss of information system data is a computer ethics related issue.					

D. The following items are related to the virtue of courage, which is defined as;

Personal honesty and determination to make ethically correct or unpopular decisions regarding Cyber security that affect decisions concerning adherence.

Please indicate your level of agreement that the following items are applicable elements of courage.

Strongly Disagree (1); Disagree (2), Not Sure (3); Agree (4); Strongly Agree (5)						
No	**courage**	**1**	**2**	**3**	**4**	**5**
CO1	Cyber security ethics involves making self-determinations rather than making choices expected by others.					
CO2	A focus on one's personal desires over the greater good is an example of good computer ethics. (R)					
CO3	Making correct judgments contributes to Cyber security strategies compliance.					
CO4	Regarding Cybersecurity, when employees commit unethical act they will try to justify to themselves that their behavior is acceptable.					

E. Behavioral intentions towards Cyber security

What is your level of agreement that the following items are indicators of ethical behavior intentions? (defined as the desire and likelihood of the individual to perform Cyber security ethical behavior).

No	**Strongly Disagree (1); Disagree (2), Not Sure (3); Agree (4); Strongly Agree (5)**						
	Behavioral intentions towards Cyber security (BI)	1	2	3	4	5	
BI1	I will take measures to protect information and computer assets from Cyber security violations						
BI2	I will take precautions against computer Cyber security violations.						
BI3	I intend to actively use Cyber security technologies.						

F. ethical behavior towards Cybersecurity

The following is a list of items that may be considered to be examples or results of employee ethical behavior in regards to Cybersecurity.

What is your level of agreement that the following items are indicators of ethical behavior?

Strongly Disagree (1); Disagree (2), Not Sure (3); Agree (4); Strongly Agree (5)						
No	***Cybersecurity Ethical behavior***	**1**	**2**	**3**	**4**	**5**
CEB1	Employees follow organizational policies and rules when making decisions regarding Cyber security.					
CEB2	Employees exhibit concern with the well-being of the organization by protecting organizational Cyber information and other Cyber assets					
CEB3	An organization experiencing a reduction in the number of events involving loss or compromise of information is an indicator of employee ethical behavior.					
CEB4	An example of ethical behavior is when employees feel uncomfortable in disclosing security issues if they believe that other employees or the organization may disagree with them. (R)					
CEB5	In the absence of specific organizational guidance employees may deviate from information system security best practices. (R)					

7.5.3.6 Section three: ETHICAL CLIMATE QUESTIONNAIRE

To analyze the moderation effect of ethical climate on the virtue constructs in connection with influencing the behavioral intention of organizational employees towards Cybersecurity ethical behavior in Uganda.

INSTRUCTIONS TO OBSERVERS:

This section contains some questions about the general climate in your company (or other unit reference). Please answer the following in terms of how it really is in your company, not how you would prefer it to be. Please be as candid as possible; remember, all your responses will remain strictly anonymous.

Please indicate whether you agree with each of the following statements about your company.

Please use the scale below and write the number which best represents your answer in the space next to each item.

To what extent are the following statements true about your company?

(1) Mostly false, (2) Somewhat false, (3) somewhat true, (4) Mostly true, (5) Completely true.						
Ethical climate scales	**Items**	1	2	3	4	5
Self interest	In this company, people are mostly out for themselves. EC					
	People in this bank are mostly concerned about what is best for themselves.					
	The major responsibility for people in this company is to consider efficiency first.					
Organizational interest	Organizational members are expected to do anything to further the financial interests and the position of this bank.					
	Organizational members are solemnly concerned with the financial interests and the image of the bank					
	Decisions here are primarily viewed in terms of the money they generate for this bank					

efficiency	The major responsibility of people in this bank is to aim at cost reduction					
	The cheapest way is always the right way.					
	In this bank each person is expected above all to work in a cost reductive way					
	Inexpensive solutions to problems are always sought here.					
Friendship	Good interpersonal contacts both with colleagues and with outsiders are considered to be very important in our bank.					
	In this bank our major concern is always what is best for the other person, weather she/he is a colleague or not.					
	What is best for each individual weather citizen or colleague is the primary concern in this bank.					
	It is expected that each individual both colleague and outsider is cared for when making decisions here.					
Team interest	The most important concern is the good of all the people in my bank					
	Our major consideration is what is best for all colleagues in this bank .					
	People in this bank view team spirit as important.					
	A good and broad cooperation among all colleagues is considered to be very important in this bank.					
Stakeholder Orientation	It is expected here that you will always do what is right for the citizens whom you deal with					
	People in the this bank have a strong sense of responsibility to the citizens they deal with.					
	People in this bank are actively concerned about the citizens they have direct contact with.					

	The effect of decisions on citizens whom we deal with directly is a primary concern in this organization.					
Personal Molarity	There is no room for one's own professional ethics or personal morals in this bank					
	In this bank people are expected to follow their personal moral beliefs and their own professional ethics					
	The most important consideration is each employee's personal sense of right and wrong					
	In this bank people are guided by their own personal ethics.					
	It is important to follow strictly the banks rules and procedures here					
	Everyone is expected to stick to the rules and procedures of the bank.					
	People are expected to comply with the law and public interest over and above other considerations.					
	In this bank people are expected to follow legal and professional standards.					
Public Interest	In this bank public interest is the major consideration.					

Thank you very much for taking the time to participate.

7.5.4 Appendix D Research Ethics approval from Mbarara University of Science and

MBARARA UNIVERSITY OF SCIENCE AND TECHNOLOGY
P.O. Box 1410, Mbarara, Uganda. Tel: +256 4854 [illegible]; Fax: +256 4854 21782
RESEARCH ETHICS COMMITTEE
E-mail: sec.rec@must.ac.ug

Our Ref: MUREC 1/7 Date: July 27, 2020

Ms Nakato Ruth
Postgraduate Student

Re: Submitted protocol on **"A model for assessing the banking sector employees' ethical behaviour towards cyber security"50/03**-20

Type: [√] Initial Application
[ ] Protocol Amendment
[ ] Letter of Amendment (LOA)
[ ] Continuing Review
[ ] Other, specify: _____

Reference is made to the above protocol which was resubmitted to the Research Ethics Committee for reconsideration and approval under expedited review process.

It is noted that you have addressed all the concerns earlier raised by the Committee.

I am pleased to inform you that your study has been approved for a period of one year from July 27, 2020 up to July 26, 2021.

As Principal Investigator of the research, you are responsible for fulfilling the following requirements of approval:

1. All co-investigator must be kept informed of the status of the research.
2. Changes, amendments, and addenda to the protocol or the consent form must be submitted to the REC for review and approval prior to the activation of the changes. The REC application number assigned to the research should be cited in any correspondence.
3. Reports of unanticipated problems involving risks to participants or other must be submitted to the REC. New information that becomes available which could change the risk: benefit ratio must be submitted promptly for REC review.
4. Only approved consent forms are used in enrolment of participants. All consent forms signed by subjects and/or witness should be retained on file. The REC may conduct audits of all study records, and consent documentation may be part of such audits.
5. Regulations require review of an approved study not less than once per 12-month period. Therefore, a continuing review application must be submitted to REC eight weeks prior to the above expiration date of July 26, 2021 in order to continue the study beyond the approved period. Failure to submit a continuing review application in timely fashion may result in suspension or termination of the study, at which point new

Technology

participants may not be enrolled and currently enrolled participants must be taken off the study.

6. You are required to register the research protocol with the Uganda National Council for Science and Technology (UNCST) for final clearance to undertake the study in Uganda.

The following is the list of documents approved in the application:

Document	Language	Version
Proposal	English	July 2020
Protocol form	English	Version 2
Data Collection tools	English	July 2020
Consent form	English	July 2020

I wish you all the best.

Dr. Francis Bajunirwe
CHAIR,
MUST RESEARCH ETHICS COMMITTEE

7.5.5 Appendix E Research Approval: from Uganda National Council For Science and Technology

Uganda National Council for Science and Technology

(Established by Act of Parliament of the Republic of Uganda)

Our Ref: SIR34ES **8 February 2021**

RUTH NAKATO
Mbarara University of science and Technology
Mbarara

Re: Research Approval: **A model for assessing the Banking Sector Employees' Ethical Behavior towards Cyber security.**

I am pleased to inform you that on **08/02/2021**, the Uganda National Council for Science and Technology (UNCST) approved the above referenced research project. The Approval of the research project is for the period of **08/02/2021** to **08/02/2023**

Your research registration number with the UNCST is **SIR34ES**. Please, cite this number in all your future correspondences with UNCST in respect of the above research project. As the Principal Investigator of the research project, you are responsible for fulfilling the following requirements of approval:

1. Keeping all co-investigators informed of the status of the research.
2. Submitting all changes, amendments, and addenda to the research protocol or the consent form (where applicable) to the designated Research Ethics Committee (REC) or Lead Agency for re-review and approval prior to the activation of the changes. UNCST must be notified of the approved changes within five working days.
3. For clinical trials, all serious adverse events must be reported promptly to the designated local REC for review with copies to the National Drug Authority and a notification to the UNCST.
4. Unanticipated problems involving risks to research participants or other must be reported promptly to the UNCST. New information that becomes available which could change the risk/benefit ratio must be submitted promptly for UNCST notification after review by the REC.
5. Only approved study procedures are to be implemented. The UNCST may conduct impromptu audits of all study records.
6. An annual progress report and approval letter of continuation from the REC must be submitted electronically to UNCST. Failure to do so may result in termination of the research project.

Please note that this approval includes all study related tools submitted as part of the application as shown below:

No.	Document Title	Language	Version Number	Version Date
1	questionnaire	english	1	29 July 2020
2	Risk Management Plan for research amidst COVID-19	english	1	20 October 2020
3	consent letter	english	1	20 October 2020
4	Project Proposal	English	1	
5	Approval Letter	English	1	2020-07-20

Yours sincerely

Hellen Opolot
For: Executive Secretary
UGANDA NATIONAL COUNCIL FOR SCIENCE AND TECHNOLOGY

7.5.6 Appendix F Research Approval: from Centenary Bank



Centenary Bank

Our ref: CRDB/MD/10/20

Your ref:

Date: 22nd October,2020

The Executive Secretary,
Uganda National Council for Science and Technology

Dear Sir,

AUTHORISATION LETTER TO CONDUCT RESEARCH AT OUR BANK DURING COVID 19

This letter serves as authorization to Nakato Ruth to conduct the research project, entitled A MODEL FOR ASSESSING THE BANKING SECTOR EMPLOYEES' ETHICAL BEHAVIOR TOWARDS CYBER SECURITY, on employees in the banking Sector in Uganda at Centenary Bank.

Upon a review of the letter sent to us by Dr. Nabaasa Everest (PhD) DEAN- Faculty of Computing and Informatics; Mbarara University of Science and Technology, we are glad to offer Nakato Ruth an opportunity to conduct the same research on our bank employees.

Only electronic questionnaires are approved and allowed to avoid their direct distribution to our staff as measure against Covid 19. Electronic questionnaires will be approved and will be fully supervised by the Human Resource Department.

If you have any concerns or require any additional information, feel free to contact the department.

Yours faithfully,

Fabian Kasi
MANAGING DIRECTOR

Centenary Rural Development Bank Ltd. Head Office - Mapeera House
Plot 44-46 Kampala Road and Plot 2 Burton Street. P.O. Box 1892 Kampala, UGANDA
Call Centre: 0800 200555 Tel: +256 (0)41 346856, 251276/7 Fax: +256 (0)41 251273
email: info@centenarybank.co.ug. **website:** www.centenarybank.co.ug

Ugandans Mr. Gustavio Bwoch (Chairman), Mr. Fabian Kasi (MD), Dr. Peter Ngategize, Mt. Rev. Dr. Cyprian K. Lwanga, Dr. Mary Theopista Wenene, Assoc. Prof. Joseph K. Ssewanyana
Kenyan Mr. Sam Kamiti *French* Mr. Richard Thil

7.5.7 Appendix G Research Approval: from ABSA Bank.



Plot 2 Hannington Road
Kampala, Uganda

Tel +256 (0) 417 122000
+256 (0) 417 122200

www.absa.co.ug

September 28th 2020

TO:

The PI and/or Executive Secretary,

Uganda National Council for Science and Technology

Sir,

Letter of authorization to conduct research at our bank during covid 19

This letter will serve as authorization to Nakato Ruth to conduct the research project, entitled A MODEL FOR ASSESSING THE BANKING SECTOR EMPLOYEES' ETHICAL BEHAVIOR TOWARDS CYBER SECURITY, on employees in the banking Sector in Uganda at our Absa bank.

Upon a review of the letter sent to us by Dr. Nabaasa Everest (PhD) DEAN- Faculty of Computing and Informatics; Mbarara University of Science and Technology, we are glad to offer Nakato Ruth an opportunity to conduct the same research on our bank employees.

Only electronic questionnaires are approved and allowed to avoid their direct distribution to our staff as measure against Covid 19. Electronic questionnaires will be approved and will be fully supervised by the human resource department

If you have any concerns or require any additional information, feel free to contact the department. Thank you

Yours Faithfully,



Edmand Nareeba
Branch Manager
Mbarara Branch

Direct line +256 417 125371
Edmand.Nareeba@absa.africa

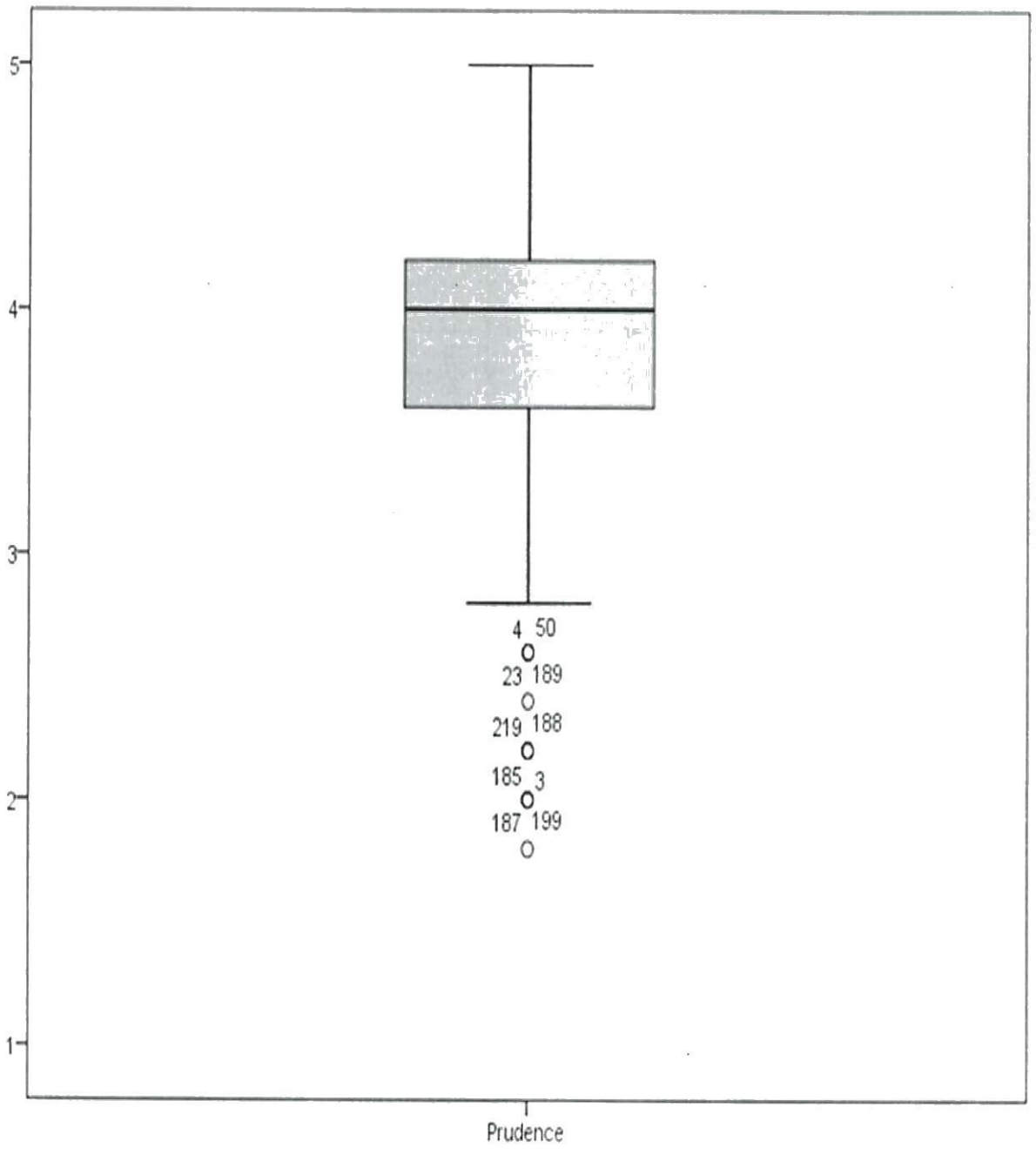
Absa Bank Uganda Limited, company registration number 4227 is regulated by the Bank of Uganda

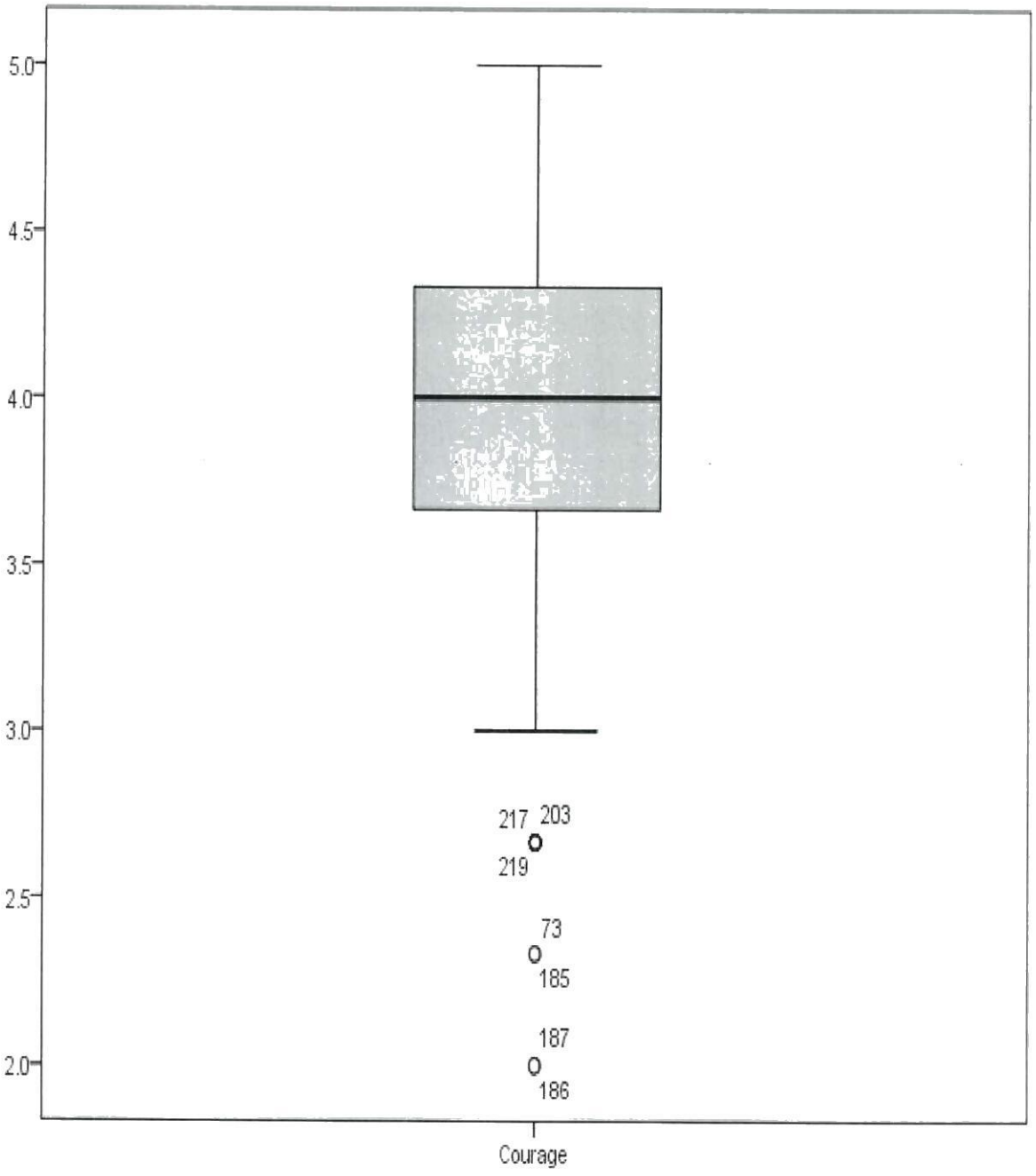
Absa Bank Uganda Limited, company registration number 4227 is regulated by the Bank of Uganda.
Customer deposits are protected by the Deposit Protection Fund

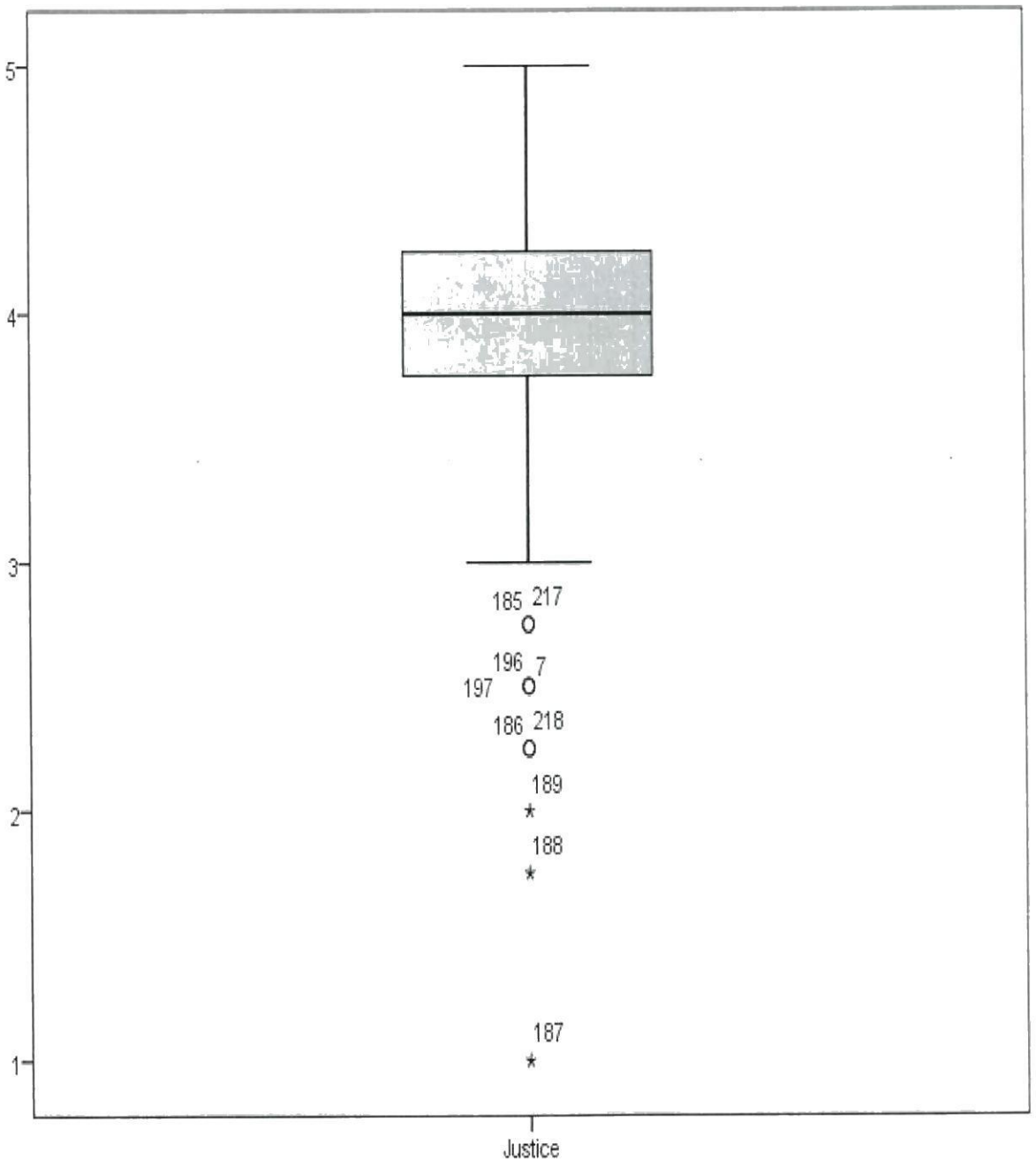
7.5.8 Appendix H Missing Values Outliers

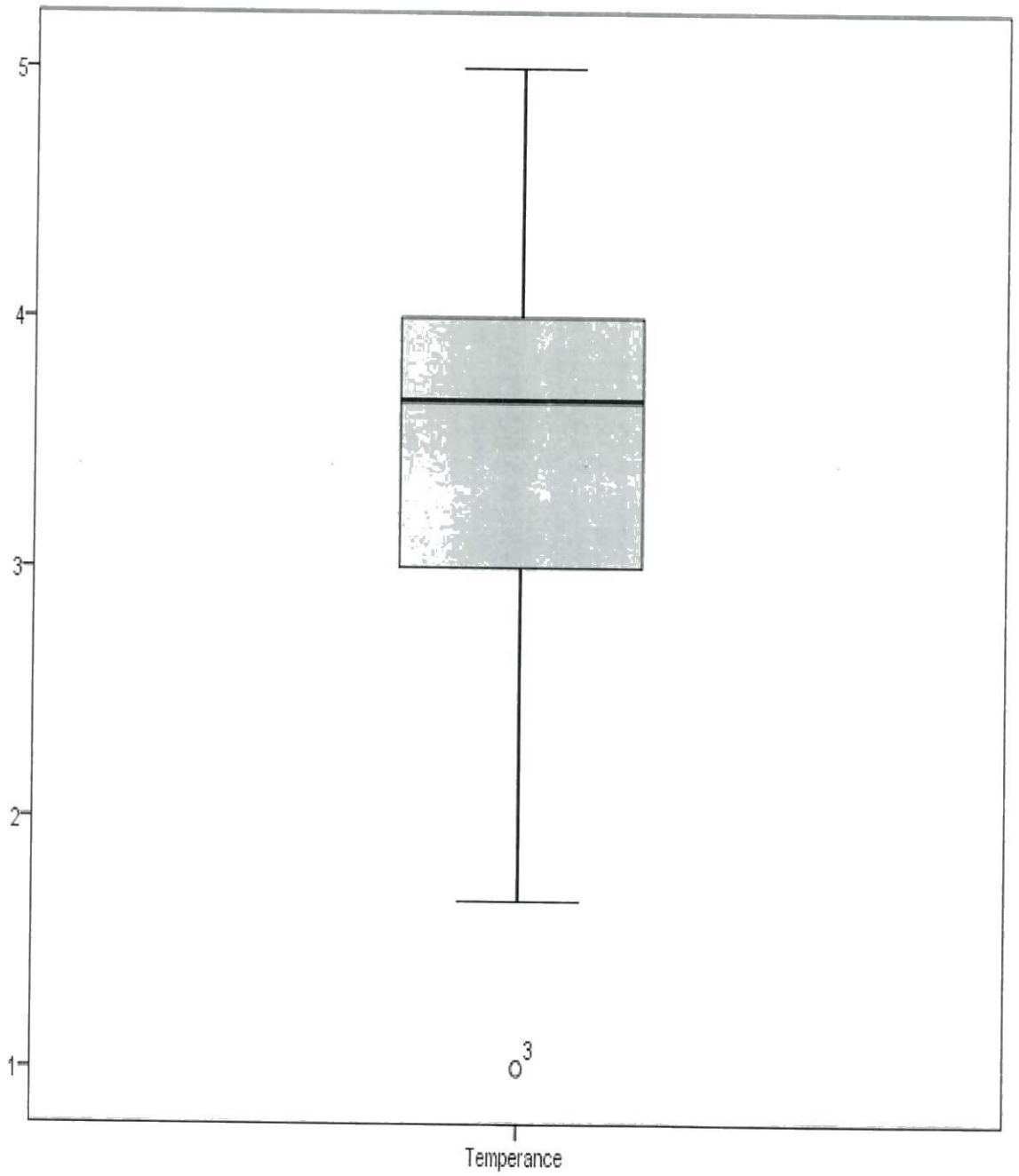
An outlier is a value that is very different from the test. It is absolutely essential to deal.:

Boxplot showing absence of Outliers in the prudence Variable Data




5.0
4.5
4.0
3.5
3.0
2.5
2.0
217
203
219
73
185
187
186
Courage


5
4
3
2
1
185
217
196
7
197
186
218
189
188
187
Justice


5
4
3
2
1
3
Temperance


5
4
3
2
1
217
EthicalClimate

7.5.9 Appendix I A list of commercial banks in Uganda

1	ABC Bank Uganda Limited
2	Absa Bank Uganda Limited
3	Afriland First Bank Uganda Limited
4	Bank of Africa Uganda Limited
5	Bank of Baroda Uganda Limited
6	Bank of India Uganda Limited
7	Cairo Bank Uganda
8	Centenary Bank
9	Citibank Uganda
10	DFCU Bank
11	Diamond Trust Bank
12	Ecobank Uganda
13	Equity Bank Uganda Limited
14	Exim Bank (Uganda)
15	Finance Trust Bank
16	Guaranty Trust Bank
17	Housing Finance Bank
18	KCB Bank Uganda Limited
19	NCBA Bank Uganda
20	Opportunity Bank Uganda Limited
21	Orient Bank
22	Stanbic Bank Uganda Limited
23	Standard Chartered Uganda
24	Tropical Bank
25	United Bank for Africa

7.5.10 Appendix J Usability questionnaire

Below is questionnaire to measure the usability of an employees' cyber security ethical behaviour assessment ECEB) model.

On a scale between Strongly Agree to Strongly Disagree, please rate the following statements concerning the ECEB model:

		Strongly disagree	disagree	Neutral	Agree	Strongly agree
1.	I think that I would like to use this model frequently.					
2.	I found the model unnecessarily complex.					
3	I thought the model was easy to use.					
4	I think that I would need the support of a technical person to be able to use this model.					
5	I found the various functions in this model were well integrated.					
6	I thought there was too much inconsistency in this model.					
7	I would imagine that most people would learn to use this model very quickly.					
8	I found the model very cumbersome to use.					
9	I felt very confident using the model.					
10	I needed to learn a lot of things before I could get going with this model.					