European Journal of
Technology
(EJT)

Establishing the Influences of Cardinal Virtues on Employees' Cyber Security Ethical Behavior in the Banking Sector in Uganda

Nakato Ruth, Mayoka. G. Kituyi, and Fred Kaggwa

AJP

European Journal of Technology
ISSN 4520-4738 (Online)
Vol.6, Issue 1, pp 1 - 13, 2022

www.ajpojournals.org

Establishing the Influences of Cardinal Virtues on Employees' Cyber Security Ethical Behavior in the Banking Sector in Uganda

[1]*Nakato Ruth

Mbarara University of science and Technology

rnakato@must.ac.ug

[2]Mayoka. G. Kituyi

Makerere University Business School

gkituyi@mubs.ac.ug

[3]Fred Kaggwa

Mbarara University of science and Technology

kaggwa_fred@must.ac.ug

Abstract

Purpose: Cyber security threats emanating from employees' incorrect behavior have escalated in the banking sector. Yet formal policies and technical solutions have failed to solve the problem. Virtue ethics may be a method that can handle this concern. This research aimed at enhancing Cyber security by confirming through statistical analysis the applicability of cardinal virtues related to cyber security ethical behavior.

Methodology: The quantitative survey method utilizing an online questionnaire was used. Confirmatory factor analysis determined causal patterns in the variables and assessed them for validity and reliability. Partial Least Squares Structural Equation Modeling was then used to test casual relations between the study's constructs.

Findings: The results reveal that there is a positive but an insignificant effect of prudence Beta 0.094. p = 0.277 on cyber security ethical behavioral Intentions; there is a positive and significant influence of Temperance; Beta 0.255, p = .000; a positive and significant influence of courage; Beta 0.247, p = .001; on cyber security ethical behavior, that there is a positive and significant influence of Justice; Beta 0.452, p = .000; on cyber security ethical behavioral Intentions. The results further showed that a positive change in ethical behavior intentions leads to a positive change in cyber security ethical behavior.

Unique contribution to theory and practice: This research makes a theoretical contribution to Cyber security ethics by promoting virtue ethics as a framework for moral investigations into Cyber security. Results can be utilized to improve methods, instruments, and tools to assess the employees' cyber security ethical behavior. Policy makers can develop virtue ethical based training programs with dedicated, continuous learning and teaching undertakings geared towards monitoring and enhancing the overall ethical behavior towards cyber security in the banks. The results are a platform to the Government of Uganda through the Ministry of ICT in generating appropriate national policies related to Cyber security ethics as a strategy aimed at improving Cyber security in the banking sector.

Keywords: *Cardinal Virtue ethics, Ethical Behavior, Cyber Security*

1.0 Introduction

The banking sector has embraced the use of Information Communication Technologies (ICTs) to offer better access and expediency to their clients and to simplify business Gana et al., (2019). Kazmi et al., (2017) posit that banks have steadily transferred their banking activities to cyberspace to cut on operating costs and increase on customer experience. Rao (2019) echoes that the progression of information technologies enables the bank clients to experience their bank undertakings 24*7 using, Automatic Teller Machines (ATMs), mobile technologies and other Web- based approaches. In all these, banks have to secure their cyber assets, thus cyber security has also increased in attempt to match with the fast growth and competencies of their cyber domain, (Edgar &Manz,2017).

However, Kazmi et al., (2017) explain that banking sectors are more prone to security attacks and that banks grieve more data breaches than any other sector. They further contend that the menace of cyber security attacks has set a great challenge for Internet banking. And the feeblest connection are mostly the internal employees who cooperate with external attackers to cause havoc. Reddy and Bhargavi (2018) posit that Cyber security threats originating from employees' incorrect behavior is still a big challenge in the banking sector. DuPont (2019) vies that banks' employees, including bank tellers pose a bigger threat to financial institutions than hackers. Mukisa (2019) clarifies that 35% of cyber security breaches in the banks are from outside, and 65% of the breaches are from the inside. And of the 35%, over 95% is aided by insiders. According to statistics from Uganda police, commercial banks in the country lost Shs15 billion shillings through electronic fraud in 2018. Malaba further posits that banks grieve of frauds or attempted scam that are organized by bank staff on a daily basis. Mukisa (2019) echoed that electronic fraud cases are on the rise in commercial banks in Uganda and that most of them are organized and executed by the insiders.

A cyber security breach upsets the affected bank both financially and in reputation. Further, Cyber security violations in the banks can make its customers lose confidence in the bank's electronic transactions. Matovu (2018) espouses that the total customer base of Centenary bank Uganda declined by 11.4%, and customer deposits declined by 7%, after electronic fraud increased by 6.3% in 2016. Strategies including formal policies and technical solutions have failed to solve these people's concerns (Gray, 2015; Kraemer et al., 2009; Hadlington, 2017).

This research suggested that virtue ethics must be considered and cardinal virtue ethics recognized because ethical behavior may spur the banking sector employee's decision-making processes. However, there exists less research on how the cardinal virtue ethics, proven through the character growth of the banks' employees can add to the improvement of cyber security in the banks. This research addressed this gap by investigating the cardinal Virtue Ethical constructs. The research built its theoretical base by fitting in the Aristotelian cardinal virtues of courage, temperance, justice and prudence (Aquinas, 2005). The review carried out by Maalem et al., (2020) recognized that behavioral aspects towards cyber security are still underexplored because extra emphasis is put on the technology strategies. It was therefore recommended that Cyber security professionals and users' behaviors and intentions be studied and considered. This research also filled this gap by investigating behavior intention and actual behavior constructs from the theory of planned behavior.

The research aimed at enhancing Cyber security by proposing a model and a means of addressing

the employees' ethical behavior. The moral prestige of an individual is significant in making ethical judgements. This study considered that the cardinal virtue ethical constructs would play a conceivable part in shaping the employees' ethical conduct towards cyber security in the banking sector.

Ayodele et al. (2019) elucidate that employee ethical behavior as the ability of the employee to form the right judgement about acceptable principles of right or wrong conduct built on suitable ethical standards. The ITU 2018) define "cyber security" as the group of implements, strategies, guiding principles, threat management methods, actions, teachings, best practices, assurance and technologies that can be applied to defend the availability, integrity and confidentiality of assets in the connected infrastructures pertaining to government, private organizations and citizens; these assets include; connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and data in the cyber-environment. Brey (2007) clarify that the consequences and results achieved after employing cyber security strategies are also recognized as cyber security. Chang &Ho (2006), Hatfield (2019) indicate that there is little research in computing focusing on management, social, and human concerns compared to those focusing on technical issues. Computer ethics studies state that a failure to understand the human context has been the cause of many computer security problems.

2. Related work

2.1 Employees' Cyber security Ethical Behavior.

Ethical behavior refers to ethical and unethical decisions and conduct, measured according to social norms (Treviño, Nieuwenboer, & Kish-Gephart, 2014). Herath and Rao (2009) claimed that behavioral aspects are among the issues that aid in stimulating the level to which employees observe cyber security practices. Anwar *et al* (2017) emphasize that security breaches are predominant in establishments and mostly are attributed to human misconduct. Thus, Organizational employees' behavior is very crucial in information security compliance. But the Cyberspace is extensive and it's not easy for an organization to guarantee ethical conduct in its daily activities, thus ethical behavior depends on an individual. Organizations need to form and maintain their employees 'good behavior and keep ethical standing in the Cyberspace. However Hatfield (2019) argue that cyber security vulnerabilities and employees' wrong behavior have continued to upsurge and to cause grief to organizations. Organizational employees are antithetical and can violate the finest cyber security strategies, controls, rules and codes of conduct put up by the organizations. Herath and Rao (2009) also report huge losses due to specifically unethical activities by employees.

Yang Lu (2018) argue that employees' unethical behaviors toward information security pose potential security breaches. Hatfield (2019) echoed that cyber security violations are most of the time carried out by organizational employees. Aşuroğlu and Gemci (2016), contended that organizations may have the best information systems and security, but they will be operated by people. Employees should possess ethical behavior to avoid making information systems susceptible to threats. Ethics provides a set of standards for behavior that helps human beings to decide how they should conduct themselves in many circumstances. Igwe and Ibegwam (2014) explain that it is very paramount to instill ethical behavior in persons for them to live well and be fruitful to society. Gray (2015) presented clear pointers of ethical behavior concerning information systems security. These include; i) rules compliance which is noticed when employees obey the

organizational security guidelines, policies, and regulations, following mandated rules of correct behavior, and demonstrating an ability to make the correct choice in ethical situations. ii) Enacting best practices which means that in the absence of specific guidance employees will make use of the proper procedures and practices that guide the industry and their professions when they face information system security dilemmas. Security incident reduction, loyalty, and a commitment to security. iii) Incident reduction is confirmation that the aggregate of occurrences of information loss, compromise, disclosure, or theft are becoming fewer in numbers. iv). Loyalty whose attributes are self-discipline and trustworthiness by upholding ethical principles and being ethically dependable.

However, Halawi (2013) argues that Cyber security ethical issues are under researched, thus this research established the influence of cardinal ethical virtues on the behavioral intentions of employees' Cyber security ethical behavior in the banking sector in Uganda.

2.2. The Importance of Cyber Security in the Banking Sector

Cyber security is a very important aspect of organizations' main business processes. When the banking industry shifts most of its transactions online, the risk of information breaches also increases every day. Zahoor et al (2016) contend that cyber security assaults in the banks are on the rise compared to other sectors. Successful cyber-attacks cause enormous financial damage to banks and their customers. Without cyber security ethical behavior among the employees, the banks will continuously face threats from impending cyber-attacks aided by insiders.

Therefore, banks need to look into the behavior of their employees on top of the other cyber security strategies implemented to defend their customers' money, private information and other treasured assets from cyber-attacks. Improved cyber security stimulates confidence and inspire trust in the banks 'clients when purchasing and using banks' products and services online.

2.3. Theories underpinning this research

The Philosophical Virtue Theory, Aquinas (2005), is the pillar of this research. The theory assessed the banking sector employees' cyber security ethical behavior. Virtue theory is one of the three major approaches in normative ethics. Normative ethics studies the rightness or wrongness of the moral deeds of individuals as they relate to the moral rules of society (Gray and Tejay 2014). In normative ethical theory, cyber security ethics fits in the part of applied ethics that deals with practical and daily moral problems that come from the use of computers and computer networks in the information society.

2.3.1 The virtue ethical theory.

Virtue ethics are the moral character traits of a person. MacIntrye's (1984) describes virtue as a learned quality or personality that forms the rudimentary components of good character. By possession of and through repeated use of virtue, an individual promotes self-knowledge, knowledge of goodness, and ultimately achieves internal and external good. Gray (2015) concludes that virtues are learnt, and with continued use, they can turn out to be part of a person's character. Courage, temperance, justice and prudence are well thought-out as cardinal virtues because all other virtues are based on cardinal virtues.

Nguyen and Crossan (2021) posit that Virtue ethics emphasizes on the character of the moral person instead of the act itself, in order to comprehend Ethical decision making. This research

therefore investigated the influence of; Prudence, temperance, courage, and justice on the employees' cyber security ethical behavior.

Prudence and cyber security ethical behavior intention

Prudence is the presentation of wisdom or intelligence and the right reason regarding taking the suitable decision according to a given situation (Aquinas, 2005, pp. 2-3). Prudence comprises of a disposition and an aptitude to make good decisions regarding good actions that benefit other humans, (Bartunek & Trullen, 2007). Alfawaz *et al., (*2010) upholds that cyber security behavior is affected by an individual's knowledge, professional skills, and values coupled with consistent behavior. The virtue of prudence helps in reasoning. Aquinas (2005) asserts that good activities have their roots on reason. Aristotle (2004) explains that a good life is a life governed by reason, which is a unique human ability and the human highest faculty. A human being's moral acts are to be in harmony with reason, and an individual's wicked acts are to be against reason. The work of prudence as a virtue is hence reasoning and decision making. It also permits an individual to make fast decisions in all circumstances. Prudence also helps a human being to battle against the temptation of unfairness and fearfulness. Gray and Tejay (2014), explains prudence as that ability to excellently think and reason and make an appropriate decision at a specific time. Bartunek and Trullen (2007) contend that common day-to-day glitches frequently need prudence. This was echoed by Vallor (2017) who clarified that Cyber security activities, roles and interests that are carried out daily need prudence because these responsibilities can be in conflict with each other. The absence of prudence might result into monetary glitches, loss of life and loss of customer confidence in an organization. So considering the importance of prudence a cyber-security professional should be ethically prudent to handle the complexities in the cyber society.

Therefore, the study proposed;

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

Courage and cyber security ethical behavior intention;

According to Aquinas, (2005), Nguyen and Crossan (2021), courage is the strength to resist the hitches which may deter proper action. It's ability to confront and bear fear and uncertainty or intimidation.

A courageous employee is brave and shows an unrelenting determination, confidence, and perseverance in confronting difficult situations and rebounds quickly from setbacks. Does the right thing even though it may be disliked, actively discouraged, or even if the act has negative results for him/her, (Nguyen and Crossan, 2021),

Cyber security professionals who possess the virtue of courage can most likely adhere to cyber security practices. Papouli (2018) contends that it is obligatory for a brave social employee to take a problematic decision in order to perform a correct act despite the intimidations and hazards. It takes courage to make an ethical choice. Employees who show courage as a virtue help their organizations to continue growing successfully.

Thus; *H3. Increased courage positively influences the employees' cyber security ethical behavioral intention.*

Justice and cyber security ethical behavior intention;

Justice is explained regarding to the relations with others; the continuous willingness to render to each individual what they rightly deserve; just or fair acts (Aquinas, 2005). Justice is being fair-minded, unbiased, proportionate, even handed and socially accountable, (Nguyen Crossan, 2021). Justice goes all-out to ensure that people are treated equitably and that implications are proportionate to contributions. A just individual stays objective and keeps personal biases to a tiniest level when making decisions. Justice offers others the opportunity to voice their opinions on processes and procedures. It provides timely, specific, and honest clarifications for decisions, seeks compensation of misconducts both external and internal to the company. Papouli (2018) posit that justice is an essential virtue for social labor and other social practice. Social justice includes positive thinking of society in which the sharing and equal distribution of resources and wealth is guaranteed to all societal members and done in a safer and secure manner. Virtue responsibility ethics are shaped by encouraging and promoting faithfulness, admiration, and trust. This is encouraged chiefly when protecting and preserving confidential and private information belonging to individuals and organizations, Gray & Tejay (2014). 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. Stamatelos (2011) contend that cyber ethics and good conduct embrace approaches to being considerate and kind. It also includes the better deliberations of individual policies, social rules, and making fair judgements and resolutions that may affect society. Employees in the cyber society should possess ethical founded personalities for the betterment and enriched cyber security. Basing on these arguments, this study proposes that;

H4; Increased justice positively influences *employees' cyber security ethical behavioral intention.*

Temperance and cyber security ethical behavior intention;

Temperance is elucidated (Aquinas, (2005), as performing willpower, holding back, and moderation of actions, desires, and emotions. According to Nguyen and Crossan, (2021), a temperant individual is patient, peaceful, serene, self-controlled. Maintains the ability to think clearly and responds reasonably in tense situations. Completes work and solves problems in a thoughtful, careful manner. Resists excesses and stays grounded. Schwarzer, Ralf (2012) posit that temperance is explained in relation to what a person willingly desists from doing; such as control from revenge and instead be calm and compassion, resisting from conceit to self-effacement and humility, restraint from excesses and restraint from excessive anger and instead exercise self-discipline. Papouli (2018) affirms that temperance consist of self-discipline such that an individual can evade doing things that are injurious to him and others. Workers temperance encourages moral behavior and can enhance Cyber security. The employees' ethics are impacted on by enhancing their moralities and competence and this can help to improve Cyber security. With the help of the existing literature Gray and Tejay (2014), Chatterjee *et al*., (2015) this study considered temperance as the aptitude 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, be true to themselves and others particularly in their cyber security dealings. Myyry et al., (2009) explained that an ethical person is self-determined and controls his urge to commit security abuses.

Given this literature, this research proposed that;

H4: Increased temperance positively influences the cyber security ethical behavior intention.

3.0 Methodology

3.1 Participants

A sample of 240 employees from commercial banks in Uganda and particularly Centenary and ABSA banks' branches in Kampala capital city participated in the study. Of the 240 respondents, 129 were male and 111 were female; with an age range of 20 – 65 years.

3.2 Instrumentation

Trusted Worker Ethical Behavior and Influences Survey;

An instrument Trusted Worker Ethical Behavior and Influences Survey developed by Gray (2015) was used in this research. The survey consisted of questions divided into two sections. Section one was used to gather the demographic data of the participants including; Gender, age, Respondents' bank, Education level, Speciality, professional role and experience. The second section of the survey consisted of 28 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 the improvement of Cyber security among the commercial banks 'employees. Cronbach alpha estimate was used to verify 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 the scale.

3.3. Analysis.

Confirmatory factor analysis was subsequently applied to approve the measurement specifications. To assess the reliability of the indicators and specifically, construct reliability, a composite reliability statistic (CR) was obtained and the construct was deemed to possess construct reliability if the value of CR is 0.6 or higher. Reliability was examined using the average variance (AVE), and in this case, an AVE value of 0.5 and higher was deemed to guarantee reliability (Hair, 2010). Discriminant validity for the reflective constructs was evaluated by comparing AVE correlations between latent variables and all were found to be acceptable. Formative construct discriminant validity was evaluated using indicator path weights and loadings.

3.4 Results

Table 3.1 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	0.383
Temperance -> Behavioral Intentions	0.255	0.256	0.061	4.183	0.000	
Behavioral Intentions -> Ethical Behavior	0.257	0.26	0.072	3.559	0.000	0.578
Courage -> Ethical Behavior	0.247	0.235	0.074	3.319	0.001	
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	

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 3.1 above. The results show that cyber security ethical behavior 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 behavior 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 behavior.

4.0 Discussion of findings;

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

Results reveal that there is a positive but an insignificant effect of prudence on Behavioral Intentions. Whereas the relationship is positive, it is not significant. Therefore, the hypothesis that increased Prudence has a positive influence on employees' cyber security ethical behavioral intention is not supported by the data. This means that a positive change in prudence leads to a negative change in the employees' cyber security ethical behavior intention. This finding does not agree with literature which argues that high prudence scores are associated with people who are reliable, detail oriented, and follow organizational procedures (Nguyen & Crossan 2021). Aquinas (2005) explains that a prudent person takes guidelines wisely with oneself and others, adjudging in the approved manner from the proof at hand, and performs his undertakings grounded on the decisions made from cautious deliberation.

H2: Increased Temperance positively influences employees' cyber security ethical behavioral intentions.

This hypothesis was supported because it was significant at the 0.000 level. 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 '*innermost self* 'from turmoil and devastation. Temperance enables managers and employees to treat colleagues with deference and understanding and grip change and conflict with consideration. Agreeing with literature, Chatterjee et al (2015), the findings of this study consider temperance as the aptitude 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 particularly in their cyber-security dealings. Papouli (2018) affirms that temperance consists 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. 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 ethical behavior.

H3: Increased courage has a positive influence on employees' cyber security ethical behavioral intention.

Results revealed that courage had an indirect influence on behavioral intentions. The results rather disclosed that there is a positive and significant influence of courage on cyber security ethical Behavior. This means that a positive change in courage leads to a positive change in cyber security ethical behavior and not through the influence of 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 the daily obligations. 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. Volkmann asserts that courage is a virtue of the respectable computer professional. Hawking (2017) confers virtues as characters required to face the life's challenges. Volkmann maintains that success requires real courage.

H4: Increased Justice has a positive influence on the employees' cyber security ethical behavioral intentions.

H4 was supported by the data. Increased justice has a positive influence on employees 'ethical behavior intentions towards cyber security. This finding is in agreement with literature. 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 Weber (2015), each person has an unchallengeable dignity, and is eligible to equal privileges; profound admiration for one another promotes justice; fair and equal access to information, enables employees to reach for a common understanding.

According to Willison et al (2018) the procedural injustice causes employees to engage in abusive behaviors. The moral method to making use of information systems is considering all stakeholders including colleagues, clientele, and the administration. Cyber security professionals should also take morally fair rulings and decisions concerning cyber security and safety policies. Stamatelos (2011) contend that cyber ethics and good conduct includes approaches to being considerate and kind. It also includes the better deliberations of individual policies, social rules, and making fair judgements and resolutions that may affect society. Cyber security professionals and other employees in different positions in the banks should possess good personality founded ethics for the betterment and enriched cyber security in the banking sector.

The findings of this study support that an employee's ethical behavior is formed partially by the direct effects of cardinal virtues. 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.

Conclusion

The objective of this study was to confirm through statistical analysis the applicability of cardinal virtue constructs by validating each construct's indicators and factors which influence the cyber security ethical behavior of banking sector employees in Uganda. The findings of this study

provide a concrete preliminary explanation of virtue elements and their influences on employees' ethical behavior towards cyber security in the banking sector in Uganda.

H1 stating that increased prudence has a positive influence on employees' Cyber security ethical behavioral intention was not supported. There was no significant direct effect of prudence on Cyber security ethical behavior. H2: *Increased Temperance positively influences employees' cyber security ethical behavioral intentions,* was supported by the data. H3: *Increased courage has a positive influence on employees' cyber security ethical behavioral intention,* was not supported. H4: Increased Justice has a positive influence on the employees' cyber security ethical behavioral intentions, was supported.

The banking sector is more prone to security attacks and data breaches than any other industry. Technological measures in the banks have been insufficient in handling cyber security desecrations. Studying the ethical behaviors of users in the banking setting helps to comprehend how to improve cyber security and may make banks more resistant to violations. As Aşuroğlu and Gemcim (2016) contended embracing ethics in information security is very significant since it can bung up the gap that people create.

The critical objective of including an ethics approach based on the employees' ethical behavior towards cyber security might help professionals to exercise more ethical behavior resulting from their own inner inspirations. Founded on the results of this research, a virtue ethics based methodology might encourage employees to make ethical decisions. This could be an effective approach to reducing employee cyber security violations.

Recommendations and future research

Results reveal that there is a positive but an insignificant effect of prudence on Behavioral Intentions. Yet the existing empirical literature proves that, prudence are excellences of character, which involve getting things right, (Harrison, 2014). Therefore, further studies on the direct influence of prudence on ethical behavior should be done to confirm the results.

The banking sector workers' temperance 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' ethical behavior is positively impacted on. It enhances their moralities and competences. This might improve the banks' Cyber security ethical behavior.

The research recommends that banks should recruit courageous people. Courageous employees are willing to embrace innovation and change which is not a characteristic of the coward especially when implementing technology and cyber security strategic plans.

The findings suggest that employees' Cyber security ethical behavior can potentially be identified through a personnel screening process or background investigation that interprets their approach to ethical challenges. Coming up with an interview tool that may help to recognize ethical virtue traits of a prospective new employee's background might provide insight as to whether the individual is ethically and morally well-grounded. This can help the recruitment panel to know that the person is a good fit for the bank into Cyber security related positions.

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 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. Future research should be conducted in order to provide further evidence in which to verify the validity of this study and extend the results.

This research utilized cross sectional data to study the antecedents and consequences 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 cyber-security using longitudinal/ qualitative methods so as to verify the findings of the current study.

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.

References

Treviño, L.K; Den-Nieuwenboer N.A & Kish-Gephart J.J., (2014), (Un)ethical behavior in organizations. *Annual Review of Psychology*, 65(1), 635–660.

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.

Aquinas.T.;(2005) The Cardinal Virtunes: Prudance, Justice, Fortitude, and Temperance; pp 159

Aşuroğlu Tunc and Cemal Gemci (2016) Role of Ethics in Information Security, *3rd International Conference on Advanced Technology & Science (ICAT)* Selcuk University, Konya, Turkey

Ayodele, F. O., Haron. H. B. and Ismail, I. (2019); Ethical Leadership, Ethical Leadership Climate and Employee Moral Effectiveness: A Social Learning Perspective; *FGIC 2nd Conference on Governance and Integrity Volume 2019*

Beycioglu. K.(2009) a Cyberphilosophical issue in education: unethical computer using behavior – the case of prospective teachers. ELSEVIER; *Computers and Education; 201-208.*

Brenton M. Wiernik1, Deniz S. Ones (2018) Ethical employee behaviors in the consensus taxonomy of counter productive work behaviors

Brey, P. (2007), "Ethical Aspects of Information Security and Privacy", in: Security, Privacy, and Trust in Modern Data Management, M. Petković and W. Jonker (Eds.), Springer Berlin Heidelberg, pp. 21-36.

Chang S. E., and Lin Chin-Shien 2007 Exploring organizational culture for information security management Industrial Management & Data Systems ·

Dupont, B. (2019). The cyber-resilience of financial institutions significance and applicability *Journal of Cyber security*. Vol. 5, No. 1

Edgar, T. W. and Manz, D. O. (2017). Research Methods for Cyber Security. Publisher: Todd Green

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 Nigeria *International Journal of Information Engineering and Electronic Business.* 2, 35-43

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

Hadlington, L. (2017). Human factors in cyber security; examining the link between Internet addiction, impulsivity, attitudes towards cyber security, and risky cyber security behaviours.

Hair, J. Black F. J. Babin, W. C. *et al* (2010). Multivariate Data Analysis: A global perspective. *Upper Saddle River, NJ:* Pearson Prentice-Hall.

Hatfield, J. M. (2019). Virtuous human hacking: The ethics of social engineering in penetration-testing. *Computers & Security* 83 354-366.

Hatfield, Michael (2018) "Cybersecurity and Tax Reform," *Indiana Law Journal*: Vol. 93 : Iss. 4 , Article 6.

Herath, T., Rao. H.R., 2009b. Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations. *European Journal of information systems.* 18(2), pp 106–125.

Igwe, K.N. and Ibegwam A. (2014). Imperative of Cyber Ethics Education to Cyber Crimes Prevention and Cyber Security in Nigeria; *International Journal of ICT and Management* Vol – II Issue - 2 : pp 102-113.

International Telecommunication Union (Itu) (2018) Guide To Developing A National Cybersecurity Strategy Strategic Engagement In Cybersecurity

Kazmi, J., Alghazo M., Latif G. (2017). Cyber Security Analysis of Internet Banking in Emerging Countries: *User and Bank perspectives*

Maalem . L Ait. R., et al. (2020), Review and insight on the behavioral aspects of cyber security. Cyber secur 3, 10.

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

Miska. C., Stahl. G. K. & Fuchs. M. (2018), The Moderating Role of Context in Determining Unethical Managerial Behavior: A Case Survey, *Journal of Business Ethics* volume 153, pages793–812

Morris M.C, Morris Z.J. (2016). The Importance of virtue ethics in the IRB. *Journal of Research ethics*

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.

Mulki, J.P.; Jaramillo, J.F.; Locander, W.B. Effect of ethical climate on turnover intention: Linking attitudinal and stress theory. *Journal of Business Ethics.* 2008, 78, 559–574.

Nguyen, B. Crossan, M. (2021), Character‐Infused Ethical Decision-Making. *Journal of Business Ethics*

Papouli, E. (2018). Aristotle's virtue ethics as a conceptual framework for EN Zalta. for EN Zalta. http://plato.stanford.edu/archives/fall2013/processes of information systems trusted workers: a Delphi study', *Int. J. Information and Computer Security*, Vol. 12, No. 1, pp.1–19.

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 threats. *American International Journal of Research in Humanities, Arts and Social Sciences* 21(1) pp. 65-71

Ringle, C. M., Wende, S., & Will, A. (2005). SmartPLS. Hamburg. Retrieved from http://www.smartpls.de.

Sommestad, T., Hallberg, J., Lundholm, K., & Bengtsson, J. (2014). Variables influencing information security policy compliance: A systematic review of quantitative studies. *Information Management & Computer Security*, 22(1), 42-75.

Tangen. K. I. (2015), The Need for Temperance on Organizational Leadership and Temperance *SJLT 2.*

Yang Lu (2018), Cybersecurity Research A Review of Current Research Topics; *Journal of Industrial Integration and Management* Vol. 03, No. 04.

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.