International Journal of Economics, Commerce and Management
United Kingdom ISSN 2348 0386 Vol. VII, Issue 8, August 2019

http://ijecm.co.uk/

INVESTIGATING EXTENT TO WHICH CYBERCRIME INFLUENCES PERFORMANCE OF COMMERCIAL BANKS IN KENYA

Phelista Wangui Njeru
Mount Kenya University, Kenya
phelistawangui2004@gmail.com

Vincent Gaitho
Mount Kenya University, Kenya ✉

Abstract

The information technology explosion possesses a major threat to the very existence of business organisations. In the last one decade, Kenya's banking sector has lost billions to cybercriminals. The business competition environment has drastically changed forcing commercial banks to adopt over 80% e-transactions. The purpose of this paper was to Investigate extent to which cybercrime influences performance of commercial banks in Kenya. The specific objectives were; to investigate the extent to which cybercrime influences detection and prevention costs of commercial banks in Kenya, to determine the extent to which cybercrime activities affects bank profitability, to evaluate effects of technological response costs on performance of commercial banks in Kenya and to investigate the influence negative brand image costs on performance of commercial banks in Kenya. Explanatory research design was used. Study targeted the tier 1 banks of Kenya purposively selected since they serve the highest number of clientele. The unit of enquiry was 200 top and middle level managers that made the target population and out of these a 30% sample was selected randomly. Descriptive and inferential statistics were applied to obtain the relationship between the variables given the model y=x0+bixi,+biixii,+biiixiii,+bivxiv+e, where each variable was represented. Pearson's correlation was calculated to show the relationship between the variables. The findings showed a direct positive relationship between the independent and dependent variables.

Keywords: Cybercrime, e-transaction, performance, system hacking and skimming, digital economy

INTRODUCTION

In the early eighties and nineties, what every business organisation or country feared was smuggling drugs trade and money laundering that went across borders. Today the worst fear that cuts across all borders is the explosion of international online crimes. The online crime is always international because the internet has no borders. Local law enforcement has limited resources and expertise to investigate online crime. The victims, police, prosecutors and judges rarely uncover the full scope of these crimes. Action against online criminals is too slow, the arrests are few and far between, and too often the penalties are very lenient, especially compared to real lost value (Mikko Hyppönen, 2010).

According to Bryan Glick, (2010), internet security doesn't just touch on government but also big businesses and law enforcers. It is an increasingly important concern for the average personal technology user, many of whom have little understanding of the issues and even less knowledge of the technical solutions. The technology explosion especially the online transactions have set every transacting player on the same platform. The volumes of customers seeking banking services, the market coverage and the networks created brings many micro and macroeconomics environments and a milliard of players, putting the banks in a vulnerable position. The online transfers of data has increased in speed, in convenience and in anonymity opening new threats to internet users due to increased criminal activities of diverse range that know no boundary. Despite much debate that tries to conceptualize and explain the term cybercrime, scholars have not come up with a universal definition to it due to its ever changing face. However cybercrime is said to be unlawful access and use of data for own goals or malicious attacks against computer hardware or software. This can be high tech crime of cyber that enables criminal access financial institutions database and conduct transactions for their benefits. The cybercriminals to our almost fear facilitate terrorism activities. Cybercrimes face changes daily leaving even the most competent anti-crime institutions like the INTERPOL that is so committed to the global fight against cybercrime look incompetent. Most times the cybercrime is reported getting these anti cybercrime fighters 'flat footed' theirs strategies of tackling cyber-enabled crimes at times are thrown into limbo. Billions of dollars held by organisations are at risk every single day. This threatens the very existence of major organisations and especially the financial institutions. In the past, cybercrime was committed mainly by individuals or small groups. Today, we are seeing highly complex cybercriminal networks bringing together individuals from across the globe in real time to commit crimes of an unprecedented scale.

The world today is witnessing Criminal organizations turning increasingly to the Internet to facilitate their activities and maximize their profit in the shortest time. According to information Security Timelines and Statistics, 2016 report, cybercrime has consistently increased. Whilst the value of the cybercriminal economy as a whole is not yet known, the most recent estimate of global corporate losses alone stands at approximately €750 billion per year (Bert Wainwright; 2010).There is now a sophisticated and self-sufficient digital underground economy in which data is the illicit commodity. Stolen personal and financial data – used, for example, to gain access to existing bank accounts and credit cards, or to fraudulently establish new lines of credit – has a monetary value. This drives a range of criminal activities, including phishing, pharming, malware distribution and the hacking of corporate databases, and is supported by a fully-fledged infrastructure of malicious code writers, specialist web hosts and individuals able to lease networks of many thousands of compromised computers to carry out automated attacks. The prospect of more than Sh15 billion being skimmed off each year through shadowy digital networks is profoundly terrifying, especially in an economic environment where private companies and the public sector are forever grappling with acute budget constraints.

according to Kaigen et al, (2015) cybercrimes targeting banks and other financial institutions is probably higher by 30% than in none financial institutions costing hundreds of millions of dollars every year. Cyber theft of intellectual property and business-confidential information probably costs developed economies billions of dollars every year. Kaigen et al, (2015) plus other studies by Jackson et al (2004), and Kshetri (2005) only describe the economic impact in general, none of this studies narrow down to what costs banks are incurring as a result of cybercrime activities and how it is affecting performance of these institutions . Therefore the study was to investigate the effects of the vice with an aim of establishing possible mitigations to cybercrime related costs for the sustainability of the banks in Kenya.

The unfortunate thing is that cyber security policies instituted in most Kenyan companies do not reflect the magnitude, complexity and full range of risks they face. This hit-and-miss approach can be very costly. In the same breathe many organisations in Kenya ignorant of the magnitude of it, continue to allow risky practices by their employees. For instance, many organisations have overwhelmingly embraced the Bring -Your-Own-Device (BYOD) practice without factoring in the risks. BYOD is simply the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace, and to use those devices to access privileged company information and applications.

BYOD can help save costs and even act as an incentive to younger employees. However, on the flipside, BYOD can severely compromise a business' data security. Staff can access proprietary company information on their personal phones, including passwords, and share it with third parties either intentionally or unknowingly. This level of vulnerability has been created in the endeavor to cut on operational costs.

According to InfoSec Guide on Dealing with Threats to a Bring Your Own Device (BYOD) Environment, it establishes that although bring your own device (BYOD) adoption has risen greatly over the past few years as companies look to improve work efficiency and lower operational costs, any organisation adopting it should device methods to counteract the major threats this practice possess.

The guide brings to perspective that as mobile devices form a large portion of an organization's BYOD ecosystem, organizations must be aware of the risks they face from malicious mobile apps downloaded by the users of these devices. Users who download through third party app stores and torrent repository websites often fail to check the authenticity of the apps they download, failing to realize that a large number of these applications are actually malicious in nature. Cyber criminals usually trick users by posing as legitimate downloads of new and popular applications such as last year's Super Mario Run. What makes some of these apps particularly dangerous is that they appear to run like the actual applications, but deliver other malicious payloads such as unwanted advertisements or even malware.

If the organisations, governments or individuals wish to defend against malicious apps, they should categorically provide endpoint security solutions to all their staff allowed to bring their devices and access important information through them**.** *In* addition, the organization's enterprise solutions should include device management and application management features that allow IT professionals to manage the installation of applications from a single, centralized console.

Speaking during the Connected Summit 2017, Cisco Regional General Manager, David Bunei said the increasing use of cyberspace and digital applications posed its own challenges, which are however, outweighed by the opportunities. He said that Kenyan Banks have become the leading target of cybercrime as people increasingly adopt the use of financial technology. According to Serianu's Cybersecurity Report 2016, African countries lost at least $2 billion in cyber attacks in 2016. In East Africa, Kenya recorded the highest losses — $171 million — to cyber criminals. Tanzania lost $85 million while Ugandan companies lost $35 million. Over one-third of organisations that experienced a breach in 2016 reported substantial customer, opportunity and revenue loss of more than 20 percent, this according to Cisco 2017 Annual Cybersecurity Report.

According to Robert Mugo, the Ag. Chief Executive Officer of ICT Authority the government was committed to developing comprehensive and offensive cyber-capabilities to protect citizens in the cyber space against threats and attacks. "We will achieve this goal through enhancing ICT security competencies and bolstering international collaboration," said Mr. Mugo.

Going by the statistics in the recent Kenya Cybersecurity Report 2016, published by Serianu Limited, Kenya lost about $175million last year. In 2016, Kenya witnessed more advanced attacks in banks mostly perpetrated by insiders, raising the concern that the banking sector is unprepared to deal with insider threats. According to the Serianu Report, other sectors that have attracted criminals are the government, telecommunications, mobile money services, Saccos, microfinance and co-operatives, e-commerce and online markets Moreover, the Report managed to establish that cybercriminals are deliberately targeting the Kenyan digital economy with the intention of wreaking havoc and making away with millions.

"Essentially, in terms of cyber resilience, the Kenyan digital economy can be likened to a slow, plump gazelle stumbling through the "cyber-savannah" in the full view of agile, informed and hungry cyber-predators keen to sink their teeth into their sumptuous prize," said Teddy Njoroge, the ESET East Africa Country manager. He observed that with more than 75.3% of Kenyan citizens formally included in financial services through financial technology, one would logically expect a correspondent increase in cybersecurity investments in the financial services sector. Regrettably this is the opposite in the case of Kenyan banks. The Kenya Cybersecurity Report 2016, highlights that about 44 percent of financial institutions run on a paltry cybersecurity budget of $1-1,000 annually, whilst about 33 percent of financial institutions in Kenya have $0 spend on all matters cybersecurity. This is very unfortunate given the amount lost by these institutions annually. The institutions should invest on technology that minimize to the lowest levels if no eradicate cyber crimes. "Effective infrastructural cybersecurity measures come at a budgetary cost which should be a strategic decision and provision if any business is to tame the constantly evolving threat landscape. According to Njoroge of ESET, Hackers collectively invest in their own expertise and tools and a non-forward looking institutions who continue to ignore this phenomenon, is headed to a collapse. At times lack of competence, lack of integrated security strategies and policy response to cybercrime costs the banks so much that the banks sustainability in Kenya today is not guaranteed. in April 2019, the Barclays bank of Kenya lost 400000 USD although system manipulation that allowed a number of ATMs to release millions of shillings undetected for a couple of hours despite elaborate systems installed by banks to detect and prevent system hacking. This was done through ATM jackpotting. This form of system interference enables exploitation of physical and software susceptibility in automated banking machines that result in the machines dispensing unlimited cash. With physical access to a machine, ATM jackpotting enables the theft of the machine's cash reserves, which are not tied to the balance of any one bank account. Thieves who are successful and remain undetected can walk away with all of the machine's cash as in the case of Barclays bank of Kenya.

At times culprits use a portable computer to physically connect to the ATM along and use malware to target the machine's cash dispenser. In this bold public approach, an attacker will often use deception and weaker targets to limit risk, like dressing as service personnel to avoid scrutiny. Stand-alone ATMs in retail and service outlets are more likely targets, away from a bank's tighter monitoring and security. Older machines, which may not be fully up to date, are also common targets. This may go on undetected due to the camouflage used in terms of fake uniform, sophisticated outlook and confidence with which this is done. A rash of ATM jackpotting broke out in Latin America in 2017. Following that, attacks, many more have been witness in Europe, Asia and the United States in 2018. In the United States, the attacks resulted to a theft of over a million dollars. U.S. intelligence agencies warned about the threat, noting that guides outlining the process have been discovered on the dark web.

There are different ways that cyber criminals use to access the organisations or individual accounts and manage to siphon money. The most common types of online fraud are called phishing and spoofing. Phishing is the process of collecting your personal information through e-mails or websites claiming to be legitimate. This information can include usernames, passwords, credit card numbers, social security numbers, the authentic-looking website asks the victim to disclose privacy-related information, such as user identification and password. Often the hook is an obfuscated URL that is very close to one the victim finds legitimate and is really a site under the attacker's control. The lure is an enticement delivered through email. The victim not able to detect provide confidential information and this allow the criminals to access their bank accounts undetected. Phishing (a deliberate misspelling of the word 'fishing') is a critical form of cyber crime. It enables criminals to tricks computer users into disclosing personal details such as usernames, passwords, PIN numbers, and credit card numbers etc., which are linked to bank accounts or on-line shopping accounts.

Clone phishing is also targeted at specific individuals or organizations wherein a previous legitimate mail will be copied/cloned so as to look almost identical to the original mail. It's also used to trick accounts owners into disclosing personal information to criminals. Criminals also use Ransom malware, or ransomware, which is a type of malware that prevents users from accessing their system or personal files and demands ransom payment in order to regain access. They may for example inform the bank account owner that their accounts have been disabled or locked for some reason and to enable the activation, they should provide some information. The unsuspecting victim may give the information like identification number, date of birth and password. Having given such, the criminal gain free access to the victim's accounts.

A new breed of ATM hackers gets in through a bank's network, beyond so-called jackpotting attacks, which cause individual ATMs to spit out money, hackers are manipulating ATM networks and the digital authentication checks in the machines to cash out fraudulent transfers they initiate around the globe. using their criminal minds and wit, hackers at times enjoin with the banks IT department staff of a financial institution and lure them to install gadgets that relay key information to external servers for a time and on a specific day when no one is vigilant enough the criminals hack into the system and get away with millions of shillings in a matter of hours. The money is then sent to many M-Pesa super agents across the country. Later confidently the agents walks to the bank and withdraw it. The hackers then go round in cars collecting their loot and paying off the agents.

According to industry sources out of 47 banks, less than 10 have their core banking system relatively safe. “The sad part is that the management in the helm of these institution have little or no relevant IT competence and due to work related pressure, they are not vigilant enough to notice a system interference as they focus on meeting set targets. Even after noticing an issue they are not interested and take too long to respond to the attacks,” said a senior industry player. In one such case hackers, installed a computer in a well-known bank in Kenya and transferred Sh150 million between Saturday, 5pm, and Sunday noon. No one has been arrested, months later.

The Central Bank of Kenya and card payments solution provider Visa held a cyber security workshop in a Nairobi hotel in march 2019. In this it was disclosed that ignorant customers and rogue bank officers colluded with hackers to aid ATM-induced cash outs. Hackers target mainly young and new bank account holders. They ride on details of ignorant account holders to find easy entry into banks and safe passage for money siphoned off. Details and scale of loss from this sophisticated fraud involving bank customers, rogue employees and hackers is top secret in the banking sector as institutions work extra hard and spend more to build solid buffers. Some are even willing to pay an arm and leg to conceal this truth. Banking insiders who spoke to the Star media officer in confidence due to the sensitivity of the matter said most accounts at least seven out of 10 bank accounts flagged belong to customers with an average age of 23 years and have balances of less than Sh1000. Most ATM cards used normally have zero transitory history and are never reported as lost," a senior cyber security officer at a multinational lender said. Experts say most of these accounts belong to students of institutions of higher learning. The students are hippy, ignorant and in need of quick funds regardless of the source, hence easy target by cyber criminals, some of who were their schoolmates. They either don’t know or care less about the consequences of providing their banking details. It gets worse when rogue bankers join this web. "There is an urgent need for cyber security sensitization among customers, especially now that most lenders are going digital,'' another Information Technology head at a fast growing local bank said.

In a survey conducted by the Star Group where they asked at random students at the University of Nairobi and neighboring Kenya Methodist University town campus if they can sell their bank details for Sh100,000, Out of the 20 students sampled, 14 said they would promptly do so while four would refuse but did not give reasons. Only two were aware of the risks involved, saying it is a crime. The simple survey showed that male students are likely to collaborate with cyber criminals than their female counterparts, with only three out of 12 sampled saying they would decline the offer. 'That is gold presented on a silver platter. I don't remember when I last deposited in my account Sh100,000, it can help me sort a few problems,'' Kibe, (not a true name) a second year UoN student said. surprisingly his friend said he would willingly give his national ID as a bonus and take even Sh50,000 after all ''It is simple to sign up for another bank account, thanks to technology. Internet and my phone are all I need to open 10 accounts in deferent banks. Selling some for such fortune is not madness,'' he said.

On Friday, the Assets Recovery Agency asked a court to freeze the accounts of a university student who fraudulently transferred Sh41 million from I&M Bank to himself.

Timothy (not his true name) of Jomo Kenyatta University of Agriculture and Technology (JKUAT) is said to have devised an intricate scheme to defraud the bank using its login credentials in the Safaricom web portal. Detective Jackson Nzau told the court that the suspect and accomplices fraudulently transferred the money from I&M's Party Paybill Number 517822 to other persons and later to himself in November 2017. The deposits and withdrawals were made in tranches below Sh1 million to evade Central Bank of Kenya's reporting unusual threshold. Any withdrawals beyond Sh1 million must be reported and the account holder should declare the source of the money.

Bevan Smith, head of risk, Visa sub-Saharan Africa, said hackers looking for easy way into banks systems are having a field day using genuine cards. ''ignorant customers especially young ones have become easy targets. A hacker needs a slight security blunder to loot. It is even much easier when genuine customers provide the way and are cleared by rogue employees in the financial sector,'' Smith said. ''Although digital innovations are aiding efficiency in the financial sector, hackers are getting smarter and are now using genuine bank details provided by customers and employees knowingly or unknowingly,'' he said, adding that most hackers attack local banks at odd hours, weekends and on eves of big holidays like Easter and Christmas when bank employees are relaxed and customers transact carelessly.

CBK's Eunice Koiyani said the regulator had witnessed poor cyber security hygiene in its investigations and asked banks to handle their reports with extra care."Cyber security audit reports are gold to hackers. They expose soft underbellies for attack and assist the hackers to strategize. Those classified information must be protected,'' Koiyanisaid. Her sentiments were echoed the following day by Bright Gameli, a cyber security expert and head of IT at the Internet Solution Kenya.

Gamely, who is also an ethical hacker, told a cyber security seminar organized by Kenya Bankers Association (KBA) on22 march 2019 that hackers can easily access cyber security reports by banks due to poor handling and security checks. ''Most banks in Kenya have naked information floating online. Banking staff don't know how to secure their emails while some institutions allow strangers like cleaners access key rooms unchecked,'' Gameli said. He warned financial institutions against giving key transaction credentials to risky employees who can be easily compromised by criminals.

''It is extremely risky to entrust transaction credentials with employees planning to exit the company however how good they are. Banks have made this mistake and paid dearly for it,'' Gameli said. Integrated Payment Services Ltd (IPSL) chief executive Agnes Gathaiya asked banks to become more vigilant and update their systems to remove 'middlemen' in virtual transactions. She said that whereas Pesalink is supposed to aid seamless person-to-person transactions. A study conducted on 30 banks in the country revealed that in 25 banks, human hand is still at the center of such transactions, hence easily susceptible to interceptions and fraud.

In March last year, technology firm Microsoft warned Kenya to prepare for a massive exploration of cybercrimes, a month after the National Bank of Kenya confirmed that fraudsters had gotten away with Sh29 million in what was suspected to be a hacking incident. According to director of Cloud strategy at Microsoft Rudiger Dorn, cybercrime cost the global economy Sh600 trillion in 2017, up from Sh300 trillion in 2016.

We are likely to see an increase in phishing- where hackers obtain account details of employees or individuals through credit cards and banking details to commit a cyber crime,'' Dorn said. In another report released by technology firm Cisco showed that more than half of such cyber-attacks result in financial damages of more than $500,000 (Sh50.55 million) annually in Kenya including, but not limited to, lost revenue, customers, opportunities, and out-of-pocket cost. In an effort to deal with the menace, the Kenyan government have tried to create regulations. In July 2017, the CBK introduced cyber security policy guidelines aimed at helping banks deal with cybercrimes and prepare for emerging threats. Banks are required to compile and file annual report with the regulator detailing on how they plan to curb cyber security threats. Last year, the regulator widened the scope to mobile money transfer networks which are demanded to notify CBK within 24 hours of any cyber security incident.

"The guidelines set the minimum standards that industry players should adopt to develop effective cyber security governance and risk management frameworks in order to maintain a sound, secure and efficient National Payment System," CBK said. Yet despite all this efforts banks and customers continue to lose money to fraudsters and hackers.

Statement problem

Cyber security is that technologies developed tor designed to ensure that organisations systems, operations or networks are free from illegal access and attack in the last one decade the internet use has reached all levels high. in a report titled 'The State of the Internet in Kenya 2016' there is a recognizable and tangible growth in use of e commerce in terms of capacity and revenues. There is an explosion of data transfer and electronic transaction. so much networking between organisations expose their programmes, processes and information. Varied environments and players are automatically are able to access the online platform for any organisation. Due to the millions of data transfer on the internet platform, banks like other organisation have become exposes to cybercriminals. This has resulted to loss of billions of shillings to unprecedented cybercrime activities across board. Atul Shah, (2016), did a survey and reported that Kenyan banks conservatively lose Sh15 billion annually to cybercrime and that this figure could be significantly higher, considering most victims are not even aware that they are vulnerable. A recent report – State of Cybersecurity in Kenya – indicates that 70 per cent of Kenyan businesses are vulnerable to cybercrime, yet most of them are ignorant. March, 2017, Kenya witnessed the arrest of a cybercriminal who has managed to consistently siphon approximately 4 billion over a number of years without being discovered from the Kenya revenue authority. The prospects of just a few individual being able to skim billions from a business unnoticed is a terrifying fact to any company. The banking sector comes second to the government as the most vulnerable institutions to cybercrime. The volume of data transfer facilitating money transactions, the number of players in this sector, coupled with the elaborate network makes this sector the most vulnerable to cybercrime. With the heavy losses, business can no longer afford to ignore the fast growing vice that could bring them down in a day. All stakeholders in the economy must have integrated measurers that collectively fight the vice if the institutions want a guaranteed sustainability. There is therefore the need for an integrated cybercrime policy, budgetary allocation to facilitate cybercrime detection and prevention as well as other mitigation measures that may include customer, clientele sensitization to control the vice. This paper sought to create an understanding on the effect of cybercrime activities on the performance of commercial banks in Kenya with a focus to highlighting relevant measures to curbing or reducing the criminal activities.

General Objective

Investigating extent to which cybercrime influences performance of commercial banks in Kenya

Specific Objectives

i. To investigate extent to which cybercrime activities influence prevention and detections costs of commercial banks in Kenya
ii. To determine the extent to which cybercrime activities affect bank financial performance of commercial banks in Kenya.
iii. To evaluate influence of cybercrime activities on response costs performance of commercial banks in Kenya
iv. To investigate influence of cybercrime activities on negative brand image costs of commercial banks in Kenya

Hypotheses

$H0_1$: There is no statistically significant effect of cybercrime activities on prevention and detections costs of commercial banks in Kenya

$H0_{2:}$ There is no statistically significant effect of cybercrime activities on bank financial performance of commercial banks in Kenya.

$H0_3$: There is no statistically significant effect of cybercrime activities on response costs performance of commercial banks in Kenya

$H0_4$ There is no statistically significant effect of cybercrime activities on negative brand image costs of commercial banks in Kenya

Scope of the Study

This study focused of eight tier 1 banks, i.e. Barclays bank, equity band and Kenya commercial bank, standard bank, family bank, cooperative bank, commercial bank of Africa and diamond trust bank. These banks serve over 90% of banking population and are high in technology use. Their market share expands to international ranks creating a wider exposure to cybercrime activities. The amount of data transacted on a daily basis is also enormous given the wide market coverage.

LITERATURE REVIEW

Cybercrimes are a new breed of crime that are perpetrated using computers, or are otherwise related to them. Access to unlimited data across the world is awesome but it comes with its fair share of problems. Criminological theories, Social learning theory, low self-control theory, general strain theory, frustration aggression hypothesis, routine activity theory, and situational crime prevention theory guided this study.

Criminological theories explains why some people engage in deviant behavior where as others abstain from crime. These theories explain the mind of those that have no difficult in deliberately breaking the law, have criminal and deviant behavior, as well as patterns of criminal activity. There are three types of closely interrelated factors that influences behavior whether negative or positive. The researcher concentrated on the deviant behaviour. These include psychological, sociological and biological factors. All three of the factors play a role in the expression of behavior. There a many different psychological models of criminal behavior ranging from early Freudian notions to later cognitive and social psychological models. The model is based on the assumption that Personality is the major motivational element that drives behavior within individuals and that normality is generally defined by social consensus. As such crimes then would result from abnormal, dysfunctional, or inappropriate mental processes within the personality of the individual. The Criminal behavior may be purposeful for the individual insofar as it addresses certain felt needs. Defective, or abnormal, mental processes may have a variety of causes, i.e., a sick mind, unsuitable learning or inopportune conditioning, the mimicry of inappropriate role models, and adjustment to inner conflicts (Mischel, 1968).

The psychological model would suggest that a variety of different causes or reasons exist for criminal behavior and that general principles targeted at the individual would be effective for crime control. However, the model also assumes that there is a subset of a psychological criminal type, defined currently as antisocial personality disorder in the DSM-IV and previously defined as the sociopath or psychopath (APA, 2002). This type of criminal exhibits deviant behavior early in life and is associated with self-centeredness, a lack of empathy, and a tendency to see others as tools for their ends. Controls for these individuals would be more extreme and general public policies may not be stringent enough to curb the behavior in this small subset of criminals. Such will perpetually commit crime of any kind without fear of punishment.

Operant learning models are based on the utilitarian concepts that all people wish to maximize pleasure and minimize pain or discomfort. Skinnerian based social psychological theories of reinforcement and punishment are influential in this model of criminal control although the idea of punishment for crime has a much longer history (Jeffery, 1990). Technically speaking, punishments are any sanctions designed to decrease a specific behavior; thus, fines, jail sentences and others are all forms of punishment. However, Skinner himself recognized that punishment was generally ineffective in behavior modification and that reinforcement worked better (Skinner, 1966).

In line with other psychological methods are policies aimed at maintaining a visible presence of law enforcement and methods to maintain self-awareness in tempting situations. Such methods are preventative. For instance, it has been a well-known social psychological principle that situations that diminish self-consciousness and self-awareness lead individuals to being less restrained, less self-regulated, and more likely to act without considering the consequences of their actions (e.g., Diener, 1979). The simple act of placing screening guards or sign to mark existence of surveillance even when there is none in any business premises creates a self-awareness and decrease chances of thinking to commit a crime. Likewise, the presence of visible security camera can cut down on crime. Making sanctions and the consequences for crime well-publicized and available to the public is another psychological method to control crime in this vein.

Thus, methods of crime control policies based on psychological principles target the individual and attempt to reform or prevent criminal behavior from that outlook. Any policies requiring therapeutic intervention, retraining, or education are psychological in nature. Any policy designed at preventing crime by targeting individuals such as raising consciousness, promoting self-awareness, or identifying individuals at risk are also psychological. Likewise, psychologists have long recognized that the best predictor of future behavior is the individual's past behavior (Mischel, 1968). So policies that are specifically designed to deal with repeat offenders are also based on psychological principles of criminality.

Sociological and Psychological principles of criminality are intertwined and technically not independent. As with psychological theories, there are numerous sociological formulations of the cause and control of criminality. Sociological theories associate an individual's criminality with the broader social structures and cultural values of society, family or peer group. The dissonance or malfunctions of all these interacting groups contribute highly to one's criminal tendencies. Similarly, the grip by these groups, a healthy interaction with the same traditionally ,help in keeping even a typical criminal on their toes and my deter errant behaviour . the social fabric is key to taming at the right time the errant behaviour that may result to criminology.

Traditional sociological theories proposed that crimes was a result of anomie, a term meaning "normlessness" or a feeling of a lack of social norms, a lack of being connected to society. The term was made popular by Émile Durkheim (1897) who originally used the term to explain suicide. Later sociologists used the term to describe the dissociation of the individual from the collective conscience or the criminality resulting from a lack of opportunity to achieve aspirations or by the learning of criminal values and behaviors. Therefore criminality results from the failure to properly socialize individuals and by unequal opportunities between groups.

Durkheim believed that crime was an inescapable fact of society and advocated maintaining crime within reasonable boundaries.

Observations show that majority of individuals that finally get into crime come from broken families, societies and live in a dysfunctional community. According to john Locke an English philosopher who lived between 29 August 1632 – 28 October 1704) in his *Essay Concerning* Human Understanding restated the importance of the experience of the senses over speculation and sets out the case that the human mind at birth is a complete, but receptive, blank slate (scraped tablet or tabula rasa) upon which experience imprints knowledge. Locke argued that people acquire knowledge from the information about the objects in the world that our senses bring. People begin with simple ideas and then combine them into more complex ones. According to his philosophy, tabula rasa theory, that at birth the (human) mind is a "blank slate" without rules for processing data, and that data is added and rules for processing are formed solely by one's sensory experiences. It is therefore clear that even the criminal tendencies are learnt, practiced, rewarded and grow within a person and the family and society write the crime data in the slate. Sociological theories states that society “constructs” criminality. Thus, certain types of human by activity are harmful and are judged so by society as a whole. But it is also true that there are other behaviors recognized society as “criminal” that do not result in harm to others and are therefore criminalized without sufficient ground, these are the so-called “victimless” crimes (Schur, 1965).

An important sociological control would be to increase legitimate opportunities for advancement and obtainment of goods and wealth in areas where these do not exist. Sociological controls targeted at this goal could originate in higher State of government as well as local levels of government and would include programs designed to guarantee equal opportunities to all individuals. Thus, social programs ranging from soup kitchens, job training, educational funding, urban renewal projects and so forth would be in line with sociological policies to control crime (Merton, 1968). Other related sociological controls for crime would consist of organizing and empowering neighborhood residents with projects like neighborhood crime watches, providing law-abiding role models for children in schools and in other venues, providing parental support for working parents, and establishing community centers in downtrodden areas to allow people to learn and engage in positive activities. Social programs aimed at socializing children properly and providing support for single family homes are also examples of sociological methods to control crime. There are a number of these programs including career academies (small learning communities in low-income high schools, offering academic and career/technical courses as well as workplace opportunities). Strengthening the family and social structures and focusing the youth energies in right activities like sports, social functions etc. could curb the errant behaviour.

Also sociological policies to control crime would advocate stronger and harsher penalties for serious economic crimes such cybercrimes. There should be enhanced and more effective law enforcement (Hester & Eglin, 1992). Interestingly biological theories of criminality basically purport that criminal behavior is the result of some flaw in the biological makeup of the individual. This physical flaw could be due to Heredity, Neurotransmitter dysfunction, and Brain abnormalities that were caused by either of the above, improper development, or trauma (Raine, 2002) biological theorists would also endorse stricter penalties and better law enforcement techniques for crime control, but there are several methods of crime control that are specific to the biological theories of criminality.

Although, these theories were originally meant to explain crimes committed in the 'real world', they can still be applied to cybercrime. These theories include social learning theory, low self-control theory, general strain theory, frustration aggression hypothesis, routine activity theory, and situational crime prevention theory. This paper analyzed aspects of the above theories, for the purpose of seeing which best explains the cause of cybercrime.

Akers' social learning theory is a general theory of crime and has been used to explain a diverse array of criminal behaviour. This work embodies within it four fundamental premises that include differential association, definitions, differential reinforcement and imitation (Burruss et al., 2012). Social learning theory is based on the idea that individuals develop motivations and skills to commit crime through the association with or exposure to others who are involved in crime (i.e., associating with deviant peers). Akers's proposed that this exposure to deviant behavior provided individuals with definitions that are seen as either approving of or neutralizing the behaviour. These definitions become rationalizations for criminals when committing a crime. Differential reinforcement refers to the rewards that are associated with a particular criminal behavior. This criminal behavior is originally learned through the process of imitation, which occurs when individuals learn actions and behavior by watching and listening to others. So, when an individual commits a crime, he or she is mimicking the actions that they have seen others engage in (Burruss et al., 2012). In regards to cybercrime, research has found that social learning theory can explain the development and ongoing issue of software piracy. In their study of software piracy, Burruss et al, found that individuals who associate with software piracy peers learn and subsequently accept the deviant conduct. Software piracy requires a certain degree of skills and knowledge to access and deviant peers to originally learn these skills from. Furthermore, the deviant individuals rationalize their criminal behavior and help in the fostering of a network that connects and teaches other individuals these rationalizations and behavior.

The study also suggested that individuals are more likely to engage in software piracy when they see others experiences positive reinforcement for their participation (Burruss et al., 2012). Not only does social control theory explain for software piracy, elements of this theory can be attributed in other cybercrimes. For example in any crime, the rationalizations and skills must be learned and behavior is reinforced through the association and observation of others. Thus, the main idea behind social learning theory is that we become who we are based on our surroundings and this explanation can be used to explain cybercrime.

While social learning theory emphasizes the importance of external factors that influence criminal involvement, low self-control theory posits that low self-control is a key factor underlying criminality. This theory was originally developed by criminologists Michael Gottfredson and Travis Hirschi. They proposed that their self-control theory can explain all types of crimes, all the time (Burruss et al., 2012). Individuals with low self-control were characterized with being risk taking, short-sighted, impulsive and prefer simple and easy tasks. These characteristics inhibit an individual's ability to accurately calculate the consequences of deviance. According to this theory, crime is seen as a means of obtaining immediate gratification, and the ability to delay such short-term desires is linked to self-control. As such, those with a propensity for criminal involvement are thought to lack sufficient self-control. Also, people with low self-control act impulsively- without much thought and based on what they are feeling at the moment. This makes them risk takers as they do not consider the consequences of their actions. Finally, low self-control people are focused on themselves and lack empathy towards others (Burruss et al., 2012). According to Gottfredson and Hirschi, low self-control originates in early socialization when parents are ineffective in their parenting. Therefore, neglecting and uncaring parents are likely to fail to socialize their child to properly delay gratification, care about the feelings of others, and restrain their impulses. As a result, children with low levels of self-control end up being more prone to crime, and their criminal propensity continues into later life. The characteristics of low self-control can be applied to some simple forms of cybercrime, including software piracy. In their study, Burruss et al , stated that levels of low self-control are directly related to the act of software piracy. For instance, an individual is likely to perform software piracy because they are impulsive and unable to wait to purchase a copy of the software. These individuals are not likely to be empathetic to the copyright holder and neglect any responsibility. Further, these individuals are likely to be attracted to the thrill and ease of engaging in software piracy. The study also found that low self-control does have an effect on software piracy and that social learning theory measures (i.e., associating with deviant peers and positive attitudes toward software piracy) condition this effect. Thus, from the characteristics of low self-control, those with low levels of self-control are likely to participate in deviant behavior both on and offline because of their desire of immediate gratification.

Robert Agnew's general strain theory proposes that strain leads to negative emotions, which may lead to a number of outcomes, including delinquency. The specific strains discussed in the theory include the failure to achieve positively valued goals (e.g., money), the removal of positively valued stimuli (e.g., loss of a valued possession), and the presentation of negatively valued stimuli (e.g., physical abuse) (Patchin & Hinduja, 2011). The first strain looks at the gap between the expectations of the individual and what they actually achieve, which leads to disappointment and resentment. The second type of strain is caused when a positively valued stimulus is removed and the result is delinquency. This criminal behavior may present itself as an attempt to ease or replace the stimuli. The final type of strain occurs when confronted with negative stimuli. This may cause delinquency as a means to terminate or avoid the negative stimuli (Patchin & Hinduja, 2011). According to Agnew, strain does not directly cause crime but rather promotes negative emotions like aggression and frustration. This is directly in conjunction with the frustration-aggression hypothesis by Yale university psychologists. They believed that anger comes before frustration, and frustration can manifest into both aggressive and non-aggressive behavior (Runions, 2013). In turn, these negative emotions necessitate coping responses as a way to relieve internal pressure. Coping via illegal behaviour and violence may be especially true for adolescents because of their limited resources and inability to escape frustrating environments. In their article, Patchin & Hinduja, concluded that general strain theory can be used to explain illegal behavior such as cyber bullying among youth.

Cyber bullying is a serious and growing problem that occurs when youth use electronics to harass or intimidate their peers in a deliberate attempt to inflict direct or indirect harm. There are some unique elements in the digital setting that are not present offline, such as: anonymity, constant connectivity, and permanence. This new technology allows victims to be attacked at anytime and the anonymity of cyber bullies makes it difficult to identify them. Agnew argues that strain makes people feel angry, frustrated, depressed, and essentially creates pressure for corrective action on the part of the victim. In response to this pressure, victims react by wanting to take a corrective action as a means to alleviate the bad feelings. Consequently for some victims, cyber bullying is one corrective action that adolescents might take to mitigate the bad feelings (Patchin & Hinduja, 2011). Together, general strain theory and frustration aggression hypothesis, provide an understanding of how people, especially youth, respond and deal with negative strain, whether it may be to bully others or do deviant acts to alleviate the strain.

Routine Activity Theory was developed by Cohen and Felson to originally fill the shortcomings in existing models that failed to adequately address crime rate trends since the end of World War II. They suggested that the behavior of most victims is repetitive and predictable and that the likelihood of victimization is dependent on three elements: motivated offenders, suitable targets, and the absence of capable guardians (Reyns, 2013). The motivated offender is someone willing to commit a crime if an opportunity presents itself. A suitable target is one that the motivated offender values (e.g., credit card information). In addition to these, a capable guardian includes anything that obstructs the offender’s ability to acquire the target (e.g., antivirus, encryption). With the increasing use of the internet, criminals have found new opportunities to victimize their targets on a whole new platform. Researchers have found some support for applying the tenets of routine activity theory to the study of cybercrime (Van Wilsem, 2011). People whose regular activities place them in situations where they have the possibility of interacting with offenders are at an increased risk of being victimized. Research has found that the amount of time spent online, more use of internet banking and online purchases, and risky online behavior make people more suitable to offenders. Individuals with these actions are more likely to be targeted for identity theft. Furthermore, the lack of antivirus and network security (capable guardians) is associated with more victimization (Reyns, 2013). So, routine activity theory can be used, to an extent, to explain certain types of cybercrime.

Situational crime prevention is a crime prevention strategy that addresses specific crimes by manipulating the environment in a way that increases the risk to the offender, while reducing the potential reward for committing the crime (Hinduja & Kooi, 2013). It is rooted in rational choice theory, routine activities theory, and crime pattern theory. Like other prevention measures, situational prevention focuses on reducing crime opportunities rather than the criminals. This theory differs from other criminological theories in that they do not look at why the offender did the crime, but rather how to prevent crime from altering the physical surroundings where the crime takes place. Essentially, it seeks to make the criminal act more difficult to commit in the first place. Like other primary crime prevention measures, situational prevention tends to focus on reducing crime opportunities rather than on the characteristics of criminals or potential criminals. In regards to cybercrime, there are ways in which space can be designed to prevent crime through: target hardening, access control, deflecting offenders, and controlling facilitators (Hinduja & Kooi, 2013). Target hardening is the actual physical (or digital) barriers that reduce chances of crime, such as encrypting sensitive information. Access control involves strategies to prevent potential offenders from areas that a crime can occur. This includes photo ID cards, passwords, and check-in booths. Deflecting offenders is concerned with initiatives to move potential offenders away from their crime targets. For example, storing valuable data off-site would deter potential offenders from searching for it. Controlling facilitators involves checking elements that may cause a crime, such as doing background checks on employees or restricting unauthorized installations on computers (Hinduja & Kooi, 2013). Research has found that situational crime prevention strategies can be used to reduce cyber stalking and other online victimization crimes. Also, prevention strategies can be applied InfoSec to effectively protect the assets of organizations from being exploited online (Hinduja & Kooi, 2013). Theoretically, if used effectively, the principles of situational crime prevention seem to be able to prevent most types of cyber crime.

Criminal behavior cannot be explained entirely by one theory; it requires the combination of various theories. Different aspects of each theory can be used in conjunction to compensate for what each individual theory failed to explain. For example, social learning theory believes that crime is learned through association with deviant peers and research has already shown that there is a relationship between the number of deviant peers an individual has and his or her participation in software piracy (Burruss et al., 2012). But, researchers have not examined whether social learning theory applies to all types of cybercrimes or just certain cybercrimes. On the other hand, low self-control theory asserts that low self-control is the cause of crime all the time. This may be true for some criminals, but many criminals, like those involved in white collar crimes, do not adhere to the principles of low self-control. However, while self-control theory is useful in explaining why individuals may act in a certain way, it does not explain the situations that must be met for a crime to occur. Routine activity theory describes the situational factors that must be present for a crime to occur. It is more difficult to apply this theory to cybercrime because the offender and victim do not necessarily have to meet for the crime to occur. Similar to low self-control theory, strain theory maintains that when an individual cannot achieve his or her goals, he or she experiences strain and as a result they may turn to crime (Patchin & Hinduja, 2011). But, researchers could further study whether an individual’s strain in the ‘real world’ affects their deviant behavior in the virtual world. So, an individual’s low self-control and negative strain combined with his or her deviant associations and regular activities can increase an individual’s risk of being victimized online. Future studies of cybercrime victimization may draw benefit from using a combination of these theories to explore the problem. Cybercrime research will be important to our understanding of crime as our society becomes more and more dependent on technology.

Prevention and detection cost

Cybercrime wave’ is an understatement when you consider the costs that businesses are suffering as a result of cybercrime. ‘it is more as an economic epidemic tht has a capability of wiping out the entire species . Three years ago, the Wall Street Journal estimated that the cost of cybercrime in the U.S. was approximately $100 billion. The estimate disputed other reports which pegged the numbers by as much as ten times higher. In 2015, the British insurance company Lloyd's estimated that cyber-attacks cost businesses as much as $400 billion a year, which includes direct damage plus post-attack disruption to the normal course of business (Lewis & Baker, 2013). Some vendor and media forecasts over the past year put the cybercrime figure as high as $500 billion and more. From 2013 to 2015 the cybercrime costs quadrupled, with worse attacks expected by the year 202 (Lewis & Baker, 2013). Juniper research recently predicted that the rapid digitization of consumers' lives and enterprise records will increase the cost of data breaches to $2.1 trillion globally by 2019, increasing to almost four times the estimated cost of breaches in 2015. According to Home Office in their 2001 report on the economic impact of crime in the UK35 define the various types of cost associated with cybercrime (Anderson et al, 2013). Such calamities calls for organisations to spend corrosive amounts on prevention and detection, responses and redeeming of negative image as much as the loss on profitability

Prevention and detection are measures to reduce the amount of loss that organisation may suffer as a result cyber related crimes (Lewis & Baker, 2013). This include installing physical and virtual protection such as antiviral software), insurance costs and costs associated with gaining compliance to required IT standards (for example the Payment Card Industry Data Security Standard, PCI DSS) (Anderson et al, 2013).

Response costs

Despite high security measures installed costing high amounts of money, the cuber criminal at times will access the bank data and siphon money and as such these organisations must respond to losses incurred as a result of cybercrime activities. The response strategies takes into account direct losses to individuals and companies (including business continuity and disaster recovery response costs), and indirect losses arising from reduced commercial exploitation of IP and opportunity costs through weakened competitiveness. Consequential cost are those that have affected the banking institution directly (Anderson et al, 2013).

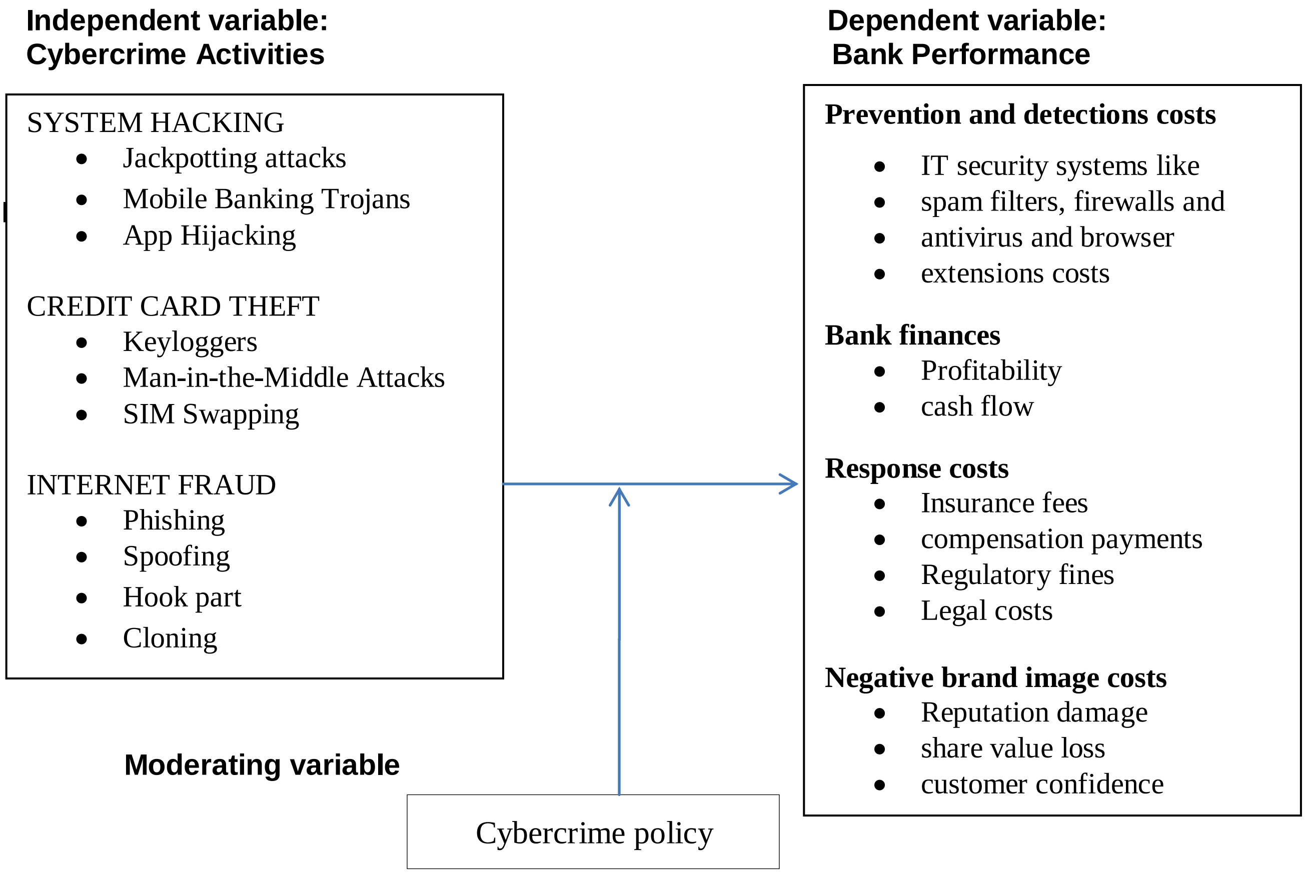
Banks finances and profitability

According to Reuter's media briefs from Cameroon, British prime minister, cyber crime costs the British economy some 27 billion pounds a year., the Economic and Financial Crimes Commission Report ranks Nigeria as third among the top ten sources of cyber crime in the world. It is estimated that after the United States with 65 per cent of cyber-criminal activities and the United Kingdom with 9.9 per cent, Nigeria is the next hub of cyber criminals in the world with 8 per cent. The growth of online banking further presents enhanced opportunities for perpetrators of cyber crime. Funds can be embezzled using wire transfer or account takeover. Criminals may submit fraudulent online applications for bank loans; disrupt e-commerce by engaging in denial of service attacks, and by compromising online banking payment systems Identity takeover can also affect online banking, as new accounts can be taken over by identity thieves, thus raising concerns regarding the safety and soundness of financial institutions.

Indirect Costs / negative image cost

Indirect loss is the monetary equivalent of the losses and opportunity costs imposed the financial institutions as a result of cybercrime (Lewis & Baker, 2013) Since the means (e.g., botnets) would not be around if there were not ends (e.g., phishing victims), we consider losses caused by the cybercriminal infrastructure as indirect by nature; irrespective of whether or not the legal framework formally criminalizes the means (Anderson et al, 2013). Example of Indirect losses include: Loss of trust in online banking, leading to reduced revenues from electronic transaction fees, and higher costs for maintaining branch staff and cheques clearing facilities; Missed business opportunity for banks to communicate with their customers by email; Reduced uptake by citizens of electronic services as a result of lessened trust in online transactions; Efforts to clean-up PCs infected with malware for a spam sending botnet.

Figure 1 Conceptual Framework



Independent variable:
Cybercrime Activities

SYSTEM HACKING
- Jackpotting attacks
- Mobile Banking Trojans
- App Hijacking

CREDIT CARD THEFT
- Keyloggers
- Man-in-the-Middle Attacks
- SIM Swapping

INTERNET FRAUD
- Phishing
- Spoofing
- Hook part
- Cloning

Dependent variable:
Bank Performance

Prevention and detections costs
- IT security systems like
- spam filters, firewalls and
- antivirus and browser
- extensions costs

Bank finances
- Profitability
- cash flow

Response costs
- Insurance fees
- compensation payments
- Regulatory fines
- Legal costs

Negative brand image costs
- Reputation damage
- share value loss
- customer confidence

Moderating variable

Cybercrime policy

METHODOLOGY

Research methodology refers to the steps or sequence of events needed to plan what data is to be analyzed. It provides a frame work of how the study is to be carried out (Stevens &Clow, 2008). Mathooko (2011) state that research methodology includes the research designs, data collection procedures and data analysis were applied in carrying out the research study.

Research design

A research design is the blue print shat guides the researcher in achieving the study objectives . According to Cooper & Schindler (2003) a research design is a framework that specifies the relationship between the variables. Explanative research design was preferred in this study since it involves gathering data that describe events and then organizes, tabulates, depicts, and describes the findings as collected. The design allows the researcher to explanatively dissect the phenomena .The method was preferred because it allowed for an in-depth study of the subject in a quantitative aspect of the overall research. Descriptive research design aims to gather data without any subjectivity.

Target Population/ Sample

The study targeted 200 top and middle level managers that works in selected commercial banks in Kenya. A sample is a smaller group or sub-group obtained from the accessible population (Mugenda and Mugenda, 1999). This subgroup is carefully selected so as to be representative of the whole population with the relevant characteristics. Sampling is the process of selecting a number of individuals for a study (Kothari, 2004). Purposive sampling was done for 30% top management staff totaling to 60 senior staff in the banks. These staff were selected since they hold the required information.

Data collection Instruments

Primary and secondary data was collected using mixed approach of both qualitative and quantitative information. Researcher used questionnaires as data collection tools due to location diversity of respondents. The questionnaire carried both open and closed ended questions to establish the relationship between the variables. These were dropped and picked by the researcher.

Reliability and validity of data

The reliability was ensured by testing the instruments for the reliability of values (Alpha values) as recommended by Cronbatch, (1946). Cronbach's recommends analysis for Alpha values for each variable under study. According to Sekaran (2001) Alpha values for each variable under study should not be less than 0.7 for the statements in the Instruments to be deemed reliable. Consequently, all the statements under each variable were subjected to this test and proved to be above 0.7. A measure is reliable when it is error free and consistent across time and across various items in the instrument. A test questionnaire was administered to 10 employees. According to Mugenda and Mugenda (2003) subjects in the actual sample should not be used in the pilot study. The pilot study was used for checking the validity of the questionnaire.

Pilot Test

Pilot test otherwise known as pre-testing is conducted to detect weakness in the design, data collection instruments and procedures that will be used to carry out the study. As argued by Mugenda and Mugenda (2003), pre-testing of tools helps the researcher assess the efficiency and clarity of the instruments and their uses. Cooper Donald & Schilnder, (2003) further explain that pre-testing allows errors to be identified and acts as a tool for training the research team prior to the actual data collection time. This study pre-tested the questionnaire on at least 10% that is 6 employees of the sample in line with Kothari (2004). He suggests that for a sample size between 0< n< 100, pre-testing 10% of the questionnaires is ideal to serve validity and reliability purposes of the data collection tool.

Data Analysis

The completed questionnaires were edited for completeness and consistency. The data was then coded to enable the responses to be grouped into various categories. Data collected was purely quantitative and it was analyzed by descriptive analysis methods such as measure of central tendency e.g. mean, mode, median and measure of dispersion such as standard deviation, ration as well as percentages. The descriptive statistical tools assisted in describing the data and determining the extent to be used. Data analysis also used SPSS to generate quantitative reports. The researcher then presented the analyzed data through tables, pie charts, and graphs.

Regression analysis was done guided by the model

$y=x_0 + bixi, + b_{ii}x_{ii},+ b_{iii}x_{iii},+ b_{iv}x_{iv}+{}_{e}$

Where,

Y the dependent variable (performance of commercial banks in Kenya), X1 is the prevention and detection cost, X2 is the bank finances X3 is the Response costs and X_4 Negative brand image costs

The researcher conducted ANOVA analysis to test the validity and the goodness of fit of the above regression model in measuring the predictive nature of the dependent variables on the independent variables.

FINDING AND CONCLUSION

From the study findings all the respondents 100% indicated they have e-banking services. This finding is in line with most studies that are recognizing the presence and importance of e-banking services in the developed and mostly in developing countries (Nyangosi, Arora, and Singh, 2009).95% or respondents agreed that cybercrime is threat to the banking sector and only 5% felt that it's not a real threat .

On the Response on number of account holders subscribed to e-banking services, 80% said majority of their customers use e banking services. According to study findings, in average the respondents agreed that the insurance cost of protecting against cyber related criminal activities affecting the bank performances are too high, this also affects the innovativeness of the banks .the banks are skeptical in introducing new products and services as was indicated at a mean of 3.70 and standard deviation of 0.560. On average the respondents agreed that banks pay corrosive charges required to meet IT compliance standards that a bank must comply to when operating on online platforms indicated by a mean of 3.90 and standard deviation of 0.542, the prevention and detection costs are high reducing the bank's profitability. The respondents agreed that it is an expensive venture to identify and assign specific responsibilities by job function for detecting and reporting suspected unauthorized activity. As shown by a mean of 3.90 and standard deviation of 0.628, the respondents agreed that the bank has different insurance accounts set aside to protect customers against losses that may arise from attacks on newly innovate financial products and services as shown by a mean of 3.55 and standard deviation of 0.926, the respondents further agreed that the banks have in place a framework for monitoring the firm's network environment to detect potential cyber security events as shown by a mean of 3.58 and standard deviation of 0.678. This finding was in line with the argument of Lewis and Becker who asserted that Companies will always have to spend on cyber security, but if we assume that some percentage of the current spending would be unnecessary in a more secure cyber environment, those additional spending counts as part of the total cost (Lewis & Baker, 2013).

Findings showed 88% of respondents indicated that cyber security is very important while 5% indicated they were uncertain. The researcher tried to pinpoint how cyber security is becoming a major concern within the financial sector, this notion was supported by the study where the majority highlighted cyber security as major issue this was also in line with findings of Fatima (2015) where pinpointed cyber security as a concern whose solution should be a concern to all stakeholders. Banks spend 2% of its revenue in compensating the victims whose information has been hacked and the image cost cannot be really be accounted. According to study findings 78% of the respondents agreed that frequent successive cyber-attacks on a bank tend to damage how customers view it, in return affecting the overall business as shown by a mean of 3.75 and standard deviation of 0.540, the respondents agreed that cyber transactions, online services, new products and processes constitute a large proportion of a banks research and development costs as shown by a mean of 3.70 and standard deviation of 0.719. Such costs should be protected so that they don't go to drain and the banks to keep incurring more and more.

From the inferential analysis all the null hypothesis were rejected since cybercrime activities had statistical significance on all the dependent variables the p-value which is the level of marginal significance within a statistical hypothesis test representing the probability of the occurrence of a given event was established through the ANOVA Test. $H0_1$ $H0_{2:}$ $H0_4$ showed P ≤ 0.05) while $H0_3$ recorded *p*< .01 which meant that the variables especially in $H0_3$ were strongly correlated. All the Null Hypotheses were rejected and the alternative hypothesis accepted. It shows strong correlation between cybercrime activities and all the dependent variables as indicated also by the model:

$y =x_0+bixi,+b_{ii}x_{ii},+ b_{iii}x_{iii},+ b_{iv}x_{iv}+_{e.}$

CONCLUSIONS AND RECOMMENDATIONS

All these have major effects on the general performance of the banking institution bin Kenya as well as in other countries in the world. The Trend still continues with more intensity yet stakeholders have not come up with a lasting solution. The cybercriminal work round the clock to beat the researched new technologies and the banks must not relent to in innovations that can reduce if not eradicate the vice that is threatening the very existence of the banking sector. Since the epidemic affects the entire world, it should be a globe consulted efforts to beat it. No country can claim to be safe. Cyber-attacks should be classified just like world terrorism and responded to as such. The most effect that banks suffer is on response costs. The banks should consider insurance against this menace to cushion themselves against the related losses. Basically the cybercrime activities have effects on all the variables. to minimize the negative brand image, banks should continuously sensitize customers and provide information to avoid vulnerability of their accounts. For detection and prevention, banks should engage on research to find innovative ways of counteracting those of cybercriminals. There should be consulted efforts from all stakeholders to ensure the effects are minimized either through relevant policies, collaborative technology, communication and punitive measures across the world. Only then are the banks sustainability and growth can be assured. Without such global efforts, it's unfortunate that the institutions existence is not guaranteed.

REFERENCES

Advance Fee Fraud and Other Fraud Related Offences Act 2006, Laws of the Federation of Nigeria 2. Agboola, A. A. (2006).

Ahmed, I. (2008) Nigeria: N10 Billion Lost to Bank Fraud in 2007 – NDIC, Daily Trust, 28 October 2008

Anguelov, C. E. et al. (2004). U.S. Consumers and Electronic Banking, 1995–2003. Federal Reserve Bulletin

Anderson, R., Böhme, R., Clayton, R., Moore, T. (2009): Security economics and the internal market. http://www.enisa.europa.eu/act/sr/reports/econ-sec/economics-sec (2008)

Brynjolfsson, E., Saunders, A. (2009): Wired for Innovation: How Information Technology Is Reshaping the Economy. MIT, Cambridge 2009.

Burruss, George W., Bossler, Adam M. And Holt, Thomas J. (2012).Assessing the mediation of a fuller social learning model on low self-control's influence on software piracy.Crime and Delinquency, 59(5), 1157-1184

Electronic Payment Systems and Tele-banking Services in Nigeria, Journal of Internet Banking and Commerce, Vol. 11, No. 3, online source: http://www.arraydev.com/commerce/ji

Hinduja, Sameer and Kooi, Brandon. (2013). Curtailing cyber and information security vulnerabilities through situational crime prevention. Security Journal, 26(4), 383-402

Lvarez, L. (2012): With personal data in hand, thieves file early and often. The New York Times.http://www.nytimes.com/2012/05/27/us/id-thieves-loot-tax-checks-filing-early-and-often.html (2012)

Patchin, Justin W. and Hinduja, Sameer. (2011). Traditional and non-traditional bullying among youth: A test of general strain theory. Youth & Society, 43(2), 727-751.

Reyns, Bradford W. (2013). Online routines and identity theft victimization: Further explaining routine activity theory beyond direct-control offenses. Journal of Research in Crime and Delinquency, 50(2), 216-238

Runions, Kevin C. (2013). Toward a conceptual model of motive and self-control in cyber-aggression: Rage, reward and recreation. Journal of Youth and Adolescence, 42(5), 751-771.

Van Wilsem, Johan. (2011). Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization. European Journal of Criminology, 8(2),

Wambui Njoroge, (2017). Effect Of Cyber Crime Related Costs On Development Of Financial Innovation Products And Services; A Case Study Of Nic Bank Of Kenya.