IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 19, Issue 9, Ver. VII (Sep. 2014), PP 44-49
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Effectiveness of Strategic Security Systems on Securing Financial Institutions in Nairobi County Kenya

George Kinoti Maingi
(Department of Peace, Security Studies and Social Studies Egerton University)

Abstract:*This study investigated the effectiveness of strategic security systems in securing banks and financial institutions in Kenya. This research project main aim was to come up with various intelligence strategies to minimize risks as low as reasonably practicable, add value to business and increase growth and sustainability of banks and financial institutions in their achievement of their business goal and overall attainment of the 2030 vision in respect to our country Kenya. This study therefore concluded that an effective strategic security system played a fundamental role in searching for accurate and actionable information about whom the enemies were, where and how they operated, how they were supported, the targets the enemies intended to attack, method of attack they intended to use and analysis of existing control measures in withstanding the threats. This study recommended that the management in these institution needs to invest in adequate physical, human and technological security systems which can be perfect deterrence to the standards required by the consumers. This huge investment should be coupled with a well trained workforce who would operate the security apparatus effectively. Just like the audit department, security should be left to operate independently without interference. Its interference amounts to intimidation and which may affect negatively on these security personnel and general output in adding value to institutions overall mission and vision.*

Keywords: *Security, Intelligence, Training, Equipments, Technology*

I. Introduction

This study explored the impact of strategic security systems and subsequent value in boosting the financial institutions in militating against risks and threats as well as meeting the set goals and objectives. Effective security strategy can be defined as a logic that drives the plan and as an actionable intelligence that adds value to decision making. The main objective of strategic security systems in securing financial institutions is to put in place predictive, penetrative and preemptive intelligence measures in identifying, assessing and analyzing institutions threats and risks accurately, timely and objectively to enable the management who may include the chief executive officer, board of directors, financial heads, operational managers, supply chain managers and all other stake holders to take timely action and always stay ahead of evolving risks and threats.

The effectiveness of strategic security systems in organizations revolve around the three pillars of security, namely human, physical and technology. The three spheres safeguard the key target of attack which is the economic growth of a country. The economic success and empowerment is the threatened target which is the core business of financial institutions. Technological pillar includes the access control systems that monitor, control and manage all access systems. It includes inter alia, various biometrics, walk through, mantraps, baggage scanners, visitors and staff access cards etc to control staff, customers, supplier's movements and other movements in respect to organizations business.

The physical pillar plays a major role in introducing time delays when accessing the premises of the organization and more so its sensitive areas.Phyisical systems like doors, windows, gates, perimeter walls, bollards, barriers among other physical provisions grant the first line of defense. To supplement the physical and technological pillar, the human pillar which includes the internal security, private security and police on duty where sourced, overseas the harmonization of the collective effectiveness in deterring, disrupting and preventing threats that may pose danger or risk to the institution. Basically, human pillar may be termed as the third master eye that is intuition driven than automated.

Preoccupation of police with law and order notwithstanding other challenges and taking into account the countries ratio of police of 1; 950 as opposed to the international standard of 1; 450, makes it impossible for the financial institutions to be policed on 24/7 with personalized attention. This is further escalated by non professionalization of the (BFIU) Banking Fraud Investigating Unit that handles all financial institutions economic crimes. Traininning, funding and other incentives ought to be provided as benchmarked with other professional bodies or corporations with a standing policy on the permanency of the investigators to encourage staff retention and discourage flight of seasoned experienced investigators to greener pastures.

Bank fraud has been on the upward trend and so rampant that criminals are obtaining money, assets, or other property owned or held by the financial institutions at a level that has rendered some to close down, others

subjected to statutory management and receivership. In Kenya, several incidents of armed robberies both inside the bank and during cash in transit operation have been experienced with fatalities to both security personnel and the banks staff.

Taking all this into account, it was important to study the effectiveness of strategic security systems in securing financial institutions in Kenya and how they could impact in revolutionalizing and modernizing security control systems that could meet the threshold of international standards, ISO certification and match the risks and threats challenges.

The statement of the problem in this study was exhaustively analyzed and a number of conclusions and recommendations made in this regard. The findings illustrated the need for Financial Institutions to effectively secure the institutions and enhance full proof security systems against penetration by unauthorized parties. The management needs to invest in adequate security systems which can be perfect deterrence while meeting the standards required by the regulators.

II. Methodology

This study focused on all Financial Institutions located in Nairobi. This study adopted a descriptive approach. This study targeted a sample of 25 commercial banks operating in Nairobi and all the eight licensed micro finances (8). Since the study population is large, the study considered 50% of the population of the commercial banks and the entire population of the licensed micro finances targeted. Primary data was collected by use of questionnaires which were used to record the respondent's responses. Questionnaires were ideal for this study because respondents were allowed to respond during their free time considering the nature of their duty. Secondary data was obtained from the respective banks records. Secondary data was useful in providing collaborative information on the problem of the study. The data from the field was first be coded according to the themes researched on the research. This was enabled by the use of a computer in summarizing of data in tables. Frequency tables were produced using the Statistical Package for Social sciences package.

III. Results and Discussions

The researcher sought information from financial institutions in Nairobi to answer questions on the effectiveness of strategic security systems in securing Financial Institutions in Kenya. When asked to describe the acquisition of modern security equipments in their organisation, majority of the respondents as represented by 52% indicated that it was moderately adequate, 40% indicated that it was somehow adequate and only 7% of the entire sampled population indicated that it was adequate. This also tells that most of the security equipments displayed are a mere public relation show gadgets which are not effective at all. Some are old and overtaken by modern technology. Most of the modern equipments are relatively expensive and the maintenance cost may be a challenge. Skills and the experience to operate them may impact negatively on the procured new modern security equipments where new gadgets were procured and not supplemented by training the manning personnel.

Table 4.1: Institution Management Facilitation on Security Team

Statements on security team facilitation	N	Min	Max	Mean	Std deviation
Acquisition of modern and efficient CCTV cameras	42	2	4	2.66	0.61
Integration of the security system	42	1	4	2.88	0.13
Facilitation by consultants	42	1	5	1.73	0.06
Hiring of Armoured cash in transit vehicles	42	1	4	2.07	0.71
Training on emerging modern and new techniques	42	1	2	1.54	0.50

The study wanted to establish the extent to which the respondents agreed on how the banks and financial institutions management facilitated the security team. It was established majority of the respondents agreed that their respective institutions frequently trained them on the emerging modern and new security techniques as represented by a mean of 1.54.They further agreed that external consultants were hired especially on the tasking issues that required special technical knowhow and this was represented by a mean of 1.73. Armoured cash in transit vehicles were also hired as shown by a mean of 2.07.The respondents had a neutral opinion that their organisations had acquired modern and efficient CCTV cameras and had integrated their security systems as shown by a mean of 2.66 and 2.88 respectively. All the standard deviations were less than one indicating that the respondents opinions did not vary that much.

The researcher was also interested in determining the general physical security of the respondent's institution and whether it was a perfect deterrence, from the study it was revealed that majority of the respondents were of the opinion that their physical security system was a perfect deterrence. This encompassed CCTV cameras, effective alarm systems, Visitors pass and login, physical deterrence e.g. electric fence, perimeter wall, Access control and armed police officers. The respondents further indicated that a lot needs to

done to effectively secure the institutions. Some also indicated that there is need for more enhancements for full proof against penetration of unauthorized persons. The management needs to invest in adequate physical security systems which can be perfect deterrence to the standards required by the regulators.

Table 4.2: Facilitatation of Security Team with Special Equipments

Equipments	Frequency	Percentage
Panic buttons	14	33
Bullet proof vests	6	14
Licensed fire arms	5	12
Communication gadgets	17	40
Total	**42**	**100**

This study wanted to establish the extent to which the targeted organisations facilitated their security teams with the above special equipments, from the findings 40% of the respondents indicated to have been fully equipped with communication gadgets,33% indicated that panic buttons have been installed in all the sensitive areas,14% stated that they have been equipped with bullet proof vests while 12% indicated that their respective organisations to have acquired licensed fire arms to help them guard their organisations effectively and efficiently. Similar findings by Boateng (2006) in Ghanaian Banking industry highlighted that for banks to have a perfect deterrence they must implemented modern security measures like motion-sensing and high resolution colour security cameras, time-locked heavy vault doors, silent alarms, exploding dye packs, bait money and locator devices.

From the study it was further established that majority of these financial institutions had few entries and exits. Majority indicated two to three which were all round managed by armed security officers. In most cases there were few entries which facilitated managing external threats. The few entries and exits are effective crowd control systems since the security officers are able to monitor what comes in and out of the institution.

Table 4.3: Specialized Training Provision

Item	Yes	No
Use of CCTV and biometrics	60	40
Use of weapons and detecting gadgets	74	26
physical analytical skills especially in lies detection	78	22
doing forensic audit and tracking credit reports	78	22
detecting forgery and money laundering	84	16

On the specialised training received by the respondents, the study revealed that 84% of the respondents indicated to have received training on detecting forgery and money laundering, 78% indicated to have received training on doing forensic audit and tracking credit reports physical and analytical skills especially in lies detection.74% indicated to be trained on use of weapons and detecting gadgets and finally 60% indicated to be trained on use of CCTV and biometrics. In short most of the security officers go through the fundamental security training but the frequency of these trainings should be increased to sharpen their analytical skills in security.

This shows that without adequate training all the security strategies application can turn to be futile. Installation of effective security systems is a very expensive process and consumes huge capital outlay. This huge investment should be coupled with a well trained workforce who will operate the security system. Without a well trained labourforce there would be no apparent reason as to why the institution should invest in such sophisticated security systems since there would be no appealing end results.

Table 4.4: Individual Performed the Training

Who performed the training	Frequency	Percentage
External local consultant	23	55
Security experts from outside the country	14	33
Head of security	5	12
Total	**42**	**100**

On who performed the security training in these organisations, the study found out that much of the in house training was conducted by external local consultant as shown by 55%.33% indicated that training was

done by Security experts from outside the country and finally 12% indicated that this was done by head of security. This shows that security officers received frequent training on the emerging security issues but much needs to be done to keep them updated especially on the modern crime methodology more specifically the cyber crime which has left institutions with very huge losses across the divide.

On whether the training offered was adequate, the respondents indicated that it was adequate but more training was needed on emerging security issues as security is dynamic. They also suggested that training should be conducted both locally and internationally. There should be periodic update to keep up with the changes in the security world.

Hutchinson, Warren (2003) stated that all bank or financial institution should train its Management and staff on physical security measures and such training should cover the importance of security measures, including at minimum: how the security systems and devices work; what to do in the event of robbery or burglary; how to be a good witness; how to preserve evidence; how to deal with threatening messages and kidnappings; and what measures to take in the event of fire outbreak.

Table 4.5: Managerial Commitment

Managerial commitment	Percentage
Procuring high tech equipments	40
Developing the institution security policy	13
Formation of security intelligence department	25
Ample remuneration of security officers	22
Total	**100**

On how the management in the respondents organisations had shown commitment in regard to the security enhancement, the study found out that 40% of the respondents indicated that the management had played a significant role in the procuring of high tech equipments.25% of the respondents indicated that the management had created an intelligence section whose main obligation is gathering intelligence, analyzing it and acting intuitively.22% indicated that the management had provide ample remuneration for the security officers and finally 13% indicated that the management had developed the institution security policy.

Table 4.6: Level of Commitment

Top management commitment	Frequency	Percentage
Yes	30	71
No	11	26
Somehow	1	2
Total	**42**	**100**

On whether the top management was fully committed in enhancing security in the organisation, the study revealed that 71% of the respondents indicated that the management was fully committed, 26% indicated that the management was not committed and only 2% who indicated somehow. This is an indication that top management plays a critical role in pre determining the security position of an organisation. Security apparatus are quite expensive and without the top management support, purchase and installation of such equipments may take very long duration leaving the financial institutions vulnerable.

Table 4.7: Interference Effects on Security Officer Performance

Interference effects	Frequency	Percentage
Yes	29	69
No	13	31
Total	**42**	**100**

On the respondent's opinions on whether such interference affects the security officer performance, the study found majority of the respondents agree to a very a greater extent that interference affects performance of security officer as shown by 69% and only 31% were of the contrary opinion. When a security officer give out specification on the security apparatus to be procured and the same process is interfered he or she will be at a loss and this may affect his or her performance due to interference. A well trained officer will always give objective reports irrespective of the opinion of the management.

The study also sought opinion from the respondents on what should be done by the top management in the organisation to fully support intelligence and enhance security, from the study majority of the respondents

stated that top management should accept security department to be like any other department in the organisation and event rank it higher because of its role. Top management should allocate enough funds to the security department and the user department should then put specification on the items it deems appropriate then forward them for procurement.

Jayawardhena & Foley (2000) in their study revealed that the Board of Directors of every bank and financial institution should ensure effective implementation and administration of the security program and other security issues. An effective monitoring process is essential for adequately managing operational risk.

The study also revealed that top management supports all initiatives on security management hence they don't interfere at all. The top management relies on the head of security to manage security matters in the organization. Any loss to the organisation which is related to theft and fraud is a great concern for management. Their participation in security issues is always pro active and supportive. The success of security process depends on the support by management. At times they give arbitrary orders that interfere with the security processes.

IV. Conclusion

Security practices in banks reflects a variety of goals: protecting and maintaining the safety of the customers and employees, attracting customers, generating profits, attracting more investors, increasing of more dividends and shares, protecting bank assets, recovering stolen money or any asset of value and apprehending offenders with the ultimate goal of propelling the institution to achieve its objective, vision and mission.

Some financial institutions have adopted more proactive security strategies that are designed to thwart any bleach in security, rule and regulation or the overall standing operating procedures, robberies or any crime before they occur. For example, some have implemented cash management practices that make robberies less lucrative by restricting the amount of cash on hand; others restrict physical access through the use of bullet resistant barriers between customers and bank employees; and still other employees access control systems to stop or deter any offensive or prohibited weapons, contraband or any material unauthorized from being brought into the institution premises.

In spite of all these measures, Commercial Banks in Kenya have been losing millions of shillings and this has rendered some to close down, others subjected to statutory management by Central Bank and others put under receivership. There are 17 such banks in Kenya including Charter Bank, Trust Bank, Daima, Thabiti, Trade, Euro, Prudential Building Society etc. This study therefore concludes that there is a big challenge in the procurement and approval of modern efficient and effective security gadgets in majority of the Financial Institutions in the country. It also concludes that training of the security officers is inadequate. This leaves the banks prone to many security threats especially at this time where cyber crime it taking it over and its giving law enforcers and financial institutions nightmares.

This study also concludes that most of the security equipments displayed by many institutions are mere public relations gadgets which are not effective at all. Some are old and overtaken by modern technology. Most of the modern equipments are relatively expensive and the maintenance cost may be a challenge, skills and the experience to operate them may impact negatively on the procured new modern security equipments.

The security department has not been given adequate space in many Financial Institutions to implement security strategies that are aimed at securing organization. Matters of security should not encourage interference from both the top management and the procurers; otherwise it may erode the primary objective of seeking to procure the items as specified and for purposes intended.

V. Recommendations

This study therefore recommends that high quality digital equipments both on IT gadgets on access control and physical infrastructure should be procured to meet the threshold of international best practices in securing Banks. This will enhance among other benefits, capture of physical appearance and mostly face/front of a person (recognition and identification) of persons transacting business at teller stations and other key locations, such as entrances and exits.

Cameras should be positioned to ensure a full frontal photograph is obtained. Video surveillance systems of the bank floor and teller areas and ATM area should be aligned properly. Those with behavioral configurations must be fixed and well positioned where smart or techno savvy criminals may try or disable to hide recognition and or identification.

Banks should therefore procure the best cameras in the market which can notice (motion detecting) recognize and identify objects like motor vehicles, individuals among others. Effective video footage would help the banks in gathering evidence and also in conducting identification parade in cases of criminal investigations and proceedings. All banks and financial institutions should be connected to the Crime Prevention units which include the nearest police station or Private Security firms. Satellite servers for

information security or data centers to be factored in the event of destruction of the main servers or institution storage servers.

An effectiveness check on all the equipments procured should be conducted by an independent expert to verify whether the equipments will function efficiently and effectively. Those in the procurement department should not be deceived by the hyped marketing done by the equipments manufacturers but they should authenticate and ascertain the real functionality of these equipments. The security officials should not forget the case of McCormick who is believed to have sold 6,000 of the detectors to Iraq and 1,000 other police and military forces including United Nations peacekeepers in Lebanon. Kenya was also a victim of these fake bomb detectors. This call for thorough verification of the equipments to avoid a repeat of such catastrophic mistakes. Marketers will always go an extra mile to sell. Some highly hyped CCTV cameras have faded within months of sale. Proper guarantee and enforceable memorandums of warranty must be executed in binding legal terms.

All the banks employees should be trained to trigger alarms and pick security alarms with speed. Cameras(CCTV) communication as interpreted or analyzed in the control room should be accorded prompt action as soon as reasonably possible to both protect the safety of customers, employees and facilitate seamless management action in the event of any security or procedure bleach. Employees should also be trained to call Police emergency numbers, eg 999, fire brigade and or ambulance as soon as reasonably possible to provide detailed description of the emergency, nature and help needed and give precise direction of crime scene.

The huge investment on the security systems should be coupled with a well trained workforce who will operate the security system. Without a well trained workforce curbing the cyber crime menace may pose a great challenge to the Financial Institutions. All the security officers should be frequently trained on forgery detection, forensic audit, use of weapons, detecting gadgets and use of CCTV and biometrics among others.

Just like the audit department security should be left to operate independently without interference for it to be effective. Its interference amounts to intimidation which may affect negatively on the security personnel mandate to deliver. Top management should accept security department to be like any other department in the organisation and rank it crucial because of its role. In most institutions Security is ranked low and placed under other departments without internal autonomy. Considered adequate funds ought to be allocated as budgeted for by the user, Security. On specification of gadget and other equipments, this should be left to security and consultants where necessary. On procurement, the security must be consulted for due diligence and functionality of the specified services.

References

[1]. Boateng, R. (2006) Developing Banking security capabilities in a Ghanaian Bank: Preliminary lessons, Journal of Banking Security and Commerce: Vol 11 No. 2.

[2]. Hutchinson, D. (2003) Security for Banking: a framework, Logistics Information Management: Vol 16 No. 1 pp 64 -73.

[3]. Jayawardhena, C. (2000) Change in the Banking Sector-the case of Internet banking in the UK, Internet Research: Electronic Networking Applications and Policy: Vol.10 No.1. pp. 19 30.

[4]. Zorkadis, V. (2004), "On biometrics-based authentication and identification from a privacy-protection perspective: deriving privacy-enhancing requirements", *Information Management & Computer Security*, Vol. 12 No.1, pp.125-37.