ISSN 2047-3338

Factors Hindering Integration of Physical Access Control and Cyber Security in the Banking Sector in Kenya

Isabella Njumbi Gitau[1] and Andrew M. Kahonge[2]
[1,2]School of Computing and Informatics, University of Nairobi, Kenya
[1]bella.gitau@gmail.com, [2]andrew.mwaura@uonbi.ac.ke

***Abstract*– Over the last few years, many industrial control systems, including security solutions, have adopted digital technology. Components of these systems, which were physically separated are now linked together over network, making them remotely accessible and thus open to cyber threats [1]. As part of the technological transformation made globally, physical access control and cyber security have been integrated so as to mitigate the risk of the existing cyber threats. However, in the Kenyan banking sector, financial institutions are reluctant to adopt the integrated security model despite its renown benefits. This research focused on determining the factors that hinder integration of physical access control and cyber security in the Kenyan banking sector. The study established factors that determine a banks' attitude towards integration of the two security functions, determinants of banks' intention to integrate their security functions and sources of pressure that would push the financial institutions to integrate physical access control and cyber security. The study also identified factors that hinder integration of the physical access control and cyber security units in financial institutions. The findings of the study were then used to develop a conceptual framework that is recommended as a guide for financial institutions that wish to integrate their security functions.**

***Index Terms*– Physical Access Control, Cyber Security, Network, Security Solutions and Banks**

1. INTRODUCTION

FOR several decades, it has been clear that the subjective division of security related activities into physical access control, IT security, information security and other disciplines has not been favorable to achieving optimal results. The increasing dire consequences of nonintegrated security efforts has caused this separation to, increasingly, be reconsidered by professionals and management. It is becoming more common to see CISOs (Chief Information Security officers) elevated to CSOs (Chief Security Officers) or both functions combined to better integrate the main security elements. Financial sector report by Raytheon [2] revealed the importance of integration of commercial banks security components, as the financial sector experienced persistent exposure to numerous security risks.

A good example being the recent hiring of Kirsten Davies who is to serve as the group chief security officer for the Barclays Africa Group. She was previously working for Hewlett Packard Enterprise where she was the Vice president and deputy chief information security officer. One of her main tasks will be to bring together Cyber security, Information Security, Fraud Strategy, Physical access control and Forensics (amongst other security functions) into a single functional unit [3].

Physical access control for many organizations has become fairly routine and is more easily integrated into information security or information systems security than the other way round [4]. The creation of the Alliance for Enterprise Security Risk Management (AESRM) BY ASIS International, Information Systems Audit and Control Association (ISACA) and the Information Systems Security Association (ISSA) is an indication of the trend in this direction. According to Ula, Ismail and Sidek [5] the access control and information systems security is vital to the overall success of the commercial bank in its operations.

Given that it is not possible to effectively deliver information security without a number of physical considerations, the evolution is natural. It is sensible to expect that convergence of many security activities will center around information security and information systems security in the coming decade as it's also an organizational [5]. As a result, integration of physical access control and cyber security will increasingly be relevant for management in the banking sector to consider.

A) Organizations that are Already Integrating their Security Functions

The New York State is one of the government agencies that has integrated their security units. This has been done through the formation of a new department known as the Center for Internet Security which mainly deals with merging cyber security and physical access control. This will help the government in dealing with emerging threats.

The Integrated Intelligence Center, which is the new department, has implemented a converged approach which is making a major contribution in creating a trustworthy relationship between the government and organizations in the

private sector. This has helped the government in developing and circulating critical information.

The main aim of the new department is to leverage the information that the CIS has obtained from the Multi-State Information Sharing and Analysis Center. This in combination with the information availed by participating partners will offer reliable intelligence products [6]. The unit intends to put into good use the information gathered. Physical access control and cyber security can no longer be viewed separately as an attack on a firm's systems can cause failure of physical infrastructure. Rich Licht, the executive director of the CIS stated that the convergence process was initiated in 2009 [6]. The process began by having monthly meetings whose main agenda was to analyze the risks and threats that they were exposed to. They also tried to brain storm on the best ways of securing the environment so as to ensure that the risks are mitigated. After holding many meetings, the convergence was implemented. This was successful due to the help received from their partners who include the FBI (Federal Bureau of Investigation) and the department of homeland security [7].

In the African continent, no organizations have made public their intention to integrate the two security disciplines. However recommendations on the same have been made by IT security professionals who recognize the need for the convergence. One such professional is Sanjay Vaid who is the director, cyber security and risk at Wipro Limited which is a global IT consulting and outsourcing company. He states that new and emerging technologies such as internet of things (IOT) open up organizations in the African continent to major risks and threats. He insists that it is essential for companies to have an all-inclusive approach as it will help in tightly securing everything from networks, to data centers, Identity & Access to infrastructure, endpoints and more [8].

To reinforce all this, it will be important to focus on converged security so as to get a clear understanding of the various attacks that the firms are vulnerable to.

As a way of preparing for the future, he suggests that a company's IT partner must have an all-encompassing cyber-security practice which must cover every part of the threat landscape. It is also essential to involve the best experts in the security disciplines. He also states that it is important for these IT organizations to include a converged security practice which should include Global security & risk intelligence centers monitoring the risk and threat landscape [8].

The Fig. 1 shows the percentage of organizations that have converged their security functions (21%), those that haven't converged (20%) and those that are not sure whether their security teams are integrated (59%). This was an analysis that was carried out by the Aladdin knowledge system [9].

Current corporate practices and future trends commissioned by the AESRM provide significant insight into the convergence or security integration issue [10].

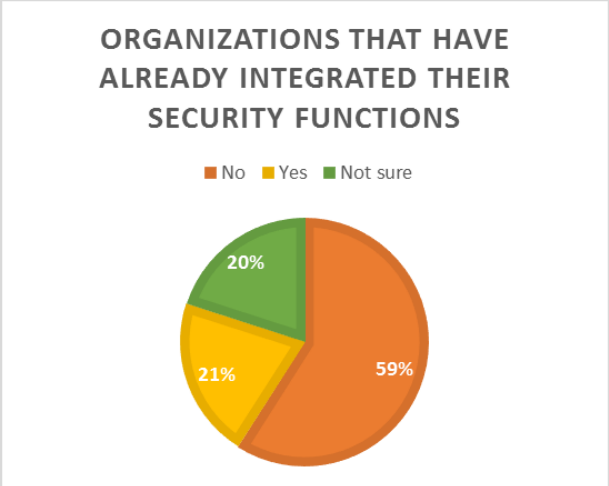

Fig. 1: Source: Aladdin Knowledge Systems 2012

B) Benefits of Integrating the Security Units

According to Aberdeen Group (2011) [11], integration of security systems wields numerous benefits, including; improved physical access control, improved IT security, sustained and improved compliance, faster response times during security incidents, lower total costs in managing the two security units and enhanced collaboration between their IT security and physical access control teams. The findings also showed that initiatives in converging physical access control and IT security are already assisting most companies to achieve improved and superior performance in a number of critical areas

C) Banking and Technology

Banking and Technology are inseparable. The banking industry highly depends on technology to contribute to its great improvement and propagation. Technology enhances and supports the execution of all round tasks in the banking sector. Given that most of the banks' functions are mainly accomplished through exchange of sensitive information, there arises a need to have the integrity of the data exchanged protected [12]. This gives more reason as to why security has to be included in service delivery. More efficient security can be achieved by having a holistic view of security which would include integration of physical access control and cyber security [13].

As new and advanced technologies are introduced to the institutions, the threats become more complex and unpredictable thus giving more reason as to why we should recognize and embrace the need to integrate the two security disciplines considering the new unique security risks facing financial institutions [14].

D) Research Objectives

The study is guided by the following objectives;

a) To establish the factors that determines the attitude of banking institutions towards integration of physical access control and cyber security.

b) To establish the factors that determine the intention of banking institutions to integrate the two security functions.

c) To determine the sources of pressure that would influence integration of the two security functions.

d) To establish the factors hindering integration of physical access control and cyber security in banking institutions in Kenya.

e) To develop a conceptual framework that will guide the implementation of existing security integration solutions.

E) Previous Research in Regards to Integration of Physical Access Control and Cyber Security

Previous studies on security in banking institutions largely focused on specific components of cyber security such as data exchange and transmission risks for commercial banks, products that will aid the convergence process, challenges faced in the integration process and importance of converging the two security disciplines.

a) In 2003, Yahya Mehdizadeh focused on the benefits and importance of convergence of logical and physical security [14]. The study mainly addressed the benefits and value of converging logical and physical security systems by using a common token such as a smart card, architectural issues that arise as a result of convergence and created user case scenarios so as to find out the impact on pricing.

b) In 2003, IBM wrote a technical report on a solution that they developed in collaboration with GE [15]. The IBM Logical and Physical Security Integration Solution helps customers achieve standardized security platforms that integrate logical (IT and data) and physical (site and employees) security programs with back-office applications such as human resources databases and e-mail systems. A comprehensive, enterprise-wide security program integrated in this fashion can help reduce overall security costs and increase security effectiveness at the same time.

c) In 2005, Christopher Michael Connor wrote a research paper on how Integration of IT and physical security can be achieved by using Microsoft active directory [16]. He demonstrated how integration between logical and physical access can enhance security and reduce time in managing both systems. This can be achieved by providing seamless link between Exgarde and the active- directory, which enables automatic updating whenever changes are made within the active directory. The logical system can further be secured by restricting login if people aren't in the building thus preventing tail gaiting.

d) In 2006, Edward Stead came up with a conceptual model for a product that integrated physical access control and IT security using Microsoft Active Directory [17]. His study developed a proof of concept solution for integrating physical and logical access security using a working Microsoft Active Directory environment.

e) In 2006, Sun Microsystems came up with a conceptual model for a product called Sun and Actividentity which was to help customers in solving the convergence challenge [18]. Together, Sun and Actividentity let businesses use a single system to connect and automate the processes for granting and revoking access rights to both physical and network resources, while leaving the control of the actual systems to the individual departments. The system uses a single Java CardTM platform-enabled smart card to consolidate all corporate access credentials, and offers the ability to audit access rights across both physical and network resources for regulatory compliance.

There has been no attempt to explore on the factors that hinder integration of security infrastructure in commercial banks. The main aim of the study will be to determine the factors that hinder the integration of physical access control and cyber security in financial institutions in Kenya and develop a conceptual framework that will guide the banks in the process of integration.

II. METHODOLOGY

The study sought to examine the factors hindering the integration of the physical security access and the cyber security amongst commercial banks in Kenya. The study sought respondent's opinions on various issues that relate to the adoption of the integrated aspect of physical and cyber security aspects of the bank security. A descriptive research design was used in the study. A descriptive research design involves a detailed analysis of a group, or an individual or an institution with the aim being to establish relationships that have ensued to the behavior of a study [19]. The research will be centered on commercial banks in Kenya. This design is ideal due to the fact that it guarantees a complete description of the situation, thus reducing biasness in the process of data collection [20].

Qualitative and quantitative research methods will be utilized. Quantitative approach is valuable as it enables the use of structured questionnaire in data collection and makes it possible to measure variables and consequently use of descriptive statistics in presenting the findings [21]. The qualitative approach encompasses studies that make no attempt to quantify the results [21].The choice of using qualitative data collection approach is influenced by the fact this design is flexible as it enables making changes and refining the research ideas as the study progresses [21].

The qualitative method mainly involves subjective assessment of opinions, attitudes, and behavior [21].

The qualitative tool has the ability to evoke a more truthful touch of the research setting which cannot be gotten by using quantitative analysis. In this study, the qualitative technique to be used will be semi-structured interviews which will be used to assess the factors hindering integration of IT security and physical access control in Kenya's banking institutions as well as the practitioners' attitude towards integrating the two security functions.

The questionnaire was used as the primary data collection tool while semi-structured interviews were used as the secondary data collection tool. The questionnaire comprised

of both open and close ended questions which were grouped in two sections, A and B. Section A mainly focused on the profile of the respondents while section B contained questions relating to the research objectives.

The study targeted the population of all employees who work in both the physical access control and cyber security units in the 43 banks in Kenya. According to the Kenya Bankers Association (KBA), there are about 5,400 employees working in Kenyan banks security units, which comprise of both cyber security and physical access control units [22]. Using the Taro Yamane statistical formula, a sample of 99 respondents was selected from the population.

A pilot study was carried out with 4 employees from two different banks, who were not included in the actual survey. The four employees consisted of two respondents from the physical access control department and two from the cyber security department. Data collected from the pilot study was not included in the actual study.

Data analysis was done using descriptive and inferential statistics with the help of the SPSS analysis software.

III. RESULTS

A) Factors that determine the attitude of banking institutions towards integration of physical access control and cyber security

Commercial banks attitude incorporates an array of factors that wield significant influence on the decision of whether to integrate physical access control security and the cyber security. The factors noted include:

a) Banks' commitment to security reforms. This will entail adopting the integrated approach when managing physical access control and cyber security.

b) Managements' willingness to reorganize the current security model. Any reforms done in any institution must be approved by management. Successful and smooth integration of the two security functions will only take place if management approval and sponsorship is obtained.

c) The ability of the integrated approach to resolve existing vulnerabilities which exist as a result of the independent management of the two security functions. Vulnerabilities are weaknesses that can be exploited by threats which would then lead to a security breach. The integrated model should be in a position to resolve all weaknesses identified in the independent security model.

d) The ability of the integrated approach to reduce the risk exposure in regards to the two security functions. Commercial banks should be convinced that the integrated model will reduce risk exposure.

e) Reduction of the banks operational costs.

Integration of the security functions should result in reduction of operational costs for financial institutions.

f) Integration and maintenance costs.

The sum of the initial integration costs and the maintenance costs should not exceed the current budget that's allocated to the two security functions. In case they do, the benefits arising from the integrated approach should exceed the costs.

These factors determine overall decision on integrating physical access control and cyber security:

B) Factors that Determine the Intention of Banking Institutions to Integrate the Two Security Functions

The findings highlight that commercial banks intention incorporate significant and diverse factors that wield considerable influence on commercial bank determination of approach to be adopted in managing security functions. The factors include:

a) *The need for detective controls that will reduce the likelihood of security breaches.* Detective controls are meant to prevent an attack from taking place. Commercial banks insist on getting assurance that the integrated model will reduce the likelihood of security breaches occurring.

b) *The need to enhance coordination in management of the security functions.* Financial institutions will only have intentions to integrate the security functions if there is assurance that the integrated model will enhance ordination of the security processes. This is important to financial institutions as it will enable easier investigation after a security breach has occurred.

c) *Improve accountability in case of security breaches.* Banks will only implement the integrated security model if accountability during and after security breaches will be improved. This is essential as it will help in identifying the source of the security breach and which loophole was exploited for the security breach to be successful.

d) *Improve internal monitoring and detect security breaches before they occur.* Financial institutions need to be convinced that the integrated model will improve internal monitoring and detect security breaches before they occur. This will be the main determinant of whether they will implement the integrated model or retain the independent security model.

e) *Prevention of insider fraud and gagging any fraud loopholes.* The banks are sometimes victims of fraud that is initiated by its own staff. From the research done, financial institutions would need to be convinced that the integrated security model will enhance detection of insider fraud and also assist in sealing all known loopholes that can be exploited by disgruntled employees.

The study established that the above factors determine if the commercial banks' will adopt the integrated strategy on security framework on integrated or separated security architecture.

C) Sources of pressure that would influence integration of the two security functions in banking institutions

The study established that commercial banks pressure may originate from both internal and external factors as described below:

Internal sources of pressure.

a) *Persistent security threats:* Financial banks are prone to security threats due to the sensitivity and nature of operations they handle. Any security threat that exploits existing vulnerabilities leads to a security breach which could easily destroy a banks reputation to its customers. Persistent security threats are thus a major source of pressure to financial institutions which could easily influence them to integrate physical access control and cyber security.

b) *The need for efficiency in security procedures:* Independent management of security functions creates many loopholes which could be exploited by attackers. Financial institutions are thus at a verge to improve efficiency of security procedures so as to seal all loop holes. This can be achieved by implementing the integrated security model which has the ability to improve efficiency of security procedures.

c) *Security breaches and incorrect responses:* Security breaches in financial institutions could lead to negative impacts which include: fines and penalties by the regulator, litigation, negative impact on reputation on customers. The integrated security model could come in handy as it has the ability to detect security breaches before they occur and also improve response to security breaches due to its ability to automatically correlate events in both physical access control and cyber security.

External sources of pressure

a) *Industrial standards:* Banks operate in the banking industry which has certain standards that they should all adhere to. The purpose of the industrial regulations is to ensure standardization in the banking sector. From the research done, financial institutions pointed out that their integration of the security functions would be highly determined by whether the industrial standards recommend the same, which in this case is not the case. The banks pointed out that they are reluctant to implement the integrated security model as it is not recommended by the industrial standards thus their preference for the independent security model.

b) *Legal requirements by the regulator:* Banks are regulated by the Central Bank of Kenya which has published guidance notes for cyber security which are to be adhered to by all banks in Kenya. From the research done, banks pointed out that they are reluctant to implement new security models as they do not know what impact it would have to their compliance to the cyber security guidelines. This would mean that a compliance review by an external party would be necessary which comes at extra cost thus their reluctance to implement the integrated security model.

c) *The need for integration motivated by competitors:* Financial institutions are reluctant to implement new technical solutions that have not been tested by their competitors in the region.

This is due to the fact that they will not have any institutions from which benchmarking can be done thus their fear of blindly implementing any untested technical solutions. Banks pointed out this as one of the reasons why they have not implemented the integrated security model as none of the banks in Kenya have implemented the integrated security model thus there are no institutions to benchmark against.

d) *The need for integration informed by continued global changes:* Globally, 21 % of the organizations have implemented the integrated security model and have reaped benefits its benefit. From the research done, financial institutions in Kenya are aware of the benefits that they could possibly reap from implementing the integrated security model. This is a great source of pressure for financial institutions which in turn makes them think about implementing the integrated security model.

The study found that these factors wield significant pressure on commercial banks which inform their decision of the security architecture to be adopted.

D) Factors hindering integration of physical access control and cyber security in banking institutions in Kenya

From the research done, the following factors were identified as the hindrance for integration of physical access control and cyber security in Kenya:

a) *Compliance to legal requirements:* Banks are regulated by the Central Bank of Kenya which has published guidance notes for cyber security which are to be adhered to by all banks in Kenya. From the research done, banks pointed out that they are reluctant to implement new security models as they do not know what impact it would have on their compliance to the cyber security guidelines. This would mean that a compliance review by an external party would be necessary which comes at extra cost thus their reluctance to implement the integrated security model.

b) *Absence of organizations to benchmark with:* Financial institutions stated that they are reluctant to implement new technical solutions that have not been tested by their competitors in the region. This is due to the fact that they will not have any institutions from which benchmarking can be done thus their fear of blindly implementing untested technical solutions. Banks pointed out this as one of the reasons why they have not implemented the integrated security model as none of the banks in Kenya have implemented the integrated security model thus there are no institutions to benchmark against.

c) *Absence of industrial regulations:* Banks operate in the banking industry which has certain standards that they should all adhere to. The purpose of the industrial regulations is to ensure standardization in the banking sector. From the research done, financial institutions pointed out that their integration of the security functions would be highly determined by whether the industrial standards recommend the same, which is not the case. The banks pointed out that they are reluctant to implement the integrated security model as it is not

recommended by the industrial standards thus their preference for the independent security model.

d) *Unknown cost implications:* Implementation of the integrated security model would definitely come with cost implications. From the research done, banks are reluctant to adopt the integrated model given that the cost implications are unknown and that no cost benefit analysis has been done for the integrated security model.

e) *Organizational culture:* From the research done, the financial institutions pointed out that there is a great division between the physical access control unit and the cyber security unit. The division is caused by the different work cultures and reporting structures that exist. The division is evident even in their recognition by the two units. Physical security personnel are merely referred to as security staff while the cyber security staff is commonly referred to as geeks. The culture is thus one of the factors that hinder integration of the two security units.

f) *Lack of a road map:* From the research done, implementation of the integrated security model would mean coming up with a strategy on how the new model will replace the independent security model. The strategy could best be established by coming up with a road map on how to transition from the independent security model to the integrated model. Financial institutions pointed out that the process of developing a road map is quite a complex and costly exercise which they wish to avoid. This is thus a major reason why they prefer retaining the independent security model.

E) Conceptual framework that will guide the implementation of existing security integration solutions

The finding from the study done indicate that integration of physical access control and cyber security is mainly informed by willingness of the commercial banks to reform the existing security model so as to implement the integrated model. The security reforms will entail:

a) *Establishing a road map that will act as a guide in the implementation of the integrated model:* This is done by doing a current state analysis of the security environment and comparing it to the future state which the banks wish to achieve. This will result to identification of existing gaps which the financial institutions can then come up with objectives of how to close the gaps.

b) *Structural changes so as to integrate the two security units into one:* This will involve structurally integrating the physical access control unit and the cyber security unit to form one unit.

c) *Making strategic decisions on how best the two security functions can be integrated:* This will involve defining the unit's objectives which should be in support of the banks business objectives.

d) *Redefine operation policies so as to guide the new integrated security model:* The policies will be guided by the strategic decisions, which include objectives of the integrated security unit.

e) *Establishing the best way to integrate the security processes:* This will be guided by the policies that will be defined for the integrated model as business processes are mainly guided by policies.

f) *Finding a suitable system that will be used to manage the two security units:* This can be done by either integrating the two existing security systems using a middleware or acquiring a new system that can handle manage operation of both physical access control and cyber security. A middle ware is a software that acts as a bridge between two systems with the intention of enabling communication between the two systems. This decision may be influenced by the banks financial ability to acquire a new system. For banks which do not wish to incur high costs in the integration process, the option of integrating the two existing systems with the help of the middleware would be most suitable.

g) *Find a suitable way to get skills needed to manage and operate the new system:* This can be achieved by either training existing personnel or getting a new team of specialists who have experience in managing a system that handles integrated security functions.

The Fig. 2 shows the conceptual framework that outlines how integration of the security functions can be achieved, the determinants of banks' attitude and intentions towards integration and sources of pressure for commercial banks in regards to integration of physical access control and cyber security. The factors indicated were identified during the research.

IV. CONCLUSION

This study unveiled factors that hinder integration of physical access control and cyber security in financial institutions. It also established factors that determine the banks' intention to integrate the two security functions and the determinants of financial institutions attitude towards integration of physical access control and cyber security. In addition, the study established sources of pressure that would push financial institutions to integrate their security functions. Results of the study were then used to develop a conceptual framework that would guide financial institutions that wish to integrate physical access control and cyber security.

The study established that banks' attitude towards integration of the two security functions is determined by the banks' commitment to security reforms, the ability of the integrated approach to resolve existing vulnerabilities and also reduce the firms' risk exposure. In addition, the managements' willingness to reorganize the current security model and the reduction of operational costs also determine the banks' attitude towards the integrated security model.

The study proved that the banks' intention to integrate their security functions is determined by the need for detective controls, the need to enhance coordination of security functions and the urge to improve accountability during security breaches. In addition the study established that the need to improve internal monitoring by detecting security

breaches before they occur and the need to prevent insider fraud by gagging any fraud loopholes determines the banks' intentions to adopt the integrated security model.

The study identified internal and external sources of pressure that would push the financial institutions to integrate physical access control and cyber security. The internal sources identified include: persistent security threats, the need for efficiency in security procedures and incorrect response during security breaches. The external sources of pressure identified include: legal requirements, industry regulations, the need for integration motivated by competitors and the need for integration informed by continued global changes.

The findings of the study were then used to develop a conceptual framework that is recommended as a guide for all financial institutions that wish to integrate their security functions.

Limitations of the study: This study was limited to the 43 commercial banks in Kenya.

Further work: Further research can be carried out to establish:

- Effects of integration of physical access control and cyber security on compliance of financial institutions to the CBK cyber security guideline.
- Effects of integration of physical access control and cyber security in Kenya.

Cost implications on organizations that have integrated physical access control and cyber security.

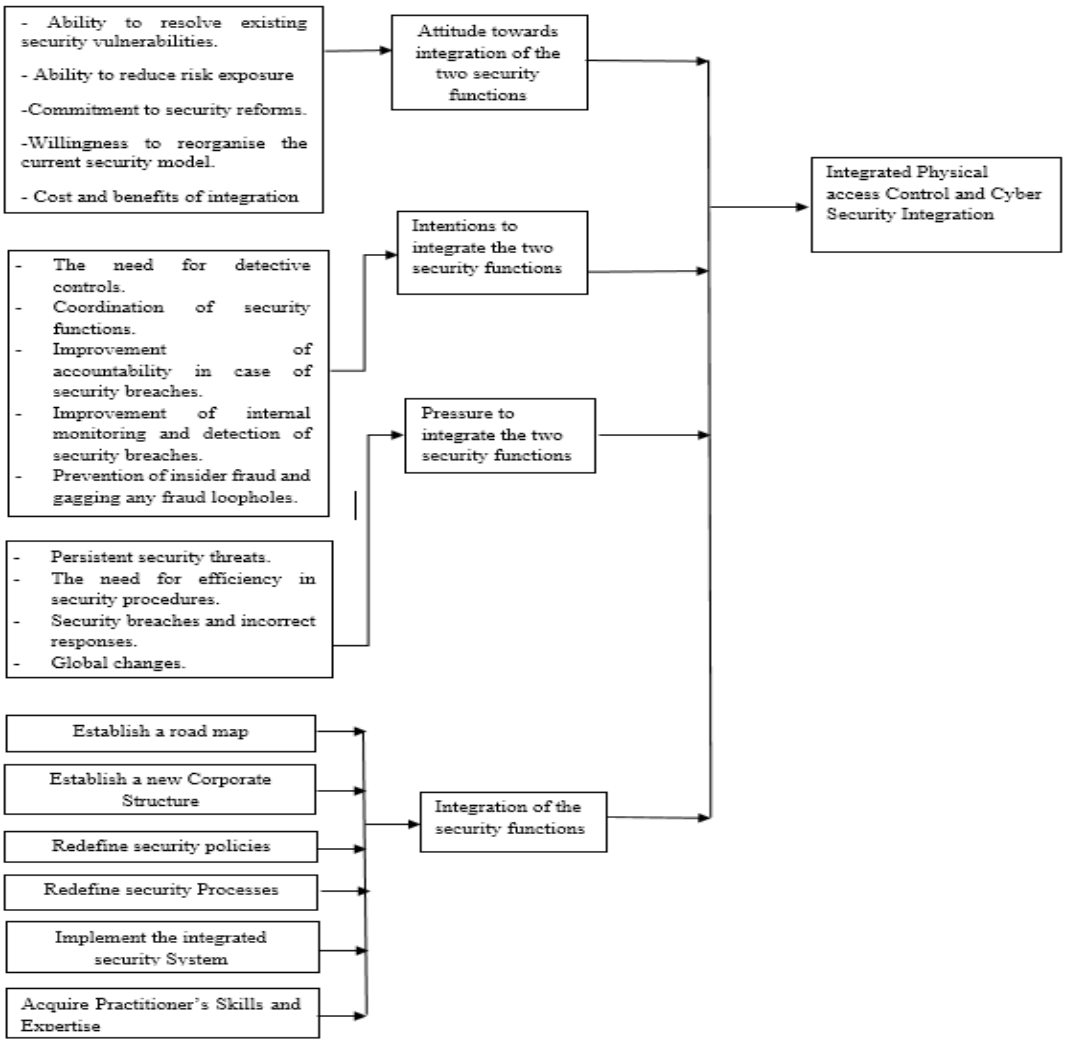

Fig. 2: Conceptual framework for integration of the security functions

ACKNOWLEDGMENT

The authors wish to thank all financial institutions who participated in this research, for their help and co-operation; without them I would not have been able to complete my research.

REFERENCES

[1] Böhme, R. & Moore, T. (2012). How do consumers react to cybercrime? *eCrime researchers summit (eCrime)*, IEEE, 1 – 12

[2] Raytheon/ Websence, (2015). 2015 Industry Drill-down Report: Financial Services https://www.websense.com/assets/reports/report-2015-industry-drill-down-finance-en.pdf (accessed; 25th August 2017)

[3] HMG Strategy (2017) http://hmgstrategy.com/network/people/kirsten-davies (accessed on 22nd September 2017)

[4] Symantec, (2012). Internet security threat report trends for 2011. Volume 17 https://www.symantec.com/about/newsroom/press-kits/istr-17 (accessed on 25th August 2017).

[5] Ula, M., Ismail, Z., & Sidek, Z. M., 2011. A Framework for the governance of information security in banking system. Journal of Information Assurance & Cyber Security, pp. 1-12.

[6] Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.

[7] Kothari, C. R. (2008). Research Methodology: Methods and Techniques. Delhi: *New Age International Publishers.*

[8] Sans institute. (2008). Convergence of physical and logical security,

[9] National Cyber Security Center [NCSC] (2014). Cyber security beeld Nederland. National Cyber Security Centrum: Den Haag.

[10] Tarimo, C.N., (2006). ICT security readiness checklist for developing countries: A social technical approach (Doctoral dissertation, Stockholm University).

[11] Aberdeen Group (2012). *In Cyber Security, It's About Time: A Case In Data Protection* http://www.aberdeen.com/research/16168/16168-KB-CyberSecurity-Value-Time.aspx/content.aspx (Accessed on August 26th 2017)

[12] Baffour, B. A. (2015). Examining the Impact of Information Technology on the Financial Performance of Asutifi Rural Bank. (*Doctoral Dissertation, Kwame Nkrumah University of Science and Technology*) Algozzine, B., & Hancock, D. (2016). *Doing case study research: A*

[13] Kurt, A. (2015). *Effectiveness of Cyber Security Regulations in the US Financial Sector: A Case Study* (Doctoral dissertation, Carnegie Mellon University).*practical guide for beginning researchers*. Teachers College Press.

[14] Yahya Mehdizadeh. (2003).Convergence of logical and physical security. Technical report, SANS Institute.

[15] IBM. (2003). Logical and physical security integration solution. Technical report, IBM.

[16] Christopher Michael Connor. (2005). Integration of it and physical security using Microsoft active directory. Undergraduate Final Year Project - University of Leeds.

[17] Integration of Physical Access Security and Logical Access Security using Microsoft Active Directory Edward Stead Computing and Management 2005/2006

[18] Sun Microsystems. (2006). Sun and Actividentity help customers solve the challenge of integrating and securing access to it and physical resources. Technical report, Sun Microsystems.

[19] Barbie, E., & Mouton, J. (2006). Research methodology by numbers-a teaching tool. *Durban University of Technology*.

[20] Kothari, C. R. (2004). *Research methodology: Methods and techniques*. New Age International.

[21] Algozzine, B., & Hancock, D. (2016). *Doing case study research: A practical guide for beginning researchers*. Teachers College Press.

[22] Kenya Bankers Association (2016). The List of Organization members: http://www.kba.co.ke/members.php (Accessed on August, 26th 2017)