ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)
Vol. 4, Issue 2 (Apr. - Jun. 2016)
International Journal of Advanced Research in Computer Science & Technology (IJARCST 2016)

# Data Security in Rural Banking Sector: A Case Study in Ashanti Region

[I]Mark Osei Gyabi, [II]Mahendra Kumar Shrivas
[I]System Administrator, [II]Lecturer & System Administrator
[I]Dept. of ICT, Rural Bank Limited, Juaben, Ashanti, Ghana, West Africa
[II]Faculty of Technology, Academic City College, Accra, Greater Accra, Ghana, West Africa

**Abstract**
*Data security in Rural Banking has to do with the managerial actions and internal technological policies (ICT policy) governing computer hardware, software, and data to ensure against unplanned, purposeful or not permitted access to computer system data. Banking Computer security is concerned with the ethical and lawful requirements to protect application software as well as data from unauthorized use. The issues in computer privacy are therefore management decisions as to who has access to software or data, whereas issues of security involve both physical and IT setup procedures for enforcing the privacy decisions. Considered banking operations, it is possible to set up some structure of operation guidelines, which allows the systems administrators to implement control and security policies which will be accountable for installation of application, user access right and server management policies. The psychological security of the operational staff is essential for successful operation security.*
*Data Security in Rural Banking Sector, Ashanti Region is justified under the ICT policy and Charter of Association of Rural Banks. The IT audit of the Banks need to use information from computers and log files to prevent, identify and react to computer security incidents defined by the Directive and it may be impossible for IT audit to establish preceding affairs with all those whose information they may handle, or even to inform them after the incident. This research work identifies these conditions and advice measures that IT audit team may use in planning and performing their activities to assure the requirements.*

**Keywords**
*Data security, Rural Banking Sector, Security Policy, Privacy*

## I. Introduction

The daily activities performed by Rural Banks has resulted the amount of data increasing exponentially, which can transform the banking as an institution in the coming years in ways that we can hardly imagine today [6]. Processing dependable data such as government salaries, individual transactions, etc can help determine certain trends, which can contribute to reducing the waste of resources and improve policy-making. Nevertheless, data can also be used to put people under complete supervision, in breach of their privileges assigned to them. As Rural Banks are gradually expanding and adapting to modern ways of banking such as short message service (SMS) banking, electronic transfers [2]. Bank Branches data is being consolidated and merging with different APIs, software applications, precautions are to be critically observed to avoid leakage of data to any third party. Data security is very important to every organization therefore extremely needed care must be taken. If a data is accessed by a hacker or unhappy employee, it could generate havoc for organization proprietary, affect company efficiency negatively, and impede the ability to participate with other businesses. Unauthorized data access can also damage a company's relationship with customers and hackers can also manipulates and alter figures in the database tables if they get access to the data [1]. Data security refers to a set of actions adopted to detect as well as to prevent unauthorized access to an organizational computers, database and websites from illegal activities. Data security also means protecting data from corruption by viruses, database crushes, and windows software. Data security is the main priority for banking of every size and type. Data security is also known as information security (IS) or computer security. The objective of data security in the banking sector is to safeguard the continuous use of database and networks that are important to the organization, to prevent the unauthorized use of data, the unintentional or deliberate destruction or distortion of data, and to minimize damage caused in both wired and wireless environment [3].In addition to protecting organizational database, preparations should be made to deal with threats that might result in the deferment of uses and to recover from such situations.

## II. Background Information

Data Security plays a very important role in every organization as it contains all the information about that particular organization. IT managers really find it difficult to curtail diverse ways of hackers and intruders who intend to attack company's data. It is therefore necessary for IT managers manage the data well by applying all the computer security policies such as confidentiality, integrity, availability etc.
With several happening of cyber attacks and data breaches [1] companies are trying their very best to strengthen their security measures by updating their IT Security policies. However, this research work shows that the Rural Community Banks has to update and implement their ICT security policies to be able to prevent hackers from getting access to their database.
This study has discovered that there are some Rural Banks that has been able to implement almost all their Security Policies and are working perfectly. The researchers find out and it was discovered that the Board of Directors on ICT Committee were highly involved with the drafting of the ICT Security Policies.
Every organization has its own way of designing their security policy. That is we don't have one way of designing a safe organization security policy. Data Security and Network has to be designed in such a way that it will fit the needs of one organization infrastructure. Network administrators should make sure not all users on the network get full access to the internet. A good ICT security policy protects both the organization network and the organization's data as well. Precautions must be taken when choosing a network provider for an organization especially banking. Data security is associated to confidentiality which consists of user identification and relies upon access control, and system security

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

management which provides login for authorization.

## III. Problem Statement

Almost every organization has a database or computer security policy that has been drafted or designed by the management of the organization but some of the drafted computer security policies lacked key technicalities and do not involve the stake holders such as a member from the board of directors, etc. As technology is dynamic but not static, things keeps on changing that some of the drafted policies need to be updated or modify to meet the current trend of technology. Hackers are becoming rampant and this makes most databases porous to hackers. The IT staffs needs to update their skills to be able to identify and prevent intruders from accessing their database. The security policies should be implemented according to rules of the organization. The Internet is a good master but a bad master too. The internet has added many new features to banking sector such as internet banking, short message service (SMS), easy access to information by customers, banking organizations merging or consolidating most of their database together and many more. In Banking sector adaption of Cloud Computing is growing thus security threats are also [9]. Most of the services provided by the banks depend on internet which means that some organizations cannot service their customers effectively without the internet.

The current data security policies of some rural banking organizations is very porous and ineffective which makes information assets vulnerable to threats such as intruder attacks, both internal and external attacks which can cost the banking sector unjustifiable amounts of money, loss of data and breach of customers confidentialities. This is the motivation why data security policy has to be formulated and implemented to keep information resources secure and safe from possible attacks.

System administration is said to be a complex and demanding task, and frequently requires that system administrators keeps updating themselves, attending workshops and receive specialized security training. Upon examination, it was revealed that the number of trained system administrators at various Rural Banks has not kept pace with the newly advanced system security threats and its measures which the banks require to curb internal IT security measures and to make sure their database are well protected from hackers and intruders and very secured in a cost-effective manner.

## IV. Aims of The Study

The under listed are the researchers major aims in data securities in Rural Banking sector;

I. That the Rural Banks will know the function of information security in making sure that customers or users have access to the information they need in order to carry out their work. Computer and information systems buttress all the banking business, and are important to its operations, reporting and administrative functions.
II. Any little fall in confidentiality, integrity or accessibility of customer information could prevent the Bank from functioning effectively and proficiently. In addition, the loss or unauthorized access of information has the likelihood to damage the bank's reputation and cause financial loss.
III. In the way of shrinking these risks, information security ought to be an important part of information management, whether the information is kept on hard drives, Compact disc or external drive.

## V. Objectives Of The Study

I. To be able to achieve these aims, the bank is committed to set up security measures that kowtow to greatest put into practice, as set out in the *Rural Bank ICT Policy and Charter*. The Bank has instituted an information security controls in order to give recommendation and direction on the technical views of information security. The information security controls is based on the information security and policy of the Bank and the Association of Rural Banks to adhere to the principles of the policies.
II. Information security warning evaluation should be carried out for all the branches of the Bank regularly in order to recognize key information risks and determine the controls required to keep those risks within satisfactory confines.
III. The Bank is dedicated to providing satisfactory instruction and training to Staff to ensure they appreciate the value of information security and, in particular, exercise proper care when managing secret information.

## VI. Importance of The Study

The importance of this study is to simply ensure the faithfulness of Banks data security controls and also to reviewing network security controls at Rural Banking Sector in Ashanti Region [8]. By the end of this study, employees and board of directors of rural banks in Ashanti region shall realize the need to energetically and wholly partake in training programs and adherence offered to them by their organization ICT policies and how they can get committed to the achievement of rural banks objectives to attain a good success for the banking association. It would serve as a source of reference for individuals, institutions and other researchers.

Data security controls and staff or directors training in piece will also contribute to the banks development. Organizations offering ICT training programs to their workforce consistently will help reduce data risk and illiteracy since training is a form of education and increase staff skills and competence, as well as their levels of performance and productivity which contributes extremely to banks development [11].

## VII. Literature Review

In addition to physical security that companies provide, making sure that their computer and network they use are also protected is very necessary. This needs awareness to avoidance, discovery, and response. Managers of companies IT infrastructure ought to understand the threats hackers can use so they can use a variety of techniques to secure the system that serve their data [12]. Encryption for logins, secure private networks for administration, automated vulnerability scans, and automated intrusion detection and monitoring are some configurations that can be performed to secure companies data. IT managers have to monitor system logs of all activities and record them for future investigations.

System attacks are identified to be either deliberate or accidental and technically intruders have interest in targeting the servers that host organizational data and computers used for transaction business. This assessment addresses how tremendously hard intruders or hackers try to go through internet networks to steal company's data despite various software and hardware securities the IT managers has set and configured. Irrespective of how determined intruders try to access Company's information, data security and network security experts are gaining a lot of techniques in avoiding attackers from contacting company data.

### A. Physical Installation Attack

Physical installation attacks are attacks that can be seen but might not be prevented due to factors such as robbery, physical attack and many more.

Firstly, the most frequent threat is hardware threat which can be classified as an instance of physical installation attack. This attack is due to old age of a computer system which has corrupt windows files that can cause the system to behave strangely. Most organizations have a physical system policy that allows them to phase off old age computers every two (2) to five (5) years.

Natural occurrences such as storms, thundering and extreme whether can be classified as environmental threat. Network switches mostly get damage as a result of electrical threat. This type of hazard is very common in countries like Ghana where the electric power supply is not stable but interrupted unexpectedly. Blackout that is unexpected interruption of power supply and many more are examples of this type of threat.

Another threat such as system maintenance can also cause problem to database by either crushing or distorting database tables. Examples of maintenance threats are poor cabling, faulty network card, defective system memory, poor cable labelling, and electrostatic discharge.

### B. Access Attack

This attack can be classified as either an outsider or insider. When an insider or outsider attempts to access the organization's network unlawfully with intent to copy some file, steal data from the system [7]. These hackers have the tendency to destroy organizations important information and they can cause havoc to the organization. People attack system for several reasons, such as data extraction, review of user privileges etc. [7]. Below can be classified as access attacks;

- **Password Attacks**: - Hackers try their maximum best to guess passwords. That is they try by using common names of users to gain access into the system. Data integrity can be altered by tampering the database tables. In many cases they insert figures and change values in the tables. The hackers do so to ensure that the data can be accessed through the network before being transmitted to their final destination.
- **Trust Exploitation**:-This type of attack usually happens at an organization, where the Employees believe and trust each-other. In this case the attacker takes advantages of believe and trust of the staff and exploit the system. In a situation where the staff trusted themselves so much that they can give their passwords to colleagues to work and rely upon them to give accounts. Similarly, a third party organization can take advantages of this trust relationship to cause serious harm to an organization.

### C. Worm, Virus and Trojan-Horse Attacks

These types of attack are common in organizations where users are allowed to plug in removable devices such as pen drives, external hard drives, compact disk and etc. Any of these infected removable devices can cause havoc to the organization files. Some companies adopt a policy to disable all removable media storage access to avoid being infected by these viruses [7].

To be able to prevent this attack, antivirus software must be installed on all the computers and the managers of the institution should make sure the antivirus signature is updated and running.

### D. Mitigation of Threats and Attack

Organizations such as Rural Banks cannot stop the use of computers, networks and internet in their activities. The use of computers, networks and internet is very common in the banking sector. Almost all their activities rely on the use of these resources therefore, there should be a way to avoid the recurrent threats and attacks that the banking go through. Below are some listed measures that the organizations should adopt to avoid or minimize these attacks;

- **Hardware Threat Mitigation: -** This type of threat is common in many organizations. At times you will see people entering server rooms without any proper checks. Many companies leave their server room unlocked and this allows people with bad intention to easily get access to their system. To be able to avoid this type of threat, physical security measures should be observed at all the offices of the institution. Intruder alarm system must be installed to be able to alert officers whenever someone enters the strong room. Moreover, access to doors, windows, ceiling must be properly check. The use of security cameras (CCTV) must be well positioned at vantage points and should be monitored by staff or security personnel of the institution.
- **Electrical Threat Mitigation: -** Companies if possible should get strong generators to support their electrical system. Generators with high capacities are able to withstand and supply enough voltage to their electrical systems such as servers, client computers, printers, air conditions and many more. But to make sure that the electric power does not fluctuate to cause data damage, uninterrupted power supply that is UPS must be installed to each computer of within the organization. When power is lost, intruders take advantages to get immediate access to the system particularly through the network to the database.
- **Maintenance-Related Threat Mitigation:-**Organizations such as rural banks regularly do maintenance on their computer systems by upgrading the memories, hard drives or formatting the operating systems. These activities should be carried on by the systems administrators of the institution. This maintenance threats should be focus on:-

1. Good Servers with Activated Operating System.
2. Making sure that Database are secure.
3. Periodic Anti-Virus Update.
4. Windows firewall well configured and active.
5. Disabling Remote Desktop Connection (mstsc) on hosting server.
6. Neat cabling through conduit and well terminated.
7. Labelling components and critical cables.

Organizations server or strong rooms should be locked at all time unless the IT managers want to carry on specific tasks. The server rooms should be accessed by authorizes personnel's of the institution. Surveillance cameras should also be installed on the entrance of the rooms to monitor those who access the rooms. Company servers should have strong passwords and the screen saver time should also be minimal and locked when idle. Microsoft remote desktop connections on servers should be disabled as intruders try to access the server from remote distance. If possible the hard drives that store the main official database should not be shared to avoid access to the database. Moreover, network security routers should be installed to monitor the internet protocol (IP) addresses of the organizations.

- **Access Attacks Mitigation:-**Organizations should contact

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

technical security personnel to train their staff how to generate passwords that are strong enough to avoid being hacked. Many users are so naive in such a way that they use their own names as their password. Some use their nicknames, friends, etc as their password. Such practices are dangerous as people can easily guess their password and use it against them. Below are listed suggestions and techniques for password;

i. Same password should not be used to open an application on a multiple system.
ii. Failure to login into an account after several attempts should be disabled. The particular user should ask for a rest to enable him/her to access the application.
iii. Password requirement policy should be tightening in order not to allow access to easy password.
iv. Strong passwords such as symbols and alpha numeric should be enforced.

- **Trust Exploitation Attack Mitigation: -** Organizational staff should be aware that, they will be responsible for their own actions therefore carefulness and awareness should be paramount in their relationships with their colleagues. It is not a good practice to give a password to a colleague irrespective of the level of your trust. This type of attack can be solved if users become aware of the danger they are putting themselves in by not giving their passwords to colleagues of use. Validation should be always observed when dealing with a third party organization.
- **Securing Remote Access:-**The remote access to switches, wireless devices and servers must be protected at all times. All these devices allow passwords to be configured. Administrators and managers of these devices must restrict access to the devices by making sure the passwords placed on them are very strong and cannot be cracked easily.

Every password enabling device has authentication process. Authentication is a process of verifying whether the username or password entered is correct.

The stages of the authentication process are:

I. The system will require username and password.
II. Usernames and password encrypted is sent to Remote Authentication Dial-In User Service for vilification.
III. The Remote Authentication Dial-In User Service server will give a reply like; successfully authenticated meaning the password is correct. Login failure meaning the username and password are not valid.

## VIII. Research Methodology

The purpose of this research is to examine data securities observed in some selected Rural Banks in Ashanti Region which is being used as a case study regarding data backup policy, network security policy, user access policy and hardware maintenance policy. The numbers of Rural Banks where the research took place, number of participants, size of sample and the estimated plan of the research has been stated. The researchers administered questionnaires to collect the sample data, the methods used for validity and reliability has been stated.

### Sophisticated user variable will include:

- IT Managers
- Network Administrators
- Computer hardware technicians
- Database Administrators

### Normal user variables will include

- Board of Directors engaged in IT security committee
- Staff (All departments)
- Customers of the banks

An appropriate methodology will be used to structure a realistic questionnaire and a feasible sampling size of the users in both categories to solicit for information to be used to conduct the research based on time and available resources.

### A. Research Approach and Design

A quantitative approach was followed. According to Burns and Grove "A quantitative research as a formal, objective, systematic process to describe and test relationships and examine cause and effect interactions among variables. Surveys may be used for descriptive, explanatory and exploratory research."[5]. In this research work authors administered the questionnaires yourself by visiting the three stated banks namely, Juaben Rural Bank, Asokore Rural Bank and Kumawuman Rural Bank. Researchers target for the response dents are the bank IT officers, Members of board of directors and some of the rural banks customers.

For data securities to work in rural banking, board of directors must be involved in the policy making and policy implementation. The involvements of customers in answering the questions are necessary because they are the stakeholders and most of them are shareholders of the banks. A descriptive survey was selected since it provides an accurate representation on account of the characteristics, for example values, pictures, figures, beliefs, and knowledge of a particular individual, situation or group. This design was chosen to meet the objectives of the study, namely to determine the knowledge and views of Staff and Customers with regard to data security at Rural Bank in Ashanti and its effect to the organization.

### B. Tools for Data Collection

Data collection and analysis for this paper will be simulated by a tool called Statistical Package for the Social Sciences (SPSS) [10]. SPSS is a computer program used for survey authoring and deployment, data mining, text analytics, statistical analysis, and collaboration and deployment.

Tools for data collection can be explained as a means of gathering and summarizing the results obtained of the study. The researchers used questionnaire to collect the data or the information from the respondents.

If a questionnaire is satisfy a question, it must determine in such a way that inferences drawn from the questionnaire are completely precise.

### C. Research Setting

The study was conducted in Ashanti Region of Ghana in three (3) selected rural bank namely; Juaben Rural Bank, Asokore Rural Bank, and Kumawu Rural Bank. These selected banks have an average of over thirty thousand customers (30,000). These banks have more than five branches across Ashanti Region and all the branches have been fully networked. Each Bank has their own database which the branches connected to the banking application through different web browsers.

Ghana banking system is characterized by a comparative bigger number of commercial banks, a broad combination in ownership structure and by dissimilarity in the Customers-base. By the earlier 1970's the Bank of Ghana realized that the normal banking institutions were not able to mobilize funds and provide banking

services to the rural community and in so doing, impact adequately on the development of the country. The Bank of Ghana therefore set up a department and called Rural Banking Department which was to see the establishment of rural banks in the country [4].

### D. The Sample

Rural Banks chosen in the sample were required to meet some specific conditions. The banks have to meet the following criteria to be included in the selection. They should;

1. Be using a computerized banking application
2. Have a data recovery plan.
3. Have board of directors engaged in information security committee panel.
4. Have policies to prevent data leakage.
5. Have clear data classification scheme.

All the three banks selected have all the above specified conditions. This will help determine whether the policies governing the data security will be fully implemented.

## IX. Data Collection

### A. Data collection instrument

The researchers decided to use questionnaires because of the stated reasons:

I. It makes sure that a high reply rate is achieved as the questionnaires were circulated to respondents to fill, comment and answer the questions personally.
II. It needs less time and energy to administer.
III. Questionnaires present the possibility of anonymity because respondent's names were not required on the completed questionnaires form.
IV. The questionnaire gives less opportunity for unfairness as they were presented in a reliable manner.

Despite the positive aspect that questionnaire have, it also has its negative aspect such as;

Questionnaire has a question of validity and accuracy [3]. The questions on the paper might not reflect true opinions of the respondents but they have to answer what they think will please the researchers, and valuable information may be lost as answers are usually brief.

### B. Data Collection Procedure

The researchers personally distributed the questionnaires to the various banks particularly to the Board of Directors, Staff and Customers to complete. The researchers completed several questionnaires for the customers who cannot read and write. The questionnaires were collected over a period of two months. The researchers found some customers in the banking hall transaction business and administered some of the questionnaires to them. Some of the customers are not IT inclined who do not really understand IT policies, IT securities and many more so I read and explain the questions to them in their local language for them to understand before answering the questions.

## X. Data Analysis and Presentation

The conclusions for the study by the researchers after data collection are shown below. The researchers summed all the collected data and arranged them in a way that answers to the research questions and the project objectives. Statistically, the researchers analyse all the data collected from the respondents in a table form.

Research analysis software such as SPSS was used to analyze the data. The information gathered was presented in tables and charts with clear explanation.


Fig.1 : Response: Does your board of directors committed to information security risks relating to your business?

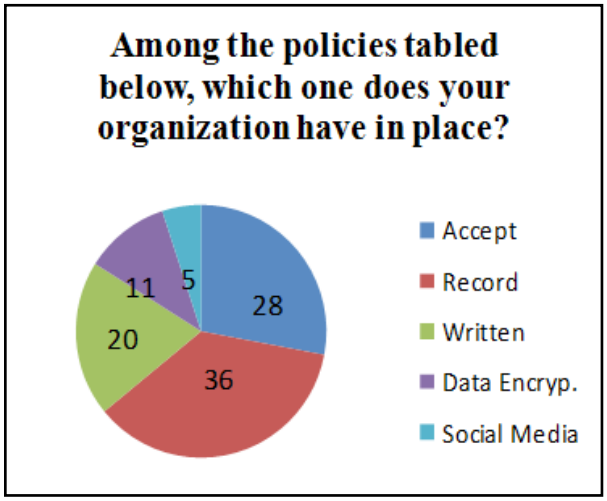


Fig. 2 : Reponses: Among the policies tabled below, which one does your organization have in place?

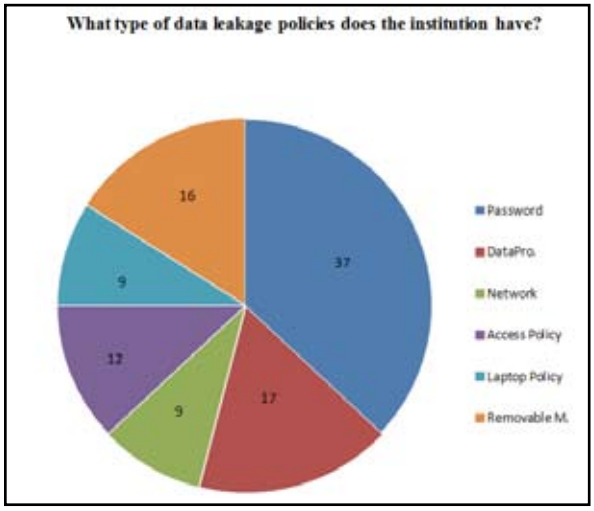


Fig. 3: What type of data leakage policies does the institution have?

In the overall response, there are a number of rural banks with different data security policies and IT charter in their organization. Rural banks whose board of directors are so much involve in computer security are appreciably higher and encouraging than the other rural banks whose directors do not appreciate and are not involve in the security policy making. The difference is quite higher and this is because most of the directors in those rural banks are not into ICT or have not taken any course or seminar in computer. The most appreciable fact is that, almost all the rural banks that the study took place have Computer Security Policies and data or disaster recovery plan. These policies have

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

laid down procedures and methods that when fully implemented will go a long way to protect the companies data as well as its infrastructure. The ICT policies serve as a guide and directs the technical managers of the organization what to do to avoid hackers or unauthorized user to access an information belonging to the bank. Data is an asset of an institution and needs to be protected to serve its purpose and to boost the confidence of the banks customers.

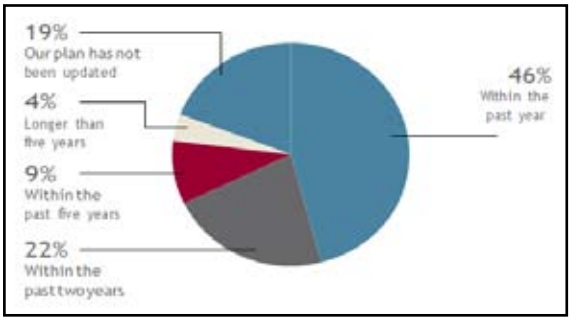


Fig.4: Response : When was your Bank incident response plan most recently updated?

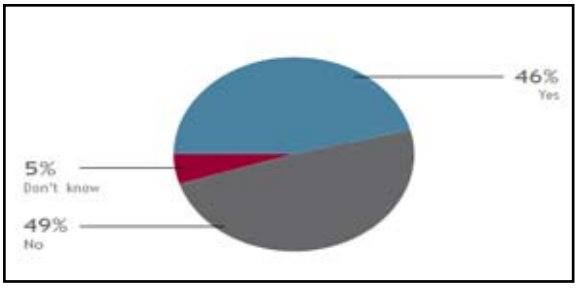


Fig.5 :With regard to IT security, does your Bank periodically perform "data recovery" to test your ability to execute the organization's incident response plan?

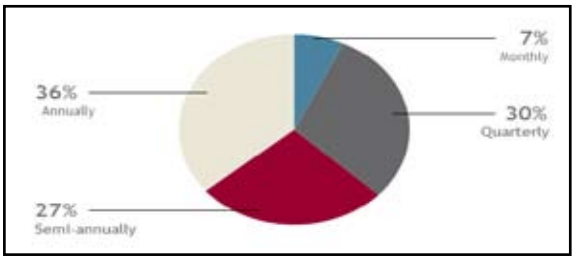


Fig.6 : Response: IF YES: How frequently does your organization perform its data recovery?

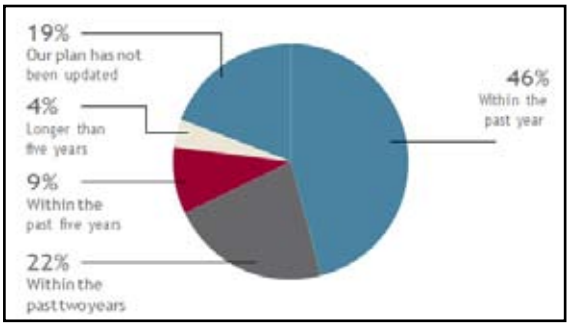


Fig.7 : Response: Does your bank update incident response plan regularly?

Large numbers of organization fails to follow best practice with regard to testing their incident response plans. Again, it's important to understand that a security incident is very likely a question of "when," not "if," for almost any Rural Bank in Ashanti Region. Every Bank or organization is unique, general best practice calls for an annual risk assessment and testing every six months. Organizations also must consider any major implementations or infrastructure changes that have taken place, and update and test their crisis response plans as needed to ensure they are aligned with the changes.

Apart from the policies that the banks have in place, there should be other security policies to be observed by the organization to safeguard the interest and image of the organization as well as the internal staff of the organizations. Policies like password requirement, staff rotation, data backup policies, user access right policies and many more are important to help prevent loss of data.

Rural Banks that keeps all their data and achieves them for future use is very encouraging. This is really a good sign as the percentage for banks that keep their data offsite is higher. It has been observed from the table that rural banks in Ashanti region do use proper devices for their backup operation. Few banks with a percentage of 19 responded YES to the question whether their institution have data security policy number of years or days to destroy the data. 16 percent of the respondents also agree that their bank achieve the data after its duration which is a good practice. From the findings, we can see that most rural banks in Ashanti region do comply about the data security policies of the institution. The important aspect of data is its security and integrity. We can say a data is secure if it has a certain level of trust, integrity, retrieval and restoration for a particular purpose.

From the table above, we can see that very small number of respondents which is the bank staff does not know how their data are kept. It is surprising that some staff of the banks is not aware about the state of their data. All these contribute to the fact that the banks do not organize training on security policies for their workers. The banks should inculcate the security measures training to their annually staff training program.

## XI. Summary Of Findings, Conclusion And Recomendation

General Response Summary

| Categories of questionnaires | Quantity of questionnaires | Respondent | Non respondent | % of respondent | % of non-respondent | Yes | No | % of yes | % of no |
|---|---|---|---|---|---|---|---|---|---|
| Physical security | 35 | 19 | 16 | 54% | 46% | 17 | 2 | 89% | 11% |
| Program change | 35 | 19 | 16 | 54% | 46% | 18 | 1 | 94% | 5% |
| Backup recovery | 35 | 19 | 16 | 54% | 46% | 16 | 3 | 84% | 16% |
| Disaster recovery | 35 | 19 | 16 | 54% | 46% | 15 | 4 | 78% | 21% |
| Computer operation controls | 35 | 19 | 16 | 54% | 46% | 2 | 17 | 11% | 89% |
| Network control | 35 | 19 | 16 | 54% | 46% | 9 | 10 | 47% | 52% |
| Personal computer | 35 | 19 | 16 | 54% | 46% | 14 | 5 | 74% | 26% |
| Internet controls | 35 | 19 | 16 | 54% | 46% | 17 | 2 | 89% | 11% |

Fig.8 : General Response Summary

### A. Discussion

Nineteen (19) responded to "physical security questions", non -respondent is sixteen, percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are seventeen (17), number of people who answered "no" are two(2), proportion of two despondences answered "yes" is 89%

and percentage of people who answered "no" is 11%. Nineteen (19) responded to "program change questions", non -respondent are sixteen(16), percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are (18), total number of people who answered "no" is one(1), percentage of people who answered "yes" is 94% and percentage of people who answered "no" is 5%. Nineteen (19) responded to "Back up recovery questions", non - respondent are sixteen (16), percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are sixteen (16), total number of people who
answered "no" are three (3), percentage of people who answered "yes" is 84% and percentage of people who answered "no" is 16%. Nineteen (19) responded to "Disaster recovery questions", non -respondent are sixteen (16), percentage of respondent is 54%, percentage of non - respondent is 46%, total number of people who answered "yes" are fifteen (15), total number of people who answered "no" are four (4), percentage of people who answered "yes" is 78% and percentage of people who answered "no" is 21%. Nineteen (19) responded to "Computer operation control questions", non –respondent are sixteen, percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are (2), total number of people who answered "no" are seventeen (17), percentage of people who answered "yes" is 11% and percentage of people who answered "no" is 89%. Nineteen (19) responded to "Network security questions", non -respondent is sixteen (16), percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are ten (10), total number of people who answered "no" are nine (9), percentage of people who answered "yes" is 52% and percentage of people who answered "no" is 47%. Nineteen (19) responded to "personal computer usage questions", non –respondents are sixteen (16), percentage of respondent is 54%, percentage of non -respondent is 46%, total number of people who answered "yes" are fourteen (14), total number of people who answered "no" are five (5), percentage of people who answered "yes" is 74% and percentage of people who answered "no" is 26%.

### B. Conclusion

The result of this research shows that some of the rural banks in Ashanti region do not fully implement the ICT policy of the bank. Moreover, the study revealed that some rural banks in Ashanti region do not have board of directors engage in their policies building. Data Security is becoming one of the most rapidly advancing techniques in the field of research especially with increase in technological advancements in internet and multimedia technology. With the technology advancing on one side, so has the rate of threat to hack, tamper or steal the data that is being transmitted over these medial also increased in leaps and bounds. This has necessitated an ever growing and systematic approach to ensure the security of data in every organization especially rural banks. The Bank has made it known that database backup policies are not instituted in some rural banks in Ashanti region. Percentage of staff unaware of data security in some banks is greater

### C. Recommendations

Companies including rural banks cannot stop using computers for their operations therefore the rural banks need to develop a security policy. To raise the awareness of the employees, who are using the system daily, a detailed and IT security training should be offered to them. Other simple steps include: protection of servers and routers by using onetime passwords and allowing only authorized users access to get to servers or routers. System administrators of rural banks can also implement a mechanism to manage incoming traffic, which can include DoS attacks against the control processors of routers.

Staying ahead of the ever-evolving threat of a data breach requires diligence on the part of the banks in understanding and anticipating the risks. This research outlines critical threats to organizations especially rural banks data and information systems. A brief description of each threat is followed by a suggestion of appropriate risk mitigation measures. As a rule, an organization can greatly reduce its vulnerability to security threats by implementing a comprehensive privacy and data security plan.

**Non-existent Security Architecture:-** Some rural banks in Ashanti region do not have established security architecture in place, leaving their networks vulnerable to exploitation and the loss of personally identifiable information (PII). At times, due to a lack of resources or qualified IT staff, organizations' networks are connected to the internet directly, or are connected using out-of-the-box network appliances with default configurations attached, with no additional layer of protection. It is important to note that having a firewall alone is not sufficient to ensure the safety of a network. Inadequate network protection results in increased vulnerability of the data, hardware, and software, including susceptibility to malicious software (malware), viruses, and hacking. Robust security architecture is essential and provides a roadmap to implementing necessary data protection measures.

**Mitigation**:- If the banks do not have the appropriate personnel to design a security architecture, it is recommended that the bank offer a data security training to the IT team or a third party be brought in to consult with the IT team.

## *References*

*[1] Mahendra Kumar Shrivas, Dr. Augustine Amoako, Samuel Odame Boateng, and Dr. Thomas Yeboah, "Migration Model for un secure Database driven Software System to Secure System using Cryptography," International Journal of ICT and Management, vol. III, no. 2, pp. 1-8, October 2015.*

*[2] Insu Song and John Vong, "Mobile Core-Banking Server: Cashless, Branchless and Wireless Retail Banking for the Mass Market," in International Conference on IT Convergence and Security, Macao, 2013, pp. 1-4.*

*[3] Rossouw De Bruin and S H von Solms, "Securing mobile applications in hostile rural environments," in IST-Africa Conference Proceedings, Le Meridien Ile Maurice, 2014, pp. 1-9.*

*[4] S.K. Amponsah, K.F. Darkwah, and C. Sebil, "Giving out loans, the best way out case study: Atwima Kwanwuma rural bank, Ashanti Region of Ghana," Journal of Science and Technology, vol. 26, no. 3, pp. 140-148, 2006.*

*[5] Susan K. Grove, Nancy Burns, and Jennifer R. Gray, Understanding Nursing Research: Building an Evidence-Based Practice. China: ELSEVIER, 2014.*

*[6] Lawrence Kwami Aziale, Elizabeth Afedo, and Emmanuel Kluivert Ahiekpor, "The Strategic use of Information Technology in the Rural Banking Sector in Ghana: Nwabiagya Rural Bank as a Case Study," Pentvars Journal, vol. 5, no. 3, pp. 77-90, 2011.*

*[7] Mabel Owusu Banie, Mahendra Kumar Shrivas, and*

ISSN : 2347 - 8446 (Online)
ISSN : 2347 - 9817 (Print)

*Thomas Yeboah, "Internet Privacy and Security Issues in Ghana," International Journal of management and Scientific Research, vol. 1, no. 2, pp. 22-32, 2016.*

*[8] Bank of Ghana. (2016, Apr.) bog.gov.gh. [Online]. HYPERLINK "https://www.bog.gov.gh/privatecontent/Banking_Supervision/REGIONAL%20DISTRIBUTION%20OF%20RURAL%20BANKS.pdf" https://www.bog.gov.gh/privatecontent/Banking_Supervision/REGIONAL%20DISTRIBUTION%20OF%20RURAL%20BANKS.pdf*

*[9] Mahendra Kumar Shrivas and Satya Vir Singh, "Implementing Added Advanced Encryption Standard (A-AES) to Secure Data on the Cloud," in International Conference On Management, Communication and Technolog, vol. III, Accra, Ghana, April, 2015, pp. 17-24.*

*[10] IBM. (2016) ibm.com. [Online]. HYPERLINK "http://www.ibm.com/analytics/us/en/technology/spss/" http://www.ibm.com/analytics/us/en/technology/spss/*

*[11] Ian Ellefsen, "The development of a cyber security policy in developing regions and the impact on stakeholders," in IST-Africa Conference Proceedings, Le Meridien Ile Maurice, 2014, pp. 1-10.*

*[12] Richard Hill, "Dealing with cyber security threats: International cooperation, ITU, and WCIT," in 7th International Conference on Cyber Conflict: Architectures in Cyberspace, Tallinn, 2015, pp. 119-134.*

## Author's Profile

*Mark Osei Gyebi has over 12 years experience in Rural Banking Sector as a Systems Administrator at Juaben Rural Bank Limited. His area of specialization includes Computer and Network Security, Banking network management, Database Management, Software Engineering. He is a member of Mozilla Ghana Community. He holds a Master of Science in Information Technology.*

*Mahendra Kumar Shrivas has over 10 years of experience in ICT Education. His area of research includes Cloud Computing, Big Data, IoT, Encryption-Decryption, Network and Cyber Security, Data Compression, eCommerce, Software Engineering and ICT Infrastructure Management. He is a member of IEEE Cloud Computing Community. He is also a Mozilla Rep and represents Mozilla Ghana Community.*