Digital Innovations & Contemporary Research in SCIENCE & ENGINEERING
Vol. 5 No. 2, June 2017

Article Citation Format
E.E. Iyobor, G. Asante & F.A. Kwadwo (2017). Data Security Issues In Corporate Environment: A Case Study of Mining Companies in Ghana. Journal of Digital Innovations & Contemp Res. In Sc., Eng & Tech Vol. 5, No. 2. Pp 63-78

Article Progress Time Stamps

Article Type: Research Article
Manuscript Received: 12th March, 2017
Review Type: Blind
Review/Acceptance Information Sent : 20th May, 2017
Final Acceptance:: 3rd July, 2017
DOI Prefix: 10.22624
Series ISSN - 2488-8699

Data Security Issues In Corporate Environment: A Case Study of Mining Companies in Ghana

E.E. Iyobor (PhD)
Regional Technical Head, Eastern and Volta Regions
Glo Mobile Ghana Limited
Koforidua, Eastern Region, Ghana
Email: eghopromise@yahoo.com
Mobile: +233543498346

G. Asante
Department of I. T Education
University of Education
Winneba, Ghana.
Email: gasante@uew.edu.gh
Mobile: +233242927029

F.A. Kwadwo
Dizengoff Ghana Limited
IT & Radio Engineer
Email: kfosu.appiah@gmail.com
Mobile: 0506060310

ABSTRACT

Data security in Information Technology today is a tough undertaking, particularly with the growing intricacy and bulk of attacks targeted at stealing information. In light of the current corporate conventional use of mobile devices in the operation of industrial and cooperative institutions in Ghana, data security has become a key challenge. In some instances, an unhappy employee or an employee who has only just resigned and gone to a competitor often can get access to delicate information of his previous employer. The need for data security optimization that groups many data-protection technologies to provide adequate coverage, besides tenacious data protection cannot be overemphasized. This research analytically assesses data security issues and challenges of corporate environments using four major mining sites in Ghana as case study and ascertains practical ways to effectively get the best out of data security.

Keywords: Data Security, Mobile, Mining, Corporate Environment, Information & Computer Security.

1. INTRODUCTION

1.1 Background of the study

The study and science of safeguarding data in computer and communication systems from unapproved access and alteration is what is termed as data security (Denning, 1982). The motivation behind data security is to ensure privacy while protecting personal or company data. Information kept in its fresh form on network servers, personal computers and databases is what is characterized as data. Data security is very important in public networks such as the internet. Encryption algorithms play key role in providing security to such networks. *Data at rest* and *Data in motion* could be best protected by password and encryption respectively. However, protecting *Data in use* is a tedious task that needs much attention.

The mining companies in Ghana handle a huge data from staff records through business models. Improper handling of these huge data will result in information leak which may affect the trade secret of the organization. Proper care must therefore be taken to protect the information of such companies.

1.2 Problem statement

Advancements in Information Technology have raised concerns about the risks to data security associated with weak IT security, including vulnerability to viruses, malware attacks and compromise of network systems and services. Data security in information technology today is a tough undertaking, particularly with the growing intricacy and bulk of attacks targeted at stealing information. In light of the current corporate conventional use of mobile devices and personal digital assistants (PDAs) in the operation of the gold mining industry in Ghana, data security has become a key challenge. Also contractors working with the mining companies may get connected to the network of the company whenever necessary without getting their devices checked by the IT department. Additionally, an unhappy employee or an employee who has only just resigned and gone to a competitor often can get to delicate information. The need for data security optimization that syndicates many data-protection technologies to provide adequate coverage, besides tenacious data protection cannot be overemphasized. This research analytically assesses data security issues and challenges of four major mining sites in Ghana and ascertains practical ways to effectively get the best out of data security.

1.3 Objectives of the Research

This research critically assesses data security issues and challenges and identifies optimum ways to effectively protect stored data and data being transferred through communication media.
The specific objectives of this study is to:

1 identify security concerns and challenges relating to safeguarding stored data and data being transferred or accessed.
2 focus on security threats and trends.
3 deliberate security techniques and practices to alleviate the threats and attacks.
4 optimize data protection.

1.4 Research Questions

1 What security concerns and challenges are there to safeguard stored data and data being transferred or accessed?
2 What are available security threats and trends?
3 What security techniques and practices are there to alleviate the threats and attacks?
4 How could data protection be optimized?

1.5 Importance of the study

As companies grow and obtain more data, the need for a security technology that integrates multiple data-protection technologies to provide complete coverage, along with persistent data protection, becomes essential.

Inadequate data security may result in compromised confidentiality, integrity, and availability of the data due to unauthorized access and alteration.

1.5 Scope and limitation of the study

1.5.1 Scope of the Research

This research mainly concentrates on looking into practical ways to optimize data security:

1. The research highlights the challenges being faced by IT experts with regard to the security of data in transition and to consider the efforts and measures being put in place to mitigate attacks and to optimize data security.
2. The research enumerates the challenges and risk exposure of stored data in local networks and when the network is connected to the internet.
3. The research examines some anticipated challenges in the near future concerning data security
4. The research looks into practical ways to mitigate future threats and to optimize data security

1.5.2 Limitations of the Research

Efforts were made to minimize all limitations that might creep in the course of the research; there were certain constraints within which the research was completed. These are discussed below:

1. The research was mainly based on information collected from the IT departments of only four major mining companies in Ghana. Although Keegan and Newmont Ghana are some of the best mining companies in the world, information collected from them cannot be considered as a proper representation of the actual state of the practice of data security in general. However, the objective of the survey was to check the challenges their IT experts face with regard to data security. Thus, this may not create hindrance in achieving the desired objective even if these two major companies cannot replicate the challenges of other major companies in the country.
2. For primary data, non-response error cannot be ruled out.

1.9 Definition of key Terms

- **Data:** Information kept in its fresh form on network servers, personal computers and databases is what is characterized as data (Spamlaws, 2015).
- **Corporate Data:** Confidential business information
- **Security:** Security refers to the defense of assets from any form of attack or threat.
- **Data Security:** Data security refers to the protection of electronic information from any method of attack or danger and the inhibition of unauthorized alteration or access.
- **Optimization:** Optimization is the realization of the highest possible level of performance taking into concern all the given restrictions and all factors affecting the circumstances both positive and negative.
- **Data Security Optimization:** This refers to the accomplishment of the highest possible level of data security

2. RELATED LITERATURE

Since 1975, Data security has developed speedily. Developments in cryptography such as public-key encryption, digital signatures, the Data Encryption Standard (DES), key safeguarding schemes, and key distribution protocols have been seen over the years. We have technologically advanced procedures for authenticating users, or hand off record data to users with minor security permissions. New controls for protecting data in databases and new approaches of getting information from these databases without proper authorization have been discovered. The hypothetical and real-world limitations to security are now better understood by IT personel (Denning, D.E. 1982).

2.1 Definition and Concepts

The safeguarding of information structures from destruction or burglary to the hardware, the software and to the information on them as well as from interruption or changing of the way the services are delivered is what is termed as Data security also identified as IT security otherwise known as Computer security, (Gasser, M. 1988). Various means of malicious acts usually from an anonymous source that attempts to manipulate, steal or destroy a specified target of an information system by hacking into it is described as an attack on the system. Mitigation techniques are used to prevent or minimize these attacks. In computing, a **firewall** is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules (Boudriga, N. 2010).

2.2 Data Security Attacks

Any efforts to destroy, uncover, modify, inactivate, steal or gain unapproved access to or make illicit use of an asset is termed as an attack. A computer security breach is therefore an attack on data and system components that may cause harm or make the network or computer vulnerable. The growing need of present society for information and computer networks has led to new expressions like cyber-attack and Cyber warfare. Data security attack is an attack aimed at subverting the reliability of the data or thieving controlled information; or an attack that makes use of Internet for the purpose of unsettling, incapacitating, putting an end to, or meanly controlling a computing environment or setup (Systems,C.O. 2010).

2.3 Attacks and Challenges

Active and passive attacks are the two main forms of attacks (IETF, 2000). Also it can be from outside, thus done by an unauthorized user of the system or from inside an institution, thus by someone inside the perimeter of the company's security.

Passive attacks

A passive attack steals information by checking unencrypted data traffic looking for important information and clear-text passwords that can be used in other attacks. For example:

1. Wiretapping- the monitoring of a telephone or internet conversation by a third-party, usually by covert means.
2. Port scanner- An application used by attackers to find services running on a host and weaknesses however it can be used by administrators to authenticate security policies of their networks.
3. Idle scan- scan technique that involves directing spoofed packets to a computer to find out what services are available. (Erikson, J. 1977)

2.3.1 Active attacks

An active attack endeavors to modify system resources or upset their operation. For example:

1. **Denial-of-Service (DoS)** attacks is an effort to make a service or resource inaccessible to its planned users, such as momentarily or open-endedly interrupts or suspend services of a host connected to the Internet. Where the source of attack is more than once it is termed as Distributed Denial-of-Service (DDoS) (McDowell, M. 2009).
2. **Spoofing attack** is a condition in which a program or a person effectively impersonates another by fabricating data, thereby getting an illegitimate benefit.
3. **Man-in-the-middle attack**, communication between two parties who believe they are directly communicating with each other is secretly controlled by an attacker who may alter the information. A man-in-the-middle attack can be used to attack many cryptographic protocols. (Trappe, W. 2005)
4. **ARP poisoning** is an attack whereby the MAC address of an attacker would be associated with the IP address of a host by sending Address Resolution Protocol messages onto a local area network by the attacker. Routing on a network can be successfully modified by an attacker permitting for a man-in-the-middle attack. (Jajodia, S. 2005) (Lockhart, A. 2007)
5. Ping flood is an attack in which the user is flabbergasted with ICMP Echo Request (ping) packets from the attacker resulting in denial-of-service.(Wikipedia Foundation, Inc., 2016)
6. A **ping of death** is a form of attack on a system that consists of sending abnormal or if not nasty ping to a computer. When a set of abnormal ping packets is reassembled by the target computer a buffer overflow can occur. This can allow injection of malicious code or affect the system to crash. (IETF, I.E.1981) (Erickson, J. 2008)
7. The **Smurf Attack** is an incident in which bulky Internet Control Message Protocol (ICMP) packets with the attacked user's hoaxed source IP are broadcast to a computer network using an IP Broadcast address. This is a form of distributed denial-of-service attack.
8. **Buffer overflow** occurs when adjacent memory locations are abnormally filled as data overruns buffers they are being written into. Memory safety is violated in this process. When there are inputs that are designed to modify a program's process or execute codes it can generate buffer overflow. It can be maliciously exploited. (Akritidis, P. ,Markatos, E.P., & Anagnostakis,K.D.2005) (Klein, C. 2004)
9. **Heap overflow** happens when a buffer overflow occurs in the heap data. Abuse is done by degrading this data in particular ways to cause the application to overwrite internal structures such as linked list pointers. Any process that may use affected memory may start behaving abnormally or data can be corrupted (Microsoft, 2004) (Phantasmal, 2005) (Microsoft, 2009).
10. **Format string attacks** can be used to disrupt a program's operation or to execute dangerous code. Format tokens such as %s and %x, can be used by an attacker to print data from perhaps locations in memory or from call stack. One may also write random data to capricious locations using the %n format token, which commands printf() (Seacord, R.C. 2005) (Cowan, C. 2003)

2.4 Important Security Issues

Confidentiality, integrity and availability of resources can be compromised as a result of data security breach.

2.5 Integrity

The correct representation of data in a system interpreting the purpose for which it is intended for is termed as the integrity of the information. The information is also checked to make sure it has not been modified by an unauthorized user to maintain its integrity.

2.6 Confidentiality

Data is prevented from being revealed to a person it is not intended for. When an unauthorized user views data from a system it is termed as loss of confidentiality. Some malicious users use social engineering to get access to

sensitive data; this is called physical loss of confidentiality. Attackers can also cause the loss of confidentiality when communication is not encrypted; this is termed as loss of electronic confidentiality.

2.7 Availability

Availability safeguards that data processing assets are not made inaccessible by mischievous action. For task critical systems this is extremely important. Availability for these systems is essential that companies need business endurance plans just for their systems to have redundancy.

2.8 Data Security Technologies

Disk encryption

Encryption technology that encrypts data on a hard disk is what is known as Disk encryption. Disk encryption typically takes form of either disk encryption software or disk encryption hardware. Disk encryption is often referred to as transparent encryption or on-the-fly encryption (OTFE). (Wikipedia, accessed 17/04/2017)

Backups

Copy of stored data can be stored on a different location from which the data can be retrieved when the main data is lost, this is called backup data. In most industries, it is essential to keep backup of any data and the process is recommended for any files of importance to a user. (Wikipedia, accessed 17/04/17)

Data masking

Structured data can be obscured (masked) within a database table or cell to ensure that sensitive information is not exposed to unauthorized personnel and data security is maintained. This may include masking the data from users, developers, outsourcing vendors and many other handlers. (Wikipedia, accessed 17/04/17)

Data erasure

Data erasure is a method of software-based overwriting that completely destroys all electronic data residing on a hard disk or other storage media to ensure that no sensitive data is leaked when an asset is retired or reused. (Wikipedia, accessed 17/04/17)

Firewall

A firewall is form of security system which serves as a barrier between a trusted and untrusted network or between internal and external network. It permits or denies information or traffic to pass it depending on the security criteria that has been configured on the network devices.

A firewall primarily uses ports and services as a reliance to allow or deny a data packet. Some data packets go through some particular ports depending on the services providing that data and the purpose of the information. For example, a port can be blocked to prevent anyone in the network from accessing the internet.

A firewall can be hardware based or software based but an ideal implementation includes both. It is the most common form of security being used by cooperative environments.

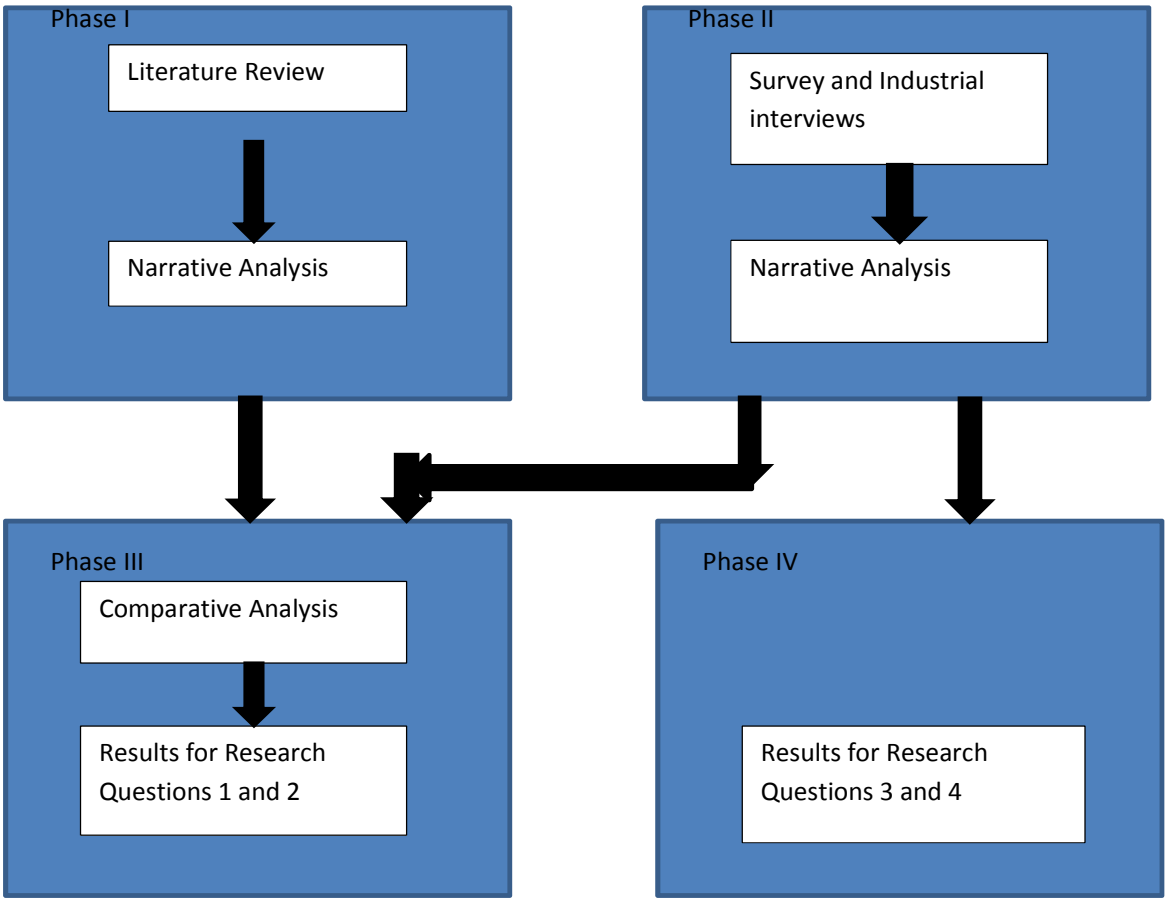
3. METHODOLOGY

In this research, we seek to give a description of a particular case, therefore Surveys and interviews which in this paper was done qualitatively have been undertaken as a primary research method whereas Literature review was considered as secondary to produce comparable data. We reviewed previous works on the topic and related topics to acknowledge the current knowledge.

3.1 Research Design

Figure 3.1 depicts the outlook of the research methods:

Figure 3.1



3.1.1 Research Questions

Research Question 1: What are the different data security encounters that are being encountered by the major mining companies, when there is the transfer of data within the confined network and to a remote site or network?

Research Question 2: What are the security procedures being used to constrain unauthorized access to data inside your company's network?

Research Question 3: Are there greater challenges to be expected in the future concerning data security in your company's network and when it is being remotely connected to and can you enlighten me on some of them?

Research Question 4: Can these expected challenges be mitigated effectively with current techniques or are the yet to be developed techniques that can be used to avert its adverse effects?

Table 3.1: Research Questions Definition

Research Question	Purpose
What are the various security challenges being faced by your company and techniques being used to prevent active and passive attacks when data is being transferred between the internet and a your local network?	To find out security attacks and the security techniques being used to safeguard data communication in the mining companies
What are the various security techniques being used to prevent unauthorized access to data within the institution?	To find out security techniques being used to protect store data in their systems
What are the major security challenges we expect in future access and resource sharing in your company?	To recognize the future data security challenges of the mining companies
How can we handle security problems that are expected in connection to the data security issues?	To propose the security procedures to handle the security problems in the future

3.2 Population

There are more than 50 mining companies in Ghana but in our research, we have chosen four of them for study. Refer to the table 3.1 for the definition of the population:

Table 3.2: Population

DEFINITION	DESCRIPTION
ELEMENT	Mining companies in Ghana, namely:
SAMPLING UNIT	• Newmont Ghana Gold Limited Ahafo (Ntotroso-Brong-Ahafo Region) • Newmont Ghana Gold Limited Akyem(New Abriem-Eastern Region) • Perseus Gold Mines (Ayamfuri-Western Region) and • Asanko Gold Mines (Manso Nkran-Ashanti Region).
EXTENT	n/a
TIME	16th January, 2016 to 1st February, 2016

3.3 Sample and Sampling Procedure

Due to limited time and resources probability sampling is not considered, hence this research is based on purposive sampling technique. We made contact with potential respondents thus IT experts and personnel with the use of telephone for the participation of this survey research but most of these respondents we met personally. More so, we had access to Keegan Mining site and Newmont Ghana Gold sites every Wednesday and Friday therefore have easy access to their IT personnel since my line of work requires me to work with them. We made sure we probe them with the questions while we work. In addition to these processes some also made some time to go through the survey questions with me until we had at least 15 respondents participating in this research. We communicated to each respondent the explanation of the purpose of the research and to complete the survey from 16th January, 2016 to 1st February, 2016. Each respondent would be sent a summary of the research results for the participation and the recommendations that will be made at the end of the research. The respondents are selected based on their knowledge, exposure and experience in the field of IT. It is through my personal work relationship with these experts that the participation and completion of this survey is ensured. The selection and ongoing maintenance of the sample is based on personal experience, updated industry news and events, referral and other information.

We selected 15 samples for quality and effectiveness of the survey. These chosen IT experts are regarded as professionals that have sufficient practical knowledge and experience in the field and are able to evaluate the state of the art and practice of data security (Kumah, 1999).

Table 3.3: Company to IT Professional Mapping

Name of Mining Company	Location	Number of IT Personnel	Number of interviewee(s)
Newmont Ghana Gold Limited (Ahafo)	Ntotroso-Brong-Ahafo Region	10	6
Newmont Ghana Gold Limited (Akyem)	New Abriem-Eastern Region	7	4
Perseus Gold Mines	Ayamfuri-Western Region	5	1
Asanko Gold Mines	Manso Nkran-Ashanti Region	4	3

3.4 Instrument for Data Collection

The method of face to face interview and survey questionnaire were chosen for this research. The two instruments were chosen for the efficiency of the data collection and the unique characteristics of the study population. The survey consisted of probing questions that were formulated to tap into the in-depth information on practical issues on data security. The survey enabled us to collect information on current issues and anticipated problems in the future. We then sought their professional opinions on practical measures that could be taken to mitigate these security issues in the future. The objectives and research questions of this research were the basics for the survey questionnaire. The questions started from current issues and progresses to expected issues in the future to the interest of respondents and gradually stimulating question answering. Thus, the questioning is from the known to the unknown. On the field while working with them we gradually drew into a conversion on issues of data security. Some respondents therefore made contribution without knowing why we were asking those questions. This was also effective in collecting the needed data since we wanted to approach the issue with open mindedness and curiosity.

The emails explained to participating respondents the purpose of this research and its relevance. Also the aims and objectives were explained on the survey questionnaire paper before answering the questions. The explanation seeks their agreement to participate in this research. Our contacts information were provided in case the respondent has any questions. The questionnaire is designed to compile knowledge and information that could help to practically optimize data security.

One of the major advantages of this instrument is the reduction of cost. The email system promotes efficiency and the respondents answer the survey questions at their own pace and convenience. Face to face interviews gave us idea of how seriously a respondent takes this research. There is the possibility of respondents' bias based on my judgment for sample selection and less spontaneous response.

The questions are organized in four sections:
Section 1: The first section is on current problems in data security
Section 2: The second section deals with current measures being taken to mitigate these problems.
Section 3: The third section is on future issues that are anticipated.
Section 4: The last section is on practical measures and way to mitigate current and future issues.

3.5 Data Collection

From the period 16th January, 2016 to 1st February, 2016 the feedback of the survey was collected. As responses are received, the data has been recorded and updated simultaneously. The results were compiled and summarized into a list of practical measures that can be used to practically optimize data security (Isaac, 2016) (Baidoo, 2016) (Yeboah, 2016) (Ralph, 2016) (Karim, 2016) (Ernest, 2016) (Billy, 2016) (Fredirick, 2016) (Jamel, 2016) (Yusif, 2016) (Poku, 2016) (Bernard, 2016) (Jeremiah, 2016) (Alex, 2016) (Alexander, 2016).

3.6 Data Analysis

Information provided by respondents was compiled into four different lists under the four major sections in the questionnaire. The information was normalized reducing points that appear twice or more in the report to one point. The relevance of every point is checked to see whether they are actually practical or just feasible theoretically. Tabulation and charts are provided for the ease of comparison of data security issues.

4. DATA ANALYSIS AND PRESENTATION

Presentation and analysis of collected data from research interviews will be discussed in this chapter. The background and information on respondents is also presented here.

4.1 Background Analysis of the Data

The goal of qualitative analysis is a thorough, meticulous description. Efforts are not made to allocate frequencies to the dialectal features which are recognized in the data, and infrequent occurrences should be given the same level of consideration as more recurrent occurrences. Qualitative analysis allows for adequate divisions to be drawn because it is not compulsory to force the data into a limited number of groupings (3equal, 2015).

Age of Respondent

The youngest of the respondents is 27 years and has been in the IT industry for at least 5 years. None of the respondents was above the age of 50.

Table 4.1 Ages of Respondents

Age	25-34	35-44	45-54
Number of respondents	7	5	3

Educational Qualification
All respondents have at least their first degree in IT or a related course that has IT at its core. All managers interviewed have a masters' degree in IT. Three of the managers have CCNA II and CCNA I.

Table 4.2 Qualification of Respondents

Qualification	Degree	Master's Degree	Degree & Professional Qualification or Certification	Master's Degree & Professional Qualification or Certification
Number of respondents	6	3	4	2

Occupation of Respondents
Most of these respondents were IT managers and technician who are employed. None of the respondents had specialized in data security but have in depth knowledge and significant experience in facing and solving data security issues (Isaac, 2016) (Baidoo, 2016) (Yeboah, 2016) (Ralph, 2016) (Karim, 2016) (Ernest, 2016) (Billy, 2016) (Fredirick, 2016) (Jamel, 2016) (Yusif, 2016) (Poku, 2016) (Bernard, 2016) (Jeremiah, 2016) (Alex, 2016) (Alexander, 2016).

4.2 Transcript
There were several interviews conducted but we have chosen points from some of the responses we got.

Research Question 1: What are the different data security encounters that are being encountered by the major mining companies when there is the transfer of data within the confined network and to a remote site or network?

- Tampering with Data
- Data theft and Wiretapping
- Impersonation of users
- Threats that are password related
- Access by unauthorized users
- Little or no monitoring of user activities
- Unstructured system architecture
- Multiple system administration
- Worms and viruses

Research Question 2: What are the security procedures being used to constrain unauthorized access to data inside your company's network?

- Basic Security System (firewall)
- Active Directory Rights Management Services
- Install an antispyware
- Encrypt user's data
- Monitor any application that has access to data
- Keep logs
- Always keep your security up to date
- Disable cookies
- Specific access control should be created

Research Question 3: Are there greater challenges to be expected in the future concerning data security in your company's network and when it is being remotely connected to and can you enlighten me on some of them?

- Malicious insiders
- Shared technology vulnerabilities
- Service and traffic hijacking
- Eaves dropping
- Hypervisor viruses
- Legal Interception point
- Virtual machine security

Research Question 4: Can these expected challenges be mitigated effectively with current techniques or are there yet to be developed techniques that can be used to avert its adverse effects?

- Update company computer security policy
- Train users
- Keep security up to date always

5. SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

Information gathered and findings are summarized in this chapter and deductions and inferences are also made based on the guide of the literature review. We have identified challenges and mitigation techniques being used in the cooperate environment. After analysis we came down to a list of practical ways to secure your data.

5.1 Findings of the study

Security challenges and mitigation techniques associated with data was discussed in the interviews. Currently Security problems and procedures that have been found so far are enumerated in chapter four. Several of these techniques were identified through our literature review. Confidentiality, integrity and availability are several of the major impacts of these security techniques.

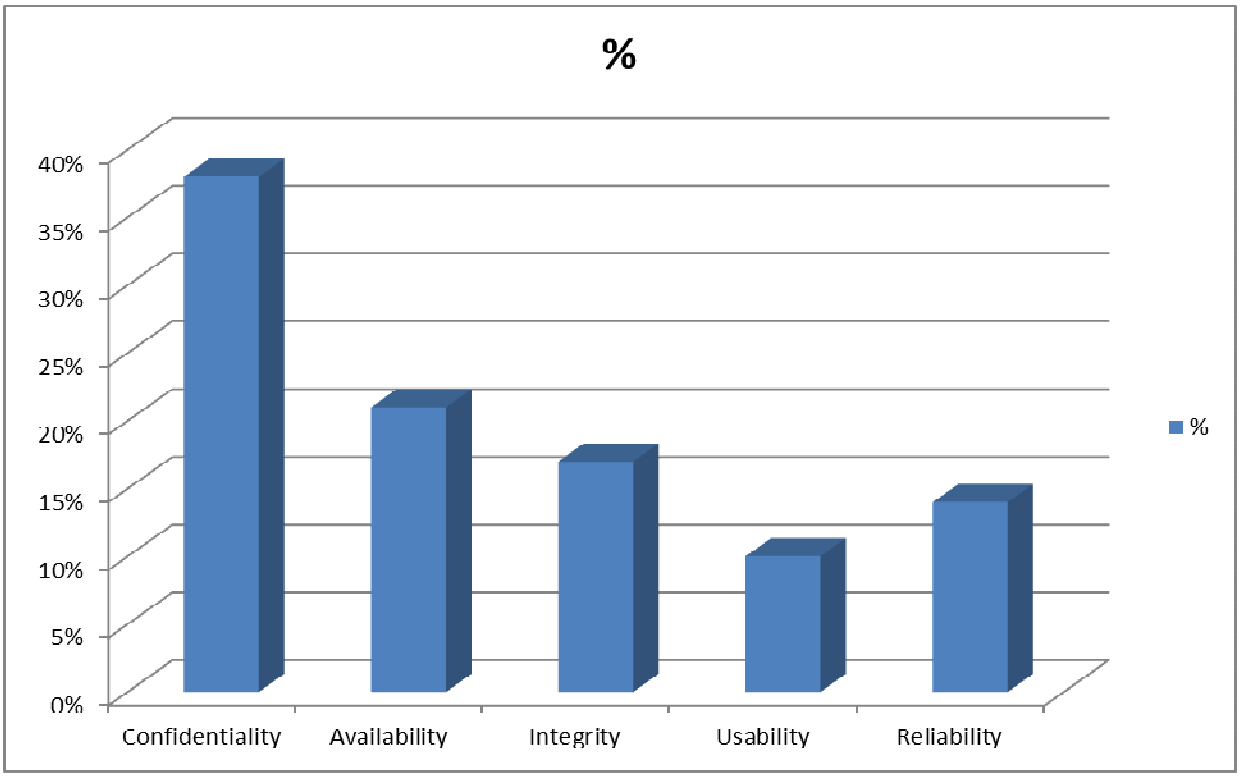


Figure 5.1 Compromised Attributes

5.1.1 Identified challenges

We gathered a number of data security challenges and issues that IT personnel face in a cooperate environment. The list of challenges consist of Tampering, Refutation or Denial of Service, Escalation of Privilege and Physical security just to mention a few. Refer to chapter four.

5.1.2 Identified mitigation Technique

A list of security techniques was compiled after analysis of the survey findings. The list consists of Active Directory Rights Management Services, Private face recognition among several others.
Refer to **chapter four.**

5.2 Conclusions

Hackers in the past understood the details of computer security and mostly highly skilled programmers. Anyone can become a hacker today by just downloading tools from the internet. Without security measures and controls in place, your data might be subjected to an attack. Data security systems cannot be designed once and for all. There is always the need to upgrade, update and sometimes to completely change the security technique being used. Considering the large number of services and systems that have access to your network you can identify the security challenges and mitigation techniques to counter them.

5.3 Recommendations/Suggestions

Technology is constantly updated in the optimization of information security. Network security solutions with time become less efficient as information technology advances and therefore cannot be designed once and for all. Once the system is setup, there should be constant monitoring, thus the implementation strategy should be an integration of security technology and management.

A reasonable solution to improve overall network design and optimization of the security system, to develop scientific, reliable, dynamic network security optimization design are as follows:

1. **Practical Measures** can be combined with the current firewall, intrusion detection / intrusion prevention technology, VPN technology to achieve rapid escalation of the information construction in the network security system, thus the basic realization of computer network security optimization design goal.
2. **Specific access control**: Users' access should be limited to the part of the system they need for their tasks by creating specific access control for every user.
3. **Maintain security patches**: Antimalware signatures and patches should always be updated to make sure software and hardware security is up to date.
4. **Train and educate users**: Naivety of users can get them lured into revealing passwords and user names to attackers. Installation of software should also be centralized.
5. **User policies**: Clearly outline company requirements and expectations in regards to IT security when new personnel come in.
6. **Monitor user activity**: Insider Threat Detection Solutions allows you to monitor users to verify that their actions meet good security practices.
7. **Data breach response plan**: This can help limit the damage a breach can do and close any vulnerabilities.
8. **Maintain compliance**: There are regulation and compliances as to how the company should run its security like HIPAA, PCI DSS and ISO to guide your business.

REFERENCES

1. 3equal. (2015). Retrieved from http://www.sal.tohoku.ac.jp/ling/corpus3/3qual.htm
2. Akritidis, P., Markatos, E. P., & Anagnostakis, K. D. (2005). Polymorphic Sled Detection through Instruction Sequence Analysis. *IFIP International Information Security Conference (IFIP/SEC/ 2005).*
3. Alex. (2016, April 6). Data Security Issues at NGGL Ahafo. (K. F. Appiah, Interviewer)
4. Alexander. (2016, March 4). Data Security Issues at Asanko Gold Mine. (K. F. Appiah, Interviewer)
5. atlasti. (2016). Retrieved from Atlasti Web site: http://atlasti.com/quantitative-vs-qualitative-research/
6. Baidoo, C. (2016, March 30). Data Security Issues at NGGL Ahafo. (K. F. Appiah, Interviewer)
7. Barwise, M. (n.d.). *What is an internet worm?* Retrieved September 9, 2010, from BBC.
8. Bernard. (2016, April 6). Data Security Issues at NGGL Ahafo. (K. F. Appiah, Interviewer)
9. Billy. (2016, March 16). Data Security Issues at NGGL Ahafo. (K. F. Appiah, Interviewer)
10. Boudriga, N. (2010). Security of mobile communications. Boca Raton: CRC Press.
11. Cowan, C. (2003). Software Security for Open-Source Systems. In I. C. Society (Ed.), *IEEE Security & Privacy.*
12. D, S. (2000). *Changing the Default for Directed Broadcasts in Routers.* IETF. The Internet Society.
13. Denning, D. E. (1982). *Cryptography and Data Security.*
14. Eric Wimberley, & Nathan Harrison. (n.d.). *Papers: general.* Retrieved April 3, 2016, from https://dl.packetstormsecurity.net/papers/general/ModernOverflowTargets.pdf
15. Erickson, J. (2008). *HACKING the art of exploitation (2nd ed.)* (2nd ed.). San Francisco: NoStarch Press.
16. Erikson, J. (1977). HACKING the art of exploitation. San Francisco: NoStarch Press.
17. Ernest. (2016, March 21). Data Security Issues at Asanko Gold Mines. (K. F. Appiah, Interviewer)
18. Fredirick. (2016, February 12). Data Security Issues at Perseus Gold Mine. (K. F. Appiah, Interviewer)
19. Gasser, M. (1988). Building a Secure Computer System. In V. N. Reinhold.
20. IETF, I. E. (1981, September). rfc791. Carlifornia.
21. IETF. (2000, May). Internet Security Glossary. *RFC 2828.*
22. Isaac. (2016, April 4). Data Security Issues at NGGL Ahafo. (K. F. Appiah, Interviewer)
23. Jajodia, S. (2005). Detecting ARP Spoofing: An Active Technique. In V. &. Ramachandran (Ed.), *Information system security: First international conference, ICISS 2005* (p. 239). India: Birkhauser.
24. Jamel. (2016, March 18). Data Security Issues at NGGL Akyem. (K. F. Appiah, Interviewer)
25. Jeremiah. (2016, March 30). Data Security Issues at NGGL Ahafo. (K. F. Appiah, Interviewer)
26. K, W., & E., P. (Nov.2010). An Investigation into CLoud Configuration and Security. *International Conference for Internet Technology and Secured Transactions*, (pp. 1-6).
27. Karim. (2016, March 21). Data Security Issues at Asanko Gold Mine Site. (K. F. Appiah, Interviewer)
28. Klein, C. (2004). *Buffer Overflow.*
29. Klein, T. (n.d.). *Buffer Overflows und Format-String-Schwachstellen.* Dpunkt Verlag.
30. Kumah, R. (1999). *Research Methodology.*
31. Lockhart, A. (2007). Network Security Hacks. *O'Reilly*, (p. 186).
32. Maddineni, V. S., & Ragi, S. (2011). *Security Techniques for Protecting Data in Cloud Computing.* Master Thesis, Blekinge Institute of Technology, School of Computing, Karlskrona.
33. McDowell, M. (2009, November 4). Cyber Security Tip ST04-015 - Understanding Denial-of-Service Attacks. *United States Computer Emergency Readings Team.*
34. Merriam-Webster. (2015). *Dictionary:Definition of Optimization.* Retrieved March 12, 2016, from www.merriam-webster.com: http://www.merriam-webster.com/dictionary/optimization
35. Microsoft. (2004, December 14). *Library: Security Bulletins*, 3.0. Retrieved April 2016, from Security TechCenter.

36. Microsoft. (2009, August 4). *Blogs.* Retrieved April 3, 2016, from blogs.technet.microsoft.com: https://blogs.technet.microsoft.com/srd/2009/08/04/preventing-the-exploitation-of-user-mode-heap-corruption-vulnerabilities/
37. Microsoft. (2015). *cc785896%28v=ws.10%.aspx.* Retrieved March 19, 2016, from Microsoft Technet: http://technet.microsoft.com/en-us/library/cc785896%28v=ws.10%.aspx
38. Phantasmal. (2005, October 11). *Papers: Attack.* Retrieved April 3, 2016, from Packet Storm: https://dl.packetstormsecurity.net/papers/attack/MallocMaleficarum.txt
39. Poku, A. (2016, Febuary 12). Data Security Issues at Perseus Gold Mine. (K. F. Appiah, Interviewer)
40. Ralph. (2016, March 25). Data Security Issues at NGGL Akyem. (K. F. Appiah, Interviewer)
41. Seacord, R. C. (2005). *Secure Coding in C and C++.* Addison Wesley.
42. Security Focus. (2007, March 13). *Post: Post Reply.* Retrieved March 23, 2016, from SecurityFocus: http://www.securityfocus.com/archive/1/462728/30/150/threaded
43. Spamlaws. (2015). *data-security.* Retrieved March 23, 2016, from www.spamlaws.com: http://www.spamlaws.com/data-security.html
44. Summers, G. (2004). Data and databases. In H. Koehne, *Developing Databases with Access* (pp. 4-5). Australia: Nelson Australia Pty Limited.
45. Systems, C. O. (2010, April 26). CNSS Instruction No. 4009.
46. Trappe, W. (2005). Introduction to Cryptography with Coding Theory. New York: Pearson.
47. *What is Data Security.* (2016). Retrieved February 2016, from Spamlaws website: http://www.spamlaws.com
48. Wikimedia Foundation, Inc. (2016, January 3). *www.wikipedia.com.* Retrieved March 20, 2016, from Wikipedia: http://osdir.com/ml/linux.redhat.release.nahant.general/2006-05/msg00176.html
49. Wikipedia Foundation Inc. (2016, January). *Data Security.* Retrieved February 23, 2016, from www.wikipedia.com: http://en.wikipedia.org/wiki/Data_security
50. Wyse, S. E. (2011, September 16). *Blog:.* Retrieved March 4, 2016, from Snap Surveys Web site: http://www.snapsurveys.com/blog/what-is-the-difference-between-qualitative-research-and-quantitative-research/
51. Yeboah, K. (2016, April 1). Data Security Issues at NGGL Akyem. (K. F. Appiah, Interviewer)
52. Yusif. (2016, March 18). Data Security Issues at NGGL Akyem. (K. F. Appiah, Interviewer)