

THE JOURNAL OF
**DIGITAL FORENSICS,
SECURITY AND LAW**

**Journal of Digital Forensics,
Security and Law**

Volume 3 | Number 4

Article 1

2008

Data Security Measures in the IT Service Industry: A Balance between Knowledge & Action


N. Mlitwa

Cape Peninsula University of Technology (CPUT)

Y. Kachala

Cape Peninsula University of Technology (CPUT)

Follow this and additional works at: <https://commons.erau.edu/jdfsl>

 Part of the [Computer Engineering Commons](#), [Computer Law Commons](#), [Electrical and Computer Engineering Commons](#), [Forensic Science and Technology Commons](#), and the [Information Security Commons](#)

Recommended Citation

Mlitwa, N. and Kachala, Y. (2008) "Data Security Measures in the IT Service Industry: A Balance between Knowledge & Action," *Journal of Digital Forensics, Security and Law*: Vol. 3 : No. 4 , Article 1.

DOI: <https://doi.org/10.15394/jdfsl.2008.1048>

Available at: <https://commons.erau.edu/jdfsl/vol3/iss4/1>

This Article is brought to you for free and open access by the Journals at Scholarly Commons. It has been accepted for inclusion in Journal of Digital Forensics, Security and Law by an authorized administrator of Scholarly Commons. For more information, please contact commons@erau.edu.



(c)ADFSL



Data Security Measures in the IT Service Industry: A Balance between Knowledge & Action

Mlitwa, N.

mlitwan@cput.ac.za

Kachala, Y.

joelkachala@gmail.com

IT Department, Faculty of Informatics & Design (FID),
Cape Peninsula University of Technology (CPUT)

ABSTRACT

That “knowledge is power” is fast becoming a cliché within the intelligentsia. Such power however, depends largely on how knowledge itself is exchanged and used, which says a lot about the tools of its transmission, exchange, and storage. Information and communication technology (ICT) plays a significant role in this respect. As a networked tool, it enables efficient exchanges of video, audio and text data beyond geographical and time constraints. Since this data is exchanged over the worldwide web (www), it can be accessible by anyone in the world using the internet. The risk of unauthorised access, interception, modification, or even theft of confidential information, leading to financial losses in information dependant “competitive” institutions is therefore high. Improving efficiencies through ICT therefore, comes with security responsibilities. The problem however is that most organizations tend to focus on task-enhancing efficiencies and neglect security. Possibly due to limited awareness about security, underestimating the problem, concerns about security costs, or through plain negligence. The activity theory of Engeström and the activity analysis development framework of Mursu *et al* are used as analytical lenses to the cybercrime challenge in this paper. A practical case study of Company X, an IT service provider in Malawi is then used to understand the extent to which organisations that offer electronic data solutions prioritise security in their operations. It is found that even better informed organisations fall short in taking adequate data security measures. A recommendation for all organisations is that they should not only have a clear policy, but also ensure that it is routinely and consistently implemented throughout the operations if information capital is to be secured. A framework towards a holistic approach to thinking about, and in addressing cybercrime is suggested, and recommended in the paper.

Keywords. data, information, security, access control, internet, networks.

1. INTRODUCTION

In today's so called information-based economy, information has become a critical asset for organisations, and a means through which individuals can access and unlock better life opportunities. It is for this reason that extensive efforts through debates, conference gatherings, and research across governments, multinational corporations, academic institutions and the international development community continue to be channeled towards information handling innovations. The world summit on information society (WSIS, Geneva2003 & Tunis2005) is a useful example.

The Webster's Dictionary defines information both as facts and data, and as the "knowledge obtained from investigation, study, or instruction". Similarly, Amiidon (1997) describes information as data with context. But what is data? Data is raw and uncoordinated pieces of facts, with less or no meaning until transformed into information, which in turn is specifically organized into knowledge (Wang, 1998)

Connection between the concepts of information, knowledge, and data is clear in this definition, to the extent that each term cannot be defined independently of the other. For example, if information is built from interpreted and analyzed data, then information cannot be independent of data. The same is true of knowledge and information. If knowledge consists of specifically arranged forms of information, it cannot be viewed separately from information. Therefore, since information is made of data, and knowledge made of information, then data must be a key element of knowledge. It follows from this explanation that if "knowledge is power" (as educators, economists, and politicians would say), that the same is true for information and data.

Like knowledge, data and information does not derive power from its content alone, but also to the tools and methods in which it is exchanged, stored, transformed, and put into use. Fast and effective access and retrieval of information for example, would enhance management processes thereby enabling an entity to gain a competitive edge over its market rivals. New information and communication technologies (ICTs) play a key role in this respect. Technology tools such as computers, internet, and e-mail facilities for example, enable effective communication within and between government officials, departments, as well as between the government and the public (Mlitwa, 2005). It is now possible to exchange voice, video, and text data across world destinations in real time, and around the clock, thanks to the power of the internet, and other networked technologies such as new generation mobile phones and computers (Wu, Hou, Zhang, 2000). The internet has made the concept of world free trade a practical reality. Now commodities can be marketed, sold and purchased online – regardless of time and geographical distances (Theilmann, Rothermel, 2000). Through internet based e-commerce, which involves the buying of products or services online (U.S. Census Bureau, 2000), we can pay monthly bills online, and purchase

items online (without setting the foot off our living rooms).

The difference between manual and networked information exchanges is that whilst fewer people may have access to your confidential data in manual transactions, online transaction such as e-commerce involve exchanges of critical and confidential data (and information) between the merchant and a customer over a network that is accessible and used by the world wide population (M.A. Badamas, 2001). In the case of Amazon.com where a variety of goods are sold online for example, to buy, one has to register first, hence providing personal information such as name, physical address and even a phone number as well as banking details. *See Fig.1 under annexes section.*

Buying an item online and settling your bill by completing this short form, and simply pressing the complete button is both convenient and efficient.

1.1 Research Problem

As Calder and Watkins (2007) warn however, the “threats to the availability, integrity and confidentiality of the organization’s information are great and always increasing” with networked platforms. Data transmitted over such a medium can be accessed by unauthorised parties. It can then be used for malicious intentions when not adequately protected. The same is true of any transaction that involves data and information exchange over a networked medium, or similar services.

In this respect, diligent organisations do more than just ensuring practical efficiencies of data storage and exchange processes. They ensure that such information is protected from unauthorized access, manipulation, and theft (Koller, Leyov, 2005). The aim of this paper is to investigate whether information service organisations take adequate measures to protect their electronic data. Moving from the assumption that organisations specializing in network data exchanges, internet access, web development and maintenance, and other related ICT services are security conscious, the paper investigates precautions taken by one of the organisations in the field: Globe Computer Systems Ltd in Malawi. A research process, method of investigation and research question/s are discussed under the methodology section below.

1.2 Methodology

The availability, integrity and confidentiality of data (and information) “*are fundamental to the long term survival of any organisation*” (Calder & Watkins, 2007). This study investigates how organisations in electronic data services prioritize the safety of their electronic data assets (data, services and infrastructure). A leading provider of IT services such as web development, software development, management systems (payroll), and internet access, Company X Computer Systems LTD (www.globecompusoftware.com) in Malawi has been selected for a case study.

The study follows a descriptive qualitative approach, using existing literature (as

secondary data) and interview questions (as primary data). Background data is sourced from existing academic literature and industry reports on dominant practices. Primary data in the form of interviews are conducted with the manager of this organisation. The activity theory of Engeström (1999) and the activity analysis development framework of Mursu et al (2007) are used as analytical lenses.

The paper opens with a background of common information security threats, risks, and related precautions in section 2. The problem of cyber-crime is closely scrutinised through the activity theory lenses in section 3. Section 4 describes the organisation under study (Company X), the nature of services they provide, type of clients (i.e. individuals, government, companies) they serve in Malawi.

Section 5 describes the findings with respect to measures taken in this organisation to protect its electronic data, with emphasis on the following questions:

- What are the services the organisation provides?
- How does it provide these services?
- What are existing security measures for each area of functionality in this organisation?
- Is there is a policy to inform and ensure information security in the organisation?
- Is this policy is implemented and how?
- What are the existing access control measures (and how they are implemented)?
- Does it have an intrusion detection system (& how it is monitored)?

Sub-section 5.1 entitled a discussion of findings describes the implications of the status of existing measures to data security in this organisation. Section 6 entitled “limitations of the study” precedes the conclusion and recommendations section (section 7).

2. BACKGROUND – GENERAL IT SECURITY PRECAUTIONS

Information technology (I.T) security involves the physical I.T. infrastructure along with its logical environment hence it is classified into two categorized, physical and logical security.

2.1 Physical Security

The protection of physical I.T. infrastructure (Servers, workstations, Phones, cabling and even the environment in which the I.T. resources are kept. A building could be a good example). Here the risks would include natural disasters such as fire, floods, earthquakes and lightning strikes as well as human risks which are theft of physical I.T. components which would render data or information availability impossible (Huff, 2003). Sometimes physical threats may impact

logical security in such a way that a person gaining physical access to a room where computers are kept, can then compromise logical security.

2.2 Logical Security

This is the protecting of data that is held and in transit through a network infrastructure. Logical security comprises of three components: confidentiality, integrity and availability which are also the main base of I.T. or electronic information security. i.e. the main purpose of electronic data security is to balance or maintain these three elements (Oliver, 2002).

2.2.1 Confidentiality

This involves the means of ensuring that secret data does not fall into wrong hands, the hands that can use it against the interest of the organisation

2.2.2 Integrity

Data integrity refers to measures of protecting information against unauthorised modifications, and ensuring the authenticity of data and information.

2.2.3 Availability

Security measures to ensure data availability refer to efforts to ensuring that information remains available at all times, to the right people, and when needed.

These threats can take place as a result of intrusion from outside the organisation (external) and or by stake holders internal to the organisation (Whitman, 2003). Thus the security precautions should address both internal and external threats. Access control measures play a significant role in this respect.

2.3 Access control

Access control is the collection of mechanisms for limiting, controlling, and monitoring system access to certain items of information, or to certain features based on a user's identity and their membership in various predefined groups (Mlitwa, 2007).

2.4 Protecting data against internal parties

This can entail protecting the physical and logical I.T. infrastructures (Mlitwa, 2007). The physical structure can be protected by the use of;

- Lock and key, and biometrics to control access to some rooms, only those who are authorized should access the room.
- Control access to computers through the use of passwords.
- Controlling access to some network resources using network groups
- Implement and enforce policies on computer usage and password management, no shortcuts when dealing with business processes.

2.5 Protecting data against external threats

External threats pose the most risk since they take calculated deliberate action – rather than happen by mistake. They always have a reason which is to destroy, steal or modify data. These threats can include people learning how to hack systems and professional hackers (Mlitwa, Lecture). These people use sophisticated software to steal passwords and to intrude into networks. Sometimes they use malicious code which they use to disrupt system operations so as to get access to it. Some of the examples of malicious code used are viruses, worms, Trojans, key loggers and spam. Lastly in case of internet transaction handling systems, they can use defacement to collect or steal credit card information from people.

To protect systems and networks from external threats, organisations can use firewalls to separate their networks from external networks, and use Demilitarised Zones (DMZ) which are networks put between an organisation's trusted and external networks such as the internet. Most of the times, the zone is between firewalls, and organisations can just exclude their internal network from the internet so that it should only be accessed from within the organisations. They also implement intrusion detecting systems to monitor and notify network managers in case of a security breach. The other threat which might befall an organisation from external parties is the use of malicious software such as viruses, Trojans, worms and spy ware (Azwat Asmat). This can be controlled by the use of antivirus and installation of updates to block and clean these malicious codes. Lastly to protect clients' credit card details, organisations should make it a point to sensitize their clients on best practices when they want to make an online purchase. For instance, looking for security features like https on the URL and a lock sign in the status bar on websites they want to conduct a transaction on (Mlitwa, 2007).

3. CYBER-CRIME, FROM THE ACTIVITY THEORY PERSPECTIVE

The basic unit of analysis in Activity Theory is the activity, individual actions, mediators or tools, goals and the process. Expanding on Vygotsky's notion of human activity being mediated by tools and signs, Leont'ev (1978, in Engeström *et al.*1990: p.140) suggested a three tier structure of understanding collective human activity. He breaks the levels of analysis into the unit (activity, action, or operation), directing factor (objective, goals and conditions), and the subject (individual or group actor/s, as well as tools and signs or mediators). Activity within the activity theory perspective therefore, is a collective phenomenon often with a shared motive (Engeström, 1999). The levels of analysis in a cyber crime context are outlined in figure 1.

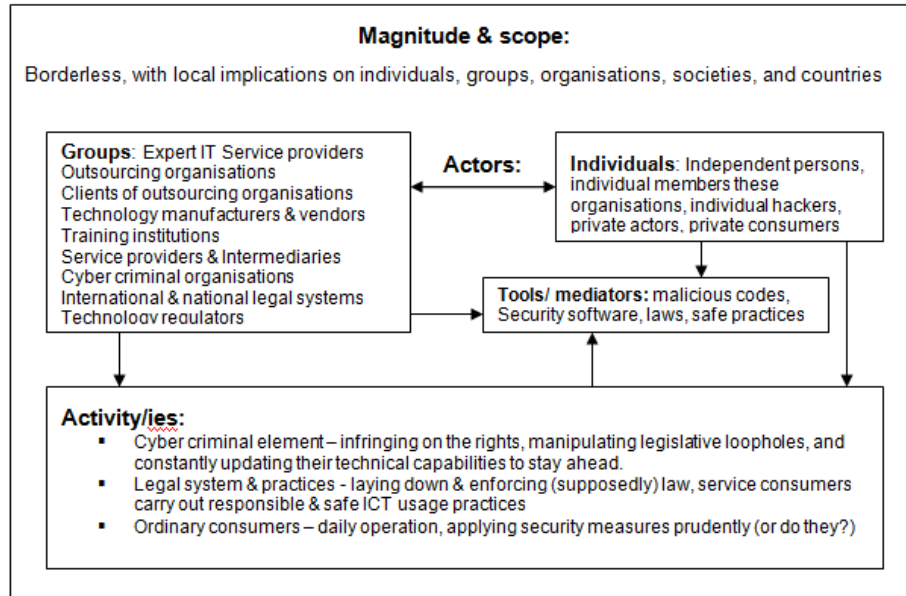


Figure 1: Cyber crime – Levels of Analysis

Since the notion of information (which is at stake in the case of cyber-crime) is a unit of communication that only makes sense when shared and exchanged, we view cyber-crime as activities carried out in a networked technology and information system environment either by an individual criminal or a group, against shared information processes of the victims. A cyber criminal cannot attack himself/ herself, but at least a network, a victim, and some activity. Collective activity with a goal/s and ultimately, some infringements is therefore implied. It is within this model of thinking that adherence to preventative measures against cyber crime in the IT service industry are investigated in this study.

4. A CASE STUDY OF COMPANY X

Company X is one of the biggest IT service providers in Malawi. It primarily focuses on providing IT solutions to Malawi and sub-Saharan Africa. Company X is demarcated into two sub companies which is Company X Internet and Company X computers of which the main division (department) is X soft (software department). This unit undertakes software development and implementation of IT solutions. The services offered by Company X’s software division are;

- Enterprise Establishment and Payroll and HR Management Systems (for large companies over 10,000 employees & government institutions with established HR policies and functions)
- Payroll and HR Management Systems (for SME’s and Companies)

- Point of Sale Systems (for SME's and Companies)
- Time Attendance Management System (for SME's and Companies)
- Insurance Management System (Insurance industry)
- Track & Trace and Mail Management System (Postal Corporations)
- Electoral Management System (Public sector/ Governments)
- Property Management System (for Real Estate Sector)
- Utility Billing System (for consumer utility distributors such as water supplies)
- Tea Blending & Stock Management System (for Tea Brokers)

And the services offered by GCSL's Internet division are;

- Broadband internet
- WIFI - Public wireless internet
- dial up internet
- IP-VPN - VPN, Short for virtual private network, is a network that is constructed by using public wires to connect user points.
- WAP - WAP stands for Wireless Access Protocol,
- VSAT Solutions - VSAT Short for very small aperture terminal, is an earthbound station used in satellite communications
- Web development
- Domain registration
- yellow pages

Some of the clients Company X has are;

- Malawi Government – Payroll & HR Solution (HRMIS) for the Civil Service and Police & Defense Forces
- Decentralization Secretariat & District Assemblies – Payroll & HR Solution
- Malawi Electoral Commission - Election Management System
- Malawi Posts Corporation – International & Domestic Mail Management and Track & Trace System
- Over 300 Clients support on Sage Financial systems

The nature of its services, given the magnitude of clients it serves, largely involves the handling of sensitive confidential data (Company X keeps databases that carry

confidential organizational or personal information of their clients). This is a strong motivation for Company X to take extra security measures to ensure the safety and security of its client's as well as its own information resources.

5. RESULTS: SECURITY THREATS

Since cases of hacking are not common in Malawi, Company X only puts limited security measures to prevent either internal or external threats:

- Company X uses the SAGE accounting system to manage its finances but there are seven employees from different departments who access the system and they all have the same access rights.
- The payroll software system has five users. Three of them (during the interview) had never changed their passwords set since the time they were being trained. The possibility is that almost all can be using the same password.
- All the systems are hosted in one server of which everyone from the software department is able to access. Since they are skilled, and have been supporting clients with database related issues it would be easy for anyone of them to access the payroll data base and commit fraud.
- There is limited physical control on who access what computer. Everyone has a computer to use, but when one is absent any one can access that computer. People even share their passwords.

According to Mr. FK, hacking and many of the external forms of external attacks are not common in Malawi. The only threat could be people who have direct access to the data,

“though we have some kind of access control, you know a person will always try other ways until he gets what he wants either intentionally or by accident. But still [Company X] has set some security measures to prevent either external or internal attacks”.

The only available security measures for the areas of functionality in this organization are;

- The use of passwords to control access to database management systems and software. The company does however, have a firewall to protect the network from outside attacks.
- The only known policy about securing electronic resources is the use of passwords. This is no security when we consider inside threats of which is the most dangerous threat for Company X.
- There is no physical control for computer access. Thus most employees have access to other employees' computers. Sharing passwords and not changing them, means that one can get access to

several computers which may make data sabotage difficult to trace.

- Believing that they are not prone to external intrusions, there is no intrusion detecting systems.

For internet subscribers, it is a bit safe as they have to be authenticated before they connect to the internet. As Mr. FK puts it,

“If you are talking from the security point of view that is, when customer details are exposed to third party and our clients know about it. Just imagine what that could do to business. I mean everyone knows that a lot of people don’t give out their person details to other people. But they trust us because they want our services and they trust we are going to use their information as intended. This is supposed to be the least critical of them all which means that all the data we have is critical as we have it on purpose and we are not ready to expose any of it.”

The only security measures within Company X are passwords and the use of firewalls, so if attackers could target these measures the company and its clients would be severely exposed.

5.1 Discussion of Findings

According to the investigation, much effort is required to improve the security of electronic data, including strong policies for the appropriate use of passwords and physical access to computers. All employees should change passwords occasionally to limit the physical access to individual work stations by other employees - unless if it is necessary and that the password should be changed after that.

This requires a paradigm shift from the misguided illusion that they will never be attacked by external parties. So, instead of using firewalls only, it is advisable to use other technologies like demilitarized zones and intrusion detecting systems to limit vulnerability to threats.

There are 7 people with the same access rights to using the SAGE accounting system. The number of people accessing this accounting system should also be reduced to a controllable minimum. The same applies to the payroll; the passwords should be set in such a way that only those responsible for payroll processing should be the ones accessing it.

6. CONCLUSIONS

The “future wealth and prosperity of industry and commerce rely increasingly on the exchange of data and information in electronic form, between business partners” (Abrahams, et al, 1995). Whether it is business partners such as suppliers, customers, manufacturers, bankers and carriers or collaborative actors of other kind – prosperity of a collective activity is largely dependent on how we keep privileged information away from competitors and criminals.

In the case of Company X, everything might seem safe since there are no intrusions or security breaches or we can say, the organisation is not aware of any. But if and when it happens, the impact of security breach can cost the life of an entity. For any other organisation in similar circumstances, paying more attention to the safety and security of electronic data should receive more attention (rather than neglect), before it is too late. A holistic approach to information security measures is therefore recommended.

6.1 Recommendations: a Holistic Framework

We recommend a holistic approach to looking at information security, and in approaching the cyber-crime threat, as illustrated in figure 2.

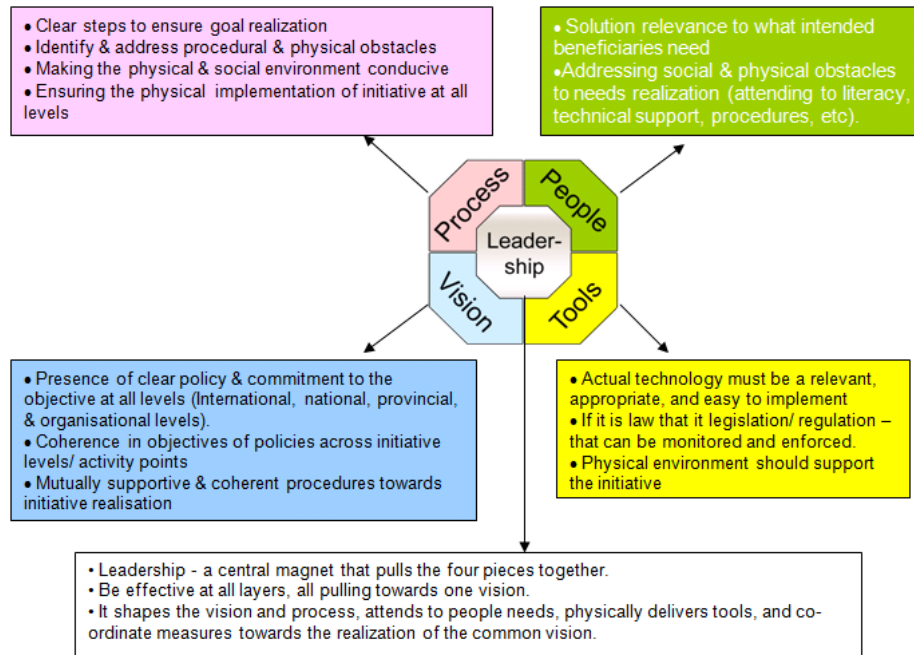


Figure 2: A holistic approach to understanding & tackling cyber-crime

Cyber-crime is just as evolving in complexity as are technological innovative solutions. Further, the global nature of the World Wide Web (www) also suggests that cyber-crime is border-less. It cannot be pigeon-holed into a specific geographic location as threats could emerge from anywhere in the world. There is a need for information-centric entities to apply optimum information security practices. The main point emanating from figure 2 is that isolated and sometimes reactionary solutions are limited as they tend to address one aspect of security whilst leaving the other open. Addressing the tools aspect alone for example, is inadequate if the people aspect is neglected as people would simply just ignore implementation procedures. Attending to the tools and the people aspect also

requires strong leadership with foresight for vision, relevance, policies, implementations, and tools updates. It is difficult to win the cyber-crime combat that way as cyber-criminal are smart enough to manipulate all available possibilities to access your information resources.

7. REFERENCES

Abrams, M.D., Sushil, J. and Podell, H.J. (1995) Information Security. *An Integrated Collection of Essays*, 1995, IEEE Computer Press.

Amazon.com <http://www.amazon.com/gp/checkout/address/create.html/102-1395993-6685731>. Accessed on 04 May 4, 2007.

Amidon, Debra M. (1997) *Innovation Strategy for the Knowledge Economy: The Ken Awakening*; by Butterworth-Heinemann.

Azwat, A. (2007) Malicious Software – Facts That Most People don't know, Avail: www.goarticles.com/cgi-bin/showa.cgi?C=632829, Accessed October 17, 2007.

Badamas, M.A. (2001) *Information Management & Computer Security* avail: www.emeraldinsight.com/Insight/viewContentItem.do?contentId=862796&contentType=Article. Accessed October 12, 2007.

Calder, A. and Watkins, S. (2002) *IT Governance: A manager's guide to information security and BS 7799/ ISO 17799*, 2002, Kogan Page LTD.

Calder, A and Watkins, S. (2007) *IT governance: A manager's guide to information security and ISO 27001 / ISO 27002 Fourth Edition*, 2007, Kogan Page LTD.

Castells, M. (2001) *The Rise of the Network Society: The Information Age, Economy, Society and Culture*, Oxford; MA: Blackwell Publishers.

Cool, A. (2003) *Solving e-commerce issues: some Web strategies*.

Engeström, Y. (1999) *Activity Theory and Individual and Social Transformation*, in Engeström, Y., Miettinen, R., and Punamaki, R. (eds.). *Perspectives on Activity Theory* (pp. 19 -38). Cambridge University Press, Cambridge, UK.

Engeström, Y., Brown, K., Engeström, R, and Koistinen, K. (1990) *Organisational Forgetting: An Activity Theoretical Perspective*, in Middleton, D., and Edwards, D, (eds.), *Collective Remembering* (pp 139 -168), Sage Publications, London.

Furnell, S. (2007) *E-commerce security*: Available online 08 August 2007.

Huff, D. (2003) *Core Audit program Information Technology Security*, Avail: www.ucop.edu, Accessed October 17, 2007.

Koller, D. and Leyov M. (2005) *Protecting 3d graphics content* <http://portal.acm.org/citation.cfm?id=1064861>. Accessed October 12, 2007.

Leont'ev A.N. (1978) *Activity, Consciousness and Personality*. Englewood Cliffs, NJ: Prentice Hall.

Merriam Webster's Collegiate Dictionary 10th ed.

Mlitwa, N. (2007) Lecture Notes, BTech Computer Security (CPZ440C) Class, 3 May 2007.

Mlitwa, N.B.W (2006) *A Network of Community and Community Informatics: An ANT Perspective*, 2006. Constructing and sharing memory: community informatics, identity and empowerment Conference, Prato 2006, available at www.ccnr.net/?q=node/151 (accessed on 04 May, 2007).

Oliver, M.S. (2002) Database privacy: balancing confidentiality, integrity and availability, <http://portal.acm.org/citation.cfm?id=772862.772866>, Accessed October 17, 2007.

Olsson, J. (2002) *Electronic Data Via a Network Infrastructure South African Journal of Information Management*.

Theilmann, W. Rothermel, K. (2000), INFOCOM 2000. Nineteenth Annual Joint conference of the IEEE Computer and Communications Societies. Proceedings. IEEE, http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=832197. Accessed October 12, 2007.

U.S. Census Bureau (2000) United Nations – Statistical Division, October 2000.

Wang, Y. (1998) A product perspective on total data quality management <http://portal.acm.org/citation.cfm?id=269022>. Accessed October 12, 2007.

Whitman M. (2003) *Enemy at the gate: threats to information security*, Avail: <http://portal.acm.org/citation.cfm?doid=859670.859675>. Accessed October 17, 2007.

Wu D., Hou T, and Zhang, Q. (2000) *Transports real-time video over the Internet: challenges and approaches*, http://ieeexplore.ieee.org/xpls/abs_all.jsp?arnumber=899055. Accessed October 12, 2007.

www.wipo.int/pctdb/en/wo.jsp?wo=2002067499.

www.sajim.co.za (accessed September 4, 2007).

8. ANNEXES

The annexure section is divided into Annexure 1 and 2. The first annexure outlines a glossary of the key terms used in this study. Annex 1 illustrates confidential information required in an online payment system for amazon.com. The second annexure presents interview data that is referenced in the body of the text.

ANNEXURE 1: ILLUSTRATIVE PICTURE OF THE AMAZON.COM PAYMENT SYSTEM

Payment System for Amazon.com

Pay with new card	Credit Card No.	Cardholder's Name	Expiration Date
<input checked="" type="radio"/> MasterCard	<input type="text"/>	<input type="text"/>	01 2007
<small>Note: Using an Amazon.com Visa Card? Select Amazon.com Visa. Using a Visa Check Card? Select Visa. Using a Eurocard or MasterMoney card? Select MasterCard.</small>			
Pay with new Bank Account (Learn more) (Need help entering your bank account details?)			
Bank Routing Number (9 digits)	Bank Account Number (up to 17 digits) (Do not enter a check number)	Account Holder's Full Name	Driver's License / State
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> / <input type="text"/>

Source: www.Amazon.com

ANNEXURE 2: INTERVIEW QUESTIONS AND ANSWERS

1. What types of information does globe have?

MB = the information in our databases ranges from our customer's (clients) details, financial details and status, clients databases, client user information, stock, internet use by clients.

FK = not forgetting document archiving database where all the documents like quotations and receipts are archived.

2. Which data is the most critical?

MB = I consider all the data we have to be critical. For instance, if you are talking from the security point of view that is, when customer details are exposed to third party and our clients know about it. Just imagine what that could do to business. I mean everyone knows that a lot of people don't give out their person details to other people. But they trust us because they want our services and they trust we are going to use their information as intended. This is supposed to be the least critical of them all which means that all the data we have is critical as we have it on purpose and we are not ready to expose any of it.

3. Does globe priorities their data?

FK = well, this is nothing of that sort now but I think since you have mentioned it, we will work towards that.

4. What are the potential threats of the company's information security?

FK = I think the main threat as hacking and many of the external forms of external attacks are not common in Malawi, are the stake holders. The people who have direct access to the data, though we have some kind of access control, you know a person will always try other ways until he gets what he wants either intentionally or by accident.

5. How does globe do to keep the stake holders from accessing some data?

As I said, by assigning access rights. Those in the account division/on will only access the accounting information.

6. Have you ever had any sort of security breach of any kind?

Well, yeah. All the time, though the intent is not always to damage or change. But we have had instances where employees accessing the payroll and monitor how their loan is being deducted, thus having access to other people's payments as well. The other thing I fear is, we use sage accounting system to manage out finances. And there are like seven people from different departments accessing the same database. I doubt the security features but am just saying that it might be a weakness.

8. Why having all those people just for the accounting system?

I don't know but it's the managing director's decision.

9. What is globe doing in terms of the change in technology? New Hacking tools are now available. Thought you have said that there are no external intrusions in Malawi, though we are not sure?

Well, I think the employed firewalls will do the trick. Apart from the firewalls, I don't know what other security measure that's there.

10. Does in their security implementation globe consider inside threats?

Yes, that's why we have access rights implemented and there is only one person who assigns the access rights, which means if we have any problem with access, he will be answerable.

11. What are the counter measures put in place in case of a break in or loss of information?

We take backups of our databases everyday just before we knock off. In case of data loss and these back ups are saved in two separate locations.

11. What can be the damage like if the data has been compromised?

Well, it depends on who has accessed the data. I mean, if it is an employee, then there won't be much damage I think. But once we had a problem when one of the employees accessed our payroll. It ended up in sit in as some employees were not happy with their pay compared to what their friends were receiving.

12. As a software developing and reseller, clients need to be assured that your systems are secured. What do you think would happen if your clients hear that you have a breach in security?

Well this can be disastrous as we most of our clients' databases. Thus when they have a problem, sometimes we just get their database and rectify the problem here at the office. so its like a great disappointment and I will mean losing almost more than 80 percent as some of our clients are banks and the government itself.

16. Apart from company's data and finances. What are other areas you can consider that they might need attention?

The physical infrastructure I think is well secured and there is nothing to worry about. But the only thing I worry about is the employees in the software department have access to most of the databases in the organization, either directly from DBMS or using the applications available. This is so because these people are the ones who test the databases and software and use common passwords to access the data.

18. You have said about your payroll system, you have said that it is in built and everyone in the software dep't knows how to go about the security and that they have direct access to the database. Though you have said that you have a log file for every change made in the system. What if the change was made from the database?

Well, am not sure if anybody has done that before (the changes) and I think it's high time we have something like a security measure on that. The problem is we are not in management, and we were never called to any meeting that ever happened in this company. What I mean is, the people in the software have never been called to most of the meetings conducted here at globe and what ever we might suggest, management might think that we are exposing to the other employees that there is a possibility that they can access the systems through the back door, if you know what I mean.

Mr. MB and Mr. FK (Company X computer systems LTD)

