European Journal of Computer Science and Information Technology
Vol.1, No. 2, pp.1- 9, September 2013
Published by European Centre for Research Training and Development UK (www.ea-journals.org)

ADDRESSING THE CHALLENGES OF DATA PROTECTION IN DEVELOPING COUNTRIES

Muli David Tovi, Mutua Nicholas Muthama
Taita Taveta University College

ABSTRACT: *Data protection is a vital tool to the development of any country. Certain challenges pose a threat to data protection in developing countries although the same challenges are evident in developed countries. For instance, technological advancement in information technology has challenged the existing mechanisms of data protection. Other threats to data protection as identified in this paper include inappropriate legislation, inadequate internet regulations, unethical computer users in the office, computer system mal-function, hardware failure, power blackouts and power failures. Certain remedies are necessary to counteract the challenges. Some of the remedies presented include internet regulation for users and internet service providers, computer ethics education and training among users, cross-border harmonization of laws on data protection and enforcement procedures, response to and preparing for power blackouts/power failures, response to system and hardware failures and introduction of national youth development forums and self employment initiatives. A conclusion is drawn from the challenges and the remedies discussed with great emphasis being laid upon curbing data crimes in the office work atmosphere, business atmosphere and stressing the need for strengthening the current legislation and enforcement procedures on data protection.*

KEYWORDS: Threats, Legislation, Computer Ethics, Remedies, Data Crimes

INTRODUCTION

The art of technological advancement is embraced by all nations including developing countries. Today, the world is like a village where people share information at the same time but in different parts of the world over the internet. Developing countries venture into new technologies without understanding the implications and the legal frame works under which the technologies operate. According to the 28th International Conference of Data protection and Privacy commissioners (2006), the technological pace keeps accelerating while the legal pace remains particularly slow. For this reason, developing countries may not effectively deal with crimes committed over the internet or in the office work environment. Spammers for instance, may send spam over the internet with little or no knowledge of users in developing countries. Although these countries may have laws on data protection, these laws are general in character and may not apply in crimes like spamming. Palfrey (2005) explains that, some countries use existing laws of general application to fight crimes like spam. Unfortunately these laws miss their target.

Bynum (2000) observes that, there must be involvement in the education of computing professionals and users. Hence training is imperative. This would ensure that data access and protection is ethical in all spheres of information and communication technologies. Data should also be protected against physical factors such as system failure, power blackouts and power

failure. Power blackouts can knock down computer systems which may lead to loss of revenue (Virginia Department of Emergency Management, 2006). When a system is knocked down, the data held in it is lost hence the need to protect computer systems and hardware against power failures. The various challenges to data protection and their possible remedies are discussed.

CHALLENGES

Technological Advancement In Information And Communication Technology

A lot of progress has been made in discovering new knowledge in the field of information and communication technology. Some of the new knowledge and advancements have been used destructively. For instance, hackers use their high-tech skills to change, intrude or interfere with computer networks with an intention of destroying information or making some money out of it e.g. a banking fraudulent deal. Bullesbach (2004) notes that, development and application of new information and communication technologies lead to challenges of data protection. Though new technologies in developing countries are a positive step of development, proper planning is necessary before applying new knowledge. Hackers use principles of new technologies. It should be noted that hackers may indeed be consultants in the particular firms they are working for. It means that such crimes may go undetected or can be detected after a long time. The reason is that the consultant (hacker) occupies a position of trust and nobody would suspect any ill motives in his operations. After all, he is a consultant. Capron (1996) explains that, most computer crimes are discovered by accident. He identifies a case in which employees of a certain city welfare department created a fictitious workforce and programmed the computer to issue pay cheques, which the employees would intercept and cash.

Spamming is a crime that is also linked to technological advancement in the field of information and communication technology. The current explosion of mobile phone communication and cheap email services has attracted a lot of spamming activities. Palfrey (2005) observes that, spam is the preferred delivery mechanism for internet security threats such as viruses which is harming the effects of those in developing countries to persuade users to begin to rely on digital communication. This is why a Kenyan lawyer, Mathew Ngugi observes that the massive gains brought by the information age are not perfect (Ngugi, 2005). This clearly illustrates how the economies of developing countries continue to suffer as they apply new technologies.

Developing countries lack specialized personnel who can effectively deal with advanced computer crime. Computer crimes have become more pronounced and more complicated to the police due to expansion of internet communications (Wikipedia, the free encyclopedia, 2006). This challenge is technological in character which can be associated with the curriculum offered to police officers during their training. They have no training based on information technology and that is why an investigation on computer crime is bound to yield no result as the investigator is not well equipped with current technology based investigative procedures. If law enforcement agents like the police detect a computer crime, Capron (1996), observes that they do not fully understand the complexities of computer related fraud.

Inappropriate Legislation And Inadequate Internet Regulations

Inappropriate mechanisms to data protection have hampered data protection in developing countries. They have laws on data protection and privacy though not specific to the target. They

use general laws such as consumer protection (Palfrey, 2005). Consumer protection is a general term that can imply personal security against physical injury. There are a lot of inadequacies in the Kenyan legislation on data protection which is also expected to be the case in other developing countries. A Kenyan lawyer, Mathew Ngugi observes that, there is lack of analogy between most cyber crimes and their conventional counterparts (Ngugi, 2005). He compares trespassing and hacking into a computer network. The penalty on trespass does not hold against hacking and accessing private data. This clearly illustrates a challenging situation whereby no relevant laws on hacking are available. A good example in the Kenyan law system is the evidence act that was amended in the year 2000 to comprehensively define a computer. The entire body of statute law remains oblivious of the changes and developments brought by the digital era (Ngugi, 2005).
Intellectual property rights are another issue that is not well catered for in the Kenyan legislation. Koigi (2006) narrates a case in which a man came up with a condom dispenser about a decade ago, but reaped very little from it.

People in developing countries are widely using the internet. Though cheap and convenient, these countries have not put sufficient regulatory mechanisms on data access. Froomkin (1996) cites Singapore government, as not being able to do much to censor the internet. Instead, the government limits access to internet and at the same time benefit from information age. This significantly illustrates how developing countries want to benefit from new technologies without laying a proper foundation of regulatory procedures on data protection. Froomkin (1996) further cites that information deemed obscene (pornography) in one jurisdiction may be legal elsewhere. This illustrates the conflicting legal provisions of internet regulation for different countries. Censorship is an important aspect of internet regulation. Governments' legal structures have been challenged in court. For instance, the Zimbabwe government was challenged by private mobile phone providers through a high court order restraining the government from controlling the information gateway system for the providers (Africa.aspx, 2006). This illustrates how data regulatory mechanisms in developing countries are still wanting.

Unethical Computer Use In The Office Or Business Atmosphere

Ethical practices in the work environment form the basis of success for any business venture. Boulton (ud) observes that, employees in small business firms are likely to pirate software, a practice that is seemingly endorsed by the management for purposes of business survival. The main challenge here is piracy within the office/business atmosphere where the superiors may not regulate their users. Otherwise, there may not be clear guidelines on ethical practice in the office. Piracy of data is practiced by experts with the necessary technical knowledge. For example, IT (Information Technology) consultants may use pirated software to complete certain projects. They accept projects that involve software they cannot afford to purchase (Boulton, ud). They seek illegal means of obtaining such software. Developing countries experience this problem because of the increasing unemployment trends, where people survive by using illegal business practices to make a living. The use of the internet in the office acts as an entry point to pirated software. Illegal transactions can be carried over a network without being noticed. For example, Froomkin (1996) observes that, trans-border gambling can go on over the internet, evading regulations imposed by jurisdictions in their countries.

Unethical computer use in the office can also be exemplified by a case in which Downey; a judge admitted viewing pornographic material in his office computer (North Country Gazette, 2006). Downey viewed his action as not being unlawful. From this case, it is clear that ethics at work place are not clearly defined and that there are no clear descriptors of what is unethical. This case illustrates the situation in developing countries.

Ethical use of computers in the office is challenged by lack of proper guidelines on privacy. Invading a computer to find out what an employee is doing is interfering with his privacy. On the other hand, restricting internet use in the office is different (Weckert, 2000). From a survey carried out in three different companies situated in Nairobi Kenya on employee monitoring, of the employees interviewed, 50% said that they were being monitored secretly when working with the computer, 30% felt that work ethics should guide a person and not monitoring from superiors and 20% felt that monitoring was okay only if it is objectively done. This illustrates the state of affairs in developing countries implying that there are no clear guidelines on privacy and information access at work place. This challenges the employee who should be an agent of privacy at work place. This is why; Bynum (2000) explains that, there are always problems in the application of computer ethics because there are no clear policies of how computer technologies should be used.

Computer System Mal-function And Hardware Failure

Data should not only be protected from people (users) but also from computer systems that either not functioning well or hard ware that fails to function appropriately. System operations are related to the software used. System failure, according to Meadowcroft (2005), may result from the complexity of the software used. Developing countries are using modern software which is more complex and efficient in operation. If there is improper coding of software, the system is likely to fail. Data held in such a system is also likely to vanish if the system malfunctions. System failure can result from the user e.g. when the user gives the computer inaccurate instructions. This may lead to loss of files and indeed data held in these files (Capron, 1996).

Certain types of hardware such as diskettes are vulnerable to conditions such as extreme temperatures, scratching, pressure and presence of magnetic fields (Capron, 1996). As such, data in them is likely to be lost because of such conditions. This is common in developing countries because the hardware being sold to consumers is of low quality and quite susceptible to the said conditions.

REMEDIES TO THE CHALLENGES

Internet Regulations For Both Users and Internet Service Providers

New technologies contribute to the national development of developing countries. However, challenges due to the technological advancement retard the growth of some sectors of the economy. Internet access is one of the main issues. Developing countries need to initiate self regulation mechanisms. Bullesbach (2004) observes that, adequate data protection is effective when countries initiate data protection by means of self regulation. This is an important aspect for developing countries because of the different cultural diversities of their people. Self regulation mechanisms would cater for all diverse cultures different from the western countries. Palfrey (2005) observes that, internet service providers must be encouraged to establish codes of

conduct that prohibit their users from using the internet to access illegal information or doing illegal business transactions. Developing countries should embrace a self regulatory approach by encouraging their internet service providers to regulate their customers by establishing regulatory mechanisms internal to their businesses. This would cultivate ethics among customers in using the internet. Spamming can also be controlled by using combined efforts between law enforcement agencies and internet service providers. Instead of chasing spammers, according to Palfrey (2005), regulators in less developed countries can only succeed by working in liaison with internet service providers who are closer to the source of the problem i.e. their customers and the technology in question. Because of the complexity of spamming, developing countries can avail resources and the necessary personnel to help combat spamming.

The primary role of data access and protection lies with the users. The users must be ethical in accessing data. Unethical users need to be legally regulated. This is why; Barroso (2001) cites that, internet use should be legally regulated besides having the users' role in its regulation.

Computer Ethics Education And Training Among Users

Ethical practices are an important component of any professional field. In this era of Information and communication technology, a lot of data relating to people, governments and business organizations is being handled by computing professionals. As a result a high level of ethical practice is essential. Ethical practices can be imparted to computing professionals during their course of study or being given in-service training. Weckert (2000) says that, there must be involvement in the education of computing professionals. The computing profession calls for excellence in its ethical perspective (ACM, 1992). Ethical practices in developing countries should serve a central role in alleviating data crimes. Computer users in these countries should be trained on ethical issues related to data protection. There is a need for refresher courses on emerging issues such as internet pornography, spamming, hacking and other forms of cyber crime. All these issues are as result of the advancement in information and communication technology. The main remedy is therefore a code of practice for all computing professionals and service providers in information and communication technology. Not all computer-related infringements are noticed. This is why all computing professionals should regulate their practices in an ethical point of view. As Barroso (2001) notes that, the cyber society in which we live needs an ethics of the internet and that internet ethics depend on the receiver or navigator. As a result, internet service regulatory bodies and internet service providers can educate their customers about certain dangers of internet communication (Palfrey, 2005).

Personal data should also be protected from unauthorized access. A culture of personal data protection should be cultivated among users. Lace (2005) proposes that, people should be made aware of how to protect their personal data and resist any mal-practices involving their data.

The integrity of data depends on the end user. For instance, if a user is well trained, the chances of the system failing are greatly reduced which improves the reliability and integrity of data (Meadowcroft, 2005).

Computer ethics education requires a global approach for harmonization. All stakeholders must be involved if meaningful solutions to computer ethics are to be provided. Weckert (2000) proposes that a number of disciplines must cooperate so that meaningful answers to computer ethics are to be provided. Employers must cooperate with their employees on matters of computer ethics. Cheung (2000) observes that, the induction of new employees to the

organizational culture is a central measure of data protection. Since different organizations may deal with data differently, new employees need to be introduced to all aspects of data protection.

Cross-border Harmonization Of Laws On Data Protection And Enforcement procedures

Data protection requires concerted efforts which must involve harmonization of new or existing legislation. These laws must have an international setting and applicable to all states regardless of whether a country is developed or not. Conflicting or no laws at all hampers the fight against illegal data access and cyber crimes. Developing countries need to establish common laws that can be uniformly applied in different countries for the same crime. Ngugi (2005) proposes that, there is a need to act in concert with the global community in combating cyber crime. He further observes that, legislations on data protection should provide for dual criminality incase a culprit crosses borders. Relevant stake holders in developing countries should therefore hold common forums within which certain laws can be harmonized. Harmonization implies cooperation between different countries. Bullesbach (2004) notes that, international harmonization of principles of data protection ensures international data transfers in global markets. This implies that illegal data access will be minimized by use of common principles.

Cooperation could be evident when different countries' law enforcement agents cooperate in fighting cyber crime .e.g. Interpol. As Brenner (2001) observes, Interpol pursues cyber crime through regional working parties. Palfrey (2005) proposes that, harmonization and collaboration are essential in fighting cyber crime. This could be an effective method of fighting cyber crime as it illustrates uniformity in law enforcement for different states. Conventions on internet crimes can also aid in fighting cyber crimes. For instance, the United States joined the Council of Europe Convention on Cyber crime on September 29th 2006 (McCormack, 2006). Developing countries should emulate the developed countries by joining such conventions. Froomkin (1996) observes that, without cooperation between the two governments involved, there may be very little the affected government can do fight the crime. The same idea is applauded by Franco (2006), when he explains that, task forces on minimizing piracy have helped stem out such crimes across the borders of Brazil, Paraguay and Uruguay.

Response To System Failure, Hardware Failure And Power Blackouts

Data needs to be protected against physical factors such as system failure, hardware failure and power blackouts. System failure may depend on the users and this is why users have a central role to play to avoid system failure. The best practices for avoiding system failure, according to Phillips (2004), include user manuals that provide system specifications and also testing the code earlier in advance. Testing of code is an ethical aspect of software development which affects the system functionality. Meadowcroft (2005) observes that system testing is important in being prepared for potential system failures. Developing countries should adopt an ethical culture of using sufficiently tested codes. This would improve data security. Users should also be trained on how to use particular computer system to avoid failure.

Faulty hardware can lead to data loss. To avoid hardware failure, essential functions could be transferred to backup components (Meadowcroft, 2005). Some types of software are also important in backup. Capron (1996) observes that, use of software that automatically backs up all files is essential for data protection. Power losses or power blackouts can lead to loss of data. Reliable power sources should be sought. Parliament of developing countries should enact laws

that allow the licensing private power suppliers to seal the gap for inadequate power supplies. For example, the Government of Kenya has enacted a law on energy, The Energy Act 2006, which allows private investors to generate electricity (Okuttah, 2006). This will save people the agony of loosing data due to power losses.

National Youth Development Forums And Self Employment Initiatives

Developing countries should view youth unemployment as the major source of the numerous economic crimes including data piracy. The youth should play an important role in data protection. Governments in developing countries should initiate forums that are aimed at educating the youth on self employment and also organizing workshops for educated but unemployed youth. They should establish youth groups whose main objective is to eradicate data crimes. An example of a youth organization is The Kenya National Youth Council, which according to Kamau (2004), creates an environment which enables young people to understand their roles and responsibilities. Such an organization can be used to disseminate ideas on cyber crimes and the role of the youth in alleviating such cyber crimes.

IMPLICATIONS TO RESEARCH AND PRACTICE

The research is a key pointer to developing countries on data protection methods. It will contribute immensely to institutions in developing countries on how to meet the challenges faced in protecting their data.

CONCLUSION

From the discussion, it is clear that the challenges of data protection continue to manifest themselves in developing countries despite the current mechanisms of alleviating them. Technology will continue advancing and this is why governments of developing countries need to review existing laws on data protection to suit new technologies. Similarly, enforcement procedures need to be reviewed. Law enforcement agents need to be trained on dealing with more sophisticated data crimes. Computer ethics education and training needs to be intensified by reviewing existing curricula and organizing refresher courses for practicing computing professionals. Service providers in computing businesses should be trained on how to deal with unethical customers. Regulatory bodies should be established to censor the service providers.

Our recommendation to developing countries is that, they should strengthen the current legislation and enforcement procedures on data protection. They should emphasize ethics education for all computing professionals and organize in-service courses for practicing computing professionals. All these will eliminate the challenges and make the culture of data access and data protection ethical in developing countries.

References

Africa.aspx (2006). Zimbabwe: *Econet and Telecell seek court order to block new regulation*, The Herald,

ACM (1992) "*ACM code of ethics and professional conduct''*
http://www.acm.org/constitution/code.html

Barroso, P. (2001) "Cyberspace: Ethical problems with new technology".Ethicomp, 2001.Gdansk, Poland.

Brenner, S. (2001) *International law enforcement*
http://www.cybercrimes.net/International/LawEnforcement.html

Bullesbach, A. (2004) ''Current challenges of data protection in the world economy''
http://www.26konferencja.giodo.gov.pl/data/resources/BullesbachA_pres_en.pdf

Bynum, T.W. (2000) *A very short history of Computer ethics*
http://www.southernct.edu.organizations/rccs/textonly/resources_t/research_t/introduction_t/bynum_shrt_hist_t.html

Capron, H.L.(ed.) (1996)''Computers: tools for an information age''. California: The Benjamin/Cummings Publishing Company, Inc.

Cheung, P. (2006) "Challenges and lessons of a national policy on data protection in the field of statistics", Statistics Singapore Newsletter, Singapore Department of statistics, October 2000.
http://www.singstat.gov.sg/ssn/feat/4Q2000/pg1-9.pdf

Franco, I.G. (2006) "Striving For Legality"
http://www.ipfront.com/depts/articles.asp?id=13202&deptid=6

Froomkin, A.M. (1996) ''The internet as a source of regulatory arbitrage'', Asian examples of practical limits to censorship.
http://www.osaka.law.miami.edu/~froomkin/articles/arbitr.htm#xtocid158348

International Conference of Data Protection and Privacy Commissioners (2006) "Communicating data protection and making it more effective"
http://ico.crl.uk.com/files/comE.PDF

Kamau, G. (2004) *Youth employment summit: National youth council draft concept*, March 13th 2004.http://projects.takingitglobal.org/YES-kenya/reports/?current=9

Koigi, J. (2006) "Make innovation work for you", Money, Your Personal Finance Magazine, December 21st 2006, The Daily Nation.

Lace, S. (2005) *Data protection challenges: responding to the risks*
http://www.ncc.org.uk/dataprotection/data_pro_dec05.pdf Accessed 24th November 2006.

Meadowcroft, B. (2005) "System failure: why systems fail"
http://www.benmeadowcroft.com/reports/systemfailure

McCormack, S. (2006) "United States joins Council of Europe Convention on Cybercrime''
http://www.state.gov/r/pa/prs/ps/2006/73353.htm

Ngugi, M. (2005) *Law on Cyber crime Overdue*: Legal Week, Computer Crime Research Centre http://www.crime-research.org/news/22.5.2005/982/

North County Gazette (2006) ''Judge: viewing pornsites on court computer not unethical''
http://www.northcountrygazette.org/articles/021106Ethicalporn.html

Okuttah, M. (2006) "Rural electrification to boost ICT penetration", Bizbytes, ICT news, December 17th 2006, The Sunday Standard

Palfrey, P. (2005) "Stemming the international tide of spam", A draft model law, Research Publication No. 2005-October 2005
http://cyber.law.harvard.edu/home/uploads/512/15/15-ModelSpam.pdf

Phillips, D. (2004) "Elements of effective software management", the project managers hand book. Wiley: IEEE Computer Society Press.
http://media.wiley.com/product_data/excerpt/06/04716742/0471674206.pdf

Virginia Department of emergency Management (2006) ‘‘Hazards and threats: manmade threats’’
http://www.vaemergency.com/business/hazthreats/manmade/unintent/blackouts/index.cfm
Weckert, J. (2000) "*Computer ethics: future directions"*
http://www.acs.org.au/act/events/2000acs4.html
Wiki/computer crime (2006). *Computer crime*
http://en.wikipedia.org/wiki/computer_crime
Corresponding email addresses: david.tovi@gmail.com, nicholasmuthama@ttuc.ac.ke