JEM

Journal of

EDUCATIONAL MANAGEMENT

A Bi-annual Publication of

THE INSTITUTE FOR EDUCATIONAL PLANNING AND ADMINISTRATION (IEPA)

University of Cape Coast, Ghana

ISSN 0855 - 3343 Vol. 6 Nov. 2012

Journal of Educational
Management Vol.6 (102-111)
November 2012

"Academic 419": Locating Computer Crimes in the use of ICT For The Management of Educational Systems in Ghana-The Case of University of Cape Coast

Aidoo, Dora Baaba
Akotoye, Francis Xavier Kofi
Ayebi-Arthur, Kofi

Abstract

The rapid evolution of information technology, the proliferation of computer and media devices and the rapid growth in the use ICT and the internet for organisational management have spawned new forms of crimes and made old crimes easier to commit. References to news in Ghanaian newspapers confirm the rising incidence of these crimes.A review of available literature, however, portrays a paucity of research that explores such crimes in African and for that matter, Ghanaian settings. In this position paper, we use "Academic 419" as a metaphor to describe computer crimes, highlighting some of such crimes from the international literature with a major focus on the types that can potentially occur in the University of Cape Coast.For us, it is imperative for leadership and management in their utilisation of ICT to be more vigilant in security issues and accept the need to safeguard their ICT systems to achieve maximal efficiency and effectiveness in their institutions. This objective can positively be attained when directed research,such as we advocate for are conducted to explore all related facilitating factors in order to align the design and change in direction for the secure and effective implementation of the University of Cape Coast ICT policy.

Background

Globally, cases of computer crimes date back to the early 1960s when the first case of computer crime was reported. Since then, there have been countless reports of computer crimes being made on a daily basis (Kabay, 2008). These early attacks often used unauthorised access to telecommunications systems to subvert long-distance phone systems which modified or destroyed data for financial gain, revenge, amusement and theft of services. Additionally, programmers in the 1980s began writing malicious software, including self-replicating programs, to interfere with personal computers.

With increased Internet access to increasing numbers of systems worldwide, criminals used unauthorized access to poorly protected systems for vandalism, political action and financial gain (Kabay, 2008). As the 1990s progressed, financial crime using penetration and subversion of computer systems increased (Rollins & Wyler, 2010). The types of malware shifted during the 1990s, taking advantage of new vulnerabilities. Illegitimate applications of e-mail grew rapidly from the mid-1990s onward, generating torrents of unsolicited commercial and fraudulent e-mail (Rollins & Wyler, 2010).

Locally, in Ghana, stories of computer crimes have become newspaper front page captions (Ghana Business News, 2009, Citifmonline, 2011). Prior to this time, computer crimes were not an issue that could be discussed because it seemed trivial and unimportant. For us in the second decade of the 2000s, however, computer crimes have become an issue of national concern because of their effects on the economy and their ability to sabotage the reputation of the country.

Combating computer crimes have earned global attention due to a number of reasons including that of relevant legislation. One of the major flaws of cyber laws is that there are no universal laws so it is very difficult to prosecute offenders across borders and in some cases, laws do not exist probably because the government and security agencies do not see the need for it. The President of the Accra Chapter of Information Systems Audit and Control Association (ISACA) commented at Information Systems Audit and Control Association (ISACA) IT Governance Summit 2011 in Accra that Ghana was failing woefully in its bid to also regulate its Information Technology environment. He stated that: "even though the Data Protection Bill was recently read in Parliament, it is just one aspect of the bigger picture, since there's no regulation or legislation that ensures the protection of government or listed company's data" (BiztechAfrica, 2011). For example, absence of a cyber-law in Ghana is frustrating the efforts of the Vetting Crime Intelligence Analysis (VCIA) unit of the Ghana Police Service in fighting computer fraud and also to prosecute perpetrators of Internet fraud (Telecoms, Internet and Broadcast in Africa, 2007).

A review of the literature portrays a paucity of research that explores such crimes in African and for that matter, Ghanaian settings. This position paper highlights some of such computer crimes from the international literature with a major focus on the types that can potentially occur in the University of Cape Coast. The awareness of such potential crimes and how they can be perpetrated can inform management decision making in strategies that can be adopted to mitigate the potential incidences of such computer crimes. This paper focuses on the importance of security and security controls as the tools to tackle this low awareness because in most cases, computer crimes are usually facilitated by insiders who divulge password or confidential information that aid criminals in carrying out their activities. It is our opinion that it is important for computer crimes to be properly investigated as history resonates with evidence that criminals will frequently abuse new technologies to benefit themselves or injure others (Charney, and Alexander, 2001).

We argue that as a university positioned as the "university of choice" within the West African sub-region, there is the need for the prompting of constituents to this upsurge in cyber crimes, as the very nature of academic activity promotes ICT utilisation and subsequently, opportunities for such crimes. We posit that "academic 419" has a high propensity to occur on the university campus, calling for heightened vigilance to avoid negative consequences. Why "Academic 419"? "419", as a term, is borrowed from Nigeria and refers to the number "419" of an article of the Nigerian Criminal Code 38 which states: "Obtaining Property by false pretenses; Cheating" dealing with fraud. This term as popularly used in Ghana refers to Nigerian Email Scam, a form of advance-fee fraud. An advance-fee fraud is a confidence trick in which the target is persuaded to advance sums of money in the hope of realizing a significantly larger gain. Overtime, "419" has come to be synonymous with fraud facilitated through computers. We use the term "Academic 419" as a heuristic to refer to fraudulent academic practices that can be committed with the use of ICT.

Defining computer crimes

What then are computer crimes? Computer crime denotes the use of computers by individuals in one of three ways. Firstly, a computer may be the target of the offence. In these cases, the criminal's goal is to steal information from, or cause damage to, a computer. Secondly, the computer may be a tool of the offence. This occurs when an individual uses a computer to facilitate some traditional offence such as fraud or theft (for example, a bank employee may use a computer program to skim small amounts of money from a large number of bank accounts, thus generating a significant sum for personal use). Thirdly, computers are sometimes incidental to the offence, but significant to law enforcement because they contain evidence of a crime. An example is students stealing/copying other students' assignments (a form of plagiarism). In a nutshell,we can say that computer crime is the use of a computer to extract or alter data, or to gain unlawful use of the computer for unlawful activities.

Management of most organisations do not realize the value of prevention in the area of computer security, but wait in ignorance until an incident occurs or is detected. An example of such crimes being people masquerading as celebrities in social networking sites e.g. Facebook to cause harm especially minors. In other instances, most computer crime perpetrators have been successful when the security infrastructure of the host organisation is not robust, hence can easily be compromised if persistent attacks are launched at it.

We propose that a thorough understanding of how these crimes can be perpetrated can enable informed management decisions. In future research, we hope to locate counter measures with which to manage the incidence of computer crimes in institutions of higher learning like the University of Cape Coast. Improved vigilance in the management in the use of ICT will improve on data protection and general university management. Anecdotal evidence gleaned from informal conversations with members of the university community suggests that the degree of awareness pertaining to aspects of computer security is very low. This paper argues the importance of creating awareness on security and security controls as well as tools to tackle computer crimes.

Typology of Computer Crimes

Computer crimes can be categorised into the following models:

Plagiarism: According to the Merriam-Webster Online Dictionary (2010), to "plagiarize" means to steal and pass off (the ideas or words of another) as one's own; to use (another's production) without crediting the source; to commit literary theft; to present as new and original an idea or product derived from an existing source. In other words, plagiarism is an act of fraud. It involves both stealing someone else's work and lying about it afterward. The expression of original ideas is considered intellectual property, and is protected by copyright laws, just like original inventions. Almost all forms of expression fall under copyright protection as long as they are recorded in some way (such as a book or a computer file).

All of the following are considered plagiarism: turning in someone else's work as your own; copying words or ideas from someone else without giving credit; failing to put a quotation in quotation marks; giving incorrect information about the source of a quotation; changing words but copying the sentence structure of a source without giving credit; copying so many words or ideas from a source that it makes up the majority of your work, whether you give credit or not (Plagiarism.org, 2009).

Hacking: The act of defeating the security capabilities of a computer system in order to obtain illegal access to the information stored on the computer system is called hacking (Oak, 2009). The act of defeating the security capabilities of a computer system in order to obtain illegal access to the information stored on the computer system is called hacking. To illustrate the hacking concept; Kernell, 22, was convicted in 2009 of a misdemeanor involving computer intrusion and a felony count of obstruction of justice (Zetter, 2010). The unauthorized revelation of passwords with intent to gain an unauthorized access to the private communication of an organization of a user is one of the widely known computer crimes. Another form of this crime is the hacking of Internet Protocol addresses in order to transact an activity with a false identity, thus remaining anonymous while carrying out the criminal activities.

Phishing: Phishing is the act of attempting to acquire sensitive information like usernames, passwords and credit card details by the perpetrator disguising as a trustworthy source (Oak, 2009). Phishing is carried out through emails or by luring the users to enter personal information through fake websites. Criminals often use websites that have a look and feel of some popular website, which makes the users feel safe to enter their details there.

Computer Viruses: Computer viruses are computer programs that can replicate themselves and harm the computer systems on a network without the knowledge of the system users (Oak, 2009). Viruses spread to other computers through network file system, through the network, Internet or by the means of removable devices

Typology of Computer Crimes

Computer crimes can be categorised into the following models:

Plagiarism: According to the Merriam-Webster Online Dictionary (2010), to "plagiarize" means to steal and pass off (the ideas or words of another) as one's own; to use (another's production) without crediting the source; to commit literary theft; to present as new and original an idea or product derived from an existing source. In other words, plagiarism is an act of fraud. It involves both stealing someone else's work and lying about it afterward. The expression of original ideas is considered intellectual property, and is protected by copyright laws, just like original inventions. Almost all forms of expression fall under copyright protection as long as they are recorded in some way (such as a book or a computer file).

All of the following are considered plagiarism: turning in someone else's work as your own; copying words or ideas from someone else without giving credit; failing to put a quotation in quotation marks; giving incorrect information about the source of a quotation; changing words but copying the sentence structure of a source without giving credit; copying so many words or ideas from a source that it makes up the majority of your work, whether you give credit or not (Plagiarism.org, 2009).

Hacking: The act of defeating the security capabilities of a computer system in order to obtain illegal access to the information stored on the computer system is called hacking (Oak, 2009). The act of defeating the security capabilities of a computer system in order to obtain illegal access to the information stored on the computer system is called hacking. To illustrate the hacking concept; Kernell, 22, was convicted in 2009 of a misdemeanor involving computer intrusion and a felony count of obstruction of justice (Zetter, 2010). The unauthorized revelation of passwords with intent to gain an unauthorized access to the private communication of an organization of a user is one of the widely known computer crimes. Another form of this crime is the hacking of Internet Protocol addresses in order to transact an activity with a false identity, thus remaining anonymous while carrying out the criminal activities.

Phishing: Phishing is the act of attempting to acquire sensitive information like usernames, passwords and credit card details by the perpetrator disguising as a trustworthy source (Oak, 2009). Phishing is carried out through emails or by luring the users to enter personal information through fake websites. Criminals often use websites that have a look and feel of some popular website, which makes the users feel safe to enter their details there.

Computer Viruses: Computer viruses are computer programs that can replicate themselves and harm the computer systems on a network without the knowledge of the system users (Oak, 2009). Viruses spread to other computers through network file system, through the network, Internet or by the means of removable devices like flash drives and compact disks (CDs). Computer viruses are after all, forms of malicious codes written with an aim to harm a computer system and destroy information. Writing computer viruses is a criminal activity as virus infections can crash computer systems, thereby destroying great amounts of critical data.

Cyber-stalking: The use of communication technology, mainly the Internet, to torture other individuals is known as cyber-stalking (Oak, 2009). False accusations, transmission of threats and damage to data and equipment fall under the class of cyber-stalking activities. Cyber-stalkers often target the users by means of chat rooms, online forums and social networking websites to gather user information and harass the users on the basis of the information gathered. Obscene emails, abusive phone calls and other such serious effects of cyber-stalking have made it a type of computer crime.

Identity Theft: This is one of the most serious frauds as it involves stealing money and obtaining other benefits through the use of a false identity. It is the act of pretending to be someone else by using someone else's identity as one's own (Oak, 2009). Financial identity theft involves the use of a false identity to obtain goods and services and a commercial identity theft is the using of someone else's business name or credit card details for commercial purposes. Identity cloning is the use of another user's information to pose as a false user. Illegal migration, terrorism and blackmail are often made possible by means of identity theft.

Datadiddling: This is the illegal or unauthorized data alteration (Oak, 2009). These changes can occur before and during data input or before output.

Doppelganger Domain Names: A doppelganger domain name is one that is spelled the same as the original, but missing the "." between the sub-domain name, the qualified domain and the extension (Gee and Kim, 2011). The strategy works on the premise that a small number of emails intended for a company will have a "to:" address incorrectly typed, or the doppelganger domain can be used in social engineering exploits to dupe workers at a company into thinking that an email requesting sensitive information comes from someone within the company, so is therefore safe to provide. A search for "University of Cape Coast" on the search engine *www.google.com* shows several links to the university such as "http://www.uccghanaportal.com", "http://www.ucclibrary.edu.gh/", "http://uccsrc.com/", "http://www.econsucc.edu.gh/index.html", "http://www.cds-ucc.edu.gh/" among others. One is left to wonder which of these URLs is the official webpage for the University of Cape Coast. It is very easy set up a doppelganger domain name of the University of Cape Coast and use it for malicious activities. In a quick search on the internet we noticed that the domain "universityof capecoast.com" was available for sale.

The different types of computer crimes involve an illegal exploitation of the computer and communication technology for criminal activities. While the advancing technology has served as a boon to modern day organisational management, the destructively directed human intellects are all set to turn technology into a curse.

The ICT for Management Profile of University of Cape Coast

The Computer Centre of University of Cape Coast provides network access for the University except for the School of Medical Sciences and the Centre for Continuing Education. Student Records and Management Information System (SRMIS) manage the information of senior and junior members; senior and junior staff including their bio-data and some other information concerning their activities on campus. The ICT Centre offers Internet facilities for members of the University community for teaching, learning and research. There could be a very high possibility of the incident of computer crime if there is a breach of confidentiality, loss of integrity and denial of service if data accessibility cannot be assured on the wide use of computers. With the ICT for management profile outlined, we move the discussion forward to the description of some of such computer crimes.

Computer Crimes in the use of ICT for Systems Management at University of Cape Coast: The Research Imperative

The University of Cape Coast is a tertiary institution and it consists of senior members; senior staff (research/administrative assistants), junior members (students) and junior staff. Databases are used to manage and monitor information concerning the academic and non-academic staff thus; a lot of computers will be involved in running these processes. This large numbers of computers ultimately mean that computer crimes can occur hence the need to investigate into the phenomenon of computer crimes. The rapid evolution of information technology, the proliferation of computer and media devices and the rapid growth in the use ICT and the internet for organisational management has spawned new forms of crimes and made old crimes easier to commit. Crimes like cyber-stalking; identity theft; pornography; fraud; scams; copyright violations, hacking and creating malicious code are some of the incidences that have been triggered by this rapid growth. It is important that computer crimes should be properly investigated because history teaches that criminals will frequently abuse new technologies to benefit themselves or injure others.

Additionally, new technologies are being released into the market to frustrate the perpetrators of computer crime and new policies are being implemented to mitigate the activities of computer criminals. However, with this entire infrastructure in place, it is evident that little progress is being made because there are always counter-measures to frustrate these criminal efforts (The United Kingdom Threat Assessment, 2010). Furthermore, because University of Cape Coast is located in a third world country, the emphasis on security is not as high as compared to those in developed economies. Also, the kind of security measures available to those in the western world may not be available in Ghana. For example, most of the antivirus software available in University of Cape Coast are either open source or trial versions probably because original software are too expensive. For two years now (2010-2011), the University has bought 1000 licenses for Kaspersky Antivirus (key informant). This purchase is however not enough for the number of computers being used by staff of the university. These are some of the security limitations that the university encounters.

Furthermore, incidences of computer hardware theft are either not reported to the authorities or are sometimes out-rightly ignored when they are reported (Standler, 2002). This is very discouraging hence most victims of computer theft do not see any reason to report to the authorities and this has encouraged the perpetrators of this crime to continue as they can always get away with it. In addition, victims of computer crimes are often not in a hurry to appeal to law enforcement bodies as it could result in bad publicity to the institution.

Many computer crimes can occur on our campuses on a daily basis because there have been reports of different kinds of computer crimes ranging from computer theft to violation of people's privacy by stealing personal information stored on their personal computers (Borhanuddin, 2010). An example of a possible computer crime that can occur in our tertiary institution may be hacking into a lecturer's email account in an attempt to steal quiz or examination questions. There have been reported incidences of intrusion into the computers of SRMIS in purported attempts to alter students' grades.

Some other kinds of computer crimes that can occur in the University of Cape Coast are identity theft, computer hardware theft, plagiarism, computer software theft, privacy violation, trafficking in password and transmission of a virus. This paper calls for the profiling of types of computer crimes which have either occurred or can possible occur in the University Cape Coast; how such crimes are perpetrated, enabling conditions for crime perpetration as well as strategies that can be adopted to mitigate them. Intended studies could explore security gaps that could be exploited for computer crime. Additionally, strategies that can be harnessed to manage the identified gaps through which computer crimes can be perpetuated will be especially useful to improve on security in the management of the system.

The findings from such studies will provide insights into security areas that need to be addressed through policy. Such policy changes can then moderate practices to mitigate the potential occurrence of computer crimes and help the university achieve its ICT policy aims of setting up 'university databases that are reliable, secure, up-to-date and easily accessible (The University of Cape Coast ICT Policy, 2003).

For practice, an exploration of computer crimes can help the university locate security gaps and adopt relevant strategies to address the problem. The realisation of the aims set out in the ICT Policy of the

University in terms of timelines attests to the fact that there exists a gap between policy intentions and policy outcomes. The location of security gaps in ICT utilization can help to bridge the policy intentions and policy outcomes gap.

Concerning appropriate methodological planning, we suggest that, considering the nature of computer crimes it will be useful for researchers to adopt a combination of designs that employ quantitative, qualitative or mixed methods. We recommend that the use of qualitative measures can unravel deeper insights into the problem of computer crimes as the sensitive nature of these crimes can be better probed with one-on-one interactions between the researcher and respondents.

With a thorough understanding of how these crimes can be perpetrated, we hope to locate counter measures with which to manage the incidence of computer crimes in the University of Cape Coast. Improved vigilance in the management in the use of ICT will improve on data protection and general university management. Anecdotal evidence gleaned from informal conversations with members of the university community suggests that generally speaking, the degree of awareness pertaining to aspects of computer security is very low.

Implications of computer crimes for organisational management

Management of most organizations often do not realize the value of prevention in the area of computer security, but wait in ignorance until an incident occurs or is detected (Prasad, Kathawala, Bocker & Sprague, 2003). Wang and Huang (2011), report that concern about computer crime is being fuelled by increased media reports (such as the WikkiLeaks) that reveal the sheer number of intrusions and the damage being caused. Furthermore, the advent of the personal computer has greatly affected the outlook toward computer crimes. Aaland (as cited by Prasad, Kathawala, Bocker and Sprague, 2003) observed that Now with 35 to 40 million PCs in the work place, organisations large and small alike are vulnerable to computer crimes.

The rapid evolution of information technology, the proliferation of computer and media devices and the rapid growth in the use ICT and the internet for organisational management have spawned new forms of crimes and made old crimes easier to commit. Computer crimes like cyber-stalking; identity theft; pornography; fraud; scams; copyright violations, hacking and creating malicious code are some of the incidences that have been triggered by this rapid growth (Chawki, 2009). Other examples of computer crimes include people masquerading as celebrities in social networking sites, for example, Facebook to cause harm especially minors. In other instances, most computer crime perpetrators have been successful when the security infrastructure of the host organisation is not robust, hence can easily be compromised if persistent attacks are launched at it (Chawki, 2009). In view of the complexities in computer crimes that can occur, there is the need for awareness to be created about some of the potential crimes that can be perpetrated in organisations such as the university.

Conclusion

The incidence of "Academic 419" describes computer crimes that can occur in educational systems such as the University of Cape Coast. References to news in Ghanaian newspapers confirm the rising incidence of these crimes. As such the import of the rising incidences in computer crimes cannot be disputed. It is therefore imperative for leadership and management in their utilisation of ICT to be more vigilant in security issues and accept the need to safeguard their ICT systems to achieve maximal efficiency and effectiveness in their institutions. This objective can positively be attained when directed research is conducted to explore all related factors, the design and change in direction for the implementation of the ICT policy.

References

Borhanuddin, M. (2010) Cyber Crime and the Bangladesh Perspective Retrieved November 15, 2011, from http://www.scribd.com/raihanborhan/d/ 3399476-Cyber-Crime

BiztechAfrica, (2011) Ghana to curb cyber crime Retrieved December30, 2011, from http://www.biztechafrica.com/article/ghana-moves-curb-cyber-crime/1533/

Charney, S. and Alexander, K. (2001) COMPUTER CRIME Computer Crime Research Center Retrieved 15, November, 2011 from http://www.crime-research.org/library/Alex.htm

Chawki, M. (2009) A Critical Look at the Regulation of Cybercrime Retrieved on November 30, 2011 from http://www2.warwick.ac.uk/fac/soc/law/elj / jilt/2009_1 /chawki/chawki.pdf

Citifmonline Ghana among top 10 on global internet fraud table Availabe at http://www.citifmonline.com/index.php?id=1.287156.1.420460 Jun 10, 2011

Gee, G and Kim P. (2011) Doppelganger Domains Retrieved 15 September from *files.godaigroup.net/doppelganger/Doppelganger.Domains.pdf*

Ghana Business News Cyber crime: Giving a bad name to Ghana February 17, 2009 Available at http://www.ghanabusinessnews.com/2009/02/17/ cyber-crime-giving-a-bad-name-to-ghana/

Kabay, M.E. (2008). Computer Security Handbook, 5th Edition, Volume I. New York: Wiley.

Merriam-Webster Online Dictionary (2010) Plagiarize Retrieved 05 October, 2011 from http://www.merriam-webster.com/dictionary/plagiarize

Oak, M. (2009). Intelligent Life on the Web Retrieved 09 September from http://www.buzzle.com/articles/types-of-computer-crimes.html

Plagiarism.org. (2009). "What is Plagiarism?" Retrieved 15 October 2011 from http: //www.plagiarism.org/learning_center/what_is_plagiarism.html>

Rollins, J., Wyler, S. L. (2010) International Terrorism and Transnational Crime: Security Threats, U.S. Policy, and Considerations for Congress Retrieved December 15, 2011 from http://www.fas.org/sgp/crs/terror/R41004.pdf

Prasad, J.N., Kathawala, Y., Bocker, H.J. & Sprague, D. (2003).The Global Problem of Computer Crimes and the Need for Security.*Industrial Management*, 24-28

Standler, R.B. (2002) Computer Crime Retrieved November 22, 2011 from http://www.rbs2.com/ccrime.htm

Telecoms, Internet and Broadcast in Africa Issue no 349 8th April 2007 POLICE ADVOCATE FOR LAWS TO COMBAT CYBER FRAUD IN GHANA Retrieved 10 October from http://www.balancingact-africa.com/news/en/issue-no-349/computing/police-advocate-for/en

The United Kingdom Threat Assessment (UKTA) 2010 THE UNITED KINGDOM THREAT ASSESSMENT OF ORGANISED CRIME Retrieved December 2, 2011 from

The University of Cape Coast ICT Policy (2003) Retrieved 18 October, 2010 from http://www.ict.gov.gh/pdf/ICT%20Policy%20-%20U.C.C.pdf

Wang, S.Y.K. and Huang, W. (2011). THE EVOLUTIONAL VIEW OF THE TYPES OF IDENTITY THEFTS AND ONLINE FRAUDS IN THE ERA OF THE INTERNET Internet Journal of Criminology Retrieved on November 12, 2011 from http://www.internetjournalofcriminology.com/ Wang_Huang_The_Evolutional_View_of_the_Types_of_Identity_Thefts_and_Online_Frauds_in_the_Era_of_Internet_IJC_Oct_2011.pdf

Zetter, K. (2010) Sarah Palin E-mail Hacker Sentenced to 1 Year in Custody Retrieved 02, November 2011 from http://www.wired.com/threatlevel/2010/11/palin-hacker-sentenced/?utm_source=feedburner&utm_ medium=feed&utm_campaign=Feed%3A+wired27b+%28Blog+-+27B+Stroke+6+%28Threat+Level%29%29