Information Security Education in Ghana: A Pragmatic Analysis of the Gap between Academia and Industry

Amankwa Eric, Devine Nii Odoi Samuel
Department of ICT, Faculty of Science and Technology, Presbyterian University College, Abetifi Ghana
amankwa@presbyuniversity.edu.gh
Samuel.nodevine@presbyuniversity.edu.gh

ABSTRACT

Majority of existing public and private tertiary institutions in Ghana seem to have integrated topics in information security (INFOSEC) into their academic curricula, yet INFOSEC related incidents appear to be on the increase in Ghanaian organisations. This paper therefore investigates aspects of INFOSEC integrated into the academic curricula of these tertiary institutions and juxtaposes with INFOSEC needs of Ghanaian organisations, to ascertain if any knowledge gap exists.

The study found most Ghanaian tertiary institutions have courses in INFOSEC mounted at the undergraduate levels with greater emphasis on technical security, focusing less on non-technical security. In addition, Ghanaian industries expect employees to be knowledgeable in both technical security and non-technical security. A knowledge gap was therefore found to exist between the INFOSEC course coverage in tertiary institutions (producers) and the needs of organisations (employers). Hence, effective communication and collaboration between academia and industry is recommended.

Keywords: information security, education, academic curricula, Ghana organisations, gap analysis

1. Introduction

The upsurge of computer related crimes and threats to Information Security (hereafter called INFOSEC) such as internet fraud, pharming and phishing, social engineering etc, has forced organizations worldwide to pay close attention to INFOSEC which was neglected hitherto. This increased interest in INFOSEC has further created an increase in the demand for security professionals; thereby resulting in the need for such professionals in organizations (Caelli, 2002; Smith et. al, 2005). In other words, there is a global need for INFOSEC professionals in almost all sectors of the economy. This has been influenced by the numerous security threats and breaches in organizations. The onus is therefore on the various educational institutions to train more of such graduate to meet the high demands from organisations.

Educational institutions, specifically universities, who are the main producers of graduates for the different industries globally, have, to some extent, responded to this call from organisations by mounting various programs in Information Security at the non-degree and degree levels (Sharma & Sefchek, 2007; Cooper et. al., 2009). In Ghana for example, Universities have aspects of INFOSEC embedded mainly in courses at the undergraduate levels, focusing on providing basic security knowledge to students in Information Technology (IT) and related departments. However, the number produced is either inadequate to meet the requests or the coverage of courses in security may be insufficient to curb security breaches in organisations (PwC, 2014; Verizone, 2014; Symantec 2014; Cisco, 2014). The content of the courses in INFOSEC mounted in various universities may be either missing the relevant aspects which address security breaches or may be inadequately covered in academic institutions.

This paper therefore investigates aspects of information security covered in the curricula of Ghanaian Universities, the INFOSEC needs of Ghanaian organisations and the knowledge gap between Ghanaian Universities and Industries. This study culminates with recommendations for bridging the INFOSEC gap between Ghanaian Universities and Industries. The relevance of this study is in two folds. First, it has the relevance of assisting academic institutions in knowing what INFOSEC knowledge industry expects of the new graduate, in order to tailor academic curricula to meet these needs. Secondly, with increasing demand for professionals to manage the IT infrastructure and information assets of many a business, it has become imperative for universities to be up to the task of producing IT experts who are well informed on INFOSEC issues. In view of this, universities positioned in the training of INFOSEC professionals would have a head start in carving a niche for themselves in the area which has received sparse attention. The findings from this study may therefore assist institutions in the design of their academic curricula.

2. Materials and Methods

The research method adopted in this study is a qualitative approach. This is because the research question requires an in-depth study into security education in industry and the academic environment. In addition, qualitative research is applicable to this exploratory study with a paucity of published research in the area. It also allowed the researchers to observe and understand the context within which decisions and actions regarding security education take place.

The primary data collection methods used in this research is interview and document analysis, which allowed the researchers to gather rich data from relevant actors involved in various roles of security education in academia and industry.

INFOSEC education has mainly been addressed by three sectors within the security community and these are government, industry and academia (Crowley, 2003; The White House, 2000; Kritzinger, 2006). Data for this study were therefore collected from two of the three sectors; industry and academia. The academic institutions include public and private universities that run several programmes and courses, and also have large enrolment numbers. The public universities are Kwame Nkrumah University of Science and Technology (KNUST), University of Cape Coast (UCC), University of Ghana (UG), University of Mines & Technology (UMT), Ghana Institute of Management and Public Administration (GIMPA) and University of Professional Studies, Accra (UPSA). The private tertiary institutions also included the Presbyterian University College Ghana (PUCG), Accra Institute of Technology (AIT), Ashesi University College (AUC), Pentecost University College (PUC), Valley View University (VVU), Garden City University College (GCUC), Methodist University College, Ghana (MUCG), Bluecrest College (Formerly NIIT Ghana College), Catholic University College, Ghana (CUCG), Regent University College of Science and Technology and Ghana Technology University College (GTUC). Data were taken from the different universities websites, handbooks, and course outlines, in addition to interviews with deans/HODs and a few faculty members of the respective universities.

Industries on the other hand included public and private organisations, in Accra, Kumasi, Tema and Tarkorade, who employ Information Technology (IT) to store, process or transmit customers' personal identifiable data. Organisations used were mainly from the service industry including banking, health care institutions, public utility companies (water and electricity), telecommunication companies, IT and oil and gas. Data were taken from the different company websites, company handbooks on acceptable use policy, as well as interviews with some IT managers, HR and some employees of the respective organisations.

3. Current State of Security Education in Ghana

The academic sector is largely dominated by tertiary institutions which are comprised of Universities, University Colleges, Polytechnics, Colleges, Schools, Institutes, Academy and Tutorial Colleges (NAB, 2012). The aim of security education in tertiary institutions, is to ensure that students and employees are equipped with the requisite knowledge relevant to their present and future endeavours. The responsibility therefore rest on academic institutions to produce adequate information warriors who will defend the present and future information resources of the other two sectors. In view of this, academic institutions worldwide have responded to the call with extensive research and have expanded their curricula to include topics in INFOSEC education both at the undergraduate and graduate degree levels. Previous security education researchers including Smith et. al. (2005), Sharma and Sefchek (2007), Cooper et. (2009), Futcher et. al. (2010), and Papanikolaou et. al. (2013), have all pointed out this fact.

To this effect, evidence gathered from academic institutions revealed that, Ghanaian universities have risen to the call by tackling the issues in various forms. In some institutions, components of information security related topics have been embedded in their courses. Others have whole courses focused on INFOSEC education, whilst some have mounted full security related programmes in their curriculum. Upon analysis of the various course contents, it was also realised that among those who run full programmes or course in INFOSEC education, much focus has rather been given to the education of students on the Technical aspects of INFOSEC, paying less attention to the Non-technical issues. This neglect often leads to the human factor, a key component in the INFOSEC arena (Deloitte, 2013), being given less attention though constitutes the weakest link (Monk, van Niekerk & von Solms, 2010).

Despite these efforts by academic institutions there are still serious security violations by employees in Ghanaian organisations. This is because, employees are arguably not only the weakest link in the security network (Monk et. al., 2010), but also a key part that is mostly overlooked in attempts to secure information and computing resources. Deloitte (2013) intimated that employees are part of the INFOSEC problems and must therefore be part of the solution by way of awareness and education (NIST, 2007). From the present study, some of the prevalent security concerns mentioned by IT/security managers, human resource managers, and network administrators, as arising out of employees' actions and inactions include the following:

- Music/video download on corporate network**:** this involves using corporate internet to search and download music and video from unsecured websites. This act has been facilitated by the proliferation of Ghanaian music and videos on the internet, and the unlimited internet access provided to employees at the work place. Almost every organisation provides at least eight (8) hours of continuous internet access to their employees. On the contrary, websites such as mp3skull, mp3ghana, and Ghana motion, just to mention a few, provide unlimited access to Ghanaian music for free downloads. Interviews with some security managers and network administrators indicated that, one of the biggest security problems they have had to deal with came from computer malware which possibly resulted from unauthorised downloads by employees.
- Social media**:** this involves the use of corporate network to access social media platforms such as Facebook, LinkedIn, Twitter and others. Employees post photos of themselves and sometimes confidential corporate information, for discussion, on social media platforms thereby exposing the organisation to various attacks by persons with criminal intent. Social media usage at the work place affects productivity and subsequently reduces profits margins. According to Ponemon (2012), 54% of employees use social media for personal reasons at work whiles 51% discuss corporate issues on social media platforms.
- Password sharing**:** despite security policies, procedures and tools, currently in place in most organisations, employees around the world engage in risky behaviours that put corporate and personal data at risk; and prevalent among these behaviours is password sharing. Password sharing is the practice of exchanging passwords among workers. Interviews conducted with

network and security managers/administrators indicate that, majority of Ghanaian workers share their passwords and other secret credentials with co-workers. This finding corroborates that by Cisco (2008) which indicated that 18% of employees worldwide share passwords with co-workers, with the number rising to 25% in China, India and Italy. This finding was also identified in a study by Ponemon (2012) to investigate how employees expose sensitive organisational information. They found that 63% of employees share their passwords with other employees. The common practice in most Ghanaian organisations with regards to passwords is that, one out of every three employees has a password written on stickers and kept on bulletin board for fear of forgetting; network administrators and security managers lamented. With this practice, any employee who enters the office can access the password and use it to perpetrate various crimes on the accounts of these unsuspecting employees.

- Unauthorised Access of Corporate Networks: Using personal laptops/tablets/smart phones on corporate networks is often not allowed in most organisations. However, most employees for one reason or the other still use their personal devices which may be unsecured to access corporate data on a corporate network. In this study, most network administrators lamented how common this practice is in Ghanaian organisations. Some network administrators added that some unsuspecting employees even allow non-employees access to corporate networks when they think no one is watching and such individual who may have malicious intent end up stealing vital corporate data. Ponemon (2012) agrees with this finding through a report which found that 59% of employees connect computers through insecure wireless networks in organisations, whiles 66% of employees access corporate networks using personal devices such as laptops, tablets and smart phones.
- Employees' persistent use of removable storage media on corporate network: With the tremendous advancement in the storage capacities of removable storage media such as flash disk, external hard drive, SD cards, and mobile devices, it is now the preferred storage media for most organisations despite the dangers associated with its use. Removable storage media are wildly popular because they are durable, reusable, easy to use, convenient and inexpensive. However, they can pose serious security threats in organisations if their usage is not properly managed. According to Ponemon (2012), 87% of employees' do not report missing or stolen corporate flash disks. Dangers associated with their usage include the introduction of malware into the organisation's networks and systems (Miller, 2009). Most network administrators lamented how they have to scan the entire network systems at least three times a week to ensure that, any malware introduced from the rampant use of removable storage media is detected and dealt with scrupulously.

From the security concerns raised above, it was realised that much of the problems are as a result of knowledge lacking in the non-technical issues of INFOSEC. This suggests that, employees have received insufficient knowledge in the non technical components of INFOSEC which are equally as important as the technical aspects.

In our analysis of the curricula of Ghanaian tertiary institutions, it was revealed that there exist a limited number of academic programmes in INFOSEC (for example B.Sc. Computer Security). Some tertiary institutions also offer specific courses in the area, whilst others have aspects of INFOSEC embedded in varying courses. It is notable that all the courses that had INFOSEC concepts covered were mainly in the Computer Science, Computer Engineering and Information Technology Departments.

Secondly, it was also revealed that the existing academic programmed in INFOSEC are mainly focused on providing technical security knowledge to students in the Ghanaian tertiary education environment. Recurring topics of INFOSEC reported in the curricula included: Virus threats and defences, hackers, Access control, Authentication methods (biometrics and passwords) and cryptography. These topics focused comprehensively on the technical issues of INFOSEC which correlate with requirements expected of IT professionals by industry, notable in table 1 below. Contrariwise, non-IT professionals, who form the majority in the use and creation of information products, are hardly attended to and obviously lack the basic security concepts which the Non-Technical aspects of INFOSEC deal with.

Finally our study found that, there were virtually no courses or topics in INFOSEC in the existing curricula of non-IT programmes like B.Sc Business Administration, Economics, Nursing, Medicine, Sociology and other related programmes.

4. Information Security Needs of Ghanaian Industries

The industry is another important sector known to address INFOSEC within the security community worldwide. This sector is largely dominated by goods and service provision companies in Ghana. Ghanaian industries are categorized by the Ghana Stock Exchange using their industry classification benchmark into basic material, consumer goods, financials, industrials, health care, media, oil & gas, technology, telecommunications and utilities.

The aim of INFOSEC in organisations is to ensure that employees who are involved in the collection, processing, storage and dissemination of electronic information are equipped with requisite knowledge to ensure that the confidentiality, integrity and availability of corporate information assets are maintained at all times. In view of this objective, the responsibility therefore lies on each organisation to ensure that current and prospective employees possess such requisite knowledge. However, organisations are dependent on tertiary institutions who are the main trainers and producers of graduates for subsequent employment into various organisations. To this end, partnership between academia and the industry would be one of the best means of achieving this goal.

This is however not the case in Ghana as tertiary institutions design their academic curricula with virtually no input from the organisations who are the supposed beneficiaries. The current situation is such that, every organisation must critically test all job applicants in both written and verbal forms, to ensure all selected applicants have the required knowledge in INFOSEC expected of them. Aspects of the expected knowledge are often stated in the responsibilities and duties attached to a position which an applicant applies for.

A critical look at some 113 Ghanaian organisations from different industry sectors indicated a need for technical and non-technical knowledge of information security by Ghanaian organisations. This is presented in Table 2 below, as a shortlisted and summarised form of the analysis for the purpose of discussion in this paper. Table 1 therefore presents Ghanaian companies, their industry sectors, job titles, responsibilities, and the expected INFOSEC knowledge.

It is clear from table 1 below that, Ghanaian organisations require all prospective employees to be knowledgeable in INFOSEC to ensure the confidentiality, integrity and availability of their information assets at all times. Organisations in the telecommunication industry largely require prospective employees to be knowledgeable in both technical and non-technical aspects. This is largely due to the fact that, work in this industry is highly sensitive and critical information is mostly handled in these organisations. Positions for prospective employees in these organisations include Network Administrator, Customer Service Engineer, Marketing Project Manager, and Optimisation Supervisor, which may require technical and non-technical knowledge for managing their information assets in the area of security.

Financial institutions also expect their prospective employees to be educated in all aspects of INFOSEC, be it technical or non-technical. For instance network administrators are expected to possess working knowledge of technical aspects, whereas other employees are to be well informed on the non-technical issues, to ensure customers' personal identifiable information and transactions are kept secured at all times.

Table 1: Aspects of INFOSEC required of employees by Ghanaian Organisations

Company Name	**Department/ Unit**	**Industry/ Sector**	**Job Title/Position**	**Responsibilities**	**Expected INFOSEC knowledge**
DATABANK	Information Technology	Banking	Systems Engineer	• Network configuration and monitoring • Configuration of servers, routers and security devices • System and email administration • Data backups • Anti-virus software installation, configuration and support	Technical and Non-Technical
VODAFONE Ghana	Information Technology	Telecommunication	Customer Service Engineer	• Doing installations at the Exchange and Customer ends. • Ensure all work is carried out in compliance with Vodafone safety requirements • Maintain high quality of workmanship standards whilst being as efficient and cost effective as possible	Non-Technical
A Reputable Company (Name Withheld)	Information Technology	Educational	Network Administrator	• Establishes networking environment by designing, directing, defining, documenting, and enforcing system standards, configuration and installation; • Maximizes network performance and optimization; troubleshooting network problems and outages; scheduling upgrades; • Secures network system by establishing and enforcing policies; defining and monitoring access	Technical and Non-Technical
KPMG GHANA	Information Technology	Financial (Banking)	Head of Information Technology	• Plan and implement/update all technology projects/strategies and ensure project documentation is maintained in line with institutional standards • Coordinate development of PC-based applications to support business products consistent with institutional procedures and best practices • Provide systems, applications and network security	Technical and Non-Technical
A Reputable Company (Name Withheld)	Information Technology	Information Technology	Software and Systems Assurance Auditor	• Develop and maintain customer after sales service support mechanism to ensure total customer satisfaction • Ensure regular availability, continuity and security of hosted data and hosted software • Supervise the performance of regular virus scans and maintain and update the Virus Log Book	Technical and Non-Technical
A Reputable Company (Name Withheld)	Management Information System	Educational	Information Security Analyst	• Implementation of security policies and procedures • Design and implement company-wide security solutions for diverse platforms	Technical

Pro credit Ghana	Information Technology	Financial (Banking)	Network Administrator	• Assure the functioning of the network and the servers • Administration and maintenance of the network and servers • Ensure security in the network • Documentation of the network systems • Putting in place disaster recovery procedures	Technical and Non-Technical
Tigo Ghana	Sales and Marketing	Telecommunication	Marketing Project Manager	• Work closely with functional managers in marketing and act as project manager for various activities in the department • Maintains and is responsible for developing detailed timelines, project plans and project deliverables and key milestones • Manage day-to-day operational aspect of projects including communication of project status to all key team members • Work closely with marketing teams to ensure smooth execution of marketing campaigns	Non-Technical
AESA Consortium	Information Services	Consumer Goods (Agriculture)	IT Administrative Support Officer	• Administrative support and follow-up with regards to the progress of data capturing and verifying authenticity. • Monitoring progress of data updates on a daily basis. • Assisting with IT related enquiries on the database system	Non-Technical
ACDI/VOCA	Information Technology	Consumer Goods (Agriculture)	IT Officer	• Provide firsthand troubleshooting for IT systems • Complete basic and system reviews for servers, e-mail & Internet service • Assist with software problems or failure on individual computers • Complete routine maintenance or ICT equipment's/systems • Update Antivirus and MS operating systems at recommended schedule	Technical and Non-technical
Securities and Exchange Commission	Policy Research and Information Technology	Financial	Assistant Manager, Information Technology	• IT programme management • Maintaining the Commission's website • Implementation of the Commission's automated information and filing system	Non-Technical
Origo Software	Information Technology	Information Technology	Data Research Analyst	• The candidate will be responsible for performing discovery across the web to find valuable sites, resources and platforms that expose big data sets and API's, which can be integrated into our cloud platforms and services. A strong knowledge of web search technologies, application trends, etc • The candidate will recommend and a weekly basis, new platforms and APIs discovered online, to be integrated into our cloud services. • The candidate must have the ability to configure and test APIs using various data sets and criteria to ensure quality and performance requirements are met.	Non-Technical

The story in the technology industry is no different from the above. IT organisations in this industry expect all prospective employees to be knowledge not only in technical security but more importantly the non-technical aspects. Organisations in this industry provide various tools and facilities for their employees to perform their day-to-day activities. However, if these tools which can be used to perpetrate various cybercrimes are not properly managed, and left in the hands of inexperienced employees, the organisation may be liable and held accountable for aiding in cybercrimes. This situation can only be mitigated through employees' awareness and education in non-technical aspects of security. This is because non-technical aspect of INFOSEC such as ethics and legal aspects can expose an organisation to various legal suits, fines and misdemeanour charges which can strip an organisation of its hard earned reputation.

The discussions above all point to the fact that Ghanaian organisations expect their prospective employees to be knowledgeable in both Technical and Non-Technical aspects of INFOSEC to ensure confidentiality, integrity and availability of information and information resources at all times.

5. The Knowledge Gap in Ghana: Academia versus Industry

INFOSEC is decomposed into technical and non-technical aspects. The former include technologies such as firewalls, intrusion detection, encryption, authentication (password and biometrics) and access control, whereas the latter, encompasses leadership, procedures, organisational structures, ethics, legal issues, security policies and compliance issues, security culture and social engineering scams (Kritzinger and von Solms, 2004; Kritzinger and Smith, 2008). However, analysis of the current state of INFOSEC education in Ghana indicates that Ghanaian tertiary institutions have concentrated heavily on technological (technical) aspect to the neglect of the non-technological (human/non-technical) aspects. This finding is also indicated in existing previous studies including Kritzinger & Smith, 2008, Stewart & Lacey, (2012), and Crossler et al., (2013). Ghanaian organisations on the contrary, require and continue to seek graduates who are knowledgeable not only in technical aspects of INFOSEC but also and more importantly the non-technical aspects, to ensure that the confidentiality, integrity and availability of the organization's electronic information assets are maintained at all times. This is because, the human side of security (non-technical aspect) is as equally important as the technical aspects. Deloitte (2013) intimated that employees are part of the problems and must therefore be part of the solution by way of awareness and education. Despite calls by previous researchers, Ghanaian academic institutions in their quest to make the teaching and learning of security more practical, have ended up investing all teaching and training efforts mostly on the technical aspects of security whilst the human and non-technical aspects have received little attention. This situation, therefore, has created a lack of knowledge in the non-technical aspects of INFOSEC, an essential requirement that industry expects all prospective employees to possess to ensure a security conscious workforce. With table 2 as evidence, Ghanaian organisations expect current and prospective employees to be knowledgeable in all aspects of non-technical security irrespective of their departments, to successfully achieve the information security goals set by the organisation.

Most often than not, when IT graduates are employed to work in non IT departments, just a fraction of the knowledge acquired in technical aspects of security will be needed, but the non-technical aspects of security such as ethics, procedures, security policies, legal issues and compliance, will always be needed irrespective of the organisation or department they are employed into. The importance of non-technical INFOSEC knowledge in organisations cannot be over emphasized. This involves non-technical oriented knowledge that is required to secure and protect information and information resources. Non-technical security focuses on the effect of human actions and inactions in attempts to secure and protect information and information systems. Such human actions can also be intentional or accidental and may come from within or outside the organisation. Unfortunately, this knowledge is lacking thereby creating a gap between academia and industries in Ghana.

6. Conclusion and Recommendation

Given the influx of private and public tertiary institutions with quite a percentage mounting full courses or embedding topics in INFOSEC into existing course, and the current security breaches in Ghanaian Organisations, this study was set out to investigate aspects of INFOSEC topics in Ghanaian tertiary institutions, the INFOSEC needs of Ghanaian industries and the existing INFOSEC knowledge gap.

The study found that Ghanaian tertiary institutions have programmes and courses in INFOSEC mounted at the undergraduate levels with greater emphasis on technical security to the neglect of non-technical security. Furthermore, the study found virtually no courses or topics in INFOSEC in the existing curricula of non-IT programmes. Ghanaian industries on the other hand expect all prospective employees to be knowledgeable in both technical security (i.e. firewalls, access control, and cryptography) and non-technical security (i.e. ethics, leadership, security policies and compliance issues, security culture and social engineering scams). Non-technical knowledge can help mitigate security issues concerning password sharing, music/video download on corporate network, unauthorised access of corporate networks, accessing social media on corporate platforms and use of removable storage media. Technical knowledge on the other hand is only required of those employees whose jobs demand it. A knowledge gap was therefore found to exist between the INFOSEC course coverage in tertiary institutions (producers) and the INFOSEC needs of Ghanaian organisations (employers).

To bridge this existing knowledge gap, it is recommended that, effective communication and collaboration between academia and industry must be fostered. Industry must promote such collaboration through yearly research funding or grants, scholarships for employees in specific INFOSEC training programmes, workshops and educational sponsored packages whilst providing real world case studies/scenario for critical analysis and teaching in tertiary institutions. Additionally, industry should show positive interest in promoting INFOSEC knowledge in their corporate environments by ensuring active participation by their employees. This can be done through awareness creation in the form of awareness training seminars and workshops for all members of staff. Focus of the training sessions should be more on the non-technical aspects. This, in turn, will help empower employees with the necessary INFOSEC knowledge, and in the long run, aid in creating a security conscious society. Academia on the other hand, must lead the way in ensuring that a security conscious society is therefore nurtured. Academia must rise to the task, by embedding INFOSEC topics in all programmes of study. This is to ensure that not only technical education is passed on to computer science or information technology (IT) students, but also non-technical issues are exposed to all students, since majority of IS users and beneficiaries are from the non-IT fields.

References

1. Caelli, W.J. (2002) Trusted…or…trustworthy: the search for a new paradigm for computer and network security. Computers & Security, 21(5): 413-420.
2. Cisco (2014). Annual Security Report. Retrieved from: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf
3. Cisco Systems, (2008) Data Leakage Worldwide: common risks and mistakes employees make. Available at: http://www.cisco.com/c/en/us/solutions/collateral/enterprise-networks/data-loss-prevention/white_paper_c11-499060.html [Accessed on 10/10/2014]
4. Cooper, D.R. & Schindler, P.S. (2008) Business Research Methods. 10th edition. London: McGraw-Hill.
5. Crossler, R.E. et al. (2013) Future directions for behavioral information security research. *Computers & Security*, 32, pp.90–101.
6. Crowley, E. (2003) Information systems security curricula development. In: *Proceedings of the fourth conference on IT curriculum on IT education*. Lafayette, Indiana, ACM, USA.

7. Deloitte (2013) TMT Global Security Study. Deloitte Touche Tohmatsu Limited. Retrieved from: www.deloitte.com. [Accessed on 15/06/2013]
8. Futcher, L., Schroder, C. &Von Solms, R. (2010) Information security education in South Africa. Information Management & Computer Security, 18(5), pp.366–374.
9. Kritzinger, E & von Solms, S.H. (2004). Five non-technical pillars of network information security management. Retrieved from: sec.cs.kent.ac.uk/cms2004/Program/CMS2004final/p7a3.pdf [Accessed on 15/10/2014]
10. Kritzinger, E. & Smith, E. (2008). Information security management: An information security retrieval and awareness model for industry. *Computers & Security*, 27(5-6), pp. 224–231.
11. Kritzinger, E. (2006). An information security retrieval and awareness model for industry. PhD Thesis: University of South Africa. Retrieved from: http://uir.unisa.ac.za/bitstream/handle/10500/2475/thesis.pdf?sequence=1 [Accessed April 12, 2013].
12. Miller, C.L. (2009) Data leakage for dummies. Wiley Publishing Inc, Indiana
13. Monk, T., van Niekerk, J., von Solm, R. (2010) Sweetening the medicine : educating users about information security by means of game play. In *Proceedings of the 2010 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists*. BelaBela, South Africa.: ACM New York, NY, USA, pp. 193–200.
14. National Accreditation Board (NAB), (2012). Classification of NAB Accredited Institutions. Retrieved from: http://www.nab.gov.gh/index.php?option=com_content&view=article&id=310&Itemid=206 [Accessed on 20/06/2013]
15. National Institute of Standards and Technology (NIST) (2007). Building an Information Technology Security Awareness and Training Program. *The NIST Handbook. Special Publication 800-50. U.S*. Government Printing Office, WashingtonNIST, 2007
16. Papanikolaou, A. et al. (2013). A framework for teaching network security in academic environments. *Information Management & Computer Security*, 21(4), pp.315–338.
17. Petrova, K., Philpott, A. & Buchan, J. (2005). Embedding Information Security Curricula in Existing. In *InfoSecCD Conference'04*. Kennesaw, GA, USA: ACM, pp. 20–29.
18. Ponemon Institute, (2012). The Human factor in data protection. Retrieved from: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt_trend-micro_ponemon-survey-2012.pdf
19. PwC, (2014).The Global State of Information Security. Retrieved from: http://www.pwc.com/gx/en/consulting-services/information-security-survey/key-findings.jhtml [Accessed on: 10/11/2014]
20. Sharma, S.K. &Sefchek, J. (2007). Teachimg information systems security courses: A hands-on approach. *Computers & Security*, pp.290–299.
21. Smith, E., Kritzinger, E., Oosthuizen, H.J. & Von Solms, S.H., (2005). Information Security Education: Bridging the gap between academic institutions and industry. UNISA Institutional Repository. Retrieved from: http://uir.unisa.ac.za/handle/10500/4005 [Accessed on: 15/08/2013]
22. Stewart, G. & Lacey, D. (2012) Death by a thousand facts: Criticising the technocratic approach to information security awareness. *Information Management & Computer Security*, 20(1), pp.29–38.
23. Symantec (2014). Internet Security Threat Report. Vol 19. Retrieved from: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v19_21291018.en-us.pdf [10/11/2014]
24. The White House (2000). Defending America's cyberspace: National Plan for Information Systems Protection. Retrieved from: http://ww.fas.org/irp/offdocs/pdd/CIP-plan.pdf, [Accessed on 17 April 2005].
25. Verizone Enterprise Solutions, (2014). Data breach investigations report. Retrieved from: http://www.verizonenterprise.com/DBIR/2014/reports/rp_dbir-2014-executive-summary_en_xg.pdf. [Accessed on 10/11/2014]