Author(s): Sethupathy, Dev Kala; Williams, Godfried: Imafidon, Chris
Title: The triple helix of information security, government regulations and offshore outsourcing in UK
Year of publication: 2009
Citation: Sethupathy, D.K., Williams, G., Imafidon, C. (2009) 'The triple helix of information security, government regulations and offshore outsourcing in UK' Proceedings of Advances in Computing and Technology, (AC&T) The School of Computing and Technology 4th Annual Conference, University of East London, pp.177-188
Link to published version:
http://www.uel.ac.uk/act/proceedings/documents/FinalProceedings.pdf

THE TRIPLE HELIX OF INFORMATION SECURITY, GOVERNMENT REGULATIONS AND OFFSHORE OUTSOURCING IN UK

Dev Kala Sethupathy, Godfried Williams and Chris Imafidon
School of Computing, Information Technology and Engineering, University of East London

Abstract: Information Security in IT, ICT, ITES sectors and associated activities is a vital solution in safeguarding tomorrow's information society and its systems. Statistical analysis proves that only 40% of UK companies have a policy for information security in a market where only one in six companies survives without IT (ENISA, 2008). This paper explores the parameters of the conceptual triple helix model in context of the synergy among IT, ICT and ITES. Based on a study of the different models employed by UK governmental authorities, the scope of this paper is to develop a model of triple helix to be employed by the IT regulatory authority of UK. This paper evaluates statistical and conceptual data from European Network and Information Security Agency (ENISA), business models for outsourcing, activities of existing UK government authorities (and organisations) regulating best practice of information security in industry and society. Hence the hypothetical triple helix model would centralize the activities of regulatory authority. It would also facilitate change in the industry and market towards a best practice of information security without distressing the flow of existing business systems.

1. Introduction:

Government regulations are the key to organise, monitor and regulate the industry and its community (Richards, 1998). This paper studies the different regulatory authority and governing bodies of leading sectors other than IT in UK. However, government regulations vary in various countries as socio-economic and political decisions contradict the globalisation of IT resources and solutions (Guasch, 1999). An empirical study of State Machine Model, Bell-LaPadula Model, Biba Model, Clark-Wilson Model, Information Flow Model, Non-interference Model, Brewer and Nash Model, Graham-Denning and Harrison-Ruzzo-Ullman Models was carried out as a part of the literature review (Chen; Hansche, 2003;. Bell, 1973, 1976, 2005; Landwehr, 1981; Sandhu, 1994; Biba, 1977; Clark, 1987; Valinevicius, 2004; Mclean, 1994; Harris, 2005; krutz, 2003)

Based on the results of empirical study this research intends to investigate the feasibility of a model based on the triple helix theory. The Triple-Helix model of IT regulatory authority provides better environment in overcoming the threats faced by the above security models. The Common threats to the above security models include 'covert channels', 'backdoors', 'Asynchronous Attack', 'Buffer Overflows'. This research also evaluates statistical and conceptual data from European Network and Information Security Agency (ENISA), business models for outsourcing, activities of existing government authorities (and organisations) regulating the best practice of information security in industry and society. Hence the hypothetical triple helix model would centralize the activities of regulatory authority. It would also facilitate change in the industry and market towards a best practice of information security without

distressing the flow of existing business systems.
Technologies of IT, ICT, ITES, Internet, VPN and E business are some of the elements with similar technical and industrial norms around the world (e.g., IEEE standards for modem, twisted copper wire, optic fibres, etc.,). This paper explores the inter-relationship of Government Regulation, Industrial Practices and Outsourcing Model while adopting IT, ICT and ITES models in the context of 'information security'. It critically confers the different parameters of triple helix while evaluating IT, ICT and ITES and its relation to the research questions.
Correspondingly, this paper puts forward a series of discussions in response to the following key research questions. Why information security a crucial parameter in determining the socio-economic and business models of potential information society? Is a regulatory authority to monitor IT business processes significant? Would a regulatory framework have an impact on the ever changing technical and business processes of IT industry? How critical are the security systems of existing E-Business within offshore communities in the context of corporate governance policies? Will it have an impact on potential information society?

2. Triple helix model:

"Approaches of The National Systems of Innovation (NSI) were widely practised for bounded phenomena within different nations and individual firms." (Etzkowitz, 2002). During World War II discontinuous innovation was largely developing within the firms, which sought a different environment across firms and institutions within and outside borders (Etzkowitz, 2002). However, to overcome the discontinuous pattern in innovation analysts explored the theory of Triple-Helix in the context of collaboration within well defined boundaries. "The Triple-Helix is a spiral model that captures multiple reciprocal relationships at different points in the process of overlapping three parameters in a three dimensional space" (Etzkowitz, 2002).
The first dimension is the internal transformation in each of the helices, such as the government, industry and community contributing towards the regulation of information security and deployment of respective models for offshore outsourcing. The second dimension is the influence of one helix on the other, for example, government transferring administrative power to regulatory authority, which influences the market in following the best practise towards securing information. The third dimension is the creation of new overlay of trilateral networks from the interaction among the three helices (Etzkowitz, 2002).
Historically triple helix structural configuration was utilized by analysts and innovators to explain the non-'systemic' layers in inter and intra relationship among three complex parameters and its components (Leydesdorff, 2005). Though the Triple Helix, to a greater extent employed in socio-economic, innovative and knowledge based environment, analysts believe that the model could also be employed in other fields of science & technology, policy and decisions. "The Triple Helix hypothesis states that the 'systems' can be expected to remain in transition" (Henry, 1998). Hence, Triple-Helix hypothesis was considered in solving the transitional issues of collaboration between University, Industry and Government. The concept of collaboration was used to influence the knowledge

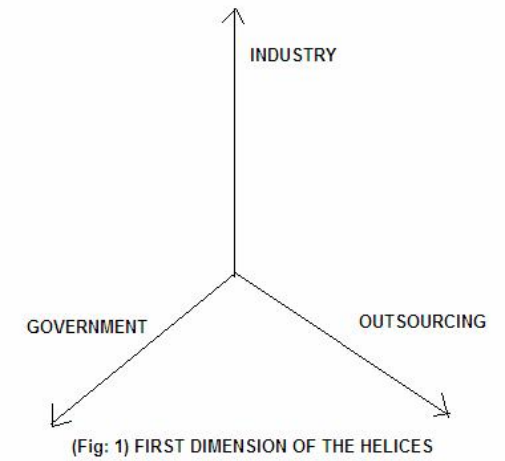
transfer and innovation within defined set of boundaries.

A model was developed based on the hypothesis to define the parameters associated with the relationship and boundaries of University, Industry and Governmental departments. Analysts considered the sceptics and debates from the scholarly community while preparing a test plan. The case was tested in USA to study the knowledge transfer and diffusion between the three parameters. The study later proved the success of the hypothetical model, which in turn attracted the scholarly community's attention to promote research. USA has been seen to exemplify the former and Europe the later mode of Triple Helix development (Riccardo, 2000). Recent scholarly breakthroughs in this field suggest the application of the Triple Helix model for evolutionary, transitional, innovative, discontinuous and rapidly changing systems and frameworks. Since the structure of 'Government Regulations'; 'Information Security' and 'Offshore Outsourcing' undergoes a rapid phase of transition, Triple Helix model would construe the overlapping region of different layers.

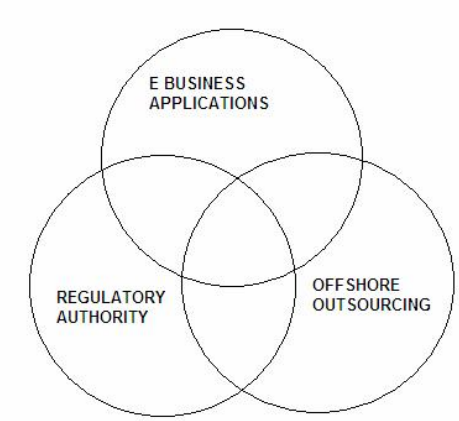
3. Government authorities (UK) and information security:

Government authority in UK does not operate on a single model or a set of regulations *[Appendix]*. According to the recent updates by European Network and Information Security Agency, it is evident that there are more than one UK governmental department or authority involved in regulating information security systems in business process, industry, organisation, community and government *[Appendix]*. Tables *[Appendix]* 1 and 2 show the list of authorities and their activities in regulating network and information security:

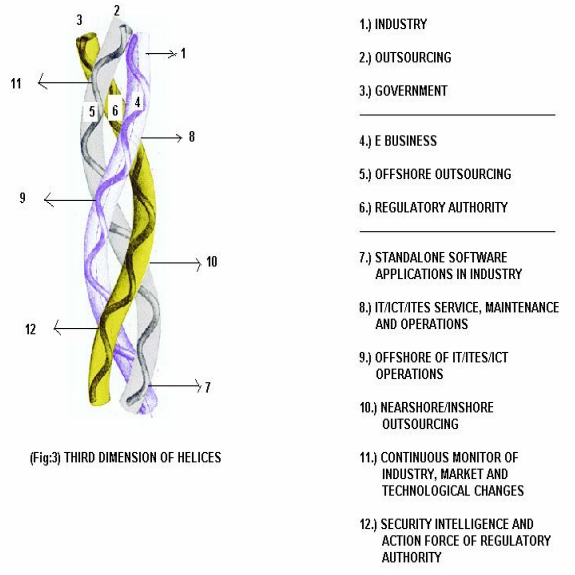
According to table 1 and 2 there are only six national government authorities involved in the regulation process of information security. By analysing the six national authorities individually we could confirm that all the authorities were held responsible for regulating information security as an additional activity alongside their core activities. However, it is evident that there is no single national regulatory authority in UK dedicated to continuously monitor information security in E Business, IT, ICT, ITES and Outsourcing. These national regulatory authorities are often criticised by industry and scholarly community for mostly being operational only during a crisis. On the other hand scholarly investigation regarding the structure of the existing UK authorities and their models would provide more results to perform a comparative and qualitative study of models and systems employed by different countries. It would also provide more results while considering the Information security policies employed by major companies and sectors.



(Fig: 1) FIRST DIMENSION OF THE HELICES



(Fig:2) SECOND DIMENSION OF THE HELICES



(Fig:3) THIRD DIMENSION OF HELICES

Financial industry in UK has a comprehensive regulatory system and a single dedicated authority to regulate the standards of the services and products offered by the industry. The Chancellor of the Exchequer announced the reform of financial services regulation in the UK and the creation of a new regulator on 20 May 1997 (FSA, 2008). The move was primarily focused on merging banking supervision and investment services regulation into the Securities and Investments Board (SIB) (FSA, 2008). The SIB formally changed its name to the Financial Services Authority (FSA) in October 1997 (FSA, 2008). The core objectives of the FSA are, to protect the community and industry from reckless business practices and to regulate financial policies towards attaining a virtuous and secure business for the future community. According to a statistical report by FSA, 68% of the UK organisations expressed concern towards regulations as a consequence of financial crime (Walker, 2007). However, when it comes to combating financial security issues like money laundering and fraud in the industry, FSA is rated higher compared to law enforcement body, trade associations and the government itself (Walker, 2007).

"In a qualitative perspective 84% firms agreed that the FSA should have a role in financial-crime issues and this was consistent across all sectors. In particular, 89% felt that the FSA should play a role in sharing intelligence, 79% felt that FSA should play a role in providing greater clarity on best practices and 67% in setting out broad principles for firms to follow" (Walker, 2007). On an average 78.6% of firms across financial industry believe that FSA's regulations in providing greater clarity in best practices would increase security and effectively fight crime in financial sector (Walker, 2007). In depth understanding of similar case studies across different sectors (e.g., customs, automobiles, food, etc.,) explained the success of regulatory authorities in promoting the best practice with increased security for both industry and community.

On the other hand, telecommunication industry is also considered in examining the framework of regulatory authority and its influence towards monitoring and regulating the market over other governmental bodies. 'Ofcom' is the only telecommunication authority of UK responsible for the duties specified in the UK Communications act 2003(Ofcom, 2008). Ofcom is a non-

governmental independent organisation reportable to the UK parliament and sponsored by the Department for Business; Enterprise and Regulatory Reform; Department of Culture, Media and Sports. The major duties of Ofcom incorporate regulating Electronic Telecommunication Services market including the High-Speed Information Services, Television and Radio. The main concern of Ofcom in the regulatory process is to make sure people are protected from being treated unfairly in television and radio programmes and from having their privacy invaded (Ofcom, 2008). This also extends to the telecommunication industry (Ofcom, 2008).

A market research conducted by Ofcom in 2005/2006 revealed that 46% of the public are aware of the duties of Ofcom, 43% are aware of FSA regulations and 26% regarding Ofgem rules. However, the results published while repeating the survey on Q2 of 2007 were different. 78% were aware of Ofcom duties, 62% regarding FSA regulation and 39% regarding Ofgem (Ofcom, 2007). Though the survey supports the success of Ofcom in reaching and protecting public as a regulatory authority, FSA and Ofgem confirmed the success of 'Regulatory Authority framework' across all three sectors by producing a sharp increase in consumer opinion. It is also evident that regulatory authority framework across all three sectors adapted to the industrial changes while influencing the best practices to protect community and people.

Ofgem is committed to regulating monopoly in gas and electricity network while safeguarding the consumers from industry's reckless practices when companies compete with each other for business (Ofgem) (Protecting Energy Consumer Interest, 2007 -2008). Similar study regarding the UK authorities 'Office of Water', 'Office of Fair Trading', 'Office of the Rail regulator', 'Health and Safety executive' and 'competition Commission' revealed supportive evidences in proving the significance and contribution of UK regulatory authorities across various sectors. It also demonstrates the increase in the efficiency of such authorities over a period of time when compared to other bodies and governmental departments. Conversely, why did development, operations and outsourcing of IT, ICT and ITES sectors were left out of the structured process towards fighting security issues, knowing its potential growth and contributions to the community?

4. Industry and information security:

Businesses in UK are now crossing a new era of IT systems and associated services. This mainly includes independent software applications, application maintenance services, web based applications, additional services for IT systems (e.g., database management, content management, network routing service, etc.), networking, hosting services, outsourced IT development, maintenance, operations and ITES services. A study by ENISA concludes that the growth of business dependency on IT systems is exponential compared to the developments in regulating security issues of IT systems and services. According to ENISA's statistics only one in every six small companies in UK could survive without IT (PWHC, 2006). The trend in today's industry to compact business needs without compromising quality is a consequence of businesses fighting against competition, resources and cost amidst globalisation and socio-economical turmoil. One of the major practises adopted by the industry to cut cost, avail cheaper and swift

resources in less time is to outsource business needs. Business needs varies based on the nature of business itself. When it comes to IT development and operations more than 53% of the companies outsource their IT operations (PWHC, 2006).

As the dependency of industry on IT systems increased scholars were more sceptical regarding the security of fast developing systems. "Many UK businesses are a long way from having a security-aware culture. Their expenditure on security is either low or not targeted at the important risks (PWHC, 2006)". Roughly two-fifths of businesses spend less than 1% of their IT budget on information security (PWHC, 2006). Businesses tend to restrict their concern and expenditure to basic rules of security framed by the government representatives. However, research conclusions demonstrates the need for businesses to extend their security concern towards best practices in industry; models employed in building services or systems; models employed in information exchange and outsourcing. Such practices in the industry would contribute towards consistency in openness, transparency of systems and business processes, socio-economic progression, safeguarding community and globalisation.

Standards for information security practices in industry set by the government failed to make a strong influence on the current practices among companies. A study by ENISA concluded that only 44% of companies have carried out any security risk assessment in the last year. This is a small increase on six years ago (PWHC, 2006). There is still a shortage of security qualified staff; only one in eight companies has any (PWHC, 2006). Revolution in internet forced companies to go online. On the other hand, Internet facilitated the growth of companies while reducing the cost and resources. Though Internet serves as a global medium of information exchange, it is still an unsecured system including its design and operation (Ofcom, 2006). Findings from the British Crime Survey of 2003/2004 concluded that an average of more than £ 238 millions is lost every year on fraud. It also concludes that the percentage of internet and technology contributions towards the overall fraud is increasing every year (Wilson, 2006).

The major milestone of a secured industry would be to attain the highest standards through design and adoption of desired policies and practices. Three-fifths of UK businesses are still without an overall security policy, though a third of these have defined an acceptable usage policy for the Internet (PWHC, 2006). Researches conclude that information security standards and policies in businesses should not be restricted to IT, ICT, ITES, Business models and outsourcing models. However, research conclusions pay much emphasis on HR recruitment process, Learning and Development and Disaster Recovery Systems. "Recruitment processes at a quarter of companies do not include any background checks; 19% of companies that believe security is a very high priority fail to check the background of their staff. One in eight organisations does nothing to educate their staff about their security responsibilities. Only a quarter of UK companies have tested their disaster recovery plans in the last year." (PWHC, 2006). Survey conducted by ENISA and PWHC states that only 40% of UK companies have a formally documented and defined information security policy. E Business and E Commerce are emerging as the industry's next giant step towards attaining business compactness and independency in a global perspective. Discussing the E Business practices and its

evolution would help government authorities to frame models and policies to adopt the best practice in safeguarding the potential industry-community framework.

5. E business:

According to Godfried B. Williams commercial activities and processes supporting online business are as vulnerable to security threats as the design of the system itself (Williams, 2007)(Williams, 2004). E Business would include Internet, Automatic Teller Machine (ATM), Electronic Point of Sale (EPOS), Telephone transactions, payment systems and gateways (Williams, 2007). E business systems and mobile service applications employing B2B, B2C and B2G activities are exposed to security risks of personal data, sensitive information, identity, money and system itself. Though international cyber crime laws and rules appear fancy, it operates predominantly on crisis situations. Analogous to the business process of offshore outsourcing IT, E Businesses too are intermittently monitored by UK national regulatory authorities.

Unsolicited Information and online services flow in to the country via internet and phone network have an irreversible effect on the framework and forecast of national economy (Ruffles, 2001). Hence, scholars debate on classifying E business, information services, IT/ITES products or service hosted in foreign servers or from foreign clients as an import commodity. Since these activities take place round the clock, researchers believe that continuous monitoring of all information exchange, data and financial transactions incoming, outgoing and within the country would be a viable approach in controlling security issues threatening the future of information society.

More and more companies are converting their physical existence in to virtual through online business systems and the technologies associated to reduce cost, easy management and operation. Some companies are moving a step further to remove infrastructure constraints from the business model by making their employees to work from home, online marketing campaign, outsourcing systems development, operations, market research and business intelligence. A recent survey by 'Office for National Statistics (ONS)' concludes that intrusion of internet usage and online presence is much higher in finance, telecommunication, services and retail sectors (Office for National Statistics, 2008). It is also evident that these sectors have direct influence on the fluctuations and forecast of UK economy (Rowlatt, 2001) (Vaze, 2001). Thus any model/system developed to regulate IT offshore outsourcing practices should incorporate E business systems as they encounter most of the security issues faced by IT oriented industries.

6. Outsourcing and information security:

Impact analysis of Information Security issues were widely discussed by scholarly community with respect to a variety of disciplines. As the IT intrusion started to get more intense scholarly community started to look in to some of the derivative business processes apart from concentring on the major fields of impact. One such process is offshore outsourcing which turns out to be a lucrative business process for the corporate sector to cut down their burden on a number of organisational issues such as human resources, expenditure, maintenance, time management, productivity, etc.,. Hence this

fast growing industry of clients and service providers has attracted the attention of the research community. Eventually a number of scholars conducted case studies in order to critically evaluate the security risks in the outsourcing business process. Khalfan presented the overview of national case study exploring the Information security considerations in IS/IT outsourcing projects in public and private sectors of Kuwait (Khalfan, 2004). Though there are a number of risks associated with every corporate global business activity, the risks are normally prioritised for short and long term by the risk management wing of the corporate governance. Studies conducted by Khalfan confirmed the speculation of research community regarding the prioritisation of Information Security risk as the most compared to other corporate risks. Respectively, the study also confirms that Outsourcing business process was listed as the top priority compared to other business processes of the industries participated in the case study (Khalfan, 2004). Though the results of case study was convincing to believe the severity of Information Security in the outsourcing process, corporate practices changes based on country, legal system, market practices and socio-economic culture. Thus the case study should be compared with the relevant case studies conducted addressing such issues. This would eventually post a better picture to have a broader look at the problem in a global perspective.

7. Government regulation and information security:

Government regulations are a key towards achieving the best practices in the offshore outsourcing process. Though there are a number of regulations, laws and restrictions in place to address the information security in the outsourcing process the existing system is not flexible enough to have easy interface between corporate governance and government regulations. M A Smith (et al) addressed this issue by developing a framework to define the entities and definitions of the activities associated in the whole process (Smith, 1996). M A Smith (et al) centred their framework around software development and deployment across boarders through the process of offshore outsourcing (Smith, 1996). According to M A Smith (et al) government authorities regulate the import/export of software, promotion of standards through use, IP Protection, trans-border data transfer restrictions, encryptions standards and laws (Smith, 1996). Though the regulations restricts the above issues they still have not explored the possibility of having a unified global regulatory authority to have end to end control of the entire outsourcing process despite the variety in issues addressed when it comes to business across boarders. There is no method in place for sampling and quality checking of IT services and products across boarders even though there are restrictions in place on the data transfer. Hence government regulations are a key towards monitoring, regulating and managing the whole process of bringing up the best practices in the market to safeguard the potential information society.

8. Corporate governance and information security:

Issues regarding Information Security have attracted a wide range of research groups to discuss about the possible impact on the different components of market (current and future) and the society. However, some group of researchers critically evaluate the

responsibilities of market players in framing policies towards attaining the best practices in the market and the society. Posthumus and von Solms proposed a framework whereby pointing out the responsibility of corporate governance to integrate information security into the corporate governance framework (Posthumus, 2004). Business information is a crucial element in corporate business activities where the flow and access is always vulnerable to security risks (Posthumus, 2004). Corporate governance treats the vulnerability of business information as a priority threat to the core business. Nonetheless, the behaviour of executive management in corporate governance has to be analysed since their concern is mostly concentrated on business activities. Questions concerning the corporate behaviour were critically evaluated by scholars in order to understand the responsibilities of corporate governance towards socio-economic and market issues. Though Information Security Governance (ISG) policies framed by the corporate management combat the security threats and breaches, they lack the integration of solutions in order to solve the socio-economic problems that would affect the potential information society. The ISG model proposed by Posthumus and von Solms categorises the business issues and IT infrastructure as internal requirements that contribute to an effective information security strategy (Posthumus, 2004). However the legal regulations and best practices are categorised as external requirements that contribute to an effective information security strategy. The ISG model has not addressed some of the crucial question on how to extend and integrate the IT infrastructure with the major market players and the government authorities to bring the best practices and normalised Information Security Governance Policies across the market (Posthumus, 2004). Eventually, the concerns regarding the effective adoption of market practices and the framing of relevant corporate policies was not addressed by the ISG model. Thus the extension of existing ISG model to incorporate the solutions concerning the best market practices and the integration with government authority framework would throw light on the development and integration of a global Information Security framework.

9. Conclusion:

Critical analysis of different issues in Information Security in the context of Offshore Outsourcing has exposed the sensitive areas within this research field. When it comes to a global picture on combating the security risks through effective information security practices, government; corporate; market and the society should develop systems and adopt frameworks accessible by each other to have better integration. This could serve as a base to spread the common practice across nations in order to develop a working global regulatory authority to bring the best practices in industry and market. Though there a number of working and experimental hypothetical models proposed by the scholarly community frequently, a complex interface of inter-operable mechanism between such models has to be adopted to facilitate the move towards the global framework. Eventually this would help in building a safe and secure information society of the future.

10. References:

A.M. Khalfan, 2004, information security considerations in IS/IT outsourcing projects:

a descriptive case study of two sectors, *International Journal of Information Management,* 24, pp. 29–42.

Bell, David (December 2005), Looking Back at the Bell-La Padula Model. *Proc. 21st Annual Computer Security Applications Conference*, pp. 337-351.

Bell, D. Elliott and LaPadula, Leonard J. (1973), Secure Computer Systems: Mathematical Foundations, MITRE Corporation.

Bell, D. Elliott and LaPadula, Leonard J. (1976), *Secure Computer Systems: Unified Exposition and MULTICS Interpretation,* MITRE Corporation.

Biba, K. J. (1977), Integrity Considerations for Secure Computer Systems, *MTR-3153*, The Mitre Corporation.

David D. Clark, David R. Wilson (1987), A Comparison of Commercial and Military Computer Security Policies, *IEEE Symposium on Security and Privacy,* pp. 184.

ENISA – European Network and Information Security Agency, http://www.enisa.europa.eu/doc/pdf/Country_Pages/Country_Page_UK_6_05_2008_SP_to%20PDF.pdf, Main source: http://www.enisa.europa.eu/index.htm, updated on 20-May-08.

Etzkowitz. H (Working paper series 2002-11), The Triple Helix of University-Industry-Government, *Implications for Policy and Evaluation*, Science Policy Institute, ISSN: 1650-3821, pp. 1-5.

Financial Services Authority, http://www.fsa.gov.uk/Pages/About/Who/History/index.shtml, Main Source: http://www.fsa.gov.uk, page last updated on 18/07/2008.

Guasch. J. L, Spiller. P. T, (1999), Managing the regulatory process: Design, Concepts, Issues and the Latin American and Caribbean Stories, *World Bank Publication*, ch: 1-3, 9, 10, 12-16

Hansche, Susan; John Berti, Chris Hare (2003), *Official (ISC)2 Guide to the CISSP Exam*. CRC Press, ISBN: 9780849317071, pp. 104.

Harris, Shon (2005), All-in-one CISSP Exam Guide, Third Edition, *McGraw Hill Osborne*, Emeryvill, California.

Henry. E, Leydesdorff. L (1998), The Endless Transition: A 'Triple Helix' of University-Industry-Government Relations, *Minerva 36,* pp. 203-209.

Krutz, Ronald L. and Vines, Russell Dean (2003), The CISSP Prep Guide, *Gold Edition*, Wiley Publishing Inc, Indianapolis, Indiana.

Landwehr, Carl (September 1981), Formal Models for Computer Security, *ACM Computing Surveys (CSUR),* New York: Association for Computing Machinery, ISSN 0360-0300, pp. 13 (3):8,11, 247 – 278.

Leydesdorff. L, (2005), The Triple Helix Model and the Study of Knowledge-Based Innovation Systems, *International Journal of Contemporary Sociology*, Vol. 42.

McLean, John (1994), Security Models, *Encyclopedia of Software Engineering 2*, New York: John Wiley & Sons Inc, pp. 1136–1145.

Ofcom: A short guide to what we do (Last Updated: April 2008), Main Source: http://www.ofcom.org.uk/consumeradvice/guide/

Ofcom Research Report Publication: The Consumer Experience (20 Nov 2007), pp. 129-131. Main Source: http://www.ofcom.org.uk/research/tce/ce07/research07.pdf

Office of Communication Research Publication: Online Protection: A survey of consumer, industry, regulatory mechanisms and systems (21 Jun 2006), Main source: http://www.ofcom.org.uk/research/telecoms/reports/onlineprotection/report.pdf

Office of Gas and Electricity Markets (Ofgem), Main Source: http://www.ofgem.gov.uk/About%20us/Pages/AboutUsPage.aspx

S. Posthumus and R. von Solms, 2004, a framework for the governance of information security, *Computers and Security, Elsevier*, 23, pp.638-646

PriceWaterHouseCoopers (2006), Information Security breaches survey, ENISA – European Network and Information Security Agency. http://www.enisa.europa.eu/doc/pdf/studies/dtiisbs2006.pdf, updated on 20-May-08.

Protecting Energy Consumer Interest: *Ofgem Annual report* (2007-2008), 'The Stationary Office' – Information and Publishing Services.

Riccardo. V, Campodall'Orto. S, (2000), Neocorporations or Evolutionary Triple Helix? Suggestions Coming from European Regions, *Presented at the Third Triple Helix Conference*, Rio de Janeiro.

Richards. D. J, National Academy of Engineering, Pearson. G, (1998), *The Ecology of Industry*, ISBN:0309063558, pp -3

Rowlatt A (2001), Measuring E Commerce: Developments in the United Kingdom, '*Economic Trends' No. 575*, Office for National Statistics, pp. 30-36.

Ruffles D (2001), Cross-border electronic commerce and international trade statistics, *'Economic Trends' No. 576*, Office for National Statistics, pp. 45-49.

Office for National Statistics (Last updated: 01/04/2008), main source: http://www.statistics.gov.uk/default.asp

Sandhu, Ravi S. (1994), Relational Database Access Controls, *Handbook of Information Security Management (1994-95 Yearbook)*, Auerbach Publishers, pp. 145-160.

Shuo Chen, Zbigniew Kalbarczyk, Jun Xu, Ravishankar K. Iyer, A Data-Driven Finite State Machine Model for Analyzing Security Vulnerabilities, Center for Reliable and High-Performance Computing, University of Illinois.

M.A. Smith et al., 1996, offshore outsourcing of software development and maintenance: A framework for issues, *lnformation & Management*, 31, pp. 165-175.

Valinevicius, A. Zilys, M. Eidukas, D (2004), Information flow model of integrated security system, *Information Technology Interfaces*, 26th International Conference, ISBN: 953-96769-9-1, pp. 567-572, Vol.1.

Vaze P (2001), ICT Deflation and Growth: A Sensitivity Analysis. *Economic Trends No. 572,* The Stationery Office, pp. 45–52.

Walker E, Cadwallader J, Gruppetta R, Young E (March 2007), Financial Crime – *Stakeholder Research, consumer research 58*, Financial Crime and Intelligence Division(FSA), http://www.fsa.gov.uk/Pages/Library/research/Consumer/index.shtml, ch. 5-6.

Wilson D, Patterson A, Powell G, Hembury R (2006), Fraud and Technology Crimes, *Findings from the 2003/04 British Crime Survey, the 2004 Offending,* Crime and Justice Survey and administrative Sources; Home Office ch. 2-3.

Williams. G. B (2007), Online Business Security Systems, *Springer publication*, ISBN 978-0-387-35771-3, ch. 1,pp. 1
.
Williams. G. B (2004), Synchronising E-Security, Kluwer Publications, ch. 3-5, pp. 27-89.

11. Acronyms:

B2B – Business to Business
B2C – Business to Customer
B2G – Business to Government
E Business – Electronic Business
ENISA – European Network and Information Security Agency
FSA – Financial Services Authority
HR – Human Resources
ICT – Information and Communication Technology
IT – Information Technology
ITES – Information Technology Enabled Services
Ofcom – Office of Communications
Ofgem – Office of gas and electricity markets
PWHC – Price Water House Coopers
Q2 – Second Quarter
VPN – Virtual Private Network