Trust in the Public Sector? On Information Security Awareness in an Audit Service

Kofi A Boateng, Rosemary B Coffie, Prosper Hayford
Department of Information Systems and Decision Sciences,
KNUST School of Business, Ghana

: kaboateng.ksb@knust.edu.gh, Framaygh@yahoo.co.u, papabish009@yahoo.com

Abstract
Trust has been a key aspect of organisational information sharing for some time now. However, the conceptualisation of the concept within the public sector as a means of creating security awareness suffers rigorous and systematic academic treatment. It remains the aim of this paper to tease out trust as it pertains in a public sector government department and project its diverse implications within the context of information security awareness creation. Through qualitative research approach driven by interpretive philosophical orientation, the paper reveals fundamentally diverse challenges that are occasioned by the application of information communication technologies in the management of sensitive and precious corporate data. Findings suggest the adoption of wide-ranging approaches in sensitizing members of an organisation to the crucial importance of not taking the sharing and distribution of information for granted. Rather, the promotion of an organisational atmosphere that is informed by mutual awareness in the treatment of diverse sources of corporate data for efficient and effective information sharing. Further research can focus on control to determine the extent to which information security awareness can be understood without trust.

Key words: Trust, public sector, information security, ICTs, Audit Service

1 Background Issues

Sharing information on diverse issues within the public sector constitutes a significant information security awareness challenge for most public sector organisations. Trust is a key component in this information propagation exercise within the public sector environment. However, the information systems research community seems to have taken the thorny issue of trust in information security awareness in the public sector for granted. As technology invades most of the information sharing activities in the public sector, security is becoming a major concern rather than an afterthought. Acceptable level of information security is achieved only when the right set of managerial strategies and technical security controls are identified, implemented and maintained (Thomson and von Solms, 1998). This means that effective management of information security in the public sector requires a combination of technical and social countermeasures.

Creating information security awareness in such an organisation as the audit service is critical, because the databases of public organisations contain confidential and sensitive information of the citizens or clients with whom such institutions deal with. Adoption of proper security measures and appropriate implementation of them could reduce the risk of sudden loss of data, unauthorised access into corporate systems and provide security tools to detect attacks and correction of security breaches. This paper considers the diverse security issues that seem to be inherent in the operations of the Ghana Audit Service (GAS). Public sector in both developed and developing countries have embraced IT to improve the services they deliver, to increase public access to information and to energise more participation in public affairs. For that reason, public sector audit in Ghana are experiencing fundamental reforms aimed at instilling transparency and improving overall security arrangements consistent with international standards and practices. As a result, ICT use and its allied systems are being deployed to provide assurance that the public sector so desperately needs.

The objective of this paper therefore is to highlight the diversity of issues that characterise information security awareness in the Public Sector. The essence is to shed insights on the need to appreciate the various security policies and strategies that are crucial to analysing security implications in information systems use within organisations. It is also to extend current conceptualisations by extending our understanding of the current literature on information technology (IT) driven auditing endeavours. It is appropriate to set out the overarching research question this paper seeks to answer. How does trust manifest in the creation of security awareness in public sector institutions? Articulating answers to this question could hopefully provide convincing responses to the need for a pragmatic approach to information security awareness in public sector organisations.

In the next section a cursory view is taken of the literature on information security to illustrate the different elements of trust issues that undergird security awareness in public sector organisations. The aim is to flesh out the various concerns that attend the idea of managing and protecting information in a manner consistent with public sector operations. A brief overview of the research method that was instrumental in gathering the requisite data for this research is outlined. Insights from the field are provided with detailed discussion teasing out the divergent matters on creating security awareness in organisations. The paper concludes with a challenge to direct future research attention to how security awareness operates in typical large-size private organisations.

2 Information Security, Trust and the Public Sector

Understanding information security trust from the standpoint of the public sector provides a fertile ground for articulating one of the serious issues confronting information sharing in such places. What makes this crucial is the likely ramifications that have the potential of damaging trust in the operations of such public sector organisations.

2.1 Conceptualisation of Information Security (IS)

Aytes and Connolly (2003) presented a model of user behaviour on security awareness that emphasised the factors relating to the user's perception of risk and the choice driven by that perception. In this model, information sources (e.g., training, media, coworkers, friends, policies, procedures and personal experience) provide information that forms the user's knowledge (e.g., about threats and vulnerabilities, awareness of countermeasures, potential consequences to self and others and the costs of secure behavior). This information must be perceived by the user to be relevant in their particular circumstances. The user's perceptions (availability and usability of safe practices, probability of negative consequences, significance of negative consequences, ease of recovery and beliefs regarding peer behavior) therefore represent an important factor in the behavioral choice process that leads to the actual behaviour associated with the choice (i.e., to use or not use a specific security countermeasure). The behaviour resulted in an outcome, either positive or negative that is fed back as a source of new information.

Banerjee et al., (1998) identified situational characteristics which exert an impact on the ethical behavior-related intention of IS employees when they are faced with ethical dilemmas about security issues. The results of the study indicated that an IS employee's intention to behave ethically or unethically is strongly related to the context of the individual's perceived organisational environment and influenced by that individual's moral obligation toward performing an act. In a related development Barman (2000) highlighted the significance of security awareness training, stressing the point that training should aim to teach the organisational information security policy to employees.

Beatson (1991) discussed the idea of avoiding security breaches that centre on psychological profiling of potential new employees, separation of responsibilities, clear data classification rules, and enforced security policies by creating and maintaining a high level of information security awareness. It is on this score that Bray (2002) pointed out the vulnerability of organisations to security breaches when considerable transformation occurs, such as a downsizing. As a means to avoid security breaches during organisational changes the study suggested a programme of information security awareness training that bears on social engineering, password protection, encouraging administrators to be vigilant when reviewing system and security logs together with heightened computer and security alertness.

2.2 Contemporary renditions on trust

"…trust which undergirds our everyday lives is a pure social construction which answers to our need for security by seeming to be a fact when it is always a projected assumption" (Lewis and Weigert, 1981).

Trust is formed when two entities, by wilful agreement, behaviourally decide to be interdependent on each other (Brehm, 1992, Berscheid, 1985), and each in turn takes due cognisance and fulfil the conditions governing their interdependence (Berscheid and Graziano, 1979). Trust, therefore, is key in oiling the relationship that sustains the interdependence (Mishra, 1993, Thompson, 1967).

Trust is not a modern phenomenon. In fact, events that took place in the seventeenth century Hudson Bay Company tell volumes that not much has changed till date in terms of trust. Rich (1948) reveals that trust was seen then in such issues as "prudence, faithfulness, honesty, diligence, good behaviour, integrity, reputation, justice, ability, courage, conduct, fidelity, and local knowledge". Contemporary literature supports this measured observation as trust is illuminated in such notions as reputation, integrity, honesty and competence; all jointly or severally captured in the works of (Mayer et al., 1995, McAllister, 1995, Kramer and Tyler, 1996). In a related development, Shapiro (1987) demonstrates the idea that trust has been implied as a conceptual representation of faith, security, confidence, anticipation, reliance, emotional property, among others.

The centrality of trust in social-technical discourse in public sector environment is reflected in the reciprocity of its faithfulness (Simmel, 1900). Trust constitutes a fundamental setting of daily interaction (Misztal, 2001); Goffman (1971) portrays a relatively parallel view, arguing that trust emanates from unplanned interaction. Given the fact that trust is not automatic, it stands to reason then that trust comes about by means of depending on the availability of information about the person, object or institution to be trusted (Bezemer, 2004). And the information generation and gathering processes take place within the framework of shared understanding and cooperation, against the background of mutuality of reinforced expectations and reciprocity (Scott, 1999). This adds a cognitive dimension to trust; implying the familiarity of the trusting party with the selective processes that precede the point at which one deposits their trust in an object or person. In other words, trust involves, and revolves around, the use of a person's volition; that is the willingness to trust, inspired by a certain amount of information in directing the path of one's trust in a particular person or system.

It is not possible to have full knowledge in terms of information about the object of trust. Was this the case, action could be taken with the highest degree of certainty; leaving no room for trust to build up in the first place. It could be argued, then, that to make a claim of trusting somebody 100%, is superfluous and redundant, and at best, "contradictory in terms" (Nooteboom, 2003). The reverse situation also holds true for the generation of trust. Thus, in a situation of absolute ignorance there cannot be any possible grounds for trust; the only option under this instance is to gamble, suggest (Lewis and Weigert, 1985). Inadequate information in terms of the current circumstances of the parties in time inevitably signals the need to produce and maintain trust in distributed settings (O'Leary et al., 2002).

Zand (1972) found that dearth of trust is inimical to information exchange which is instrumental in reducing the effectiveness of managers in finding common ground in problem-solving endeavours. Granovetter (1985) directs his contribution to the discourse on trust in a radically different direction; focusing on social relations as the driving force behind the production of trust in economic life. Emphasising the effectiveness of proximity to trust formation and its subsequent maintenance, Handy (1995) hypothesises that "trust needs touch". Granovetter however admits that, social relationships could not necessarily be an assurance for averting malfeasance and conflict; on the contrary, reveals Granovetter, they inspire their occurrence.

No wonder trust is considered as a decision under risk. Risk in trust finds expression in one of two ways. First, that trust occurs in an environment of limited information; highlighting the concept of bounded rationality against the backdrop of cognitive restriction (Simon, 1957). Lastly, that trust involves one party being vulnerable to the potential abuse of another. It is this risky aspect of trust that potentially introduces complexity into the picture. Luhmann (1979) argues for the case that trust reduces complexity or uncertainty. The complexity-reduction component of trust, triggers the possibility or even the probability of raising the level of cooperation (Misztal, 1996). This conditions an enabling environment for "social interactions to proceed on simple and confident basis where, in the absence of trust, the monstrous complexity posed by contingent futures would again return to paralyse action" (Simmel, 1964). Drawing on this, Luhmann (1979) could not be far from right in cautioning that the alternative to trust is to court "chaos and paralysing fear".

Trust has a functional relationship with time; in other words, the level of trust rises with the maturity of a relationship; 'trust is developed over time as individuals gain confidence in the reliability of others through a series of interactions' (Fountain, 2001 p. 72). This reflects Fine and Holyfield's observation (1996) that trust changes over time as members gain knowledge of an organisation. They argue that initially an organisation seeks to act as validating the trust of new members. The organisation's position then shifts to an "arena in which trusting relations are enacted and organisational interaction serves as its own reward" (p. 29). It is along this line of reasoning that (Ba and Paylou, 2002) put forward the idea that trust act as a catalyst for raising buyer-seller expectations in their commercial relationship. The same opinion finds favour with the social capital literature (Putnam, 2000,). Fukuyama (1995) therefore submits that trust constitutes one of the most key expressions of social capital; for this lies in its ability to stimulate an impulsive social interaction.

It should be noted that trust holds a promise for building enduring social networks and relationships both within and between organisations. In view of this Huff and Kelley (2003) similarly contend that the association of trust with certain cultures is key to their gaining of competitive advantage on the global market. Trust could also play an influential role in initiating industrial decline (Kern, 1988), and could also be implicated in the determination of the political destiny of a national entity. Avgerou et al., (2006) attest to the chief role

trust played in the citizenry's response to, and subsequent trust in, large-scale e-government ICT initiatives in two Latin American countries, namely Brazil and Chile. Technological systems have the tendency to blunt the sharpness of trust (Kramer, 1999). Zuboff provides us with some kind of insights to support this claim. Her path-breaking work captures a complaint made by a manager at the installation of a surveillance system:

"If I didn't have the Overview System, I would walk around and talk to people more. I would make more phone calls and digress, like asking someone about their family. I would be more interested in what people were thinking about what stresses they were under. When I managed in another plant without it, I had a better feeling of the human dynamics. Now we have all the data, but we don't know why. The systems can't give you the heartbeat of the plant; it puts you out of touch" (Zuboff, 1998 p. 326).

A firm's ability to generate trust through its internal structures and between its external trade alliances could be helpful fostering competitive advantage (Lane, 1998). Trust is seen to promote dependability, efficient product planning and the enhancement of quality management in internal business processes. The effect could presumably be the just-in-time delivery, good quality goods and services production thereby leading to efficient customer satisfaction. Therefore trust is necessary for the establishment of interorganisational networks against the conditions of varied organisational cultural practices and beliefs operating in competitive global, commercial environment where market uncertainties are high, product life is transient and unpredictability is the norm (Lane, 1998).

2.3 Information Security Awareness and the Public Sector

The Public sector identifies the part of a national entity entrusted with the duty of providing basic government services to the citizenry. The composition of the public sector varies from one country to another, but in most countries, the public sector includes such agencies as the police, military, Department of Urban Roads, Public Education and Healthcare among others. It is a well-known reality that the behaviour of a user is critical to information security (Cox et al., 2001). In line with this Denning (1998) advances the significance of training programmes as an integral aspect of defensive information warfare. Forcht, Pierson and Bauman (1988) discussed the significance of ethical awareness for information security and highlighted the role of people, their attitudes, actions and sense of right and wrong in dealing with issues of information security. The study proposed the design of strong foundation in terms of ethical awareness and vigorously reiterated the need to maintain this base. The intention is for organisations to heighten their information security awareness and countermeasures.

Furnell, et al. (2001) presented a prototype tool for information security awareness training. The tool was meant for employees to avail themselves of security training by providing an environment that permits them to simulate the introduction of security measures in a

number of pre-defined case study scenarios. The tool was expected to be particularly useful in small organisations where specialist knowledge is scarce and issues need to be addressed by existing employees. Furnell et al., (1997) discussed the need to promote information security issues within healthcare establishments. They argued that promoting information security in organisations requires information security awareness training. Furnell et al., (1997) proposed that all staff should be aware of disciplinary action resulting from non-compliance with the organisation's information security procedures.

Murray (1991) described some of the problems associated with poor Information security. He argued that the biggest security problems result from the incompetence of employees who do not understand the dangers connected with their actions. He emphasised the need for an organisational Information security awareness program to overcome this problem.

3.0 Research Methods

The section addresses the ways and means of the whole research effort. The procedural method is fundamental for outlining the scheme for grounding the various parts and procedures of the entire study (Grunow, 1995). In short, the methodology goes to a greater length at laying down a sturdy and robust validity of the outcome of the research undertaking (Yin, 2003). Research methodology outlines a general plan of how researchers go about providing responses to their questions (Saunders et al., 2009). The path to this methodological examination is followed with the aid of the three primary mechanics of human perception, namely, rationalism, empiricism and faith (Thieme, 2003).

Rationalism identifies reality by means of reason. Empiricism does so through a support on the senses of sight, touch, taste, smell and sound. And faith defines reality via the confidence in the authority of another entity. Using all three systems of perception in the data-collection process would be beneficial in the sense that 'rational proof and instruction do not fully exhaust the sphere of knowledge' (Gadamer, 2004 p. 21). Therefore appropriating all three systems in a methodological process would ensure a demonstration of consistent and logical thinking thereby effectively limiting the researcher from going arbitrary with his judgements; so that the conclusions would not be treated 'as a figment of my imagination'(Thieme, 2003 p. 2).

To this end, the following data collection techniques were adopted for this study. The aim is to better appreciate phenomena-in-context inquiries against the background of certain professionals' in their natural, operationally distinct but electronically connected environment and their cross-subjective predilections, this work mainly used qualitative data.

3.1 Direct Interviews

To develop detailed insights into information security awareness endeavours at GAS, face-to-face interviews were conducted with different stakeholders who were crucial to both information generation to its dissemination. This purpose was to understand how conscious these people were in dealing with sensitive information and the extent to which they

adopted mechanisms to minimise the risk of exposing such information to unnecessary intrusions and other security threats. Most of these interviews lasted up to an hour. The intention was not to make these respondents see the provision of these data as an extra responsibility, which has implications on the quality of data and also the extent of openness they are to provide such information.

3.2 Documentary analysis

Documentary evidence in the form of previous meetings that largely focused on security arrangements the GAS has put in place were also captured to enrich the qualitative data that informed the analysis of this work. Again, historical records such as previous memos, policy manuals and information security awareness training aids were also captured to build a general impression on how seriously GAS viewed security issues and the sort of significance attached to such matters.

4 Findings: Research Setting – Ghana Audit Service

The Audit Service of Ghana is a constitutional body under the direction of a seven (7) member governing board. The Service is headed by the Auditor-General who is mandated to audit the public accounts of all public sector organisations and public offices including Metropolitan, Municipal and District Assemblies, Public Corporations and Organisations established by an Act of Parliament and report the findings to Parliament. Audit Service is therefore the monitoring and accountability organ of the state, and the Supreme Audit Institution (SAI) of Ghana. The 1969 Constitution made it an oversight body to promote good governance, ensure accountability and transparency in the Public Sector and Article 188 of the 1992 Constitution reaffirms this position. Thus, Audit Service is the only institution mandated by the Constitution to monitor the use and management of all public funds and report to Parliament.

By Article 187(2) of the Constitution, the audit service carries out the following functions: The auditing of public accounts of Ghana which include the central government, ministries, departments and agencies, the judiciary or courts, parliament, metropolitan, municipal and district assemblies, the houses of chiefs and traditional councils, public educational institutions, governing bodies established with public funds such as corporations and other state enterprises. It also audits half yearly foreign exchange receipts and payments statement of the Bank of Ghana for the period ending 30 June and 31 December.

This apart, the audit service is also mandated by the 1992 Constitution via the Audit Service Act 2000 (Act. 584) to undertake a variety of audit activities which are consistent with international standards. These include: Financial Audit / Regularity Audit, Performance/Value for Money Audit, Forensic Audit, Environmental Audit, IT/Computerised Systems Audit and Payroll Audit.

Policy statement of GAS states that, "It shall be the responsibility of the Ghana Audit Service (GAS) IT Department to provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorised members of staff, and to ensure the integrity of all data and configuration

controls." This has led to many information security policies in the service, but with a lot of challenges.

4.1 Information-sharing practices at GAS

Article 187(5) of the 1992 constitution states that "The Auditor-General shall, within six months after the end of the immediately preceding financial year to which each of the accounts mentioned in clause (2) of this article relates, submit his report to parliament and shall, in that report, draw attention to any irregularities in the accounts audited and to any other matter which in his opinion ought to be brought to the notice of Parliament."
Policy statement of GAS states that, "It shall be the responsibility of the Ghana Audit Service (GAS) IT Department to provide adequate protection and confidentiality of all corporate data and proprietary software systems, whether held centrally, on local storage media, or remotely, to ensure the continued availability of data and programs to all authorised members of staff, and to ensure the integrity of all data and configuration controls." This has led to many information security policies in the service, but with a lot of challenges.

4.2 Categorisation of Information at GAS

All GAS information is classified into two key areas: GAS Public and GAS Confidential. GAS Public is information that has been declared public knowledge by someone with the authority to do so, and can freely be given to anyone without any possible damage to GAS' Systems. GAS' Confidential on the other hand contains all other information that is more sensitive, and should be protected in a more secured manner, such as development programs, audit reports that are not yet ready for press and other information integral to the success of GAS.
It can be seen that there is no clear way of securing information at GAS, and keeping backups as a way of guaranteeing confidentiality has its difficulties. Pen drives and other removable disk can be used but these may be picked by anybody which can leak confidential information. Sending reports through mails without encrypting it means that, it is still vulnerable to be accessed by external person. This breaks integrity and confidentiality of the information.

5 Discussion: Trust and Security Countermeasures

5.1 Tensions between Trust and Security Awareness

The importance of information security for an organisation like the Audit Service cannot be underestimated as they have to process data for the entire country. The researchers realised that majority of the staff find information security as a necessity at GAS. This

paper observes that with proper information security systems in place, it helps to trace users who may alter or misuse information at GAS. If there are no ways to trace people who alter any changes in the system, anybody will tamper with the records which will undermine the integrity of information. It is obvious that to point out that, systems of technology presents both benefits and challenges to the GIS outfit.

Proper administration of information security helps to prevent information fraud in the service. Because of systematic information security measures put in place by IT Officers, there is the need for personnel to enter alphanumeric passwords to gain access and entry into GIS data systems. This prevents unauthorised access to audit information enhancing, and in the process, enhancing confidentiality and integrity of information at GAS. Though there are some challenges in it as the information sent through e-mails are not encrypted, only information on the CDs are encrypted. Even when it is encrypted, the storage procedure is not safe from external attacks. This means information integrity and confidentiality cannot altogether be assured.

One interesting revelation about that this paper seeks to highlight is compliance with security procedures that goes to underscore the systematic security lapses that characterise most of the activities at GAS. This is exemplified in the following scenario: data security, level of access to users, exposure of confidential information, vulnerability to cyberattacks, loss of electronic files, USB keys and laptops, protecting sensitive information and ignorance about the sensitivity of data were some of the challenges of IS at GAS.

According to the interviewees, there are Closed-Circuit Television (CCTV) cameras in the Accra server room but GAS Kumasi is now trying to implement such security measure to protect information. This helps to monitor those who enter the server room and what they do there. The respondents also recounted the point about measures and processes in place to apply users' biometric data to give access into server room and the server. Interviewees believed that, if all these standards are implemented and followed, it will secure their information.

The reputational damage and distrust for the audit service in cases of information being tampered with are usually characterised by devastating consequences (Banerjee et al., 1998). This makes IS standard a very pertinent issue in GAS, despite this challenges, effort should be made to ensure information integrity and confidentiality. These standards as seen in the interview and the questionnaires are not followed which may be a contributing factor to these challenges. This has led to auctioning computer with hard disk in it as asserted by the IT officer in his interview. This raises a question on professionalism, image, integrity and confidentiality of GAS information. Despite these, the study revealed that, the service can boast of doing well in IS since from its inception there has not been any legal issue from their clients: they feel safe to release their information to GAS because; they have confidence and trust in the information security system at GAS as revealed in the study.

According to the IT Officer, there are CCTV cameras in Accra server room but GAS Kumasi is now trying to implement such security measure to protect information. Measures

are in place to use users' biometric data to give access into server room and the server. This shows how serious GAS is as far as their information security is concerned; since transmission of information to different stakeholders and department through e-mail are not normally encrypted. It is possible for third parties to gain access to anybody's confidential information either by wilful interception or accidental breaches. From the IT officer, efforts were being made to put measures in place to heighten and enhance security. Not only information on Compact Disk (CD) should be encrypted but those transmitted through E-mails such as notes and reports should also be encrypted to increase information integrity. There should be adequate training and education on information security to staff. Hopefully, they would get to appreciate the importance of information security, sensitivity of data and the probable danger when information falls into the wrong hands. Again, such a move is likely to profit the employees to meaningfully involve themselves in responsible information security practices since some kind of shared responsibility is inevitably required.

There should be proper compliance to security issues, standards and policies on information. The study revealed that members of staff do not comply with information security policies. This calls for management to have mechanisms in place to ensure compliance with these policies and standards by employees. Additionally, management of organisations should provide storage devices such as pen drives, external hard drives including official laptops and any equipment that is used to store data to officers. This is because many members of staff use their personal equipment for official purposes, which is a threat to information security. Authorities should ensure that, these machines are not sent home for personal use. Again no personal device that can store information should be allowed in their premises. This will prevent people to send confidential information outside the work place which can be accessed by an external person.

When computers are auctioned, the hard drive(s) are removed even if it is spoilt or formatted. This is because there are some advance software to retrieved information from formatted hard drive. It came out that, only information on Compact Disk (CD) is encrypted but those transmitted through E-mails such as notes and reports are not encrypted. To enhance information transfer within departments in an organisation, all information transmitted should be encrypted. Again, the encryption procedure should be improved to prevent unauthorised access to such information to protect the integrity and confidentiality of information. There should be proper backup system. Keeping backups on only one laptop and hard drive is not adequate looking at the weakness of technology. CCTV cameras should be installed in server rooms. Access to the server should also be improved by using biometric features like fingerprints as means of access into the server.

5.2 Concluding Thoughts and Research Implications

The aim of the paper was to explore information security in public organisations specifically, the Audit Service in terms of the information security policies, practices, as

well as challenges of securing information. The study strongly advances the point that the Audit Service, like most public organisations in the country, does not effectively manage their information. This situation was because the employees of the case institution have undesirably limited knowledge and understanding in information systems security issues or practices, let alone ensuring the security of such information. Secondly, the numerous challenges as well as difficulties encountered, presented the institution under study with the ominous task of effectively managing its data and information systems in a manner consistent with strong corporate image and goodwill. To this end, management of organisations such as the audit service has to seriously invest in its human resources so as to equip its personnel guard against a casual approach to sensitive organisational information with potentially harmful and image-denting consequences for, often preventable, information security breaches.

Again, it can be seen that the concern of GAS on information is to always make it available but not to secure it from external people. This is because no proper cryptography has been specified but concentration was on how to keep backups which is exposed to breaches of confidentiality and integrity. The limited scope of information security arrangements therefore constitutes a part of the broader challenge to what appears to be an abiding vulnerability to the audit service's information security systems.

Given these viewpoints, it is the considered opinion of the researchers for future research directions and orientation to be directed at private sector trust in information generation and dissemination. This should, presumably, provide the basis for striking a comparison between the public sector and its private counterpart to determine if the sense of urgency is the same in matters of trust and security awareness in their respective areas of operations. Part of future research directions can also focus on control to examine the extent to which trust can be supplanted by control in ensuring commendable security orientation in creating awareness of information sharing practices.

References

AVGEROU, A., CIBORRA, C., CORDELLA, A., KALLINIKOS, J. & LONGSHORE, S. M. 2006. E-Government and trust in the state: Lessons from electronic tax systems in Chile and Brazil. London School of Economics and Political Science.

AYTES, K. & CONNOLLY, T. A Research Model for Investigating Human Behavior Related to Computer Security. Proceedings of the 9th Americas Conference on Information Systems, 2003. 2027-2031.

BA, S. & PAYLOU, P. A. 2002. Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behaviour. *MIS Quarterly,* 26**,** 243-268.

BANERJEE, D., CRONAN, T. P. & JONES, T. W. 1998. Modeling IT ethics: A study in situational ethics. *MIS Quarterly,* 22**,** 31-60.

BARMAN, S. 2000. *Writing Information Systems Security Policies,* Indianapolis, New Riders Publishing.

BEATSON, J. Security - a Personal Issue: The Importance of Personal Attitudes and Security Education. Proceedings of the Sixth IFIP International Conference on Computer Security, 1991 North-Holland.

BERSCHEID, E. 1985. *Compatibility, independence and emotion,* New York, Springer-Verlag.

BERSCHEID, E. & GRAZIANO, W. 1979. *The initiation of social relationships and interpersonal attraction.,* New York, Academic Press.

BEZEMER, D. J. 2004. Trust: Forms, Foundations, Functions, Failures and Figures. MA, USA.

BRAY, T. 2002. Security Actions During Reduction in Workforce Efforts: What to do When Downsizing. *Information Systems Security,* 11**,** 11-15.

BREHM, S. S. 1992. *Intimate relationships,* New York, McGraw-Hill.

COX, A., CONNOLLY, S. & CURRAL, J. 2001. Raising Information Security Awareness in the Academic Setting. *VINE,* 123**,** 11-16.

DENNING, D. 1998. *Information Warfare and Security*, Addison Wesley.

FINE, G. & HOLYFIELD, L. 1996. Secrecy, trust and dangerous leisure: generating group cohesion in voluntary organizations. *Social Psychology Quarterly,* 59**,** 22-38.

FORCHT, K. A., PIERSON, J. K. & BAUMAN, B. M. Developing Awareness of Computer Ethics. ICIS, 1988 Helsinki, Finland.

FOUNTAIN, J. E. 2001. *Building the Virtual State*, Washington, DC, Brookings Institution Press.

FUKUYAMA, F. 1995. *Trust: The Social Virtues and the Creation of Prosperity,* New York, Free Press.

FURNELL, S., GENNATOU, M. & DOWNLAND, P. Developing Awareness of Computer Ethics. Proceedings of the ACM SIGCPR Conference on Management of Information Systems Personnels, 2001 College Park, MD, USA.

FURNELL, S., WARREN, M. & SANDERS, P. 1997. ODESSA: A new approach to healthcare risk analysis. University of Plymouth.

GADAMER, H.-G. 2004. *Truth and Method,* London, Continuum.

GOFFMAN, E. 1971. *Relations in Public: Microstudies of the Public Order,* New York, Basic Books.

GRANOVETTER, M. 1985. Economic Action and Social Structure: The Problem of Embeddedness. *The American Journal of Sociology,* 91**,** 481-510.

GRUNOW, D. 1995. The Research Design in Organization Studies: Problems and Prospects. *Organization Science,* 6**,** 93-103.

HANDY, C. 1995. Trust and the Virtual Organisation. *Harvard Business Review***,** 40-50.

HUFF, L. & KELLEY, L. 2003. Levels of Organizational Trust in Individualist Verses Collectivist Societies: A seven-Nation Study. *Organisation Science,* 14**,** 81-90.

KERN, H. 1988. Lack of Trust, Surfeit of Trust: Some Causes of the Innovation Crisis in German Industry. *In:* LANE, C. & BACHMANN, R. (eds.) *Trust Within and Between Organisations: Conceptual Issues and Empirical Applications.* Oxford: Oxford University Press.

KRAMER, R. M. 1999. Trust and Distrust in Organizations: Emerging Perspectives, Enduring Questions. *Ann. Rev. Psychol.,* 50**,** 569-598.

KRAMER, R. M. & TYLER, T. R. 1996. *Trust in organizations: Frontiers of theory and research,* Thousand Oaks, CA, Sage.

LANE, C. 1998. Introduction: Theories and issues in the study of trust. *In:* LANE, C. & BACHMANN, R. (eds.) *Trust within and between Organizations.* Oxford: Oxford University Press.

LEWIS, D. J. & WEIGERT, A. 1985. Trust as a Social Reality. *Social Forces,* 63**,** 967-985.

LEWIS, D. J. & WEIGERT, A. J. 1981. The Structures and Meanings of Social Time. *Social Forces,* 60**,** 432-462.

LUHMANN, N. 1979. *Trust and Power: two works,* Chichester, Wiley.

MAYER, R. C., DAVIS, J. H. & SCHOORMAN, F. D. 1995. An integrative model of organisational trust. *Academy of Management Review,* 20**,** 709-734.

MCALLISTER, D. J. 1995. Affect-and cognition-based trust as foundations for interpersonal cooperation in organizations. *Academy of Management Journal,* 38**,** 24-59.

MISHRA, A. K. 1993. *Breaking down organisational boundaries during crisis: The role of mutual trust.,,* Pennsylvania State University.

MISZTAL, B. A. 1996. *Trust in Modern Societies,* Cambridge, Polity Press.

MISZTAL, B. A. 2001. Normality and Trust in Goffman's Theory of Interaction Order. *Sociological Theory,* 19**,** 312-324.

MURRAY, B. Running Corporate and National Security Awareness Programmes. Proceedings of the IFIP TC11 Seventh International Conference on Information Security, 15-17 May 1991 Brighton, UK. 203-207.

NOOTEBOOM, B. (ed.) 2003. *Trust: Forms, Foundations, Functions, Failures and Figures,* Cheltenham, Uk: Edward Elgar.

O'LEARY, M., ORLIKOWSKI, W. & YATES, J. 2002. Distributed Work over the Centuries: Trust and Control in the Hudson's Bay Company, 1670-1826. *In:* HINDS, P. & KIESLER, S. (eds.) *Distributed Work.* Cambridge, Massachusetts

London, England: The MIT Press.

PUTNAM, R. D. 2000. *Bowling Alone: The Collapse and Revival of American Community,* New York, Simon & Schuster.

RICH, E. E. (ed.) 1948. *Letters Outward, 1679-94,* Toronto: Champlain Society.

SAUNDERS, M., LEWIS, P. & THORNHILL, A. 2009. *Research Methods For Business Students,* Edinburgh Gate, Pearson Education Limited

SCOTT, J. C. 1999. Geographies of Trust, Geographies of Hierarchies. *In:* WARREN, M. E. (ed.) *Democracy and Trust.* Cambridge: Cambridge University Press.

SHAPIRO, S. P. 1987. The Social Control of Impersonal Trust. *The American Journal of Sociology,* 93**,** 623-658.

SIMMEL, G. 1900. *The Philosophy of Money*, Routledge & Kegan Paul, 1978.

SIMMEL, G. 1964. *The Sociology of Georg Simmel*, Free Press.

SIMON, H. A. 1957. *Models of Man*, New York, Wiley & Sons.

THIEME, R. B. 2003. *The Plan of God,* Houston, Texas, R B Thieme, Jr., Bible Ministries.

THOMPSON, J. D. 1967. *Organisations in Action,* New York, McGraw-Hill.

THOMSON, M. & VON SOLMS, R. 1998. Information Security Awareness: Educating your users effectively. *Information Management and Computer Security,* 6**,** 167-173.

YIN, R. K. 2003. *Case Study Research: Design and Methods,* Thousand Oaks, SAGE Publications.

ZAND, D., E 1972. Trust and Managerial Problem Solving. *Administrative Science Quarterly***,** 229-239.

ZUBOFF, S. 1998. *In the Age of the Smart Machine,* New York, Basic Books, Inc.,.