Computers & Security, 20 (2001) 384-391

A Framework for the Implementation of Socio-ethical Controls in Information Security

C. M. Trompeter[1], J. H. P. Eloff[2]

[1] *Department of Computer Science, Rand Afrikaans University, colette@adam.rau.ac.za*
[2] *Department of Computer Science, Rand Afrikaans University, PO Box 524, Auckland Park, 2006, South Africa*
February 2001, Tel: +27 11 489-2847, Fax: +27 11 489-2138, eloff@rkw.rau.ac.za

Introduction

The advent of electronic business ("E-business", for short) has not only created an ever-growing demand for information security, but also given information security ("infosec", for short) a new dimension. The author of this paper has opted for the term "E-business" to be used in this context for the very reason that it encompasses the monetary transactions effected in and by an organization, as well as all its other commercial activities.

Organizations are privy to information that is deemed evermore valuable, not only to themselves but also to their competitors. In many instances, it is possible even to set a monetary value on such information. This has, naturally, created a clamant need to secure all such information, which has, in turn, led to the advent of infosec.

For many years now, securing an information technology ("IT", for short) environment has meant that infosec be addressed primarily from a technical viewpoint. Unfortunately, infosec has, for the most part, been reduced to the implementation of firewalls. More recently, however, the functional aspects of infosec have come to the fore. In terms of this trend, many organizations have decided to employ IT managers in a bid to exercise some form of managerial control. As a result, these IT managers would implement a common baseline standard to prove that the organization was, indeed, protected. In terms of this development, infosec was, therefore, approached from a business-functional viewpoint for the first time, as opposed to merely from a technical viewpoint.

Even though many people may find solace in the fact that infosec is addressed in both a technical and functional manner, its implementation must also take cognizance of ethical and human considerations. In this way, information could be secured so as to unleash the full potential of infosec to enrich jobs and to enhance productivity. Such implementation would, however, call for an in-depth investigation into infosec itself, particularly into the ethics involved. In terms of such

implementation, people will have to be placed at the centre of the equation, rather than at its periphery. The diagram below (figure 1) is illustrative of the ideal relationship between the technical and functional aspects and the socio-ethical aspects of infosec.

In the following, the author will attempt by means of an example to elucidate the need to put the ethical aspects of infosec on a par with its technical and functional aspects.

Supposing that a newly graduated programmer has just been employed to develop a computerised incubator [1]. Without either evaluating or testing the system properly, the newly appointed programmer's superior pressurises him/her to finish the job quickly. Management, too, is only too happy with its rapid development and sells the product to several maternity wards at hospitals across the country. The anomalies sustained in the software, however, lead to the death of several infants. The question that arises is this: who is to be held responsible? The hospital administrators in question have certainly acquired the systems in good faith, especially in the light of the fact that they are no IT experts in this field. The responsibility, therefore, clearly lies with the developer. The author trusts that this example illustrates the oft-times emotionally charged aspects of technology - especially the need for some form of ethical awareness and accountability.

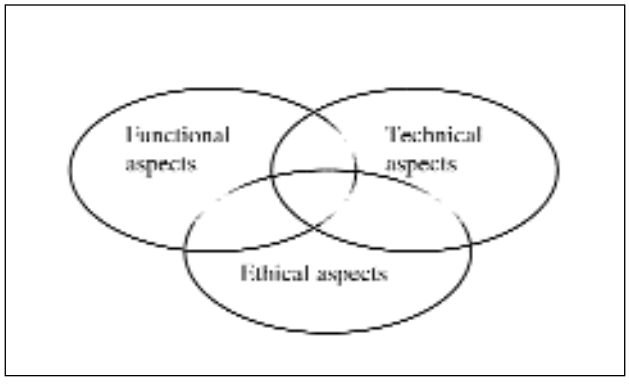

Figure 1: The equalization of the three fields of infosec

The clamant need for socio-ethical infosec awareness can, however, be best illustrated by means of an actual event. In October 2000, Microsoft suffered a breach of security with respect to its corporate network that had all the markings of a group of hackers attempting to penetrate its systems [2-5]. Security personnel were alerted to this illegal activity shortly after its occurrence and although they proceeded promptly to track the hackers' attempts to expand on their unauthorized access over a 12-day period, they could not be sure of the full extent of the breach. Rumour has it, though, that at least one valuable source code for a future product had been accessed. The question, therefore, remains: what are the full implications of that security breach for the organization? Could Microsoft be assured that no attempt had been made to alter the said product or to analyse it for some form of trapdoor through which to launch future security breaches?

Although they remain largely unanswered, the questions that arise from the above two cases, hypothetical and real, serve further to impress upon us the clamant need for creating and heightening socio-ethical infosec awareness within the IT environment of all organizations.

The remainder of this paper will be devoted to a discussion on the following questions:

- Where did ethics originate, what is its function and why does it need to be applied to the science of Infosec today?
- Will a pillar of strength be formed, should an organization decide to allow for and further a socio-ethical infosec awareness in its ranks?

In conclusion of this section, an example will be cited to illustrate the application of such a pillar of strength in any organization.

An Ethical Background

In 430 BC, one of the world's most famous philosophers first set out to define the term "ethics" [6].

Socrates succinctly defined the term as that state in which it is "conceivable to master pure virtue and achieve the ultimate truth".

His definition paved the way for a more recent and more widely used definition, as contained in *Collins English Dictionary*: ethics is "the dealing of moral questions and involves the conforming of a person to a recognised code" [7]. It is, therefore, a science in itself, as it deals with a system of principles and the rules of conduct of a person or an organization. In short, it can be summarized as a code of behaviour or a system of moral beliefs about what is right or wrong in accordance with the principles of a professional conduct.

How then, do society and ethics fit into the science of IT? "It is an area of study regarding what human behaviour is acceptable and what is unacceptable in terms of IT" [8]. Ethics could also manifest as a power struggle, with the one in the most powerful position having the upper hand, which is exactly where ethics is needed to protect those with less power or those unable to defend their rights.

The Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers (the IEEE) and the Data Processing Management Association (the DPMA) all are organizations that have developed codes of ethics for their members already [9-11]. Although membership of one of these organizations does not guarantee a specific level of competence, responsibility or experience in computing, it does guarantee a member's subscription to and aspiration to attain a certain level of competence, responsibility and experience. The ethics contained in these codes, therefore, form an excellent springboard for the analysis of all ethical issues that may arise in these organizations. In addition, they enable the information officer in each of these organizations to lay a professional ethical foundation in the organization and to tailor it specifically to suit that environment. Note, though, that these codes are defined for the software engineering field. We will presently show why it is vital to implement such viewpoints in the field of infosec too.

Before attempting to define the term "ethics" for the IT security realm, it is important first to define this for the infosec paradigm. In the latter context, this can be defined in terms of "the protection of assets against vulnerabilities that have been identified and the reduction or complete elimination of the threats to which information and information systems are exposed" [12]. The International Standards Organization has recommended that all secure systems adhere to five infosec services in order fully to secure the systems of an organization (ISO 7498-2), namely (i) identification & authentication, (ii) authorisation, (iii) confidentiality, (iv) integrity and (v) non-repudiation. These services are, for the most part, viewed as technical services that support mechanisms which, in turn, enable the implementation of infosec. It is also possible, however, to consider these services from a socio-ethical infosec awareness point of view.

The concept "socio-ethical infosec awareness" can, in its turn, be defined as "the conforming of an organization to recognized information security ethical principles". For the purposes of this paper, the latter principles encompass privacy, property and obligation. The onus, therefore, solely rests with an organization to create this socio-ethical awareness in every one of its members and among all its clients and affiliates. Furthermore, it must be the constant endeavour of an organization to incorporate socio-ethical issues with the inception, development and maintenance of its IT system. Organizations must be made aware of what behaviour is deemed acceptable and unacceptable under varying IT circumstances.

The selfsame socio-ethical infosec awareness must then be applied to all organizations implementing an IT product. This awareness should govern the expected IT security controls and measures that must be effected and taken in accordance with the infosec policy of an organization. This awareness specifically manifests in the understanding that both customer and organization must adhere to certain ethical principles. These principles include the right of both the individual and the organization to privacy, to property of their information and to the obligation to

uphold this socio-ethical commitment. Where then, does such socio-ethical infosec awareness fit into the organization specifically?

A Pillar of Strength

Each organization should adopt an information security policy that includes its viewpoint on socio-ethical infosec awareness issues. This policy can then be used to guide staff members as to, for example, the various ways in which to protect client information (privacy). Such policy should also inspire staff members to its adherence. In so doing, it will not only lend support to the infosec initiatives taken in the organization, but it will also provide a means of deterrence and a framework for disciplinary action, if and when required. By educating, guiding and supporting the staff members in this way, they are made aware of their obligation legally to adhere to the accepted code of behaviour in their organization. This process will serve to involve the clients and trading partners of the organization too, albeit by implication only, as they will also become aware of the socio–ethical infosec awareness policy of the organization and their obligation to uphold it.

The diagram below (figure 2) depicts a logical yet holistic approach to infosec management (ISM) in an organization. It also indicates exactly where the socio-ethical awareness of infosec issues fits into the organization.

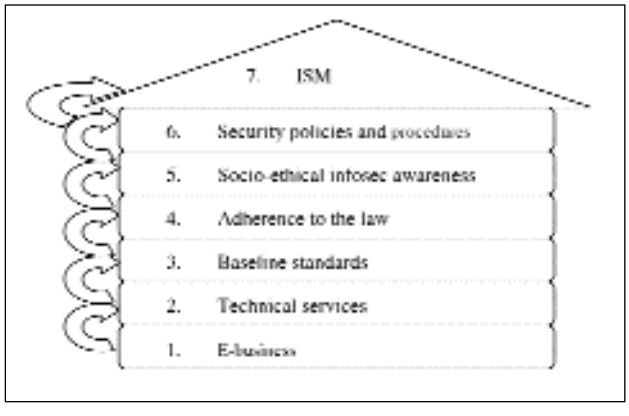

Figure 2: A pillar of strength

Figure 2 depicts an ideal organization in terms of the socio-ethical approach to infosec management. As is evident from the above structure, each block in the pillar builds onto the previous one, thus creating a pillar of strength for infosec. The various levels can be explained as follows:

- **E-business** - The first block constitutes the organization at entry level. At this, the very first level, there is a clamant need for protection against all outside intrusion. It is at this level, too, that the initial interface with clients takes place, thereby creating an almost insatiable need for security and security assurance. The organization, however, is obligated to provide such assurance to its clients.

- **Technical services** - The very next block up, representing technical services, already invokes certain technical issues. The technical services and mechanisms in this block can be put into place not only to protect the organization but also to provide a service to its e-business clients. These security mechanisms will, typically, include biometrics, intrusion detection systems (IDS) and firewalls.

- **Baseline standards** - How could an organization be assured that its protection is on a par with the minimum acceptable level? Every organization should, as a first line of defence, implement a certain baseline level of security assurance. In so doing, it could subscribe to any of the existing internationally accepted standards that many organizations adhere to already, such as the British Standard 7799, in terms of which a "baseline standard" has been defined as "the security level adopted by the IT organization for its own security and from the point of view of good due diligence" [12]. One such control, which could, for instance, be applied to intrusion detection systems, is as follows:

    - 9.7.2 Monitoring system use - unauthorized access attempts such as alerts from proprietary intrusion-detection systems, access policy violations and notifications for network gateways and firewalls.

The question that arises, however, is whether or not this would ultimately provide the necessary assurance to an individual or a trading partner; which brings us to the next issue, namely what is required by law?

- **Adherence to the law** - Unfortunately, the only sure thing in IT security is the very criminal element that induced its inception in the first place. To this block, therefore, people's need to know what their rights are and the punishment to be meted out if they were to transgress or infringe upon other people's rights. This block is strictly regulated, as the law requires that specific controls be put into place. In this way, the UK Computer Misuse Act of 1990 protects against all computer-misuse offences by protecting against unauthorised access to computer material; unauthorised access with intent to commit or facilitate commission of further offences and unauthorised modification of computer material [14]. The question, however, is whether or not the law amply provides for all such offences.

- **Socio-ethical infosec awareness** - As ethics is more situational and personal than the law, it does not have to change with time. Even if the courts were to side with you, however, you would not always want to resort to the law, as the legal process could be painfully slow, as well as emotionally draining and, above all, costly. It is vital, therefore, to have certain socio-ethical infosec controls in place. These controls may include the following aspects: privacy, property and obligation. Property of information would, for instance, constitute the right of an individual and an organization to ownership of all information about them or of all information that has been gathered at their expense. Often, property is also protected by law, such as copyright on program code. Privacy of information concerns the right of an individual or an organization to have its information deemed secret. Finally, an organization is obligated to adhere to these socio-ethical infosec awareness controls, as well as to follow through on the client's e-commerce wishes; in other words, the obligation, upon receipt of order and payment, actually to follow through with delivery of the required goods. This block in the pillar of strength exerts a profound influence on all preceding and subsequent blocks. The question that arises here, however, is whether or not all organizations do indeed incorporate such controls with their security policies.

- **Security policies and procedures** - The above-mentioned socio-ethical infosec awareness must be incorporated with the security policy of the organization. It must be made an integral part of the everyday procedures of the organization, as well as of its guidelines for good practice. Members must, in addition, sign a contract to this effect, thus acknowledging the socio-ethical infosec awareness policy of their organization. This will serve legally to bind them to it, especially in the event of their breaching it. This policy could also be made public, so that the clients and other trading partners of the organization would also be made aware of their obligation to uphold it.

- **Information security management (ISM)** - ISM is an involved and multifaceted science. It is vital, therefore, that any form of protection put into place in terms of this realm be closely managed. If managed correctly, the seven blocks that make up the pillar of strength shall ensure a safe, sound working environment for all parties involved.

Company_X has been Hacked!

Finally, it is important to illustrate the application of this model by means of an example. Supposing that a large and prominent company, Company_X, had suffered a serious breach of security on its corporate network, in terms of which newly developed software coding was hacked into, studied and possibly compromized. Although Company_X had since assured its clients that no vital information was revealed, the question remained: what assurance could Company_X give its clients that that was, in fact, the case? Information deemed vital to an

organization may not necessarily be valued equally by its clients. Another question that may be posed is this: if security standards were so poor for a major organization such as Company_X, how secure were its products? Although Company_X had assured its clients of the safety of both its information and products, clients might rightly ask questions as to the chances of such incident being repeated.

Furthermore, it is evident that, from a security point of view, Company_X has come up against the infamous ethical dilemma of hacking. Although the ethics of hacking (or lack thereof) is not covered in the scope of the present paper, the implications of such a security breach will be discussed. Company_X needs, in short, to assure its clients of the fact that their privacy will be guaranteed. Another socio-ethical implication that could be considered by the company is the piracy of its newly developed source code. Much time and money have been spent on its development and now, due to insufficient controls, that source code could have been stolen, which again illustrates the need to create and further socio-ethical infosec awareness both inside the Company and among its clients.

The figure below (figure 3) serves, once again, to indicate the various levels that must be managed and implemented correctly to secure an IT environment:

Following, a discussion on each step in creating such pillar of strength:

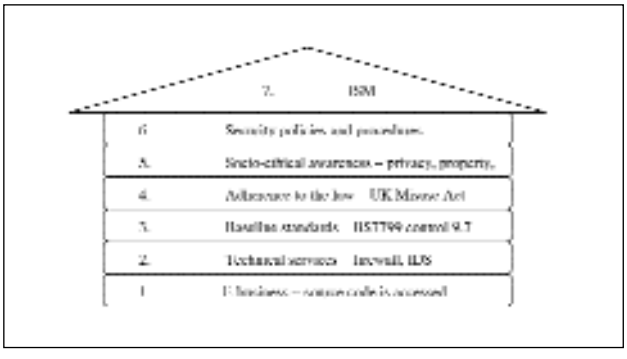

Figure 3: Company_X has been hacked!

- **e-business:** Virtually every business is connected to the Internet at present. The first level, therefore, constitutes the need for protection from all intrusion at a very basic level. In terms of our example, Company_X needs protection against the hackers accessing its corporate network. In addition, its clients need to be assured that their privacy will be protected. Company_X should, for this reason, also ensure that the interface used for trading with clients be rendered secure and tamper-proof.

- **Technical services:** At a more technical level, such system should adhere to the five infosec services of (i) identification & authentication, (ii) authorisation, (iii) confidentiality, (iv) integrity and (v) non-repudiation. One such mechanism that could be implemented to support the service of authorisation would, for instance, be a firewall, whilst another would be to install an access-control list in Win NT for all registered clients. Company_X should ideally have these mechanisms in place, along with other mechanisms such as an IDS.

- **Baseline standards:** Company_X should be able to guarantee its trading partners that they enjoy a minimum acceptable level of security, such as a certificate to prove that it has been audited by a BS7799 auditor and, in the present case, approved specifically for BS7799 rule 9.7 [13]. In this way, the system will be protected against unauthorized activities such as a false user trying to gain access to the system for malicious purposes. As access attempts made by false users are being monitored, the infosec manager will be alerted to suspect attempts without delay.

- **Adherence to the law:** Now that Company_X is aware of the illegal access to its information, what can be done about it? What law is invoked in the country in which the breach occurred? Even though the USA, UK and other countries will co-operate in extraditing IS offenders, it is important that organizations be made aware of havens where these hackers do, in fact, enjoy protection.

- **Socio-ethical awareness:** The law's arm, it seems, is not always long enough, which means that other, more stringent controls need to be put in place, such as controls for property of information. Even though, for example, the source code belongs to Company_X, that is no guarantee that its code has no latent trapdoors and that those hackers have not compromized it. The Company also needs to assure its current clients of the fact that their private information has always remained just that and that it has done its utmost to maintain the status quo. The Company is, in fact, obligated to reassure its clients in this manner. The clamant need to implement an IT policy is manifested in these socio-ethical infosec controls.

- **Security policies and procedures:** Company_X should include all of these aspects in its infosec policy, from a high to a low level. These aspects should be deemed an integral part of everyday procedures for all employees, as well as for all clients and trading partners. Company_X should, for instance, word its employment contracts in such a way as legally to bind its employees to the enforcement of stringent security controls.

- **Information Security Management (ISM):** Finally, Company_X would be fully secured, on condition that all of these aspects be implemented and managed correctly. It would have adopted a holistic approach to infosec management and it would enjoy protection from its weakest link - the human element.

Conclusion

The framework for implementing socio-ethical infosec awareness controls will assist organizations in creating an infosec awareness among all its members, clients, affiliates and other trading partners. The three socio-ethical infosec controls of privacy, property and obligation will be instrumental in establishing such awareness. Especially in today's electronic era, it has become vital to establish norms of behaviour for both organizations and clients. Individuals and organizations trading over the Internet must be assured of their rights to privacy, the property of their information and an obligation correctly and ethically to control such information. The creation of a socio-ethical awareness of infosec that takes cognizance of the human dimension will help organizations and clients alike to start comprehending the full impact of the electronic age on modern civilization, especially as we have, once again, proven to be our own worst enemies.

References

[1] Gotterbarn, Dr. COMPUTER PRACTITIONERS: PROFESSIONALS OR HIRED GUNS? Available online: http://csciwww.etsu.edu/gotterbarn/articles.htm

[2] Hancock, B. 1 Dec 2000. FEELING SORRY FOR MICROSOFT? Computers & Security. Elsevier Science Ltd.

[3] Uhlig, R. & Cave, A. Hackers open window on Microsoft's inner secrets. The Telegraph London. 29 October 2000.

[4] Computer News. Feb 2001. MICROSOFT HACK IS THREAT TO NATIONS. Computer Fraud & Security. ISBN 1361-3723. Elsevier Science Ltd.

[5] Hancock, B. 10 Jan 2001. HOWEVER, MICROSOFT COULD USE SOME SYMPATHY - DUTCH HACKER BUSTS MICROSOFT WEB SITE - AGAIN. Computers & Security. Elsevier Science Ltd.

[6] Beck, Sanderson. 1998. SOCRATES, XENOPHON AND PLATO. Available online: http://www.san.beck.org/EC21-Socrates.html#2.

[7] Collins Paperback English Dictionary. 1992. ETHICS. Harper Collins Publishers. England.

[8] Wombat. 2000. COMPUTER ETHICS. Available online: http://www.wombat.com.

[9] Gotterbarn, Dr. 2000. SOFTWARE ENGINEERING CODE OF ETHICS AND PROFESSIONAL PRACTICE (5.2). Available online: http://www-cs.etsu.edu/seeri/secode.htm.

[10] ACM. 2000. CODE OF ETHICS. Available online: http://www.acm.org

[11] IEEE. 1990. IEEE Code of Ethics. Available online: www.ieee.org/about/whatis/code.html

[12] Pfleeger, C.P. 1997. SECURITY IN COMPUTING. Prentice Hall, New Jersey. 2nd Edition.

[13] BS 7799. BS 7799 CODE OF PRACTICE FOR INFORMATION SECURITY MANAGEMENT. BSI 1999.

[14] COMPUTER MISUSE ACT 1990 (C.18). The Stationary Office Ltd. 1996. ISBN 0-10-541890-0.