THE EMERGENCE OF OBLIGATION RIGHTS IN ETHICAL INFORMATION SECURITY AWARENESS

CM Reekie

RAU Standard Bank Academy for Information Technology

cmt@rau.ac.za

27 11 489-3245

RAU

PO Box 524

Auckland Park

2006

ABSTRACT

As organisations become larger and increasingly complex, they become more reliant on their information systems and their employees. Therefore the securing of their information systems is paramount to the organisation's success along with the ethically correct behaviour of the organisation and its employees. However, how do organizations create and maintain ethically correct information security awareness within their organisation and among their trading affiliates?

Misuse of power, poorly implemented security applications, hyper reality problems, Internet scams are all examples of ethical information security infringements that occur within organizations. So much so that these infringements relate to the dire need for organizations to become aware of their ethical information security obligations. Obligation is a new area of concern in organizations and requires a new understanding among individuals and organisations. The creation of an ethical information security awareness is an obligation that rests on organisations. The principal aim of this article is to illustrate possible obligation problems that may occur in organisations and create an awareness of ethical information security obligation solutions among organisational managers and their trading affiliates.

KEY WORDS

Information Security Awareness, Ethics, Obligation, Legislation, Security Standards, Security Policy

THE EMERGENCE OF OBLIGATION RIGHTS IN ETHICAL INFORMATION SECURITY AWARENESS

1 INTRODUCTION

The principal aim of this paper is to create an awareness of obligation rights whilst maintaining an ethical approach to information security. Obligation rights within information security are a new area of concern and require a new form of understanding for organisations and individuals. Organisational managers are at a distinct disadvantage. The obligation vocabulary and its terrain are often *terra incognita* or, worse still, wrongfully equated with the implementation of information security. Security, with its attendant information security services of identification and authentication, integrity, non-repudiation and confidentiality, are necessary prerequisites for implementing ethical information security awareness obligation rights. Weak or inadequate security can easily compromise these obligation rights, but obligation entails more than merely providing these information security services; it entails an awareness of the consequences of breaching them.

The diagram below illustrates the ethical information security control of obligation, which will be the focus of this paper.

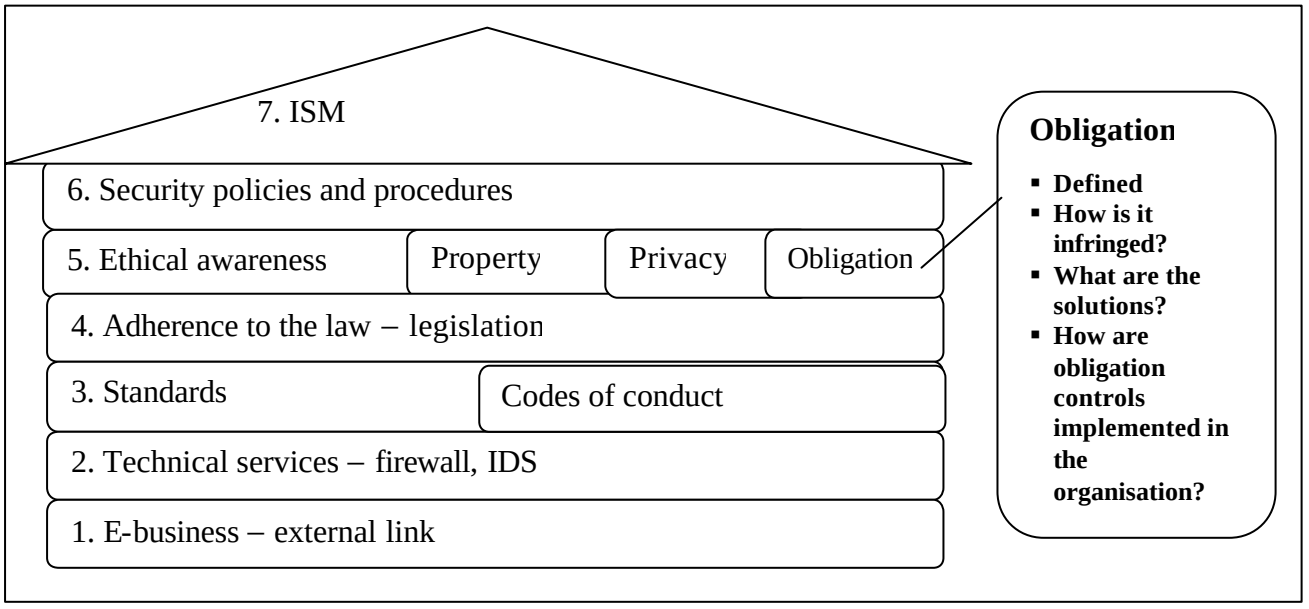

Figure 1 Ethical control of obligation

In order to create a pillar of strength within an organisation, the final ethical awareness control needs to be established. Many organisations have already implemented ethical awareness controls to protect intellectual property as well as protection of privacy. However there is a distinct lack of consideration for obligation rights. This paper will elaborate on how to create a pillar of strength in an organisation by focusing of obligation rights. To do so, a definition of obligation will be described first, followed by solutions to any form of breach to which organisations and individuals may be exposed.

2 OBLIGATION DEFINED IN TERMS OF ETHICAL INFORMATION SECURITY AWARENESS

In order to create an awareness, organisations and individuals need to understand the term "obligation". The *Oxford Dictionary* defines obligation as a constraining power of the law [OXFO 98]. In an electronic world, this definition is not sufficient. The International Chamber of Commerce has defined obligation as forcing an employee to adhere to the well being of an organisation regarding its information security policies [ICCO 97]. Therefore based on these two definitions, obligation can be defined in terms of the ethical information security control.

Obligation as an ethical information security control is defined as the creation of a commitment on behalf of organisations, trading affiliates and individuals to behave ethically and responsibly. In many instances, organisations attempt to maintain the goal of improving their image. However, this should not be their sole focus. They should focus on addressing the professional ethical obligation of those affected by the practice of the organisations, i.e. they are obliged to assist customers in an ethical manner as well as to keep their systems secure.

The above definition is best explained with the help of the following example. Two software engineers were expelled from the Association for Computing Machinery (ACM) for engineers for violating a section of the code forbidding remarks that are critical of other engineers. However, the question must be posed: What if they had been reporting the other engineers for the usage of inferior equipment in an incubation thermostat [GOTT 00]?

There are two ethically opposed scenarios here. The first is that these engineers were expelled for violating an ethically upheld oath, but they did so to protect the potential customers. The second is that these engineers infringed the other software developers' rights by making remarks about them and did not protect the software engineering profession above all else. Each individual would probably have reported these software engineers in a life-threatening situation. The fact that they were expelled shows that perhaps they followed the incorrect procedure for reporting these software developers.

Obligation entails the responsibility of all members of an organisation to uphold the organisation's policy regarding the safety of information. Employees should be legally and, more dependably, morally bound to perform their duty. In many instances several departments share the same information; therefore there is joint ownership of the data. This implies an obligation on behalf of the users to adhere to any constraints placed on them by the organisation. Obligation also implies a level of accountability for an action. All staff should be made to sign an information security agreement when they are employed by the organisation in terms of which they are then obliged to uphold that agreement. This agreement should be signed regularly by employees, as they may not remember certain clauses to which they have agreed.

The next section discusses all concerns relating to obligation and suggests possible solutions.

3 HOW ARE OBLIGATION RIGHTS INFRINGED?

How do organisations, government agencies and various virtual communities breach obligation rights? Once again, an extensive literature review revealed several methods [GREE 00] [SCHN 00] [ARNO 00]. These methods can be categorised as either technical or functional. It is interesting to note here that technical methods that have been grouped together often breach obligation rights because of a deliberate intent to cause harm. They consist of web sites and other programs that have been specifically developed to infringe the obligation rights of organisations or individuals. The infringement of obligation rights through functional methods involves the direct neglect of obligation policies. Infringement of obligation rights is not always clear-cut and there are often conflicting ethical opinions about a particular situation. Figure 2 summarises these methods.

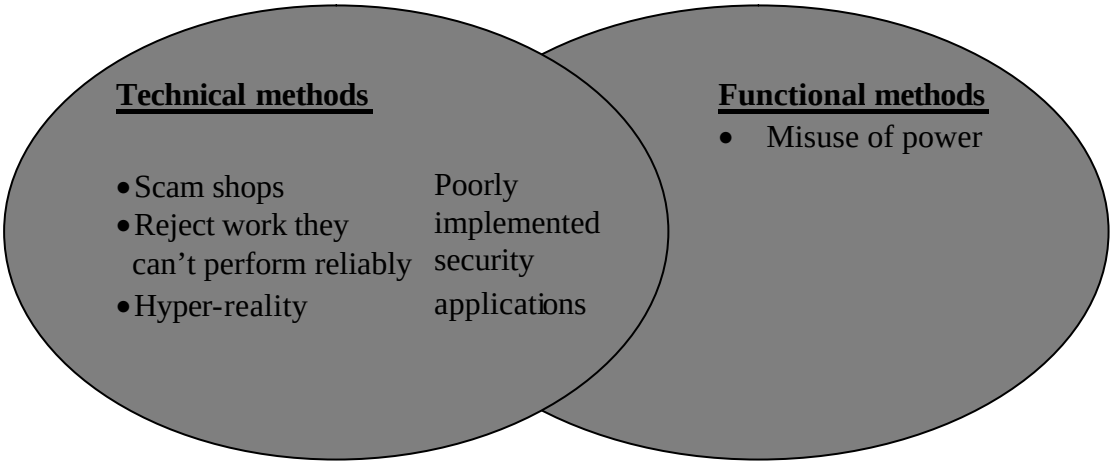

Figure 2 Categorisation of obligation infringement methods

3.1 Technical methods

These methods explicitly infringe obligation rights through the deliberate usage of programming code.

3.1.1 Internet Scams

Internet scams include the sale of Internet services, the sale of merchandise, the auctioneering of goods and services, as well as pyramid and multilevel marketing services and business opportunities. An example of a recent Internet scam is as follows:

> Subj: earns loads of cash
>
> From: TipToe
>
> To: Subscriber
>
> Hi I sent you this letter because of your email address was on a list that fit this category. With this new business, you can work from home and earn up to $20 000 a month! To find out more contact me at the following address. Registration into this wonderful opportunity is minimal. You can send cash or a money order to me.
>
> Send your order to :
>
> TipToe
>
> Attn: Mr Smith

The above example illustrates how easily uneducated or even totally ignorant people can lose money on unrealistic business propositions. E-mail listings are used to send out unsolicited information to a large number of recipients [GREE 00]. Many web sites have been set up to try to sell business opportunities to unsuspecting victims, but these sites are fraudulent in their objectives. They give out useless information after receiving the victim's money order. This in itself does not make the transaction illegal in that information has been exchanged for money. However, this is a gross infringement of the individual's rights. Obligation is viewed from two perspectives: the first is that the organisation is obliged to adhere to promises made to clients, and in this example this has not occurred. The second is that the organisation is obligated to protect itself. Surely firms will be discredited by potential customers if they fail to fulfil the customers' expectations? The Internet has a global span, so unfortunately the opportunity for Internet scams is great!

3.1.2 Acceptance of work that cannot be done

Many organisations are fighting tooth and nail for the contracts for software development that are out there [DPMA 00] [BOWE 00]. Some of them take on too much and often do not have the resources or expertise necessary to create this software. Organisations and individuals have a responsibility to produce quality software. A well known example of a breach of this obligation right to act responsibly is illustrated below:

> Students recently defeated the security of an ATM. They defeated the encryption system used by banks to protect ATM machines. PIN numbers and credit card numbers were stored encoded on these older machines by the DES encryption algorithm. Unfortunately this algorithm had expired in 1999, and the newer version was not updated and used .

This example shows how an organisation did not perform the correct maintenance of their machines, that is, the ATMs. They were obligated to protect their customers' interests. The software developers merely implemented the encryption system and did not take any notice of obsolete encryption algorithms. They were obligated to implement AES or 3DES encryption, but failed to do so.

3.1.3 Hyper-reality

The final form of technical obligation infringement is termed "hyper-reality". Individuals and organisations operate in an online environment in which they never come face-to-face with their customers. Operating in such an environment tends to cause organisations to forget that they are dealing with real people. A newsworthy example is as follows:

> "See you later!" I called out to nobody in particular. In the lift I called Lisa and told her I'd pick her up in five minutes. I put my phone back in my pocket and it immediately rang. I pulled it out and looked at it. Then I switched it off. It was time to run.

The above excerpt is by Nick Leeson, who describes the event of leaving Barings Bank with an estimated £830 million in losses. Leeson falsely invested this money in the stock market on behalf of Barings Bank. Having made his first loss of £20 000, he tried to cover up his mistake and continued to double the amount invested to recover his losses. The bank finally noticed the large irrecoverable loss. Leeson admits to not having comprehended the fact that the money he was "gambling" with was money belonging to actual people. He never met the people and never saw the actual funds. If he did not like what was happening, he simply ignored the trading losses, as to him everything seemed to be only a representation of a very real computer game.

Barings Bank had an obligation to their clients to keep firmer control over their finances. Leeson was also obligated to report his initial loss to the bank before it went out of control. As both of these factors were ignored, the customers lost millions and Barings Bank had to close their doors!

3.2 Functional methods

These methods infringe obligation rights through the direct neglect of obligation policies.

3.2.1 Misuse of power

There are individuals who are capable of developing tools that bypass controls installed by software manufacturers. Often these individuals have a grievance against large corporations and they violate the organisation's right to protect its development. Once such example is detailed below in which XP was cracked within hours of being released [CAMB 01].

Illegal installation files bypass registration system. This tool can be downloaded from warez sites.

Organisations have to protect their interests. Microsoft attempted to control the proliferation of unauthorised copies of their software by creating a registration system. However, hackers created software which bypassed this system and Microsoft now need to rely on enforcers of the law to help protect them and retrieve compensation for all losses incurred. Hackers should be obliged to act responsibly and to prevent tools that can harm organisations from being displayed freely.

3.3 Technical and functional methods

The combination of the two methods is a vital area that no organisation can afford to neglect.

3.3.1 Security applications poorly implemented

Few organisations and individuals regularly change passwords, which should be a minimum of 8 characters [WEBS 01]. Organisations should be obligated to inform staff members that they must change their passwords regularly. Organisations must also perform regular security checks on their systems and remove all users that have left their employ.

4 SOLUTIONS

Decisions made by organisations are based predominantly on economic rather than ethical considerations. The obligation rights of an organisation or of an individual are more difficult to assess. However, the solutions suggested below and illustrated in figure 3, should aid an organisation in implementing obligation controls that are both technical and functional.

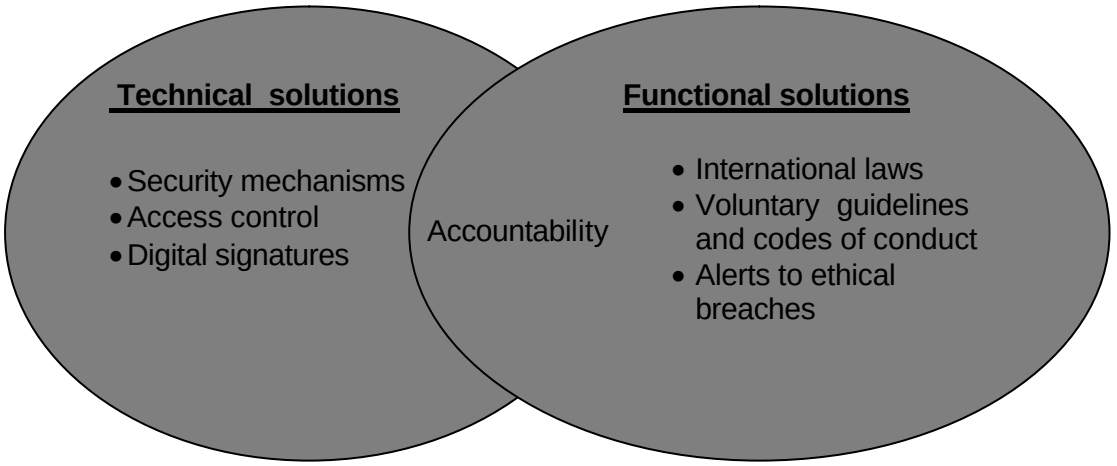

Figure 3 Categorisation of obligation infringement solutions

4.1 Technical solutions

These solutions centre around the use of technical mechanisms such as encryption.

Numerous security controls and mechanisms are used to protect the individual and mostly the organisation. All organisations are obligated to implement some or all of these controls and mechanisms [PFLE 97].

4.1.1 Access control

It is critical that organisations be aware of poorly implemented access controls to their systems. To protect their interests they must change passwords regularly. Their employees should be prompted to change their passwords once a month. Employees should also be aware of their obligation to actually change the password. Strong passwords are also vital for the success of the correct access control. Another key area that administrators of access controls must perform regularly is the correct removal of former employees from their systems.

4.1.2 Digital signatures

Digital signatures are a unique electronic mark that can be attached to an electronic message so that organisations and individuals can prove the source of the message. This helps to protect obligation rights as organisations are forced to deliver goods and services because they have legally signed a document. Digital signatures use public key encryption to enforce non-repudiation. This takes place as follows:

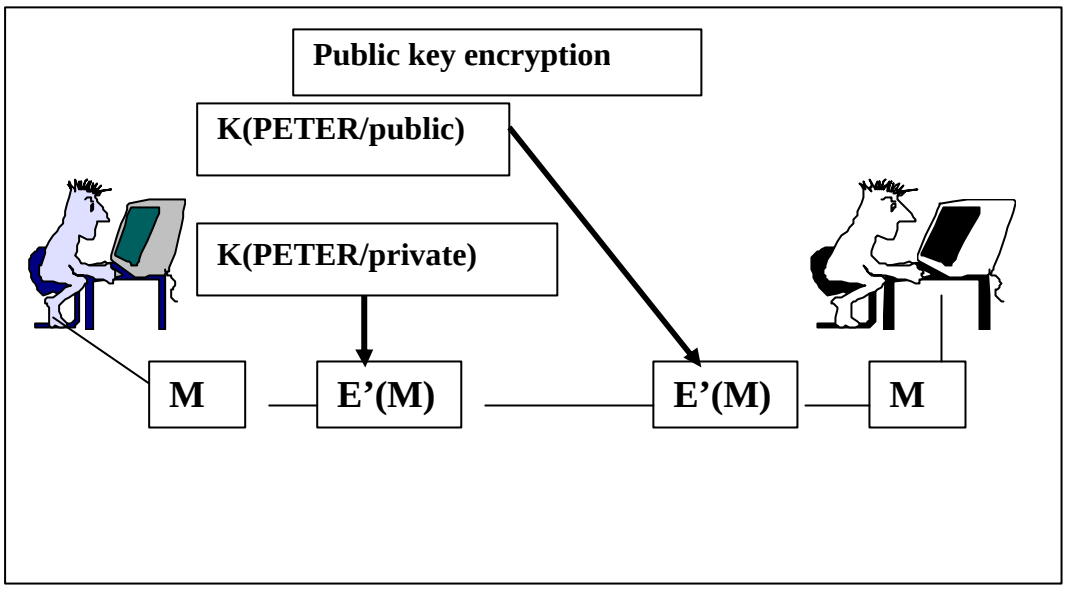

Figure 4 Digital signature using public key encryption [VSOL 99]

Figure 4 illustrates the use of a digital signature. Peter encrypts the message (M) with his private key, thus creating E'(M). This signed message is sent to Alice. Alice verifies that Peter was the originator of the message by retrieving Peter's public key and decrypting the message. Anyone can retrieve the clear text of the message as Peter's public key is freely available. However, only Peter is in possession of his private key. Therefore anything encrypted with Peter's private key must have come from Peter. This proves non-denial of a message, an important tool to secure obligation rights. In signing documentation, the originator of the message is obligated to deliver goods and services as promised and this will ultimately assist in creating a trustworthy environment.

4.2 Functional solutions

These solutions prompt individuals and organisations to act ethically and be accountable for their actions.

4.2.1 Voluntary guidelines and codes of conduct

Numerous codes of conduct and guidelines are available for organisations. In many countries employees must conform to a code of conduct before a company will employ them [GOTT 00]. These codes of conduct help to enforce an expected behaviour of professionals, who will be obligated to act ethically. Two such codes of conduct are the ACM and Institute of Electrical and Electronics Engineers (IEEE) codes of conduct. These codes will not be discussed here, however, it must be noted that these codes of conduct will help to resolve the issue of misuse of power by obligating the professional to act in a trustworthy manner.

4.2.2 International laws and regulations

Organisations and individuals need to know what their legal rights are and what punishment will be meted out if they infringe others' obligation rights to act responsibly. Organisations need to be aware of international as well as local legislation. As previously mentioned, the UK Computer

Misuse Act of 1990 has been used internationally by countries in an attempt to provide for protection against ill-intent methods [COMP96].

4.2.3 Alerts to ethical breaches

If an individual or an employee opens an e-mail attachment and immediately realises that they are looking at information that they were not supposed to see, what should be done? This is one of the most important obligation issues. The creation of a trustworthy environment is pivotal to the success of e-business partnerships. Organisations should assist employees in this situation by creating an awareness of obligations involved in these partnerships. If such an e-mail were opened, the employee is obliged to perform the following tasks:

- Alert the boss or employer immediately.
- The e-mail should be deleted from all backed up copies and archives that could have been stored by the organisation to monitor e-mail usage.
- It is probably wise to seek legal counsel!
- Take heed of the organisation's obligation policy.

An ethically correct principle and one that organisations should be obligated to adhere to is the notification of such a breach of information to the originator of the e-mail. Following the correct obligation policy will help organisations and employees understand the behaviour expected of them in these circumstances.

4.3 Technical and functional solutions

As with the infringement methods, it is necessary to define overlapping solutions that are considered to be a combination of technical and functional solutions.

4.3.1 Accountability

Organisations should be obligated to adhere to seal program standards institutions. It is vital that the security of the organisation as well as its ethical code of conduct be verified by an independent third party [ELEC 00] [ROSS 00]. This will force organisations to be accountable for their actions. Customers will have a degree of comfort in knowing that a third party has accredited this organisation and therefore they are obliged to behave ethically.

5 IMPLEMENTING OBLIGATION CONTROLS IN THE ORGANISATION

The ethical information security awareness control of obligation is a complicated process for organisations. Organisations need to implement the correct obligation controls. Once again they need to reengineer their information systems and information handling practices. Five stages of obligation policy implementation for reengineering an organisation have been identified. These stages describe the “what” of implementing a reengineered obligation policy controlled system. They are described in the following table as:

	Stages	Description – What must be done to implement a obligation policy?
1	**Obligation policy development**	Active involvement from government institutions, virtual communities and individuals is needed for development. Initiated through a response from these participants.
2	**Intellectual obligation handling assessment**	IT department and the user departments must be trained and made aware of all legal and obligations that this organisation ascribes to. They must identify all procedures for the handling of information.
3	**Compliance and risk assessment**	A comparison must be made of the actual ethical procedures in the organisation with that which they are obligated to uphold as stated in the organisation's obligation policy. Is there a discrepancy with how it is approached to how it should be resolved?
4	**Enforcement**	If there is a discrepancy, there should be an enforcement and upgrading of their obligation policy, in line with the actual procedures.
5	**Monitoring and auditing**	All future transactions should be monitored for compliance to the upgraded obligation policy.

Table1 The implementation of an obligation policy in an organisation

Adopting these five stages to will help to correctly assess, develop and monitor all issues to which the organisation is obliged to conform to. Unfortunately, for each stage there is an implication. This next table describes the "how" of developing a reengineered *obligation* policy.

	Stages	Implication – how can this be achieved?
1	**Obligation policy development**	It is necessary to design a clear, effective and comprehensive obligation policy so as to gain support for this new form of policy development from employees within the organisation, its trading affiliates and its customers.
2	**Intellectual obligation handling assessment**	Information handling practices must also be digital. If obligation policies are in a digital format, such as XML, it is easier to assess the information handling procedures based on written versus practiced procedures.
3	**Compliance and risk assessment**	These obligation policies must be modelled with the actual practice of handling intellectual and tangible obligation so that true gap analysis and conflict identification can be identified
4	**Enforcement**	It is necessary to include intelligence into the systems so that there will be some degree of automation and adaptation to this changing obligatory environment.
5	**Monitoring and auditing**	Standards and legislation will govern the implementation of an obligation policy. Interoperability among standards will assist in the further monitoring and implementation of obligation policies within the organisation as well as among organisations.

Table 2 Implication for each stage of obligation policy development

For an organisation to be able to understand this new outlook on their ethical requirements, will be a mammoth achievement.

6 CONCLUSION

This paper argued that a set of ethical obligations, based on an organisation's responsibility to the client, can be created. Obligation consists of an organisation's responsibility to fulfil a customer's request, as well as its responsibility to itself to protect its interests. The awareness of protecting obligation rights must be created. This awareness will also help with the implementation of countermeasures to control obligation infringement. This paper has evolved the development of an organisation's information security management to include the implementation of an obligation policy.

7 REFERENCES

[ARNO 00] Arnold, Tom. 2000. INTERNET IDENTITY THEFT. SIIA. Available online: http://www.siia.net.

[BOWE 00] Bowen, J. 2000. THE ETHICS OF SAFETY CRITICAL SYSTEMS. Communications of the ACM. Volume 43, issue 4.

[COMP 96] COMPUTER MISUSE ACT 1990 (C.18). The Stationary Office Ltd. 1996. ISBN 0-10-541890-0.

[DPMA 00] DPMA. 2000. THE DPMA. Available online: http://www.dpma.org.

[ELEC 00] Electronic information report. 2000. SEAL PROGRAM TO ADD BITE TO HI-ETHICS ETHICAL PRINCIPLES. Electronic information report. Volume 21, issue 45.

[GOTT 00] Gotterbarn, Dr. 2000. SOFTWARE ENGINEERING CODE OF ETHICS AND PROFESSIONAL PRACTICE (5.2). Available online: http://www-cs.etsu.edu/seeri/secode.htm.

[GREE 00] Greenstein, Feinman. 2000. ELECTRONIC COMMERCE. McGraw-Hill, Singapore.

[ICCO 97] International Chamber of Commerce. 1997. General Usage for International Digitally Ensured Commerce. Available online: http://www.iccwbo.org/home/guidec/guidec.asp.

[OXFO 98] The Oxford Dictionary. 1998. PRIVACY. Cape Town University Press.

[PFLE 97] Pfleeger, C.P. 1997. SECURITY IN COMPUTING. Prentice Hall, New Jersey. 2nd edition.

[ROSS 00] Ross, B. 2000. SO YOU WANT TO BE AN ETHICAL MANAGER? Available online: http://www.cw360.com.

[SCHN 00] Schneier, Bruce. 2000. SECRETS AND LIES – DIGITAL SECURITY IN A NETWORKED WORLD. John Wiley & Sons, Europe.

[VSOL 99] Von Solms, S.H., Eloff, J.H.P. 1999. INFORMATION SECURITY. Available online: http://www.osjspm.org/cst/q_ca.htm.

[WEBS 01] Websense. 2001. HOW TO STOP PIRATED SOFTWARE. Computer Fraud and Security. Volume 2001, issue 12.