SOCIAL ASPECTS OF INFORMATION SECURITY

Evangelos D. Frangopoulos[1 *], Mariki M. Eloff [1 **], Lucas M. Venter[1 **]

[1] School of Computing, University of South Africa (UNISA).
[*] 215, Alexandras Avenue, Athens, GR 11523, Greece.
Tel./fax: +30 210 6428-483. eMail: vfrangopoulos@hol.gr
[**] TvW 8 Theo van Wijk Building, UNISA, Pretoria, South Africa.
Tel.: +27 12 429-6368. eMail: {ventelm,eloffmm}@unisa.ac.za

ABSTRACT
Social Engineering (SE) threats have constituted a reality for Information Technology (IT) systems for many years. Yet, even the latest editions of the generally accepted Information Security (IS) standards and best practices directives do not effectively address the Social Engineering aspect of IS defences.

SE attacks target the human element of IS by exploiting human relations to the maximum possible extent. The social relations between interacting individuals who are involved in an Information Security Management System (ISMS) structure, combined with the frequently unpredictable fashion that humans act and react to stimuli, provide opportunities that Social Engineers may and do exploit. In the ongoing effort against Social Engineering attacks, if the social elements of IS are ignored, fallacious working assumptions may be made. These inadvertently result in the creation of insufficient controls against identified SE threats. Hence, simply put, Information Security scientists can no longer afford to ignore the nature of the social structures that govern all aspects of human relations, and in particular those that lie within the context of an ISMS.

This paper attempts to strengthen the pursued research on SE threat identification and control, by applying sociological principles to IT and ISMSs, thus bringing into the light their nature as social structures. This constitutes part of a larger effort by the authors to systematically identify and subsequently cater for SE threats to IS, in the context of which the social foundations of IS are examined.

www.manaraa.com

KEY WORDS
Information Security, social aspects, social engineering, ISMS, objective reality, subjective reality, Actor-Network Theory, black box

www.manaraa.com

SOCIAL ASPECTS OF INFORMATION SECURITY

1 INTRODUCTION

Social Engineers are frequently successful in exploiting the social relations between the individuals who operate within the context of an Information Security Management System (ISMS) structure, aided by the sometimes unpredictable fashion that humans act and react to stimuli. Although great effort has been invested in forming Information Security (IS) standards and procedures, these, so far, prove inadequately equipped to ensure Information Security against Social Engineering (SE) attacks. It is stipulated that the design flaws do not result from the standards' structures being technically incomplete. Despite being complete from a technical viewpoint, Information Security standards do not encompass provisions for the idiosyncratic nature of the human element, especially within a social context. By providing some insight on the social mechanisms at work in the development and function of an ISMS, certain design flaws of the related standards and procedures may be brought to light and steps be taken towards rectifying them.

The average person's notion of *Information* Security stems from the general idea of Security. Security in general, on the other hand, has been traditionally related to the police, law enforcement, the military etc. In many modern languages, even the word for "security" is used to signify the police force in general or one of their main branches dealing with public safety. Furthermore, whenever and wherever it was needed, security has always been applied in a stern, bureaucratic way, actually taking advantage of bureaucracy and the hierarchical structures associated with it. By using such hierarchical structures, the application of security is achieved through regulation and control (Foucault, 1989, p.65). This mentality is accurately expressed in the age-old saying: "*To trust is good but to control is better*". The idea of security has been applied to material and immaterial issues alike since the birth of the first human societies. Be it the protection of gathered sustenance supplies and, later, capital (material) or the protection of information and even life itself (immaterial), security against the ever-present foe has been one of our most basic needs. As the bureaucratic

www.manaraa.com

application of security has constituted standard practice for a long time, long before the arrival of the computer, it was the obvious step forward to achieve the security of (non-computerised) information in the same way. Furthermore, with the evolution of computer systems as information-handling devices, the existing principle was simply extended to include Information Technology (IT) Security by adding more appropriate controls.

It can thus be safely deduced that any modern ISMS implementation still relies on bureaucracy for its fundamental functions. It could even be argued that a bureaucratic structure through which regulation and control are applied, is a necessary pre-requisite for an ISMS to exist, on the assumption that the imposed technical and physical controls can mitigate all identified risks. However, it must be stressed that the current bureaucratic system was conceived, defined and described by Max Weber in the late 19th and early 20th centuries and still functions along the prescribed way (Bottomore, 1990, p. 203). This, in principle, should constitute an indisputable oxymoron as the futility of attempting to secure Information in the 21st century by using 19th century models and tools is obvious. Consequently, the controls existing within this context may prove inadequate in today's terms.

In the following sections of this paper an attempt is made to first establish the ISMS as a social construct and then analyse it by applying traditional sociological principles to it. This is followed by the application of Actor-Network Theory (ANT) principles to the ISMS, in an effort to better identify those social aspects of IS that may help significantly the ongoing effort against SE attacks. In particular, section 2 discusses the current ISMS practices from a modernist viewpoint. In Section 3 the ISMS as a social construct is investigated. Sections 4 and 5 discuss the Objective and Subjective realities of the ISMS. Sections 6,7 and 8 approach ISMSs from an Actor-Network Theory viewpoint. Section 9 examines Powerplay within the ISMS and, finally, the concluding remarks are given in section 10.

2 CURRENT PRACTICE - THE MODERNIST APPROACH TO THE ISMS

Information Systems are designed and built in a purely deterministic fashion. They are created to bring order to organisations by forcing human actions to take place within the strict context and limits of ordered workflow

www.manaraa.com

implementations. Such strict implementations ensure that human actions are disciplined and unambiguous and that the results of those actions are predictable, clear-cut and exact and, if necessary, securely leading to further pre-defined actions.

In transcribing the processes of the analogue world into workflows for computer-based Information Systems, all uncertainty must be eradicated. The tools of the trade for such an accomplishment are business process analysis, flowcharts and, of course, Boolean logic. In this way, all processes and user actions are transcribed into algorithmic sequences of exact questions strictly requiring unequivocal "yes/no" replies.

All of the above ideally lead to the design and implementation of an Information System which has all ambiguity removed from it and is no more and no less than a finite-state system. All state transitions must be fully reproducible and all user actions must be clear and exact. Such an implementation would thus lead to business practices that are also clear, exact and deprived of all ambiguity. (The feasibility of such a system is unimportant for the present discussion).

As the Information Security Management System must form an integral part of the Information System, the above notions are extended to cover Information Security Management as well. The ISMS is thus covered by the same providence and governed by the same principles described above.

Stemming from the concept of Reason as this was set forth during Enlightenment (Mendelssohn et al., 1989, p.28), rational knowledge is assumed to possess an objective existence which is independent of the observer's posture. This forms the basis of Modernism (Deligiorgi, 1996, p. 18) which builds intellectual structures on rational knowledge and through these promotes innovation and progress. In the context of Modernism, the complexity of intellectual structures is anything but limited as even large-scale processes can be described through modernistic methods and principles.

Indubitably, Modernism has actually been the motive power behind the industrial revolution that resulted in modern technology. Information Technology is clearly modernistic as its very nature requires the observer to be detached from the system being observed. In their inspired paper, Low et al. (1996) argue that software engineering is at present solely viewed from a modernistic perspective. This principle can easily be expanded to

www.manaraa.com

encompass the whole of the Information Technology construct. IT Systems are thus confronted as objective entities that are exact, discreet, identifiable, predictable and independent from the observer.

This leads to Information Systems being viewed as machines that function in a precise, repeatable and predictable way.

Gareth Morgan, in his book "Images of Organization" (1996), discusses a number of ways to view and understand organisations which he calls "Metaphors". The first of these metaphors calls for the organisation to be viewed as a machine with interchangeable components, which is firmly set on a goal. According to this metaphor, human and technological components form a stable machine that operates in a repetitive, predictable and secure way. This is achieved by having rational actors make rational decisions with predictable, reproducible and unambiguous effects in a purely modernistic fashion.

For such a system to function, everything must fall in its place in a larger, well-described framework. Such a framework can only be created by the existence of processes that are governed by standardisation, control and regulation. The interlocking components of the machine are thus combined together according to a complex blueprint and their roles in the machine are fully prescribed.

Hence, all systemic issues are addressed in a default manner within procedures that result from the application of current analysis and design techniques to any IT-related project. Tools and techniques used in system analysis, such as top-down or bottom-up design methods, data-flow diagram methodologies etc (Schach, 2005; Whitten & Bentley, 2007) fully comply with the modernist approach. It must also be noted that all of the above are governed by strict standards leading to normalisation and making control, regulation and evaluation possible.

Furthermore, as businesses and organisations do not just rely on their IT department for number-crunching but are instead built around a skeleton and nervous system formed by that department, it is not unusual for global change and business process re-organisation to initiate within the IT department. The reason for such a decision is that IT is the one centre of operations that is de facto regulated and aligned to processes governed by standards, thus forming a solid and flexible platform to build upon. Information Systems thus tend to dictate the way that an organisation evolves and govern its responses to the ever-changing business demands.

www.manaraa.com

To drive the above points home, one only has to consider the various issues that lead to successful Information Security management by today's standards:

Use of rules and regulations aiming to provide a secure environment.
Commitment of everyone involved to a set of prescribed guidelines or policy. This in effect constitutes behaviour control.
Use of technical measures for controlling the application of (a) and the upholding of (b) above.
Use of non-technical measures to complement (c) above.
De facto existence of a technocratic elite of Information Security professionals that oversees the application of (a), (b), (c) and (d) above.

On closer inspection, the above list reveals three important issues:

First, the above points are by definition dealt with in ISO/IEC standards 17799:2005 (ISO/IEC, 2005a) -corrected and renumbered in July 2007 as 27002:2005 (ISO/IEC, 2005f)- and 27001:2005 (ISO/IEC, 2005b). This proves the modernist character of these standards which may well be inadequate for today's challenges.
Second, the above five points and perhaps more significantly point (e) show that an ISMS is indeed a social construct that has to be examined in detail.
Third, as a whole, points (a) to (e) above form the modernist blueprint for an organisation viewed as a well-oiled machine according to Morgan's (1996) metaphor of "*organisation as machine*" discussed earlier. Furthermore, these points conform to bureaucratic definitions as presented by Max Weber a century ago. Max Weber is assumed to have written "*Wirtschaft und Gesellschaft*" (Economy and Society) between 1910 and 1914. This work was first published around 1922, after the author's death in 1920 (Oakes, 1998) and has watermarked all organisational efforts ever since. Using the translation -obtained from L. Ridener's (1999) website- for "*Wirtschaft und Gesellschaft*" (part III, chap. 6, pp. 650-78), the first of the characteristics of bureaucracy is described as:

I. There is the principle of fixed and official jurisdictional areas, which are generally ordered by rules, that is, by laws or administrative regulations.
1. The regular activities required for the purposes of the bureaucratically governed structure are distributed in a fixed way as official duties.
2. The authority to give the commands required for the discharge of these duties is distributed in a stable way and is strictly delimited by rules

www.manaraa.com

concerning the coercive means, physical, sacerdotal, or otherwise, which may be placed at the disposal of officials.
3. Methodical provision is made for the regular and continuous fulfilment of these duties and for the execution of the corresponding rights; only persons who have the generally regulated qualifications to serve are employed.

As ISMSs currently adopt the above principles, their nature becomes fundamentally bureaucratic, thus causing a deficiency in the level of democratic processes within the organisation structure that are deemed necessary by prevailing trends in management. Bureaucracy pre-supposes strict hierarchical structures of a vertical nature while, today, the push is towards flat, horizontal organisational structures, the governing principles of which were described by Ostroff and Smith (1992).

According to Dhillon and Backhouse (2000), the fast progress of the electronic age and the evolution of IT have caused the emergence of new organisational structures. Consequently, the traditional hierarchical organisations are being transformed into loosely coupled networks that are characterised by co-operation on a horizontal level rather than hierarchical control in a vertical direction. As a result, direct interpersonal and inter-organisational communication, connectivity and the sharing of information have seriously augmented in volume compared to the time when the traditional organisational models based on hierarchy were solidly and exclusively in place.

Hence, the inadequacies of the current bureaucratically-built ISMS are bound to create opportunities for social engineers to thrive in. The assumption that all members of an organisation will play their ISMS-prescribed roles flawlessly during an attack, because of bureaucratic pressure, is wildly optimistic at best. Furthermore, bureaucracy may even hinder essential practices such as reporting of security-related incidents. This will come as a direct result of the inconvenience caused to the person reporting the incident by necessary paperwork etc.

3 THE ISMS AS A SOCIAL CONSTRUCT

Bruno Latour, in his two books, "Science in Action" (1987) and "Laboratory Life" (1986), among other things discusses how Science and Technology affect social constructs and how they are in turn affected by them. This strengthens the idea that all systems that are based on science and/or technology constitute social constructs and should be treated as such. An

www.manaraa.com

ISMS, comprising both human as well as technological components, is thus indeed socially constructed.

In their book "The Social Construction of Reality", which was first published in 1966, Berger and Luckmann (1991) provided one of the definitive works on Social Constructionism. The functionalist interpretations presented by Berger and Luckmann can be readily applied to the ISMS structure in an effort to analyse and understand the social construction of such systems, as has been attempted by Albrechtsen (2004).

Although it may sound oversimplified, for the purposes of this analysis it suffices to concentrate on the discussion of Berger and Luckmann on the dual nature of societal objective and subjective reality. The notion of **Objective reality** concerns the production and maintenance of a shared sense of reality. This reality is ultimately constructed through the processes of externalisation, habitualisation, institutionalisation and legitimation. On the other hand, **Subjective reality** according to Berger and Luckmann (1991, p.167) differs from objective reality in the sense that it refers to the reality "*as apprehended in the individual consciousness rather than on reality as institutionally defined*". In other words, subjective reality is the sense of the socially created objective reality that each individual human being acquires as its own (internalises). This acquisition takes place mainly through the process of secondary socialisation.

Through the application of Burger and Luckmann's principles to ISMS structures, some of the system's inherent shortcomings can be identified and perhaps catered for. In this sense it was decided to follow the same structure as the one adopted in Berger and Luckmann's (1991) book, in order to properly present the application of their principles to ISMSs.

Thus, the social construct of the ISMS as an objective reality and then as a subjective one, according to Burger and Luckmann's work, will be discussed in the next two sections.

4 THE OBJECTIVE REALITY OF THE ISMS: EXTERNALISATION, HABITUALISATION, INSTITUTIONALISATION AND LEGITIMATION

The first step in the social construction of Information Security objective reality is that of externalisation. **Externalisation**, is defined in (Berger & Luckmann, 1991, p.70): "*Human being is impossible in a closed sphere of quiescent interiority. Human being must ongoingly externalize itself in*

www.manaraa.com

activity". Externalisation as such, is an anthropological necessity originating from human biological pre-disposition. Human beings must continually externalise themselves through activity. Furthermore, (Berger & Luckmann, 1991, p.122): "*As man externalizes himself, he constructs the world into which he externalizes himself. In the process of externalization, he projects his own meanings into reality.*" The inherent instability of the human organism makes it imperative that humans produce for themselves a consistent and stable environment for conduct and social order in general. It is exactly such a need that is covered by the creation of an ISMS. Externalisation with respect to ISMSs has taken place through the evolution of the notion of security and the measures that are taken for ensuring it in general. As the threats particular to Information Systems were identified, it became obvious that if left uncontrolled, these threats would result in Information System chaos and disarray. As a result, action against the threats was taken by appropriate controls being applied etc. Hence, a computer user who decides to turn off and secure a PC when unattended, to set up password protection of files and systems or to make backup copies of a day's work is actually externalising.

According to Berger and Luckmann (1991, p.70), **Habitualisation** denotes the principle that "any action that is repeated frequently becomes cast into a pattern, which can then be reproduced with an economy of effort and which, ipso facto, is apprehended by its performer as that pattern". Human actions have an innate tendency to habitualise. Hence, all the actions that are taking place as a result of Externalisation with respect to ISMSs, eventually fall into a pattern that helps the individual go automatically through the motions necessary to apply essential controls. Thus, the simple examples of actions described above, after a certain point in time, are carried out as a matter of course. The user who free-mindedly decided to go through these motions, having established that these are good and effective things to do against data loss or compromise, incorporates them into a daily routine. This way, the necessity of such actions does not have to be re-examined every time they are carried out.

Habitualisation is the first and necessary step towards **Institutionalisation**. As can be found in Berger and Luckmann's work (1991, p.72), Institutionalisation "*occurs whenever there is a reciprocal typification of habitualised action*". They further go on to state that "*any such typification is an institution*" and that "*the institution posits that*

www.manaraa.com

actions of type X will be performed by actors of type X". Finally they claim that "*institutions further imply historicity and control*.". Habitualised actions regarding social relationships form the basis for the creation of institutions that in turn enforce action. The interesting turn takes place as the established institution is "*objectified*" by bequeathing it to the subsequent generation that did not invent it initially. For the new generation, this socially created institution appears as a fully objective reality and, as such, is taken for granted. This is why Institutions always have a history, of which they are the products. "*It is impossible to understand an institution adequately without an understanding of the historical process in which it was produced*" (Berger & Luckmann, 1991, p.72). Institutions thus, by definition, control human conduct by setting up predefined patterns thereof. Shifting back to the ISMS paradigm, Institutionalisation takes place when the actions of individual user(s) like the ones described above, give rise to and become parts of an Information Security Policy.

Legitimation is defined (Berger & Luckmann, 1991, p.110) as "a 'second-order' objectivation of meaning. Legitimation produces new meanings that serve to integrate the meanings already attached to disparate institutional processes". The purpose of legitimation is to explain and validate the existing institutions. This is an important process if the presence of institutions is to be seen by individuals as subjectively plausible. If this is achieved, then the institutions themselves become acceptable. Legitimation is viewed as a 'second-order' objectivation in juxtaposition to the 'first-order' objectivation. 'First order' objectivation denotes the process by which principal meanings are attached to the institutional directives themselves. Legitimation is thus a 'second order objectivation' process in the sense that through it, the institutional directives are explained and justified via the application of cognitive and normative elements. This means that through legitimation actors are told not only how things should be done but also why it should be so and what things are in the first place. In this sense, legitimation provides a balanced combination of knowledge and values. Legitimation in ISMS comes in the form of Information Security standards and guidelines. IS standards such as the prevailing ISO/IEC 27002 (ISO/IEC, 2005f), 27001 (ISO/IEC, 2005b), 13335 (ISO/IEC, 1997; 1998; 2000; 2001; 2004), 15408 (ISO/IEC, 2005c; 2005d; 2005e) and the like, by means of their existence, legitimise the institutional directives of IS. It must be highlighted though, that IS standards effectively incorporate a high level

www.manaraa.com

of formalism in IS management, at the same time bringing forth its bureaucratic nature that is largely based on control and regulation.

In order to better demonstrate how the creation of the social construct of the ISMS as an objective reality is effected, one may consider that aspect of an ISMS that deals with the protection of data against loss or corruption: the creation of backup copies of data.

Making copies of important documents must be as old as writing itself. It is at least as old as the ancient Egyptian civilisation. The fact that surviving hieroglyphics have been identified as copies of important legal manuscripts (University College London, 2003), shows that by making copies for safekeeping, the Ancient Egyptians externalised themselves by taking positive action against whatever they perceived as a threat that might result in the loss of important information. Quite interestingly, the control they created, i.e., making copies, has been very effective, as we are still able to obtain the data the ancient scribes tried to preserve thousands of years earlier. This externalisation, has changed in form over the millennia: During the middle ages it was monks who preserved whatever information they saw fit to preserve, by making elaborate, hand-written copies of it, and, later, typography made the production of copies even easier. However, in essence, the action of making copies of important information has always been the result of the same principal externalisation. It is exactly this externalisation that gave rise to the action taken by today's PC users, that of making backup copies of their computer data. The only difference from ancient times is that these data backups are now stored in electronic form.

In the given context, Habitualisation is portrayed by the fact that the need for data backup is never challenged. Data backup is nowadays considered necessary by any type of user and in any type of data processing system. Computer users routinely create backup copies of their data, and even those who don't, know that they should. Furthermore, computer systems can be programmed to automatically perform these routines with minimal intervention by the user. Again, not only these automated procedures are never challenged, but even more so, it is inconceivable not to incorporate such procedures in a system.

Subsequently, such actions and procedures are Institutionalised by being incorporated in an Information Security Policy. No Information Security Policy is complete without a section on data backup procedures. By being incorporated in an Information Security Policy, the data backup

www.manaraa.com

procedures -not just the principle of data backup- become part of the subsequent user generation's objective reality that is taken for granted and as such remains unchallenged.

Finally, by explaining and validating the institutionalised procedures in an IS standard or set of recommended practices, Legitimation occurs and the social construct of the creation of backup copies is complete.

By expanding the above example to cover all aspects involved in an ISMS, the socially constructed objective reality of the ISMS is effected.

5 THE SUBJECTIVE REALITY OF THE ISMS

As it has already been discussed, Subjective reality is that "version" of objective reality that is internalised by individuals through secondary socialisation. Berger and Luckmann (1991, p.150) define socialisation in general as "*the comprehensive and consistent induction of an individual into the objective world of a society or a sector of it*". Primary socialisation takes place during childhood. It is the process through which people first become members of society. Secondary socialisation is "*any subsequent process that inducts an already socialised individual into new sectors of the objective world of his society*". This is effectively the process of internalising institutional directives. Within this process, an individual acquires behaviours and knowledge that are specific to the role the individual is called to assume within the society. A typical example of secondary socialisation is the educational process.

To shift the notion of the subjective reality into the context of ISMSs, it must be first considered that the socially constructed objective reality of an ISMS has evolved from existing objective realities in the pre-computer era and the relevant security efforts. As such, it relies heavily on a bureaucratic infrastructure and in turn offers a number of Information Security solutions. The ISMS objective reality is internalised as a subjective reality by all those who actually follow the offered Information Security solutions. "Those who follow the offered solutions" can be identified as three major groups in any type of organisation: a) the Information Security professionals who are responsible for carrying out the ISMS development, design, evaluation, maintenance and operation, b) the Management and c) the end-users.

The three identified groups have differences in interests, perspectives, goals and agendas. It is these differences that warrant the division into

www.manaraa.com

groups. The segregation of the three groups is more important than it may be assessed at first, as it severely affects the secondary socialisation process and the way subjective ISMS reality is internalised by each group. As Berger and Luckmann put it (1991, p.158): "*Secondary socialisation requires the acquisition of role-specific vocabularies, which means, for one thing, the internalisation of semantic fields structuring routine interpretations and conduct within an institutional area*". Hence, different roles result in (or require) different role-specific vocabularies and may lead into a lack of common ground that the three groups can share. This, in turn, inhibits communication and co-operation between the groups. Berger and Luckmann (1991, p.158) give a good (and frequently adopted) example to clarify the point: "*a differentiation may arise between foot soldiers and cavalry*". In that example, the cavalry have their own language and employ their own methods for achieving their goal that the foot soldiers do not comprehend, as they don't need to. However, the foot soldiers have every confidence in the cavalry's actions that always get them out of a dire position.

In the case of the three groups involved in an ISMS structure (IS professionals, Management and End-users) the case is quite similar. Bearing in mind that in most cases the group of IS professionals is a subgroup of the organisation's IT professionals or a group that has evolved from IT, the Management rarely fully understands what the IS professionals do and how they do it. Nevertheless, management trusts the IS professionals with the 'crown jewels' of the organisation. Furthermore they assume that the IS professionals will keep the end-users in check with respect to Information Security. Again, management has a rather vague notion on how this is accomplished, generally assuming that technological measures applied by the IS professionals will do their work for them. Thus, it is not unusual for the IS professionals to be under-powered to carry out their work.

The disparity between the subjective reality internalised by the two groups, creates a serious gap of understanding between them with respect to IS. On the other hand, the end-users group view the Management group with respect to IS as being very remote and detached from practical issues, feeling that it is they, the end-users, that are overburdened by security measures and who are also frowned upon when something goes wrong. The end-users also view the IS professionals with scepticism, more-or-less as a 'necessary evil'. Although the end users do place their confidence in the IS

www.manaraa.com

professionals' abilities to help avoid disaster or rectify situations that have gone astray, they also view them as 'techno-mages' performing black art and not doing any 'real' work within the organisation, as the product of their work is neither always tangible nor consistent in volume. Sometimes, the IS professionals are compared to a cruise-ship's doctor who is not busy unless a crisis situation brews. The doctor is certainly not needed every hour of every day on the ship but when the need arises, it is absolutely essential that he is present. Again, mentality gaps with respect to IS are created between End-users and IS professionals as well as End-users and Management. Lastly, in the case of the IS professionals' group, the situation is also quite complicated. Sometimes there is a tendency to deal with Management on a competitive basis, always struggling for more of the power that is in principle denied to them. If that is not the case, there is always the case of differing mentalities as management officials view the world under a different light compared to computer engineers and scientists who usually fill the ranks of IS professionals.

To further aggravate things, when IS professionals have to deal with the inability and, worse, with the reluctance of members of the other groups to internalise the ISMS objective reality in the same sense as they do, the IS professionals may develop a tendency to dispraise the other groups as conglomerations of technologically ignorant people. The gap in the internalisation of the ISMS reality is thus enlarged and the common effort towards the mitigation of IS threats becomes even more difficult to achieve. (It is interesting at this point to note that what is described by Leiwo and Heikkuri (1998) as an ethical divide between hackers and IS personnel is really also a result of the differences in the two groups' subjective realities).

All in all, the above analysis provides the theoretical justification of what is being described as "*lack of IS culture*" in organisations. What is lacking though, is not IS culture per se but the common internalisation of the objective reality regarding IS. The push towards "*holistic*" security is based on the creation of such a common ground that is necessary to advance understanding and co-operation between the organisation's groups towards attaining the required level of IS. By attempting to establish an IS culture, what is in effect being done is moving towards bringing together the naturally diverging agendas towards IS of the different groups. This, though, can not be attained by simply bringing each of the groups to the same level of expertise that each of the other groups has attained in their respective

www.manaraa.com

fields. That would be a futile exercise, as experience is not easily or efficiently transferable.

As we currently stand though, differences between the groups within an organisation remain very severe and the main problem lies with the fact that each group can not identify with the methods and tactics imposed by the other group(s) with respect to IS. As IS professionals are responsible for IS within the organisation, they are the ones who set the pace by defining the essential directives and practices. The other groups although in theory are bound to follow the IS directives (top-level management commitment to the security policy is essential as is strict control of end-user compliance), in practice they usually fail to do so.

It is exactly this difficulty in common acceptance and internalisation of the security effort by all members of an organisation that creates innumerable security holes and provides social engineers with the opportunity for successful attacks.

6 ACTOR-NETWORK THEORY AND THE ISMS

In his "Science on Action", Bruno Latour (1987) brings forth the "Actor-Network Theory" (ANT) and in "Reassembling the Social", Latour (2005) redefines the notion of "the Social" and provides a fresh view of ANT as the "*sociology of associations*". ANT, considered as a subset of Social Constructionism, originated in the field of science studies. It is described as a 'material-semiotic' method used to map relations that occur simultaneously between people and/or objects (hence its 'material' nature) and between immaterial concepts (thus 'semiotic'). As a result, any system in the context of which the interactions between people, their ideas and their technological tools involve simultaneous material and semiotic relations, forms a single "*network*" for the purposes of ANT. The banking system is traditionally used as an obvious example to demonstrate a typical ANT network. Even everyday activities like driving to work every morning can be examined under the light of ANT. The network in that case comprises people, their behaviour on the road, their cars, the road network, the traffic regulations, the Highway Code and the interactions between all of those components.

In the Information Technology sector in general and in ISMSs in particular, interactive relationships exist between the management, IS professionals, end-users, technological solutions, equipment, security policy, bureaucracy, administrative practices and the experiences,

www.manaraa.com

behaviours and ambitions of all individuals involved. Therefore, the ISMS makes a prime subject for study from the ANT viewpoint. Tatnall & Gilding (1999) and Albrechtsen (2004) present strong cases for examination through ANT of Information Systems Research and Information Security Management respectively. Their arguments certainly hold true for the particular case of ISMSs under examination in the context of this work.

Latour's view of the world as a network of "*actants*" (human and non-human actors) connected by complex links and relations, makes ANT useful in examining the reasons behind the success or failure of systems, technologies, scientific theories and social endeavours, as the direct result of changes in their network integrity. ANT does not give answers to the question of why a network is formed in a particular fashion. It is rather a tool for examining how actor-networks get formed and subsequently either hold their form and integrity or fall apart. In ANT, one of the central issues is the study of the forces that hold the network together.

In the interest of clarity, a few points must be clarified before attempting to apply ANT to ISMSs regarding "*actors*" and the notions of "*black boxes*", "*inscription*" and "*translation*".

"*Actors*" are, first of all, assumed to lie within the network of relations. Second, all actors are assumed to be shaped through their relations with one another. Third, it is assumed that there is no difference in the abilities of actors, irrespective of their form, nature or function. Fourth, as soon as an actor engages with an actor-network it too becomes part of that network and is actively introduced in the network's web of links and relations.

"*Black boxes*" are used by Latour (1987) to describe an entity (material or immaterial, human or non-human etc) that has been thoroughly dealt with, examined and transcribed into a particular known function where the output is a direct and predictable result of its input. If x and y denote input and output respectively, a black box can be seen as the function $y = f(x)$. These black boxes can represent various constructs such as a) the actions of users in an Information System, b) a known and generally accepted theory or practice, c) applied technologies etc. Hence, actors in an ANT network can be considered as black boxes and whole networks can also be black-boxed and viewed as entities with specific input/output transfer functions. When "opening up" such a black-boxed network, it can be viewed as a collection of other, smaller black boxes interconnected to

www.manaraa.com

and interacting with one another. This notion helps both in employing a divide-and-conquer approach to dealing with ANT networks, as well as explaining the tendency of taking things "for granted".

"*Inscription*", according to Hanseth and Monteiro (1998, ch.6), "*refers to the way technical artefacts embody patterns of use".* In the same work, they also quote Akrich (1992, p.205) who makes the following statement regarding inscription: "*Technical objects thus simultaneously embody and measure a set of relations between heterogeneous elements*". Hence, Inscription is the process through which a 'pattern of use' or 'action' is coded or embedded in an artefact. However, this does not necessarily signify a strictly deterministic process. Artefacts can either be seen as "*determining their use*" or, on the contrary, be "*flexibly interpreted and appropriated*" (Hanseth & Monteiro, 1998, ch.6). Thus, inscription can be seen as the process through which, the designer's expectations including the desired form of future 'patterns of use' or 'actions' are involved in the development and use of the technology that is expected to enforce them. At the same time though, a feedback path exists as this technology definitively contributes in shaping the designer's expectations.

Insofar "*Translation*" is concerned, Latour (1987) postulates that in the context of ANT, stability and social order are dynamically and continually negotiated as a social process of aligning interests. This is achieved through "*translation*". According to Law (1992, p.366) translation "*generates ordering effects such as devices, agents, institutions, or organisations*". In simpler terms, according to Singleton and Michael (1993), translation is "*the means by which one entity gives a role to others*". Furthermore, in the context of Information Systems, "*In ANT terms, design is translation*" according to Hanseth and Monteiro (1998, ch.6), who go on to explain that interests of all actors involved in the network are translated into specific "needs" according to typical ideal models. Furthermore, the specific needs are translated into more general and unified needs that, through further translation, result into one, all-encompassing solution/system. When the solution/system enters production mode, it becomes adopted by the involved individuals by translating the solution/system into the context of their specific roles.

Translation is of paramount importance to the well being of ANT networks, as through the process of translation, the integrity of the network is maintained. This is achieved by the perpetual occurrence of translations

www.manaraa.com

along links, in order to maintain the network's functionality and thus ensure its success. As translations along the links pre-suppose communication among actors, the overall process of translation and communication leads to power relations among human and non-human actors. ANT is thus perfectly equipped to deal with power relations in ISMSs, something that can not be efficiently done using the frameworks discussed so far. This ISMS 'Powerplay' will be later discussed in detail.

7 BLACK BOXES IN THE ISMS

ISMSs are full of black boxes. This is primarily done in an attempt to break large and complex problems into smaller, more manageable morsels. Through the process of dealing separately with every individual vulnerability, devising an appropriate control for it and including this as a solution in the ISMS, the vulnerability and its control are effectively black-boxed. This black box is then assumed to have a known transfer function and as such it interacts in a predictable fashion with other entities in the ISMS, becoming effectively an actor of the ISMS network. Hence, in the context of an ISMS, technology constitutes a black-boxed actor in its own right.

From the ANT viewpoint, the users involved in the ISMS are also considered as black boxes. The conformance of their actions to the enforced directives is supposed to be unquestionable and their actions rational, governed by the ISMS rules and human logic. Thus, with an assumed stable transfer function, the black-boxing of human actors is complete. In the extended sense, groups of users with common characteristics and/or roles can also become larger black boxes that are more than the sum of their constituent individual user black boxes. The reason for this is that the black box for the group does not merely contain the user black boxes but, instead, also contains their relations and translations between them. From an ANT perspective, the user group is a stand-alone network which can nevertheless be itself black-boxed for the purposes of the larger ISMS network.

Expressing almost everything in terms of black boxes facilitates the breakdown of problems and the synthesis of a solution such as the one provided by an ISMS. The down side of this process is that simplifying assumptions must occasionally be made in order to "*close the lid*" on black boxes. In the ISMS context the most dangerous such assumption is that the humans can be viewed as rational actors -the equivalent of black boxes with

www.manaraa.com

known transfer functions. The fallacy in this assumption comes in total support of an earlier statement presented in this work in the discussion of the modernist view of ISMSs according to which "The assumption that all members of an organisation will play their ISMS-prescribed roles flawlessly during an attack is wildly optimistic at best".

The problem lies in the fact that according to ANT, if the operation (or transfer function) of a black box is proven to be inaccurate, the lid of the black box must be "re-opened" and the black box definition be revisited. Consequently, the links or relations of that black box actor with other nodes as well as the relevant translations running along those links must also be re-examined and amended. To aggravate things, the larger black box that contains the amended entities (smaller black boxes and the relations between them) must also have its lid opened and its operation re-evaluated.

This approach provides a more systematic view of the shortcomings of the modernist view of a mechanistically designed ISMS where all constituent parts are supposed to execute their function flawlessly in a fully predictable manner. It goes to prove that a wrong design assumption at the basic level of user behaviour may lead to the collapse of the whole system. The ISMS may fail to protect the Information if a single user in a critical position falls prey to the attacking Social Engineer.

The only way to avoid such design flaws as much as possible, is to constantly keep re-evaluating the validity of the user black boxes and be ready to re-define the black boxes to any extent required, in order to cater for their shortcomings. The current tendency is to bundle all users under the lowest level of generic incompetence with respect to Information Security and, based on that assumption, attempt to "idiot-proof" systemic functions and operation. This simplistic approach is definitely ignoring the following facts: a) that users are neither simple-minded nor ignorant by default, b) that users may indeed yield under the pressure of a Social Engineering attack but they can also be the only effective means of defence against such attacks and c) that the level of resistance of users against Social Engineering attacks can be raised through training and the promotion of a security-aware culture. By looking at user behaviour in detail, new black box definitions for users will arise, with more appropriate controls for user-related vulnerabilities.

One issue that ANT is particularly capable of analysing is the relation between technical and non-technical actors. In this sense, ANT can provide

www.manaraa.com

a really good insight of how technical measures can be used to control non-technical vulnerabilities. In other words, how technical measures can be employed to steer the users' behaviour in such a way that it becomes resistant to Social Engineering threats. Extensions of this notion can have many repercussions, one of which is that political decisions can be inscribed in any solution/system in the form of a technical measure able to actively affect the organisation's culture-building effort and direct the human element towards a particular goal.

Black boxes can also help in providing an insight on the (previously discussed) issue that was raised by Berger and Luckmann on the differentiation of role-specific vocabularies between groups (Berger & Luckmann, 1991, p.158) and the resulting lack of common ground, communication and co-operation between the groups. Individual group members actually view other groups as black boxes and do not attempt to "open the lid" on them.

In similar fashion, technological issues and solutions remain in tightly closed black boxes for the majority of users who simply assume that these black boxes magically "do their job". This may lead to overconfidence on the part of users. Hence, the users become complacent, lowering their level of alertness as well as their defences. This is not unlike what can be observed when a user installs an antivirus solution on a PC and automatically assumes that the PC is fully protected against all Internet threats. What most users do not realise is that this sense of protection may become a false one if, for example, the scope of the solution is not understood, if regular virus list updates are not carried out or if the users themselves take such actions that compromise the integrity and effectiveness of the solution.

Through the above discussion it is made clear that Actor-Network Theory, through the use of 'black boxes' a) comes in direct support of the corollaries of Social Constructionism regarding ISMSs, b) goes further into providing better understanding of the issues involved and c) may even lead the way into devising appropriate solutions.

8 INSCRIPTION AND TRANSLATION IN THE ISMS

The notions of Inscription and Translation certainly help in the formal analysis of phenomena present in ISMSs. It was stated earlier in this text that "Inscription is the process through which a 'pattern of use' or 'action' is

www.manaraa.com

coded or embedded in an artefact ". (An example of this statement can be obtained by considering how traffic rules are embedded in the traffic lights' patterns at a crossroad). In the case of the ISMS, the 'artefacts' of the previous statement are the technical and non-technical measures that are applied in an effort to reduce vulnerabilities. These artefacts ensure, among other things, that the human element of the ISMS behaves in a particular and predictable manner. In the context of the ISMS, a technical measure would be the use of passwords for logging-on to systems. A non-technical measure on the other hand would be the requirement for a user to not disclose and adequately protect his/her password and, on a different note, the administrative directives that govern reporting of possible social engineering attacks.

According to the already stated definition of translation by Singleton and Michael (1993), as "*the means by which one entity gives a role to others*", the above technical and non-technical measures seriously affect the behaviour of other actors (human users in this case) in the ANT-defined ISMS network.

For example, users are not accepted into a system if they do not use a password that uniquely identifies them and sets their rights properly on the system. Thus, the password infrastructure technical artefact defines the behaviour of the user to the extent that a password *must* be used. Having said that, the fact that a password infrastructure does exist as a technical measure, does not mean that users will not write down their passwords in obvious places or that they will not voluntarily share them and thus, in effect, compromise the system. If this technical measure is supported by the non-technical administrative measure of establishing serious penalties for such negligent behaviour, the overall result will indeed be better password protection.

On the other hand, assuming that a system-wide, password-strength checking algorithm is not in place, only a non-technical measure / artefact / directive may enforce the use of strong passwords. Such a non-technical measure also defines the behaviour of users, but to a different extent than a technical measure does. Directives of this type should be followed but, as practice shows, are not *necessarily* followed by all users.

The same holds true as far as SE attack reporting is concerned. There is no way that a user can be *forced* to take such reporting action. It is rather an issue of having convinced the users beforehand as to the importance of

www.manaraa.com

reports been filed in the case that a SE attack is suspected. Ultimately, unless this type of behaviour becomes the users' "second nature" in their everyday dealings, SE attacks will remain unnoticed. The responsibility for such a goal remains with the management that must promote the appropriate security culture and thus effectively establish yet another, very important, non-technical measure.

As standard procedure, when a new or amended security policy is effected, all office workers sign statements that they have been duly notified of this and thus the security policy is considered to be active. As organisations are feeling the pressure to adopt IT methods in order to become more efficient or more competitive, the integration of IT into the business process is not always a carefully planned one, especially with respect to security. Even if this is not so and the new security policy is indeed a carefully produced one, the hysteresis involved in the office workers' understanding and internalisation of the new situation, usually lies at the basis of the inefficiency or even of the de facto demise of any security policy. Office workers may well be acquainted with the security requirements governing physical access or those requirements relevant to protecting a filing cabinet. They usually, though, understand very little regarding the security of an IT system and consider this to solely be of interest to, as well as the responsibility of, the IT department. Having being notified of and having signed documents pertaining to the new security policy, does not actually make the average worker more security-aware neither does it help in altering the office workers' day-to-day activities towards achieving a higher level of IT security. Combining this with the fact that the average office worker is the first weak link that the Social Engineer will attempt to exploit on the way to the primary target, clearly demonstrates the gravity of the situation. Hence, once again, the need for the promotion of a security culture that appropriately caters for the IT-based organisational reality is brought forward as an indispensable non-technical measure.

Strong incentives and counterincentives can support non-technical measures, as can additional technical measures. An example of such a technical measure would indeed the upgrade of a system to include a password-strength-checking mechanism that rejects weak passwords.

Thus, technical and non-technical measures can come in efficient reciprocal support, effectively dissolving the idea that IS is either a purely technical or purely administrative issue.

www.manaraa.com

Furthermore, an ISMS that is realised under the assumption that users are rational actors, is probably doomed by design. The reason for such a failure is that the assumption of a fully rational and predictable behaviour by the human users involved, leads to the adoption of a minimal set of inscriptions. This would in turn produce inadequate or incomplete translations. Thus the deciding question in this case would be what the full set of inscriptions and translations for a given ISMS is.

Unfortunately, there is no deterministic way of identifying every potentially vulnerable aspect of an organisation and incorporating it in the design of an appropriate ISMS, especially when Social Engineering is factored in. On a more optimistic view though, more SE vulnerabilities can be identified if the diverging subjective realities of the users are acknowledged and examined.

From that point onwards, the greater the number of SE vulnerabilities that are catered for in the context of an ISMS, the harder it will be for the next Social Engineer to mount a successful attack, especially when the Plan-Do-Check-Act (PDCA) cyclic process for the ISMS' continual improvement is adopted.

The diagram of Figure 1 should help in visualising the effect that a correctly implemented PDCA cycle may have on the divergence of the users' subjective realities.

As it can hopefully be seen, the PDCA cycle causes the users to espouse more of the actual policy directives as their own subjective reality (hence the double-shaded area increases) and thus the opportunity for a Social Engineer to act, diminishes.

9 POWERPLAY WITHIN THE ISMS

Having dealt so far with the shortcomings of the modernist approach to Information Security and having identified the inherent difficulties stemming from the differences of individual groups within an organisation, it would be naïve to ignore the repercussions that the balance of power in the context of an ISMS has on its own functionality and effectiveness, as well as on the organisation in general.

www.manaraa.com

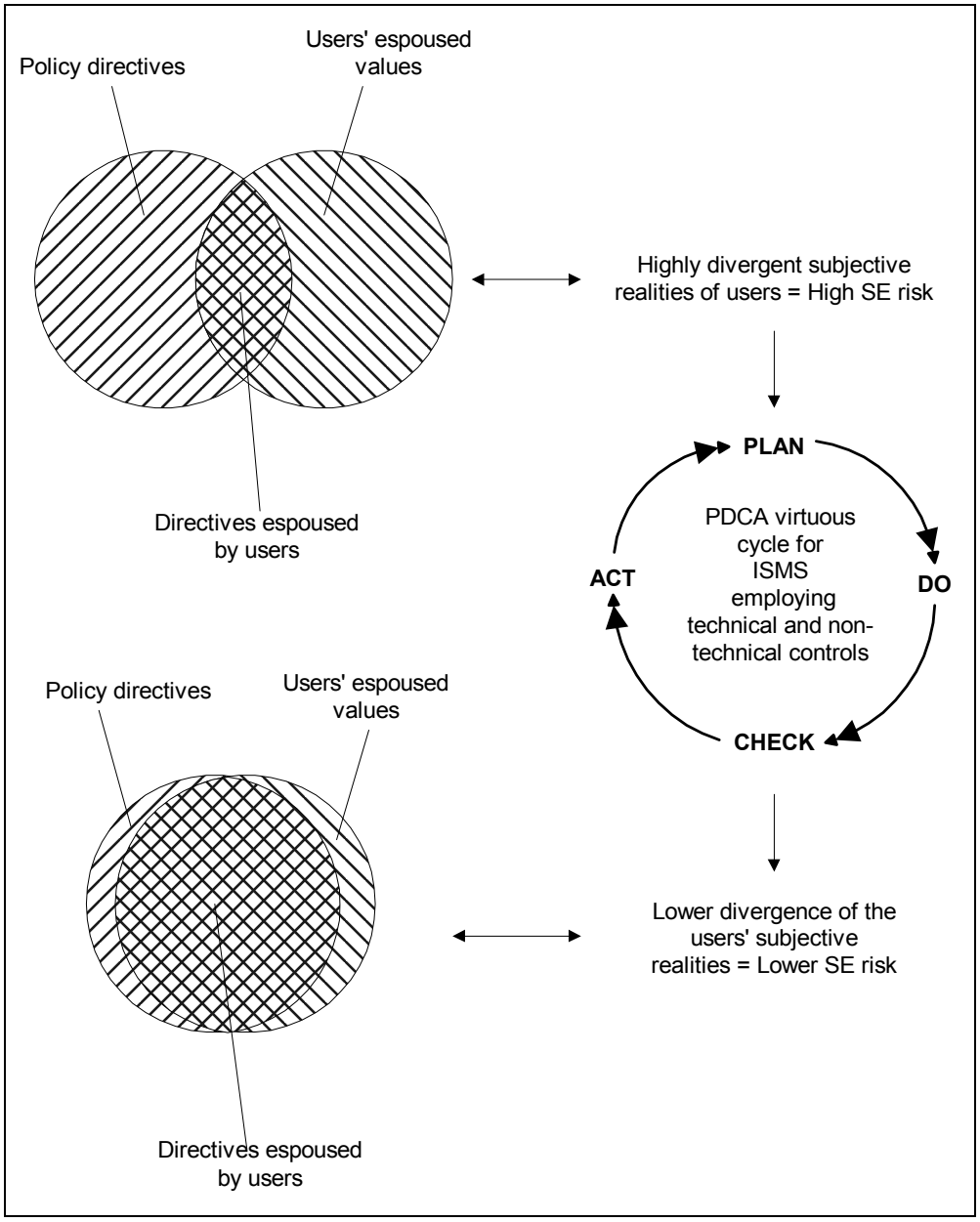

Figure 1: Effect of PDCA cycle on users' diverging subjective realities

www.manaraa.com

"*Power*" is generally accepted to be the ability of an individual or a group of people to realize their own will in communal action, even against the resistance of others (Giddens, 2001, p.420). In viewing the ISMS as a social construct, it has to be taken for granted that the individual groups involved in its operation will ultimately fight for power. The Marxist view is that the struggle for power always has economic motives and in particular the possession of goods and opportunities for income. Also according to Marx, a grouping of people constitutes a "*class*" and class action ensues, when a class becomes conscious of its interests, in the context of its relation, as a class, to other classes (Giddens, 2001, p. 669). Weberian theory gives a more refined view of power and classes that aptly conforms to any bureaucratic system, including ISMSs: According to Weber, the Marxist view of a single source for power is dogmatic. Instead of having motives of a strictly economic nature, Weber argues, that individuals seek power for its own sake due to its intrinsic values and the social honour it carries (Bottomore, 1990, p.238). This notion is then taken one step further and Weber sets the foundation for the "*politics of power*" (Doujon, 1990, p.13).

Regarding classes, Weber introduces an additional structural category, that of the "*status group*". Marxist classes are defined with respect to their place in the market or in the process of production. Furthermore, classes may or may not exist as communal groupings. In contrast to those, Weberian status groups are, in principle, communities formed and held together by commonly accepted values, shared beliefs, similar lifestyles and, most importantly, by the social status, esteem and prestige conferred upon them by others (Giddens, 2001, p.285). Thus, "*social distances*" are established between status groups. Furthermore, according to Weber, status groups are independent of class divisions. Status may vary independently of class.

When a status group gradually develops the idea that the magnitude of the social distance between it and the next superordinate group is too great and that it should be diminished or even nullified, conflict takes place. This conflict ultimately upsets the existing stratification until a generally acceptable equilibrium point defining subordination and superordination is reached. When such a point is reached, conflict subsides and tranquility returns, with members of groups accepting their position and assuming their place in the hierarchy. When the situation is such that warrants the ascension of a group to a higher status stratum, conflict eventually begins

www.manaraa.com

again and the cyclic procedure re-iterates itself. During the time of tranquility (which is the usual case), subordination tends to become more prominent. Under those circumstances, the members of the subordinate group tend to acknowledge the authority that the members of the superordinate group exercise over them. Furthermore, the members of the subordinate group usually become fearful of displeasing those that are higher in hierarchy than themselves. It is this fear of displeasing one's superiors that is frequently exploited by Social Engineers during their attacks.

What can be seen clearly at this point is the obvious need for an equilibrium point to be reached in the social distances between the groups. This equilibrium point should neither be unstable, thus leading to perpetual conflict between groups, nor predispose members of one subordinate group to carry out orders supposedly coming from their superordinates, in an automatic and mindless fashion. Social Engineers are very apt in using authority, fear and intimidation to their advantage and would thrive in either of the two situations.

In the particular case of the ISMS, the stratification phenomenon and the separation of the individuals involved into various users' groups, is justified not only by the divergence of the groups' interests, but also by the distinction in the life-styles, views of the world and postures of their constituents. As IS professionals seek the status and authority to carry out their mission, management group members fear that this may constitute a flanking attack against their own hard-earned status. The highly technical nature of the means employed by the IS professionals in the line of their work, is seldom fully understood by management. This makes members of the management group feel insecure and even aggravates the chance for conflicts between the groups.

Additionally, the group of IS personnel, frequently, does not occupy a clearly defined position in the organisation's hierarchy. In effect, this creates a two-fold status problem for the IS experts group. The first facet of the problem is that high-ranking officials may disregard the security-related control attempted by the IS personnel. This disregard can be passive, in the sense that high-ranking officials may simply ignore the efforts of IS personnel to control them, or active, through intimidation and commination of the IS personnel. Secondly, as long as the higher status of the management group in the hierarchy is undisputed, members of the

www.manaraa.com

management group may use the vagueness of the IS group's status to their advantage by discreetly fuelling the status struggle of the lower-ranking groups in the organisation, as part of a typical divide-and-conquer strategy that results in the strengthening of their own status. As a result, the members of the IS group are viewed by members of the other groups as 'floating' within the organisational structure, not having any particular role or real control over the other groups' members' actions. This fuels inter-group competition, and in effect further undermines the IS group's role while crippling the IS effort. A Social Engineer will definitely make the most of such a situation, either by using the weaker spots in the crippled security system or by actively (and carefully) assuming the role of a high-ranking official in order to achieve the SE objective through intimidation or by otherwise using the status of the assumed role.

The above analysis follows the modernist view of power and although useful in analysing the social structure of an ISMS, it would be unacceptable to ignore the post-modernist view of power that can also apply to ISMSs. The best known such view of power is presented by Foucault, a self-pronounced champion of post-modernism, throughout his works (1988, p.39; 1989, p.65; 2005). Foucault views power as one of many societal controls aiming at a variety of targets from production for financial gain to disciplinary systems to normalisation procedures, all the while being dispensed through historical institutions and exalted by definitions of normal vs. abnormal. Translating this into the reality of the ISMS, power can be seen as originating from the set of technical and non-technical controls that effectively influence the behaviour and actions of the human actors. In effect, power in the ISMS is stemming from the conglomeration of tools, instruments, techniques and procedures that are defined in it.

The fact that ISMS implementations are currently highly technological in nature, has the effect that power is *de facto* passed to the IS professionals who have the responsibility of specifying, designing and implementing the ISMS as well as maintaining its operation. In ANT terms, the IS professionals are responsible for the inscription and translation of the bulk of the effort towards IS. It is interesting to note that apart from the technical controls which are obviously within the scope of the IS professionals' work, non-technical controls have both technological and administrative inscription components which also require the extensive involvement of IS professionals. The controlling artefacts of an ISMS are the fruits of the IS

www.manaraa.com

professionals' efforts and mentality. These artefacts thus function as conduits for the power of the IS professionals which permeates all aspects of the organization, not just the ones related to the ISMS at hand.

Using the barrier of technology, the group of IS professionals can effectively create an impenetrable perimeter, that neither end-users nor management can break through. This may lead to inadequate ISMS inscription and translation as groups other than that of the IS professionals are isolated from the ISMS design process. For efficient and generally acceptable ISMSs to exist, they should not be designed by IS professionals alone but with the active participation of all groups within the organisation. Every ISMS inadequacy is bound to be exploited by the Social Engineer under the proper circumstances. Hopefully, if all groups participate in the creation of the ISMS, it will be easier for members of groups other than the IS professionals to espouse the directives of the ISMS (or in ANT terms "*internalise*" those directives), and make the ISMS function more efficiently. The possible disadvantage to this is that there may exist a higher level of conflict between the groups during the design phase of the ISMS. Care should be taken for such a situation not to become explosive and either hinder the creation of the ISMS or produce an ISMS with severe design flaws.

Either the absence of an ISMS altogether, or the existence of a flawed one, will give ample opportunity for the Social Engineer to act.

10 CONCLUDING REMARKS

By attempting to create a security policy that governs any kind of hierarchical structure, complex interactions come into existence. The social construct underlying the hierarchical structure affects, or even defines, the design, functionality and efficiency of the security policy. On the other hand, the security policy itself affects and transforms the dynamic relationships within the social construct. When this mechanism is set in motion and until an equilibrium point is eventually reached, a period of tumult may be incited. Inconspicuous vulnerabilities that are due to purely sociotechnical reasons arise during such periods, leading to a significant drop in the efficiency of the security policy. Consequently, a Social Engineer may find ample opportunity to mount successful attacks. Furthermore, there is always a possibility that some of the vulnerabilities of the described type are not identified and may thus remain unmitigated for a

www.manaraa.com

long period of time after the initial establishment of the security policy. Thus, emphasis must be placed in the effort to identify these 'socially-induced' vulnerabilities and establish controls for them, if SE attacks are to be repelled.

The study presented in this paper actively supports the research towards combating Social Engineering threats, by providing an insight into the socially-defined opposing forces and interactions within an ISMS that Social Engineers attempt to exploit.

11 REFERENCES

AKRICH, M. 1992. The De-Scription of Technical Objects. Bijker, W. and Law, J.(Eds.). Second printing,1997. *Shaping technology/Building society studies in sociotechnical change.* pp. 205-224. Cambridge, MA: MIT Press.

ALBRECHTSEN, E. 2004. *Information managed securely? An approach to the social construction of information security management* [online]. Term paper, Norwegian University of Science and Technology. Available from URL: http://www.iot.ntnu.no/users/albrecht/rapporter/OTE_paper_Eirik_Albrechtsen.pdf. [Last access on May 4, 2005]

BERGER, P. L. and LUCKMANN, T. 1991. The social construction of reality. A treatise in the sociology of knowledge. London: Penguin Books.

BOTTOMORE, T. B. 1990. Κοινωνιολογία - κεντρικά προβλήματα και βασική βιβλιογραφία. [Greek] [Sociology - A Guide to Problems and Literature]. Translated from English by D. G. Tsaoussis. Athens: Gutenberg

DELIGIORGI, A. 1996. *Ο Μοντερνισμός στη Σύγχρονη Φιλοσοφία : Η αναζήτηση της χαμένης ενότητας.* [Greek] [Modernism in Contemporary Philosophy : The search for the lost unity]. Athens: Αλεξάνδρεια [Alexandria].

DHILLON, G. and BACKHOUSE, J. 2000. Information System Security Management in the New Millenium. In: *Communications of the ACM.* **43**(7) 125-128.

DOUJON, J.-P. 1990. *Histoire des faits économiques et sociaux.* [French] [History of economic and social events]. Grenoble: Presses Universitaires de Grenoble.

FOUCAULT, M. 1988. *Τι είναι Διαφωτισμός;* [Greek] [What is

www.manaraa.com

Enlightenment?]. Translated from French by Stefanos Rozanis. Athens: Εκδόσεις 'Ερασμος [Erasmos Publications]
FOUCAULT, M. 1989. *Επιτήρηση και Τιμωρία: Η γέννηση της φυλακής* [Greek] [Discipline and Punishment: The birth of prison]. Translated from French by Kate Chatzidimou and Ioulietta Ralli. Athens: Κέδρος - Ράππα [Kedros - Rappa]
FOUCAULT, M. 2005. *Εξουσία, Γνώση και Ηθική* [Greek] [Power, Knowledge and Morality]. Translated from French by Zissis Sarikas. Athens: Ύψιλον [Ypsilon]
GIDDENS, A. 2001. *Sociology* (4th edition). Oxford: Blackwell Publishing Ltd.
HANSETH, O. and MONTEIRO, E. 1998. *Understanding Information Infrastructure*. (e-Book) [online]. Available from URL: http://heim.ifi.uio.no/~oleha/Publications/bok.html [Last access on Aug 28, 2006].
ISO/IEC. 1997. International Standard ISO/IEC TR 13335-2:1997. Information technology - Guidelines for the management of IT security - Part 2: Managing and planning IT security. Geneva: ISO Copyright Office.
ISO/IEC. 1998. International Standard ISO/IEC TR 13335-3:1998. Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security. Geneva: ISO Copyright Office.
ISO/IEC. 2000. International Standard ISO/IEC TR 13335-4:2000. Information technology -- Guidelines for the management of IT Security -- Part 4: Selection of safeguards. Geneva: ISO Copyright Office.
ISO/IEC. 2001. International Standard ISO/IEC TR 13335-5:2001. Information technology -- Guidelines for the management of IT Security -- Part 5: Management guidance on network security. Geneva: ISO Copyright Office.
ISO/IEC. 2004. International Standard ISO/IEC 13335-1:2004. Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management. Geneva: ISO Copyright Office.
ISO/IEC. 2005a. International Standard ISO/IEC 17799:2005. Information technology -- Security techniques -- Code of practice for information security management. Geneva: ISO Copyright Office.

www.manaraa.com

ISO/IEC. 2005b. International Standard ISO/IEC 27001:2005. Information Technology - Security techniques - Information security management systems- Requirements. Geneva: ISO Copyright Office.
ISO/IEC. 2005c. International Standard ISO/IEC 15408-1:2005. Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model. Geneva: ISO Copyright Office.
ISO/IEC. 2005d. International Standard ISO/IEC 15408-2:2005. Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional requirements. Geneva: ISO Copyright Office.
ISO/IEC. 2005e. International Standard ISO/IEC 15408-3:2005. Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance requirements. Geneva: ISO Copyright Office.
ISO/IEC. 2005f. International Standard ISO/IEC 27002:2005. Information technology -- Security techniques -- Code of practice for information security management. Geneva: ISO Copyright Office.
LATOUR, B. 1986. *Laboratory Life: The Construction of Scientific Facts*. Princeton, NJ: Princeton University Press.
LATOUR, B. 1987. Science in action: How to Follow Scientists and Engineers Through Society. Cambridge, MA: Harvard University Press.
LATOUR, B. 2005. Reassembling the Social. An introduction to Actor-Network-Theory. Oxford: Oxford University Press.
LAW, J. 1992. Notes on the theory of the actor-network: ordering, strategy, and heterogeneity. *Systems Practice*. **5**(4) 379-393.
LEIWO, J. and HEIKKURI, S. 1998. An Analysis of Ethics as Foundation of Information Security in Distributed Systems. In: *Thirty-First Annual Hawaii International Conference on System Sciences*-Volume 6. IEEE.Also: [online] available from URL: http://computer.org/publications/dlib/ [Last access on June 27, 2005].
LOW, J. et al. 1996. Read this and change the way you feel about software engineering. *Information and Software Technology* 38,77-87.
MENDELSSOHN, M. et al. 1989. *Τι είναι Διαφωτισμός;* [Greek] [What is Enlightenment?]. Translated from German by N. M. Skouteropoulos. Athens: Εκδόσεις Κριτική [Kritiki Publications].
MORGAN, G. 1996. *Images of Organization* (2nd ed.). Thousand Oaks,

www.manaraa.com

CA: Sage Publications, Inc.
OAKES, G. 1998. On the Unity of Max Weber's Methodology. In: *International Journal of Politics, Culture, and Society*. **12**(2) 293-306
OSTROFF, F. and SMITH, D. 1992. The Horizontal Organization. *McKinsey Quarterly*. **1** 148-168.
RIDDENER, L. R. 1999. *Dead Sociologists Society - Max Weber - Bureaucracy*. [online]. Available from URL: http://www2.pfeiffer.edu/~lridener/DSS/Weber/BUREAU.HTML [Last access on July 5, 2006].
SCHACH, S R. 2005. Object-oriented and Classical Software Engineering. 6th ED., McGraw-Hill
SINGLETON, V. and MICHAEL, M. 1993. Actor-Networks and Ambivalence: General Practitioners in the UK Cervical Screening Programme. *Social Studies of Science*. **23** 227-264.
TATNALL, A. and GILDING, A. 1999. Actor-Network Theory and Information Systems Research. In: *Proceedings of the 10th Australasian Conference on Information Systems*. p.955-966
UNIVERSITY COLLEGE LONDON, 2003. *Digital Egypt for Universities - A learning and teaching resource for higher education - Law in ancient Egypt* [online]. Available from URL: http://www.digitalegypt.ucl.ac.uk/administration/law.html [Last access on Apr. 20, 2008]
WEBER M. 1978. *Economy and Society. Edited by Guenther Roth and Claus Wittich*. [Wirtschaft und Gesellschaft]. Berkeley: University of California Press.
WHITTEN, J. L. & BENTLEY, L. D. 2007. *Systems Analysis & Design for the Global Enterprise*. Seventh Edition. McGraw-Hill.

CONSULTED BIBLIOGRAPHY

FOUCAULT , M. 1985. La vie: l'expérience et la science [French] [Life: experience and science] In: *Dits et Ecrits,* t.IV, p.763-776
HACKING, I. 1999. *The social construction of what?* Cambridge, MA: Harvard University Press.

www.manaraa.com