UNIVERSITY OF SOUTH AFRICA

SCHOOL OF COMPUTING

SOCIAL ENGINEERING AND THE ISO/IEC 17799:2005 SECURITY STANDARD: A STUDY ON EFFECTIVENESS

by

Evangelos D. FRANGOPOULOS

STUDENT NO. 3481-121-4

SUBMITTED IN PART FULFILMENT OF THE REQUIREMENTS FOR THE DEGREE OF MASTER OF SCIENCE IN INFORMATION SYSTEMS AT THE UNIVERSITY OF SOUTH AFRICA

SUPERVISOR: PROFESSOR M. M. ELOFF

JOINT SUPERVISOR : PROFESSOR L. M. VENTER

MARCH 2007

ACKNOWLEDGEMENTS

I wish to thank my supervisor, Professor M. M. Eloff and my joint supervisor, Professor L. M. Venter, for their guidance and support through the many phases of the research presented here.

I also wish to thank my friend and colleague, Mr. Eutychios Dellis for the long, eye-opening discussions that gave me a different perspective on science and stimulated a significant part of this research.

This work would not have been possible without the loving support of my wife, Afroditi and our two children, Dionyssis and Semeli who bring balance and happiness to my life. My apologies go to them for the time irrevocably stolen from them in the pursuit of this research.

Summary

As Information Security (IS) standards do not always effectively cater for Social Engineering (SE) attacks, the expected results of an Information Security Management System (ISMS), based on such standards, can be seriously undermined by uncontrolled SE vulnerabilities.

ISO/IEC 17799:2005 is the subject of the current analysis as it is the type of standard not restricted to technical controls, while encompassing proposals from other standards and generally-accepted sets of recommendations in the field.

Following an analysis of key characteristics of SE and based on the study of Psychological and Social aspects of SE and IS, a detailed examination of ISO/IEC 17799:2005 is presented and an assessment of the efficiency of its controls with respect to SE is provided. Furthermore, enhancements to existing controls and inclusion of new controls aimed at strengthening the defense against Social Engineering are suggested.

Measurement and quantification issues of IS with respect to SE are also dealt with. A novel way of assessing the level of Information Assurance in a system is proposed and sets the basis for future work on this subject.

Key terms:

Social Engineering; Information Security; Security Policy; ISO 17799; ISO 27001; ISO 27002; Subjective Reality; Objective Reality; Actor-Network Theory; Persuasion; Influence; Information Assurance

Table of Contents

List of Figures

List of Tables

1. The problem of Social Engineering in Information Security.

Social Engineering (SE) is neither new nor strictly related with Information Technology (IT) systems. SE methods are best applied against individuals who can be convinced, against their better judgement, to do or believe things that they shouldn't. If these facts are combined with the inherent complexity and intricacies of present-day IT systems that can not be fully understood by the systems' users, the unavoidable result is that Information Security (IS) can certainly be compromised by SE methods of attack. Current IS standards do provide a framework for improved Information Security. However, as it is shown by this work, even in an environment governed by standards, there is always room for a Social Engineer to mount an attack. The very nature of SE methods makes it difficult to design controls for SE-related vulnerabilities. Hopefully, this work will shed some light in the direction of devising schemes for better protection against Social Engineering.

1.1 Problem Area, background

A trend has been under way for quite a while; that of the digitisation of the modern world. We are presently moving away from the analog models of the sovereign state and closed (or "finite") communities that governed the development of the current legal system and hence our notion of "security". With the evolution of the modern e-world, borders, in the traditional sense of the word, have already been abolished. In fact, the digitisation of our world which is bringing people closer and giving them the ability to interact, is actively demolishing the traditional social structures, replacing them with new types thereof. Such a transition has already taken place in the past when mankind passed from the society of the village communities of yesteryear that was governed by ethics, to the national, and progressively international, society which was made possible through the existence of a complex legal system. This legal system is now being proven incapable of dealing with the effects of societal changes that are already under way. It can thus be deduced with reasonable certainty that the emerging e-society requires a new form of

governance. The very nature of e-society actually aggravates the problem of ensuring the legality of its members' actions in general, as it is now possible -or even easy- to physically be in one part of the world and commit a crime in another.

In this transitional day and age, one can take advantage of the shortcomings of the existing legal system that is not yet adequately equipped to deal with the arising situations, and offenders can slip from the grasp of the proverbial -but no longer truly so- "long arm of the law".

As IT systems form the pillars on which e-society is being built, the security of the information handled by those systems becomes of paramount importance. Many examples corroborating this statement can be identified:

- Computer systems are increasingly relied upon for monetary transactions, e-money being just a small part of the bigger picture of the new digital economy.
- The advantages of e-government (such as the simplification of the bureaucratic procedures) are made possible only through the implementation of complex systems that do away with the outdated bureaucratic models of the past that are still in use around the world.
- In the war against crime and terrorism, national law-enforcement agencies rely on distributed computer systems to securely identify individuals and collaborate with corresponding organisations at an international level.
- Personal data is being handled by computer systems for medical, insurance, financial and other purposes.
- Communications are governed by computer systems. "Least Cost Routing" ensures that people can communicate efficiently and as cheaply as possible. When a call is placed from one side of the Atlantic to the other, the subscriber has neither control nor interest over the type of the voice channel used, the bandwidth allocated for the conversation, the physical medium etc., as long as the communication is of acceptable quality and cost.

All of these applications and many more play a major role in everyday life. The extent to which the operation of these computer systems affects modern society can be indirectly deduced by considering whether there exists a way that these systems can be abolished altogether, perhaps by reverting to older techniques, and how society would react to such a change. If the credit card system were to stop functioning, there is a good chance that people would feel trapped as their freedom to finance purchases or easily carry out transactions and conduct business outside geographical confines would be curtailed. Add to this an abrupt failure of ATM machines and permanent interruption of Internet banking services at a global scale, and economy would probably come to a grinding halt. Eventually, alternative methods to conduct business would probably emerge, but the blow to the economy could be crucial and hard -if not impossible- to recover from. Similarly, global loss of the computer systems handling telecommunications, would almost definitely result in chaos.

1.2 The problems of measurement and comparison

All of the above stress the need for Information Security (IS). Two simple questions immediately arise: the first one is "how can an Information System be made secure?" and the second is "how secure is secure?". The notion of security in general, is neither one that can be readily defined and achieved nor can it easily be quantified. When it comes to the issue of the security of **Information**, the problem becomes even more complicated and difficult to measure, as the object to be protected is an immaterial one.

In an effort to provide streamlined methods of securing Information Systems, several Information Security standards and recommended practices have emerged over the past decade. These security standards and practices, although they all deal with the general notion of IS, have different mentalities and tend to approach the issue of IS in different ways. Their focal points are also different but in many cases, these standards and sets of practices prove to be complementary to each other in the common effort to ensure security. A

comparative study of some representative security standards and recommended best practices is presented by Frangopoulos & Eloff (2004).

It can be argued that the measurement of security is not necessary and that any system should be made "as secure as possible" (non-availability notwithstanding). The problem is that no isolated information system really exists nowadays. Thus, when information is transferred between systems, the issue of the level of confidentiality immediately comes into play. It is absolutely unacceptable to pass information from one system to another without first ensuring that the level of security is **comparable** between the two systems. For the notion of comparison to even exist, a common measure must be devised against which both systems are compared for a useful deduction to be made. To this end, security standards for information systems already exist and the degree of conformity of similar systems to the same standards is currently used as a ruling factor on whether the systems are compatible with each other with respect to their level of security.

Furthermore, as e-society is being developed, various types of pressure towards the measurement of IS are emerging. Such an example is the growing concern voiced by insurance companies that need to base their risk assessments on solid metrics. Another example is the need of top management to first establish a baseline and then exactly identify the return on its investment on security in terms of improvement in overall IS. An organisation also needs to know its security standing with respect to its peers to assess its relative position and not over- or under-budget for security.

Thus, the measurement of the level of security as this applies to the information handled within the scope of operation of an organisation, is becoming one of the principal questions pertaining to IS. To address this issue, the establishment of a holistic risk-management framework that is based on quantification and metrics, is necessary. The quantification of IS is an indispensable component of the objective assessment of the current or projected security status of any information-processing system. Clearly, the scope of such a quantification can neither be limited to the computer system

in operation, nor can the security of the computer system handling the information be judged irrespectively of other information handling systems and procedures active within the organisation.

To this end, the current mentality of security planning, lies on principles that cover a very broad base of security measures and controls as these are applied to all of the organisation's operations and procedures.

1.3 The application of standards

A mentality such as the one described above is displayed by the ISO/IEC 17799:2005 standard (ISO/IEC, 2005a). This standard evolved directly from the British Standard BS7799 of 1995 (British Standards, 1995) as ISO/IEC 17799:2000 (ISO/IEC, 2000a) and was further revised in 2005, leading into its present status. This standard can be viewed as a collection of sound practices that govern all aspects of IS within the bounds of an organisation. As described by Ted Humphreys (the ISO/IEC JTC1/SC27 WG1 Convenor) in (Humphreys, 2005), in the 2005 revision of ISO/IEC 17799:2005 steps have been taken in order to update the standard with new or updated controls, to delete obsolete controls, to include new developments, to clarify the standard's text in an international context, to improve the user friendliness of the control text and to include a detailed section on IS incident management.

In an effort to streamline the creation and maintenance of an Information Security Management System (or ISMS) based on the original ISO/IEC 17799:2000 / BS 7799:95 standard, BS 7799-part 2 was created in February of 1998 (British Standards,1998). This British Standard has been the de facto universal standard in recent years for the creation and maintenance of an ISMS. BS7799-part 2 has undergone a number of revisions, the most recent of which was in late 2005 when the standard was presented by ISO/IEC as the first in the new 27000 series of IS-related ISO/IEC standards, in its current form as ISO/IEC 27001:2005 (ISO/IEC, 2005b).

It must be noted that the ISO/IEC 17799:2005 standard will also take its place in the new 27000 series. According to Humphries (2006) ISO/IEC 17799:2005 will be renamed into ISO/IEC 27002:2007 and will be introduced to the 27000 set in April of 2007. It is expected that the renaming of the standard will not include a revision. Hence the content of the new 27000-series standard will not be different from that of the current ISO/IEC 17799:2005 standard. If this holds true, any discussions relevant to ISO/IEC 17799:2005 that are presented in this work will be directly applicable to the new ISO/IEC 27002:2007 standard.

ISO 27001 is still based around the Plan-Do-Check-Act (PDCA) model as part of an iterative management system approach that leads to the development, implementation, and continual improvement of the effectiveness of an organization's IS management system. This, latest, revision includes changes to the areas of risk assessment, contractual obligations, scope, management decisions as well as measuring the effectiveness of selected controls.

ISO/IEC 27001:2005 currently requires a) the measurement of the effectiveness of selected controls and consequently b) an assessment of their effectiveness (as described in the standard's sections 4.2.2d & 4.2.3c) in a way that it produces "*comparable and reproducible results*". However it neither describes how to achieve this, nor requires that the assessment be based on a fully quantified evaluation. Instead, the degree of effectiveness of the ISMS can be deduced in conjunction to audits, security incidents, changes in external factors such as legislation, etc. This approach is indicative of the difficulty of the quantification of IS which, thus, remains a rather elusive system quality.

It is also true that most methods of assessing the need for the introduction of security in information systems are based on Risk Analysis. As it is discussed by Kokolakis et al (2000), this Risk Analysis is founded on a rather simplistic model of information systems that consists of assets, i.e. data, hardware and software, that are vulnerable to a range of threats. As a result, such a risk analysis does not take into consideration the organisational environment in

which the information systems in question, operate. Kokolakis et al (2000) go further in discussing the view that "*a comprehensive methodology for information systems security analysis and design should incorporate both risk analysis and organisational analysis that is based on Business Process Modeling (BPM)*".

For the sake of argument it can be assumed that whether based on BPM or otherwise, a quantification scheme for an IS structure that is based on generally accepted IS standards, may indeed be possible. From such a scheme, a measure for applied IS can be extracted and consequently, IS methodologies that are applied to information systems can be made more efficient. Thus, quantification should lead to improvement. However, this deduction can be placed in jeopardy as there exist other, very important factors stemming from human behaviour that, to the knowledge of this author, have not been sufficiently addressed in the context of IS standards. The effect of these factors can seriously destabilise both the expected results of the application of IS standards on Information Security as well as the quantification construct related to IS. Although generally acceptable IS standards and best practices are very useful in streamlining the design and implementation of security controls against a large variety of threats, they do not seem to sufficiently address the obscure area of vulnerabilities stemming directly from the exploitation of the human factor of Information Systems. There are many reasons that justify the "weaknesses" of the human factor in this respect, a crucial one being that due to the speed of the onset of the "digital age", **e-society ethics'** development is definitely lagging.

1.4 The introduction of e-ethics and their relation to Social Engineering

The ability that humans have to distinguish between "good and bad" evolved through millenia of human existence. It has thus become our second nature to assess any potential decision or action and make a conscious decision on whether to follow it or not, based on our ethics and the existence of the legal

system. However, all is not so clear when it comes to e-crime. Apart from blatant examples such as someone breaking into a bank's computer system and adding trailing zeros to an account, most people today do not have a concise notion of what is legal and what is not so when it comes to potentially criminal acts that pertain to information miss-handling. Thus, people can be fairly easily convinced to seriously underestimate the repercussions of their actions and the potential destructive consequences that these may have in the context of IS. Such persuasion methods are the standard tools in SE attacks that are directed towards the one element that ISMSs (or any other security level assessment procedure) so far, do not efficiently cater for - that of the human psyche and its shortcomings when dealing with IS.

If the wide proliferation of IT systems is further considered under the light of their resulting inter-dependencies and the reliance of so many aspects of modern life on them, it can be easily understood that the isolation and study of particular IT subsystems in terms of their individual merits and elementary qualities is virtually impossible. Hence, accurate assessment of the necessary security level of IT systems is very hard to achieve. Adding to this conclusion the increased complexity induced by the effects of SE vulnerabilities, the problem becomes daunting, at best. The only way to address this problem is by breaking it down to its individual components and dealing with each of those in a manner appropriate to each one.

1.5 Research Questions, hypothesis

All of the above lead to the conclusion that the inherent difficulty in effectively applying IS, stems from the fact that the task of enforcing such security should be an interdisciplinary one. The increasing level of reliance upon sociological and psychological issues in order to achieve IS, causes divergence from the trodden path of simply applying technical countermeasures against well-specified vulnerabilities.

As a result, it is becoming increasingly complex to form the technical, legal and social framework through which IS can, primarily, be enforced and,

furthermore, measured. In true reverse causality, it can even be argued that the need for successful IS enforcement (and measurement) could even **lead** to the establishment of a complex enough framework that is necessary to have IS applied (or a least have it strengthened through accurate and quantifiable feedback on its efficiency).

Modern IT systems are much more than "number-crunching" machines or extended repositories of useful data. Such IT systems provide an extremely powerful means of communicating ideas -sometimes even at a transcendental level- a very potent decision-making aid, and, to a large extent, their design and inherent limitations even dictate the structure of an organisation. To be optimally efficient, it is common practice for organisations to be set-up from zero or get re-organised around the capabilities of their IT backbones, with executives and administrative personnel tapping into those backbones in order to perform their duties. The sociological effects are obvious as many organisations promote remote working (from the employee's home or in the field), desk space sharing on co-location-optimised premises, de-centralised corporate structures etc. Furthermore, as all of the technology necessary to realise such schemes can not be assumed to be grasped by all employees, even the slightest degree of computer illiteracy can be frowned upon and result in professional and social isolation -hopefully, only in the most extreme of cases.

It is, thus, the demanding nature of this proliferation of Information Systems that causes a certain degree of insecurity to the non-expert users and makes them vulnerable to the indirect nature of SE attacks.

The security standards (and recommended best practices) that have been developed in relatively recent years, all have the common goal of minimising -and ideally, nullifying- the effects of attempted security breaches. However, their provisions do little in the field of counteracting the effects of SE attacks, as most such standards are centered on the technical issues involved in designing, specifying, building and administrating Information Systems. Examples of this mentality are the 5-part ISO/IEC 13335 standard (ISO/IEC,

1997; 1998; 2000b; 2001; 2004) and the 3-part ISO/IEC 15408 (ISO/IEC, 2005c; 2005d; 2005e). ISO/IEC 17779:2005 (ISO/IEC, 2005a) deviates from the above standards in providing for IS at all levels of the structure of an organisation, but still does not directly cater for the SE factor.

It would thus be interesting to investigate the effect that attacks of the SE type could have on the existing provisions of IS standards and practices.

The above statement effectively forms the **primary research question** that is addressed in this work. It will be attempted to study each group of controls presented in ISO/IEC 17799:2005 (ISO/IEC, 2005a) and identify its weak points with respect to SE.

It will be shown in subsequent chapters of this work that a significant number of the stipulations in the ISO/IEC 17799:2005 IS standard, can be severely undermined or even rendered useless by a clever attacker using SE methods. Furthermore, it will be made obvious that although the research carried out involved only the current version of the ISO/IEC 17799:2005 standard (soon-to-be ISO/IEC 27002:2007), the results obtained can easily be extended to other IS standards and recommended practices.

Hence, extra controls must be devised for inclusion into standards and practices in order to guard efficiently against SE attacks.

The above statement forms the **secondary research question** addressed in this work. An attempt will thus be made to present additional or alternative controls that offer better resistance to SE attacks.

The optimised process of evaluating the effect of SE attacks on existing standards and practices in an effort to provide enhanced controls for such attacks, can be summarised in figure 1.1:

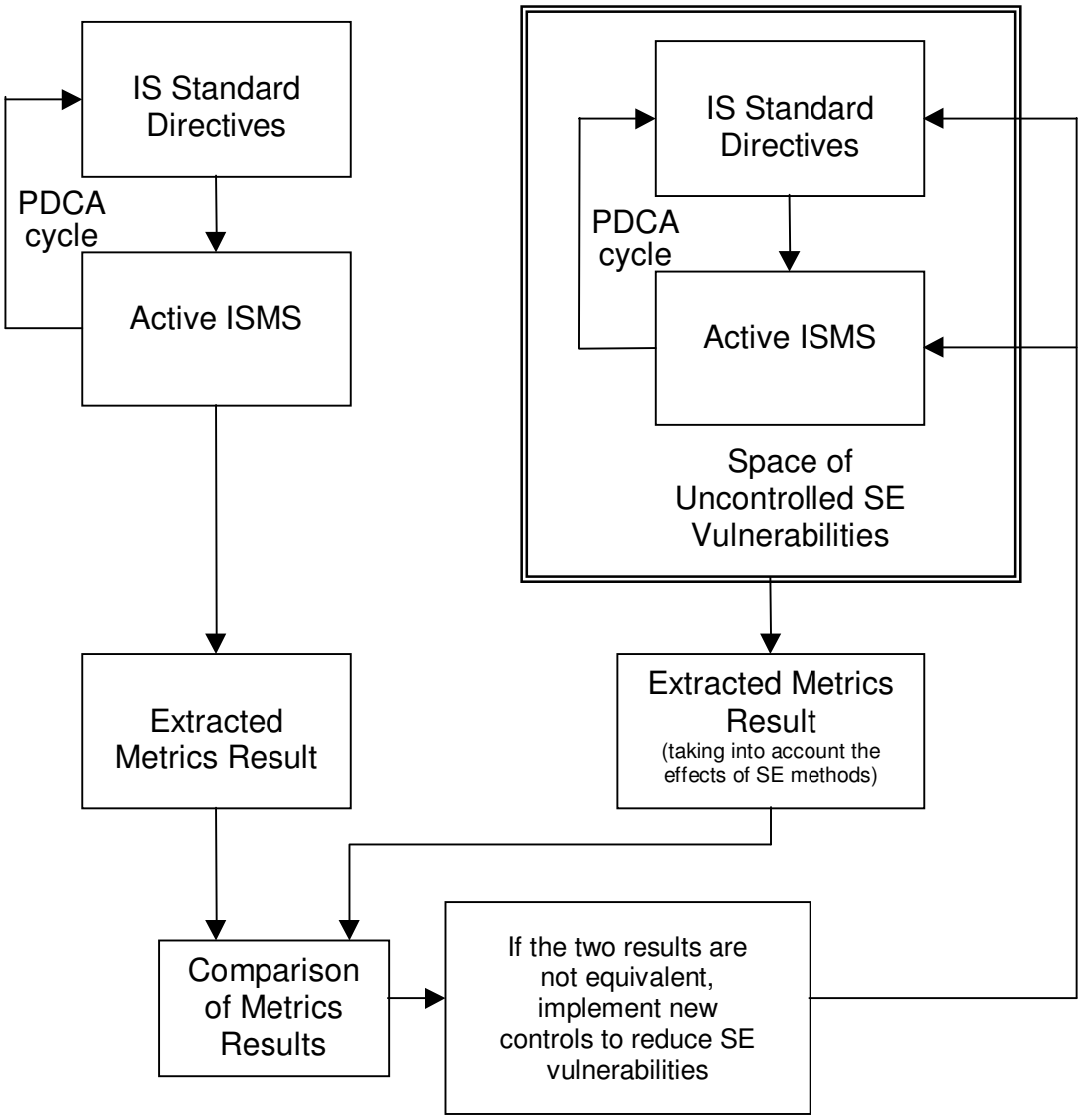

Figure 1.1: Identification of the effect of SE vulnerabilities

In the hypothetical process presented in figure 1.1, above, two distinct paths of evaluation are followed and their results compared.

First, it is assumed that an ISMS based on the applied IS standard is in place and that a metrics result can be made available from that ISMS. This result does not take into account the effect of SE attacks as SE vulnerabilities are not particularly catered for in the IS standard and the resulting ISMS.
Next, each control or group of controls described in the adopted IS standard (as well as the resulting ISMS) will be examined under the light of a possible attack that falls under the methods of operation of Social Engineers. In order

to quantify the effects of possible SE attacks, new measurement methods will have to evolve from the above examination. If metrics that are particular to the effects of SE methods are added to the original set of metrics, the effect of SE attacks will be reflected in the new result. By comparing the original result to the "SE-adjusted" result, it is reasonable to expect that the effect of SE attacks will definitely be non-trivial, and will show a significant reduction of the level of security of the Information System under examination.

Thus, SE vulnerabilities will have to be identified and SE controls be devised and implemented in order to ideally eliminate the risks stemming from Social Engineering (i.e. to make the direct and SE-adjusted metrics' results as close to being equal as possible).

1.6 Value of research in context

The present work attempts to identify the shortcomings of standards and practices pertaining to IS, with respect to the security risk stemming from SE methods of operation. Given the inherent complexity of the Social Engineering problem, it was decided to address the problem of Social Engineering from a variety of angles. In this context, an approach from a Social Sciences perspective was even attempted. The main effort was to address as many issues pertaining to SE attacks as possible in real-life situations and study their effect on the controls and directives described in IS standards and best practices. This analysis resulted in the definition of controls that can be considered as "add-in" modules for IS standards and practices geared towards countering SE attacks. This could lead to the creation of broader, SE-encompassing, versions of the said standards and practices.

Current IS standards and practices are of a predominantly technical nature. According to these standards, technical controls are provided against technical vulnerabilities. That is to say, technical countermeasures are created and adopted against the loopholes created by technical shortcomings of the system that can be exploited by potential intruders.

For example, in the above sense, as a security "undocumented feature" (or "bug") in a firewall hardware or software is discovered after being sufficiently exploited by attackers, a new technical countermeasure in the form of a "patch" is applied. Or, to guard against the possibility of information leakage, fundamentally technical measures against an overlooked technical capability of the system, such as removing floppy disk drives and locking USB ports of physically secured computers, are employed.

In the case of SE attacks, the vulnerabilities that are being exploited could not be any further removed from being technical. It is the mind and psyche of perfectly legitimate and fully authorised users that the Social Engineers target and through whom the attack against the system is mounted.

Building controls for non-technical vulnerabilities should both be a technical and a non-technical issue. Technical controls could be those that make the realisation of SE attacks unfeasible by altering the situation and conditions under which the Social Engineer operates. For example, in controlled office entrances where employees must present a personal ID token to be allowed entry, "tailgating" or "piggy-backing" may be possible and an unauthorised person can follow an authorised person in. To control such a vulnerability, an ordinary triple-bar access-control turnstile could be used, one 120 degree turn of which should be allowed per ID token presentation. As a result, even if the person being manipulated into allowing the attacker to follow through an open door were prone to do so, the system in place would simply not allow it. This way, the psychological tendency to be polite to one's assumed co-worker, can not be taken advantage of by a Social Engineer. Hence, a technical control can be used to eliminate a non-technical vulnerability.

On the other hand, non-technical controls such as security-related education, the promotion of ethical standards in the workplace, the redefinition of the notion of responsibility within the working environment etc, clearly form non-technical controls that are essential in maintaining a state of raised awareness against security breaches.

Furthermore, the fact that many, if not all, technical controls described in the current IS standards and practices can be proven inadequate when examined through the prism of a SE attack, necessitates the protection of Information Systems in an indirect way. If IS is viewed in such a lateral way, it could be proven that the whole arsenal of IS standards and practices as these currently stand, could be brought down if an effective layer of protection against non-technical attacks is not incorporated in them.

For the above to be effected, two issues that rather deviate from the usual approaches to IS must be examined. The first of these issues is how psychological principles actually apply to the notion of SE, while the second has to do with the analysis of the social aspects of IS. The results of this study can then be put to good use in the assessment and further development of the controls of IS standards which are the prime objectives of this work.

Ideally, the outcome of this work will be used to strengthen the structure and provisions of IS standards and practices against SE vulnerabilities. It can also lead to the creation of a "yardstick" against which (in the context of an ISMS) the effectiveness of any given Information Security System will be assessed. Such a yardstick would be based on a scheme according to which, SE vulnerabilities and their respective controls are defined and transformed into security-wise-quantifiable entities. This could form the basis for the creation of a metrics-based standard tool, with obvious added value for SE-related risk analysis.

Given that this assessment / measurement scheme will have to be dynamically self-adjusting, continually permitting new factors to be taken into account as new SE-related circumstances arise, allowances will have to be made for temporally-spaced results obtained during the course of life of the evolving system to be comparable to one-another. This comparison will provide the feedback necessary for the effectiveness of the self-adjusting system. Hence, the proposed system will allow for the continual re-assessment and adjustment of the measurement procedure itself, in an effort

to extract objective results of higher accuracy with respect to the Information System under examination.

Hence, this research contributes in the following areas:

- Provision of better understanding of the mechanisms involved in Social Engineering methodology
- Study of the psychological considerations in SE
- Analysis of the social aspects of Information Security
- Evaluation of existing controls in IS standards and practices with respect to SE
- Proposals on additional technical and non-technical controls for the mitigation of SE-related risk
- Foundation of an assessment scheme for SE-related controls based on metrics.

1.7 Limitations and delimitations, scope

The method presented in figure 1.1 takes for granted that a result based on metrics can be obtained with and without factoring in the effect of SE attacks. This, as it was realised during the course of this research, was definitely not an easy task to accomplish. Although security metrics schemes that are used to assess the effectiveness of security policies and controls do exist, measuring the possible effect of SE vulnerabilities is not as straightforward. Hence, if exact results are required, it will be necessary to first devise metrics geared towards SE issues and only then attempt to make the comparison described in figure 1.1.

It can be argued though, that **exact metrics are not necessary** for assessing the effect that SE attacks have on the controls described in IS standards and practices. For this work to advance, it was assumed that as long as a control is shown to be susceptible to an SE attack, if it can somehow be strengthened to resist the attack, or complementary controls be devised to aid in this

direction, the prime objective is reached. This still holds true even though an exact metric for the procedure can not be obtained.

The proposed research is, de facto, limited to standards and practices that are geared towards creating practices for IS and that do not solely address the technical aspect of IS. It was considered most appropriate to examine the ISO/IEC 17799:2005 standard (ISO/IEC, 2005a) because of its nature that covers the whole spectrum of IS and not just the technical part of it. A stronger case for this choice is presented in the relevant chapter containing the detailed examination of the Standard. The standard was examined from the perspective of possible SE vulnerabilities, the existing loopholes were identified and appropriate controls were proposed.

What this research attempts to prove, is that compliance to standards and recommended practices (as they currently stand), does not -on its own- suffice for either fully securing an information system or determining the level of applied security. This is so because other factors that are not technical come into play. These factors originate from the methods used by Social Engineers who take advantage of the vulnerabilities in human behaviour to mount a successful attack.

The indirect attacks targeted against the human element of security which fall under the general category of "Social Engineering" can prove detrimental to IS. Social Engineers base their method of operation on well-proven applied psychology and persuasion techniques that are being adapted to suit the needs of e-criminals. To a large extent, countermeasures to control risks of a psychological nature must be based on psychology themselves. Furthermore, as the general title "Social Engineering" suggests, such attacks take advantage of certain aspects of social interaction in order to be successful. Hence, returning to the issue of metrics, it may well be that quantification of SE issues can not be made possible unless a significant contribution can be made from a social sciences standpoint.

On the other hand, it is not only psychological countermeasures that can be established in order to control SE attacks. Technical controls such as state-of the-art identification tokens can -and should- also be applied to counter SE attacks. The application of technical countermeasures to control non-technical, SE threats should be seen under a different light from technical controls applied against technical threats and a separate quantification method be employed.

Hopefully, the reader will be convinced that, as is the firm belief of the author, SE attacks that are mostly unaccounted for in IS standards (and, hence, ISMSs), can seriously undermine the effectiveness of a policy based on the said standards and cripple the usefulness of ISMSs. Hence, it is imperative that a) the effects of SE issues are identified and catered for in the design of IS standards and b) that the outcome of this study is also applied to the ISMSs resulting from such standards.

1.8 Research methodology

1.8.1 Solution approach

First, an attempt was made to identify the problem of Social Engineering and discuss as many of its aspects as possible. The better the understanding of the nature of the problem and its roots, the more efficient the defenses against it.

Armed with a solid understanding of the SE problem, the analysis of the ISO/IEC 17799:2005 standard (ISO/IEC, 2005a) took place by reviewing the existing security controls under the light of a possible SE threat. For each of the resulting SE vulnerabilities, an attempt was made to create an appropriate control that diminishes the effect of that vulnerability.

The applied methodology was rather straightforward in the sense that the individual controls were re-assessed in the context of SE threats.

From this analysis an obvious categorisation of existing controls resulted according to whether a) the controls are not affected by SE threats, b) the controls could be affected indirectly by SE threats or c) the controls could be affected directly by SE threats. Obviously, for case (a) above, little -if anything at all- was necessary to be added in order to achieve the desired "SE enhancement" of the standard. When controls falling under category (b) above, were identified, existing controls were improved or new ones proposed to act as countermeasures for the hysteresis involved. Furthermore, the controls of group (b) were found to benefit from the set of general measures against SE (such as training and promoting awareness) that effectively cater for the indirect effects of SE. The controls of group (c) above, were the ones that definitely required the creation of further controls particular to SE in order to withstand scrutiny under the light of SE threats. The SE controls resulting from the study of controls falling under category (c) above, in most cases, also have an indirect positive effect on the existing controls of group (b).

It was made clear in the course of this research, that it is not sufficient to "provide extra padding" to a standard by adding controls against SE threats, but that some existing controls or even groups thereof should
undergo a complete re-design.

1.8.2 Research outcomes

The first outcome of this research was the systematic study of Social Engineering that resulted in the fundamental principles behind SE methodology being identified. The basic forms of SE attacks were discussed, backed by a presentation of the most important Persuasion tactics and Influence techniques as modern psychology accepts them. It was further deduced that to defend against SE an organisation must invest upon its human resources through security awareness and psychological training programs. The objective of these programs should be a controlled exposure of employees to SE methods that sets the foundation for effective defense against SE attacks.

The second outcome was obtained through the study of the social aspects of Information Security. This study provides the means to identify "socially-induced" vulnerabilities (i.e. vulnerabilities stemming from the social relations and interactions of people) and establish controls for them. It is thus shown that the social construct underlying the IS hierarchy severely affects the design, functionality and efficiency of the security policy. As soon as the security policy is in place, it affects and transforms the dynamic relationships within the social construct of the IS hierarchy. Care should thus be taken for this feedback mechanism to ultimately lead to an equilibrium point of maximised security efficiency rather than an explosive and uncontrolled situation.

As was anticipated, the third outcome of this research was an assessment of the degree in which the security clauses and individual controls specified in ISO/IEC 17799:2005 may be affected by SE threats. It was found that although the set of controls presented in ISO/IEC 17799:2005 is very comprehensive and effective, it was not written with SE in mind.

As a fourth outcome and directly stemming from the third result, the general effectiveness of the ISO/IEC 17799:2005 standard was assessed under the light of SE threats. Although the sets of controls present in ISO/IEC 17799:2005 do have the indirect effect of raising the level of security with respect to SE threats, there is still room for improvement and "tuning" of the standard with respect to SE.

The fifth outcome was that through the discussion of ISO 17799 controls insofar their susceptibility to SE threats is concerned, the weaker areas of the standard, in this respect, were identified. This provides the necessary information by which individual controls, control groups or whole sections of the standard may need to be re-designed. The weaker areas of the standard with respect to SE were:

a) physical security where more technical controls need to be introduced to counterbalance the psychological hysteresis which is interwoven with human nature,

b) security against SE attacks over the telephone which remains largely untouched in the current version of the standard,
c) security against SE attacks over the Internet and email that needs to be strengthened under the light of emerging SE attacks and
d) the need for education related to SE and IS awareness building (especially where SE is concerned).

As a sixth outcome, new controls were devised or "tuning" of existing controls was proposed in the detailed discussion of ISO/IEC 17799:2005, specifically addressing the SE issue.

Seventh, this analysis, by providing adequate SE-related data can be further used for the assessment of ISMSs that are based on ISO/IEC 17799:2005. Such an assessment though lies well outside the scope of this Dissertation.

Eighth, this work could be of assistance to all involved with designing IS based on the ISO/IEC 17799:2005 standard by providing enough insight on how vulnerable systems may be from SE threats. The residual risk even after the application of the controls defined in the said standard may be quite higher than expected if SE vulnerabilities are taken into consideration. Hopefully, this work will result in raising the level of alertness and diminishing the false sense of security that the application of the particular standard may have instilled.

Ninth, although far from having fully exploited the concept, the chapter on SE-related metrics, does provide firm ground on which to build for subsequent work on the quantification of SE issues.

Lastly, this work could provide the basis of a future revision of ISO/IEC 17799:2005 (and even of ISO/IEC 27001:2005) with emphasis on the aspect of SE.

1.9 Structure of the dissertation

This dissertation is structured in a way that eases the reader into the reality of Social Engineering within the context of Information Security. Hopefully, by the time the reader reaches the final chapter, the notion of Social Engineering and the degree to which it is being addressed by the current state of the ISO/IEC17799:2005 will be clear enough to be of further use.

Figure 1.2 graphically depicts the overall structure of this dissertation and the relations between the individual chapters.

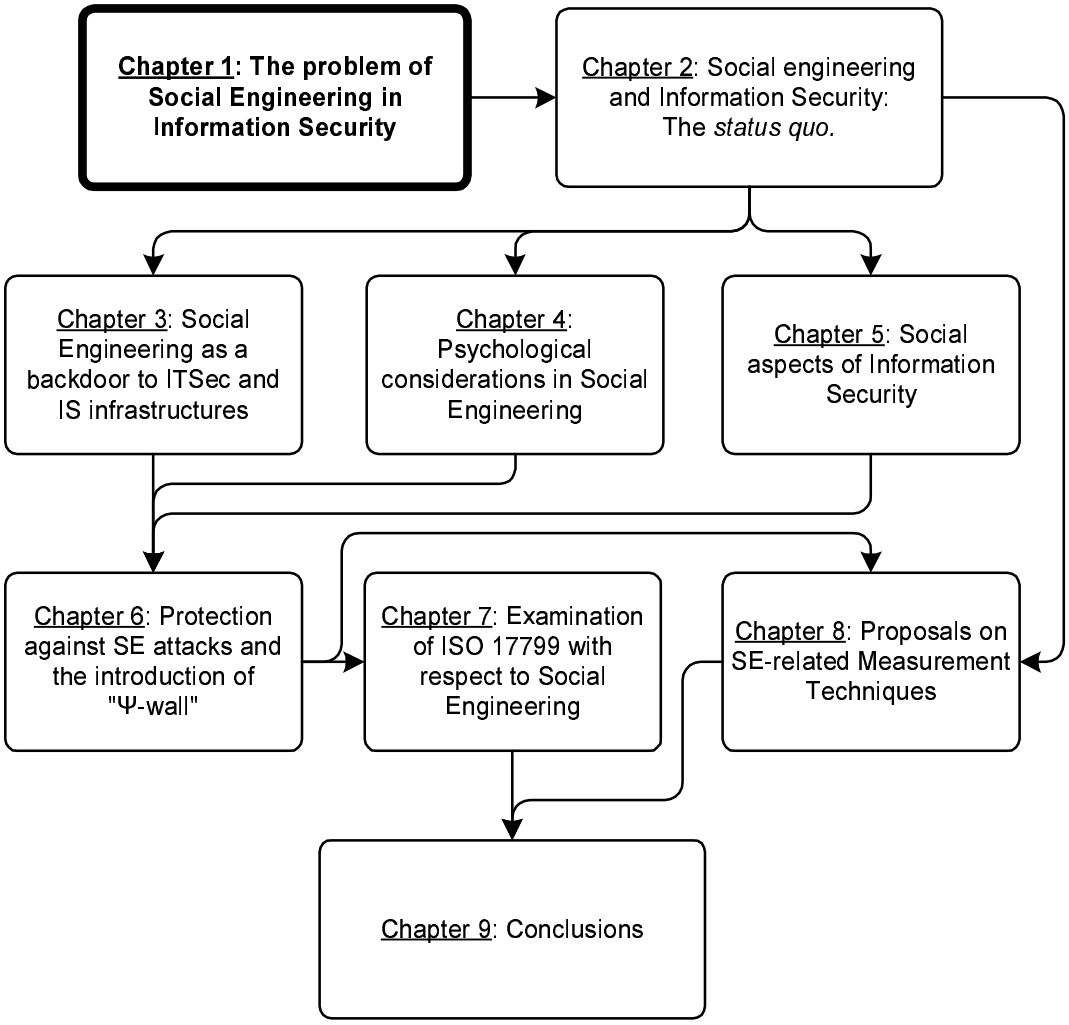

Figure 1.2: Structure of the dissertation and role of chapter 1.

The current, **first chapter** defines **the problem of Social Engineering** as a serious source of threat to Information Security and presents background information, the research question, the methodology that was followed, and a layout of the dissertation's structure.

This is followed by the **second chapter** where the **current situation of SE with respect to IS is presented**, along with and a literature survey.

A discussion of the principles behind Social Engineering follows in the form of the **third chapter**. This discussion is essential as it **defines the multi-faceted nature of SE** and provides enough insight for identification and efficient mitigation of the SE-related threats.

The **fourth chapter** focuses on the **psychological aspect of Social Engineering**. By identifying the psychological component of SE, the first step is taken towards building effective defenses against it.

The **fifth chapter attempts an approach of IS from a social sciences' standpoint**. Although in the mind of the author, upholding Information Security is to a very large extent a problem with sociological roots that reach deeply into the very foundation of any organization, there is very little work being done in this area. This chapter sets a starting point by providing a different than usual perspective.

In the **sixth chapter** an attempt is made to **devise defenses against SE methods**, based on the combined background of chapters 3,4 and 5. This sets the basis for the review of ISO/IEC 17799:2005.

The **detailed study of the ISO/IEC 17799:2005** standard from a Social Engineering perspective follows in the **seventh chapter** and **new SE controls are also proposed**.

The **eighth chapter** on the **quantification of SE issues** attempts to create a starting point from which further work can be done. By accepting the multi-

faceted nature of the SE problem and the complicated matter of devising defenses against it, a novel approach is adopted to yield measurement results.

A **final, ninth, chapter** reviews the work carried out, presents the conclusions of the research and proposes directions for further development.

A list of bibliographical references follows and appendices are included comprising the terminology and abbreviations used throughout the dissertation (Appendices A and B respectively) and the details of the ISO/IEC 17799:2005 examination with respect to SE (Appendix C).

2. Social Engineering and Information Security: The *status quo*.

2.1 Introduction

Having identified the problem of Social Engineering (SE) in the context of Information Security (IS) in the previous chapter, an attempt is made in this chapter to establish the current state of IS and indicate why IS is threatened by Social Engineers. The basics of IS defence are also discussed in an effort to set the stage for the analysis that will follow in subsequent chapters.

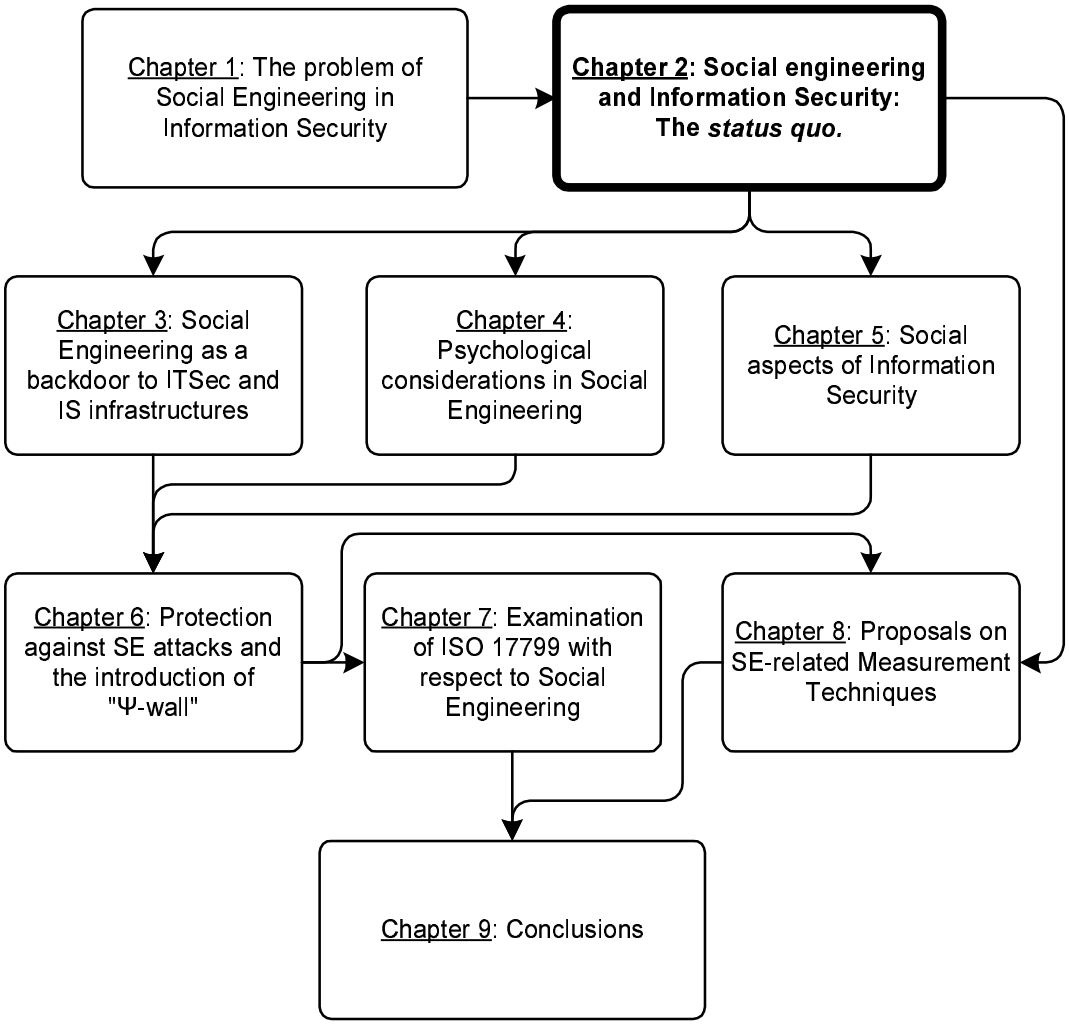

Figure 2.1: Chapter 2 within the context of the overall dissertation structure

The literature survey presented in the third section of this chapter also aims towards the same objective. Many of the ideas present in the literature survey were either used directly in the discussions that follow, or helped define the direction in which this research progressed.

The relative role of the current chapter in the context of this dissertation is graphically depicted in figure 2.1.

2.2 Information security

The idea that Information is an asset worthy of serious protective measures, has never been more justified. During the past three decades the object of security schemes has shifted from ontological units such as money, valuable objects and paper documents, to the more abstract concept of Information in all forms. Apart from the traditionally highly-valued -and worthy of protection- forms of Information (such as those pertaining to issues of corporate, strategic or national defense nature), at this time and age, the notion of the value of information has risen to dizzying heights, mainly because of the way information is stored and handled (Pfleeger, 1997, p. 2). The ability of databases to hold millions of records with every type of information, enables us to keep searchable records of anything and anyone in an organised and highly efficient manner. Access to even seemingly unimportant, catalogued information may prove to be a very powerful tool against individual people or groups and as such, in the wrong hands, may cause serious damage.

One example that may help illustrate the validity of the above point is that of the everyday need for exchange of information for authentication purposes, e.g. for banking transactions over the phone. Only fifteen, or so, years ago, in order to authorise a banking transaction, one would either have to be physically present in one of the bank's branches and sign the relevant documents, or send in a signed letter (usually via a registered postal service) requesting that a transaction be made. Twenty years ago, in most countries around the world, credit card charges could not be made unless the owner of

the card was physically present during the transaction and, furthermore, was able to prove his or her identity by producing two different forms of ID.

Obviously, the reason that these practices were in place was that they were considered necessary to avoid fraud at the expense of the legitimate owner of the bank account or credit card. In our time and age such measures are seen as more of a hindrance that does not allow us to transact swiftly and from a distance -even from across national borders. If this attitude is examined from a slightly removed point of view, it definitely seems highly unreasonable as it is more-or-less devoid of most of the security controls that would be considered essential for monetary transactions of any sort. However, every time someone tries to pay by credit card for an item won at an online auction that took place halfway around the globe from that individual's physical location, all reservations are magically removed. A prime example for such behaviour is none other than the world's best-known trading place on the Internet, "eBay" (eBay, 2006). On a less personal basis, one of the reasons international commerce is evolving is the ability of traders to conduct business (including banking transactions) from a distance -usually a very long one- and with "reasonable" security. The problem, though, is that nothing could be more difficult to define than the level of "reason", for security to be "reasonable". A highly subjective quality by definition, "reasonable security" can not really be measured. On the contrary, it is infinitely variable. A person's perception of the degree of security varies not only between different people, but also depends on the nature of the transaction, the amount of money involved in the transaction and the general psychological situation of that person at the time. In the end, in most cases, this highly subjective degree of security involved in a transaction, will be set in the mind of a person based on his/her notion of the extent to which he/she can trust the other party. **Thus, the notion of trust between humans through social interaction comes into play**. (Castelfranchi & Falcone, 2001). In common life this trust is built gradually over the course of a conversational transaction, usually based on the exchange of information between the two parties. As an example, consider an everyday procedure in a banking transaction. Suppose that a transfer of money (neither an unusually high nor an insignificant one) is

required from one bank account to another. The person requesting the transfer can call his/her branch on the phone and ask for the clerk usually dealing with his/her accounts. After a brief conversation, the clerk agrees to move ahead with the transfer, provided that an authorising letter is sent by fax to the bank to that effect. The fax is sent, the transfer is carried out without the physical presence of the account holder and, furthermore, without an original signed document authorising the transaction in the Bank's possession. Normally, such a transfer is never challenged. Thus, it is "business as usual" at the bank. In the event, however, that the transfer **is** challenged, there is very little that the bank can do to prove that their actions were legitimate.

Although there is definitely no section of the security policy of any bank that endorses such a procedure, it is a well-known fact that these things happen in the course of an ordinary day. The reason that this is so, lies in the trust relationship that has been built between the clients and the bank personnel over time, and in the desire of the bank personnel to keep the clients satisfied. If they don't, maybe the personnel of another bank will. Recognising the potential source of problems that can arise this way, many banks around the world choose to follow one of two routes. The first route is that of explicitly denying to process any order that arrives via fax and require the client to either perform the transaction in person at the bank premises or send a signed order to the bank by registered mail or go through the phone-banking authentication procedure. The other route is that many such institutions choose to delegate the full risk associated with faxed transaction order to the clients by having them sign "fax indemnity" statements that practically relieve the bank of any responsibility stemming from following a counterfeit faxed order (FBN Bank, 2006; Fletcher Kennedy Limited, 2007). It has to be taken into consideration though that still, from the author's personal experience, many banks in various countries around the world have not activated such procedures and still rely on trust and the rapport between the staff and clients for ordinary, everyday transactions.

One may argue that such rapport can only occur between the bank's clients and personnel after a long trusting relationship has been built. But what would

the situation be if an imposter plays the role of the well-known and trusted customer? This is not an easy scheme to bring to fruition, but nevertheless it can be achieved over the telephone, after some investigation and after an appropriate authorisation document bearing a "cut-and-paste", non-original, signature is faxed to the bank to tie loose ends.

Although this is a definite possibility for fraud, the bank personnel will most probably not challenge the validity of such a document. Such an action (or, actually, the absence thereof) is based on the bank personnel's subjective assessment of the risk associated with the transaction. In practice, the clerk carrying out the transaction, based almost solely on the recognition of the voice of a familiar client over the phone, vouches for the sincerity of the client whom he/she has a long-established direct and interpersonal relation with. Clearly, the clerk's decision is hardly based on solid facts and as such is most definitely unsafe.

If on the other hand, an unknown client calls a phone-banking clerk, then this contact is devoid of any personal element of recognition or trust. In this case the clerk has to go through an authentication process with the client, in order to subsequently accept the client's requests and demands. Such authentication is usually based on personal information being passed from the client to the bank clerk. Even today, this information, though, does not necessarily comprise a special password or PIN that the client is assigned for phone banking. If a phone banking service has been correctly structured and is correctly operated, then a PIN will have been assigned to the customer (Barclays, 2006). On the other hand, most banks will be happy to process the requests of a client provided the client gives some bits of personal information such as mother's maiden name or home telephone number. Sometimes, a social security or national ID card number may also be requested. Once this information is presented to the phone-banking clerk, the client is assumed to be authenticated and his/her requests are dully processed (*"Right Sir, how may I help you today?"*).

Thus, in actual terms, **these bits of information take on a monetary value that equals (or exceeds) the sum of the balances of one's bank accounts**. In a similar fashion, orders for all types of goods and services can be placed over the phone and charged on credit cards. Fifteen years ago, a policy used to be enforced, according to which orders would be shipped only to the address registered with the credit card company through which the payment was made. At some point, sellers began to accept requests for shipment of charged goods to alternative addresses provided they had the client's registered address on file. Nowadays, from the author's personal experience, nobody seems to care where they ship goods paid for by credit card, as long as they have the credit card details as they appear on the card and request no further information. Furthermore, when the sale has to do with a service or a downloadable good (such as software, books, music etc), in practice, the address of the credit card holder is not involved in the transaction. It is thus of little wonder that credit card fraud flourishes these days.

Although the examples discussed so far have to do with a specific type of personal information that if compromised can financially hurt someone, all forms of personal information have to be protected. For example, it can not be overlooked that in most countries of the world -even western ones- it is very easy to call up a microbiology laboratory and get your blood test results over the phone on the pretext that you can not make it to the lab on time but you need to relay the results to your doctor. Most of the time, the lab secretary will just give out the results without any challenge of the caller's ID. In some cases they may ask for the doctor's fax number to send the results directly to the clinic, but very rarely they will actually verify the number which could correspond to anyone's fax machine.

All this brings forward the fact that the nature of stored personal information has dramatically changed in the past thirty years, and that its significance has increased by orders of magnitude. This increase in significance is aided by the way that personal information is stored and the ease by which it can be retrieved, referenced and cross-linked. The age-old motto of "getting anything

on anyone" is changing into "getting everything on everyone" and this alone stresses the fact that personal information must remain personal and not fall prey to those seeking to acquire it for their own illegal purposes.

Thus, systems handling personal information should be treated with the same meticulous methods that are being used for the protection of those types of information that are traditionally accepted as invaluable, such as corporate and strategic secrets, or pertaining to issues of national security.

Furthermore, it should by now be clear that since information of seemingly low value such as disjointed morsels of personal data can be combined to grant access to progressively more sensitive information that may in turn lead to further compromises, any and all information-related security breaches must be avoided.

2.2.1 Defending IS

The evolution of information handling that lead to the effects described above, has functioned both as cause and effect for the proliferation of Information Technology systems in all aspects of our life and all levels of organisational structures.

As information processing routines are getting more sophisticated and a plethora of information is becoming more and more accessible, security levels appropriate to the value of the information must be established. The three principal issues of **confidentiality**, **integrity** and **availability** must be delicately balanced if an efficient Information Security scheme is to be achieved (Pfleeger, 1997, pp. 5-6).

Applying security measures to an information system definitely makes the system harder to use. A system can be completely secure if no access to it is allowed -an extreme example of the "Security through obscurity" principle (Pfleeger, 1997, p. 325)- or be totally open and thus totally vulnerable. The optimal solution for real-life systems lies, of course, in the gray area between

the two extremities. The exact point of equilibrium, i.e. the basic security level, is defined according to the value of information being processed by the system.

In a corporate structure, very seldom can a single basic security level be set for the whole structure. As the number of information-processing systems increases, the need for a multitude of basic system security levels arises. Each piece of information must be protected according to its value and position in the corporate structure. Setting the highest required basic security level as the common denominator for all systems leads to the unnecessary over-protection of data that in turn causes the availability of that data to drop without reason.

To deal with this kind of a situation, informed decisions must be made not only at the technical level but, most importantly, at the managerial level where the particular security requirements for each of the information systems have to be specified. Thus the responsibility for Information Security must be dealt with as a managerial issue as well as a technical one.

Furthermore, not all aspects of Information Security can be dealt with by the application of technical measures. As long as human users are relied upon for the secure operation of a system, the system is inherently vulnerable because the man at the keyboard of the computer is vulnerable to non-technical forms of attack. To reduce this level of vulnerability, a clear and concise set of instructions related to security (in the form of a security policy) must be established. The end-users must carefully comply with these instructions and directives. Technical measures being in most cases inadequate to deal with human behaviour, appropriate mechanisms must be in place to limit the effect of attacks being directed towards the human side of the information-processing system.

Such mechanisms include -but are not limited to- efficient methods of personnel training on security issues, promoting security awareness through education, actively pursuing a raised everyday level of security among end-

users through the use of appropriate reminders and the existence of feedback paths that allow alarms to be raised and counter-measures to kick in once an attack on security is suspected (Desman, 2001).

The above resolution makes it all the clearer that end-users can not just be told to obey directions when it comes to security issues. Security policies and directives must be understood if they are to function efficiently. Thus, bringing the end-users up to the required level of awareness, should be seen as part of the overall investment in security and must not be overlooked (Kajavaa & Siponen, 1997). A misinformed employee may provide the shortest path an attacker will follow to bypass all security measures that are in place.

2.2.2 Information Security (IS) Policies

An organisation's information security policy is a set of management directives that establish the business goals, the security framework, the responsibilities of all those involved, as well as governance.

Furthermore, an organization's Information Security Policy must be a single document that articulates the philosophy, regulatory requirements and beliefs that the organization has with respect to securing its information assets. In this context the IS policy document must specify the scope of the environment, the personnel to which the policy applies the processes involved and finally, describe the consequences for non-compliance (ISO/IEC, 2005a).

In an organisation, there exist many policies governing areas critical to the function of the organisation. Policies addressing resource management, logistics, financial issues etc, are essential to the organisation. Hence, the IS Policy is just one of many policies that must be followed concurrently. In a typical situation as this, the IS Policy must not excessively hinder the other policies, but, instead should complement and support their application. Furthermore, after an IS policy is established, it must periodically be reviewed within the context of the constantly changing security requirements as well as

the evolving business environment of the organisation (that inevitably leads to changes in the other organisation policies).

Establishing a security policy is only the first step in efficiently securing the information within an organisation. Steps must be taken towards making the commandments of these policies "second nature" to personnel to whom any degree of responsibility within the scope of the IS policy is assigned, and raising their awareness on security issues as stated above (ISO/IEC, 2005a, section 8.2.2). This is not something that can be achieved just by establishing accountability and counter-motives in the IS policy. It must rather be addressed through positive methods and incentives. Such incentives may be in the form of prizes for employees who have been found to comply to the security policy during penetration testing or an internal audit for secure practices.

The non-technical issues are the most difficult ones to address in an IS policy and those invariably have to do with the reactions of people under unexpected circumstances. In this context, it is impossible to predict all possible attack scenarios and devise countermeasures against them.

2.2.3 Physical vs. (psycho)logical protection

With a well-designed and specified IS policy in place, an organisation can ascertain to a high degree that the applied information protection is appropriate for each type of information involved. In such a policy, countermeasures against physical attacks must be specified and followed.

Efficient physical security may seem easy to apply if access rights are assigned to authorised personnel and an access control system is in place and operational. However, apart from controlling physical access to secure areas, for complete physical security, there are other aspects that have to be considered. For example, procedures must exist according to which sensitive documents must be kept in filing cabinets under lock and key and the keys be carefully protected (ISO/IEC, 2005a, section 9). A "clean desk" policy may be

enforced, obliging employees to lock away all documents pertaining to their work before they leave their office. Official documents should not be allowed to leave the premises except when such removal is appropriately authorised (checks must be in place to enforce such rules). Official documents (of any classification) should not be disposed without being shredded. All magnetic media should be sanitised and all write-once optical media should be physically destroyed, perhaps through the use of CD-ROM shredders (Time Magazine, 2003). Modems should not be installed on Intranet computers. In special cases, even Floppy Disk drives and other removable storage devices should not be available on secure PCs either. (This is becoming more difficult with the current state of technology that provides us with gadgets such as ball-point pens equipped with on-board 512 MB USB drives).

This list of countermeasures against physical attacks is far from being complete but gives an idea of the bigger physical security picture.
On the logical side of security, passwords should be protected and never be disclosed, accounts should be set up following particular security procedures and access rights of users should not be upgraded by the IT department without formal authorisation (ISO/IEC, 2005a, section 11). The above two categories of attacks can be addressed successfully to a large extent, provided that the personnel are aware of the policy and procedures are followed.

The type of attack that is very difficult to cater for is the one that targets a person in such a way, that all the countermeasures provided by the security policy are bypassed. This is achieved by the clever manipulation of the target (or "Mark") by the attacker, so that the target never realises that he/she is tricked into deviating from the security procedures. For such an attack to be carried out, the arsenal of the perpetrator comprises a mastery of psychological techniques that disorient the victim and achieve the desired breach in security.

As far as physical security is concerned, any person can use his/her judgement and feelings and avoid finding him/herself in a situation leading to

a security breach. Under an attack based on psychology, the victim can be manipulated in ways much more subtle than being blatantly asked to cross a physical barrier or remove a document from the premises. The attacker has to assume an average level of common sense on the part of the Mark. People may be persuaded to act in compromising ways only if the request made to them through manipulation does not make them function **outside the limits of their usual scope**.

Furthermore, a cunning Social Engineer will design his/her attack in such a way that no coherent pattern is formed from the information disclosed by the Mark. To disassociate the bits of disclosed information even further, the Social Engineer will not obtain all the information from one person but rather "spread out" his/her efforts by questioning a number of different employees, preferably from different levels in the hierarchy. This way, the chance of two victims coming together and figuring out that something is suspicious, is minimised. Hence, the victim(s) of the attack are usually unaware that a security breach has taken place. This causes the extended problem that there are no alarms raised. It could thus be claimed that every SE attack that is carried out successfully, is tantamount to a "perfect crime".

2.3 Literature survey

At this point it was considered necessary to include a (non-exhaustive) list of annotated bibliography in order to provide enough insight into the background work that gave rise to the train of thought which in turn resulted in the outcomes of this research. It is hoped that this list gives substance to the claim that Information Security is and should be treated as a multi-disciplinary subject.

It should be obvious by now that in order to productively address the research questions, a number of peripheral issues will also have to be resolved. This can be justified by the fact that although the issue of Social Engineering seems to be in everybody's minds these days, comparatively, very little formal work has been done in this field. (An indication to this can be obtained by

examining the comparatively very small number of hits returned to a library search based on "Social Engineering"). This is justified by the difficulties inherent to the subject, its non-technical nature and its obvious dependencies on sociological and psychological principles.

It is undeniable though that a lot of work that has been done in the past in many peripheral fields, is related to the issues dealt with in this proposal. The degree of this relation, of course, varies immensely, to the extent that sometimes only morsels of past work can be of benefit to the issues at hand. Nevertheless, some of this work will be presented here in the form of annotated bibliography.

Some of the issues that need to be explored in the context of the current work and play a major role in the formation of defenses against SE attacks are: 1) ethics in the work environment, 2) development of an IS culture, 3) interdisciplinary nature of IS, 4) quantisation and metrics of abstract values relevant both to IS and to the defenses against SE attacks, 5) IS education, 6) IS policy effectiveness and assurance measurement and 7) the relation between social interaction and Information Security. The list is by no means exhaustive and it is almost certain that as research in the field advances, other, equally important, factors may be brought to light.

The annotated bibliography that follows can only "scratch the surface" of the issues but can provide and indication of the complexity of the issue at hand and a solid foundation for further research.

Schlienger and Teufel (2003) in their research "Analyzing Information Security Culture" claim that in order to improve the security level of an organisation, socio-cultural measures must be employed alongside the technical and organisational measures in an effort to "*make IS a natural aspect in the daily activities of all employees*". With this in mind, they go on to present the idea that IS is part of a grander "Organisational Culture" that in turn is a collective phenomenon which can be influenced (or even designed) by the management. In this sense they describe security culture as a **three-**

layer entity which begins with the **employee education** necessary to set the foundations of security awareness, moves on to the level where the employees start making **conscious decisions regarding security** and culminates at a point where the notion of security becomes embedded in the employees' minds, thus functioning at a **subconscious level** to protect the organisation.

In order to achieve such a scheme, a tool is needed, by which the state of IS culture at any given moment within an organisation can be analysed and assessed. An attempt to measure the collective values, norms and knowledge, can not yield substantial results as values are theoretical constructs and can be officially stated but do not necessarily reflect the real values governing everyday practice. Hence, an alternative tool for analysis must be found, based on the artifacts that function as cultural indicators and thus help to **qualitatively** derive the true values and assess the culture. (A quantitative relation between the artifacts and the values can not be extracted).

As human behaviour is ultimately driven by cultural, social and ethical values, security culture must encompass all three types of respective measures to improve employee behaviour with respect to security.

The authors then continue with the discussion of methods necessary to collect the data and analyse it to produce useable indicators of security culture. The staff is subjected to anonymous questionnaires and interviews carried out by unbiased observers. The results are plotted in a so-called "Radar plot" in an attempt to obtain an as objective as possible picture of IS culture within the organisation. This result can help the management in taking corrective steps in their effort to further build a stronger IS Culture.

The reviewed work by Schlienger and Teufel (2003) puts forward the notion of assessing the level of IS culture as a tool in the effort to control the non-technical aspects of security within an organisation. The ideas presented

could be helpful in designing controls against SE vulnerabilities as well as in providing for relevent metrics.

In their work "System Architecture for Psychological Customization of Communication Technology", **Turpeinen and Saari** (2004) elaborate on the notion of customising the way information is presented at the content level of a Digital Communication System, with the intention of inducing a predictable psychological effect to the user of the system. From the context of the discussion it can be deduced that the term "Digital Communication System" can be applied to the digital Man-Machine Interface present in all modern Information Systems. To formalise the above notion, the term "Mind-Based Technologies" is used, the basic concept of which is that **the way of presenting information to users falling under certain psychological profiles may have a predictable psychological effect**.

According to the authors, the term *"Psychological Customisation"* is considered as *"an operationalisation technique of implementing the concept of Mind-Based Technologies in system design"*. They then continue by describing a basic system architecture to implement such as Psychological Customisation.

By analysing a Digital Communication System into three layers:

a) the *physical layer* which comprises the technological devices and communication channels,
b) the *code layer* which consists of all the protocols and software necessary for the physical layer to function and, finally,
c) the *content* layer where information resides,

the authors isolate the content layer and act upon it to achieve their goal. They further break down the content layer into i) the *substance* (or core message) of the information and ii) the *form* of the information (i.e. the aesthetic and expressive ways of organising the substance of the information.

Although the larger part of the reviewed paper moves in directions digressing from the scope of the current research, there are many points being raised in it that would be beneficial to the needs of this research.

a) When users collaborate over what is described as: *"computer mediated social interaction"* (e.g. when working together and communicating on-line over a computer network), a state of *"social presence"* may be experienced, such as intimacy of interaction or a feeling of togetherness within the bounds of virtual space. As far as the current research is concerned, this can lead to serious SE vulnerabilities and should be controlled.
b) The authors state their view that the psychological effects on users during *social presence* when in *computer mediated social interaction* have not been sufficiently researched. Elsewhere in the paper it is stated that research has been concentrated on the relation of user emotions to information and how these change the way in which users respond to a message. They further make reference to studies of experimental psychology, which show that "*recognition and memory can be influenced or even enhanced by previous exposure to subliminal visual or auditory images*".
c) Reference is also made to the notion that if one wants to produce emotion with respect to particular pieces of information presented through a given user interface, one needs to know which types of variations of the form of the information may cause which qualitative types of emotion to users with different psychological profiles. As this principle may apply to persuasion among other psychological effects, the relation to the research at hand is made obvious.
d) Another idea that is put forward is that within limits, the form of information presented can be automatically adjusted for a certain category of substance of information, thus creating varying emotions to the user. This can be of value to the research at hand in the sense that sensitive material could be automatically presented in a way that triggers different levels of subliminal user defenses. This "modulation" of the form of

information could be based on a criterion of access rights to the data and/or the sensitivity level of the data.

e) For successful psychological customisation, a modeling process of individual users or groups of users is necessary. The authors consider three different types of modeling: i) user modeling based on individual profiling, ii) user clustering which works by automatically grouping users together based on similarities between their individual profiles and iii) community modeling which attempts to model a social group as a whole. In the context of the research at hand, as all three types of model must supply computer-accessible presentation of information regarding individuals, groups and social structures, these must be considered as data of high sensitivity and all measures must be taken to ensure the privacy of the users.

The authors conclude by stating that "*Psychological Customization is founded on the idea of creating a desired psychological effect with the available means of automatic variation of substance and form of information*". They also state though that "*what is lacking is the systematic and explicit, communicable, knowledge of what exactly in the elements of design may produce such effects*".

The work of Turpeinen and Saari (2004), as it is presented in the reviewed paper, may seem at first to be of a different scope than that of the current research. However, it is hopefully easy to make the short mental leap and apply the principles they describe to the issue at hand. This researcher believes that the principles of Psychological Customisation may well apply in strengthening the psychological defenses of users against SE attacks.

Tsujii (2004), in "Paradigm of Information Security as Interdisciplinary Comprehensive Science" through a philosophical analysis of present-day computer systems, stresses the interdisciplinary nature of IS. The national, social and public security, the protection of privacy and the restriction of unnecessary monitoring over people, require comprehensive measures. These measures require close coordination between different systems such

as administration, management, insurance, information system security and auditing, information legislation, information morals and other such systems that are radically social in nature.

The author identifies the changes brought to social structures by the digitisation of the modern world. Digital technology is tearing down traditional limits imposed on society such as geographical separation and national borders, by creating new social continuums.

The author claims that the evolution of computers and networks has formed a new cyberworld which, as any other unexplored world, requires solutions to its very particular issues like security, freedom and privacy. The multi-faceted nature of these issues requires a comprehensive set of measures if the issues are to be upheld.

To the traditional triad of Confidentiality, Integrity and Availability that defines IS, the author adds the notion of *provability* that provides detailed records of transactions as solid proof that transaction *actually took place*.

The author considers encryption technology as the cornerstone of the construction of the "Digital Society", more than just a framework for protection. However, apart from the technical measures necessary to ensure IS, the author also places great importance on ethical standards and an appropriately developed legal system.

Ultimately, the author focuses on four major requirements for effective IS: i) Technology, ii) Management and Administration, iii) Legal System and iv) Ethics.

The **Technology** aspect should rely on *Cryptography* and *Secure Computer Networks*. **Management and Administration** should be governed by well-accepted IS standards such as ISO 17799 and ISO 15408. The adjustments necessary to modernise the **Legal System** should be in the form of new laws and rules designed to a) develop social infrastructure and b) prevent injustice,

both under the light of the digitisation of the modern world and society. Thus, the general principle behind this modernisation should be to transform the current legal system to apply both to corporeal entities (as it traditionally has done) as well as to information assets that are, by nature, intangible. Finally, on the aspect of **Ethics**, the author bases his dialectic on the argument that "*barriers should be withdrawn between the social-cultural sciences and natural sciences*". The author then goes on to suggest ways in which ethics research could be conducted from an engineering or economic viewpoint, in an attempt to define what the author calls "Information Ethics".

Finally, the author also discusses the necessity of a) international cooperation in the context of improving Information Security and b) human resource development for IS, identifying four major classes: organisation leaders knowledgeable in IS, IS system engineers, ISMS experts and, finally, IS researchers.

This paper by Tsujii (2004) clarifies the interdisciplinary nature of IS, if an attempt to comprehensively address security vulnerabilities is to be effective. The notions put forward in this work can help view traditional measures for IS under the light of moral and ethical implications, that can help control SE vulnerabilities.

The paper by **Kokolakis et al** (2000) "The use of business process modeling in information systems security analysis and design" deals with the way IS is incorporated in modern organisational structures. Risk Analysis methods are used to justify the investment in IS which is usually seen as a necessary add-on to the existing Information System. Risk Analysis (RA) alone does not provide for an understanding of the organisational environment in which Information Systems operate as it is usually based on a very simplistic model of Information Systems, consisting of hardware and software assets that are vulnerable to threats. Consequently, although the resulting countermeasures may help in reducing vulnerabilities, the way the organisation operates is not improved security-wise. The authors thus propose a comprehensive methodology for Information Systems Security Analysis and Design, that

incorporates both risk analysis and organisational analysis that is based on Business Process Modeling (BPM) techniques. In this context several BPM techniques are classified, reviewed and compared with respect to their individual merits under a security perspective and their possible contribution to Information Systems Security Analysis and Design.

By coupling BPM with RA the authors hope to re-target organisational procedures towards a) obtaining a better understanding of the organisational framework within which a secure Information System is to operate, b) re-designing secure processes and c) integrating IS into Information Systems instead of importing it as an add-on.

The paper concludes by stating that either existing BPM techniques will be adapted with respect to IS or several of them combined in order to contribute to Information Systems Security Analysis and Design, or new specialised BPM techniques must be developed particularly for Information Systems Security Analysis and Design.

The work presented in the paper by Kokolakis et al (2000) emphasises the notion of designing for security preemptively, instead of attempting to adapt security solutions to fundamentally insecure systems. They stress the fact that an information system is much more than the sum of its assets as it relies upon its users for secure operation. Elements of this work can be used to give a Business Process perspective to the current research.

The paper "An Analysis of Ethics as Foundation of Information Security in Distributed Systems" by **Leiwo and Heikkuri** (1998) attempts to analyse the notion of Ethics as a foundation of IS in distributed systems. The authors accept that IS requires both technical and administrative foundations, the latter being based on several non-technical layers added on top of technical communication protocols such as cryptography etc. They then try to impartially describe the situation regarding ethics both from the point of view of the Hacker community and from that of the IS personnel. Due to the major differences between hacker and IS personnel ethics, significant problems in

establishing ethical protection measures against violations of IS, arise. The authors, very early in the paper, stress the fact that their analysis leads to opposite results than the generally accepted idea according to which the security of information systems can be founded upon common ethical standards.

The two conflicting ideologies (hacker vs. IS personnel) lead to both groups claiming that "*they have a right to tell each other what is ethical and what is not*". However, it seems that the IS personnel group currently have law enforcement on their side.

Apart from the above philosophical and practical conflict, the expansion of the Internet brings communities and cultures with different ethical standards and norms of acceptable behaviour closer to each other. As a result, a de facto enforcement of policies for ethical use of the Internet governing these heterogeneous cultures may not be practically possible.

Hence, one of the most important questions of the paper is if and how a common ethical foundation for IS is possible. No clear answer to this question is furnished in the paper; instead, many facts are presented and the reader is allowed to draw his/her own conclusions.

One of the most important points made in the paper is that "*ethics in information technology is such a large question that system designers, developers and users are not alone enough to give answers. Instead,* (the) *entire society should be involved in the discussion concerning responsibilities of different groups involved*". Furthermore, an interesting definition of the dual character of ethics' purposes is presented: to find criteria to distinguish between good and bad, and to promote good desires and discourage bad ones. Ethics can be approached either as deontological, or rule-based, ethics, or as consequential ethics. According to deontological ethics there are actions that should be taken and other actions that should not be taken. Consequential ethics, on the other hand, examine not the actions themselves but their value as determined by the outcome. IS personnel tend to take the

root of deontology while hackers claim that their actions provides good outcome for the IS community and is thus venerated.

Due to the fact that proposed ethical protection measures are collective in nature and attempt to provide a commonly agreed upon high moral code for the usage of communication networks, it is very difficult for hackers to accept these measures as they tend to maintain their individualism and independence in their approach towards computing and ethics. If this is co-examined along with the fact that a large percentage of computer crime is generated within the bounds of organisations rather than from the outside, the problem of creating acceptable ethical standards is augmented.

Any attempt towards the creation of a framework for strengthening IS must take into consideration three fundamental requirements: a) the natural behaviour of human beings must be supported by the framework through the establishment of social contracts, b) the frameworks must be of an iterative nature, so that larger systems can be composed from smaller subsystems and c) the feasibility of the framework must be ensured based on current technologies. All this should lead to a two-phase application, comprising an **Ethics negotiation phase** where "*organisations or individuals representing themselves negotiate the content of ethical communication agreement over specific communication channels*" and an **Ethics enforcement phase** where "*each organisation enforces changes in the ethical code of conduct by specifying administrative and managerial routines, operational guide lines, monitoring procedures, and sanctions for unacceptable behaviour*".

In conclusion, the authors re-iterate the difficulties in bridging the gap between the ethics of hackers and those of IS personnel and identify the potential risk of increasing the underground computing community through more stringent law enforcement.

The reviewed paper by Leiwo and Heikkuri (1998) does not provide any complete answers to the question of formulation of ethics with respect to the secure use of information systems. The real value of the paper lies with the

fact that a comprehensive review of the foundation of such ethics **is** presented, along with the problems that do arise in this context. As far as the current research is concerned, it helps in placing non-technical measures and controls under perspective and will further help evaluate the feasibility of such measures.

van Niekerk and von Solms (2005), present in "A Holistic Framework for the Fostering of an Information Security Sub-Culture in Organisations" a framework for fostering a sub-culture for IS in organisations. They base their dialectic on the accepted dependence of information resources on human co-operated behaviour. Both intentionally or through negligence, and often due to lack of knowledge, users may pose the greatest threat to IS within an organisation. Users must thus have a sufficient degree of knowledge on information security so that IS controls are effectively implemented and maintained. Users must also exhibit the correct attitude towards IS. These two qualities of users can not exist without one another, as knowledge without correct attitude can not ensure IS, neither a correct attitude towards IS can be sufficient without the foundation of relevent knowledge.

Generally accepted standards and practices such as ISO 17799 / ISO 13335-1 and NIST 800-16 (ISO/IEC 17799:2000a; 2004; National Institute of Standards and Technology, 1998 respectively), stress the need for user education and appropriate training on IS. However, no document defines "appropriate training". It is thus necessary to tailor the training program to the needs of the individual users in the context of the organisation under examination. Furthermore, even if users have acquired sufficient knowledge on their role with respect to IS, it is not guaranteed that they will adhere to a security policy because it might conflict with their beliefs and values. It is thus necessary to restructure users' beliefs and values, in a way that promotes IS. This can only be achieved by cultivating an organisational subculture on IS. By combining various methodologies used for employee education and for the establishment of an IS sub-culture into a single holistic framework, the successful secure management of information systems resources in an organisation can be achieved.

The authors work results in a proposed framework that is structured as follows:

1. Attain top management commitment.
2. Define the culture change in the context of the specific business problem for each business problem.
3. Educate the employees using outcomes based education.
4. Define culture change metrics.
5. Provide feedback to the employees that is backed by both rewards and counter-incentives or punishments.
6. Review and refine the culture change process in an effort to strengthen the culture and assist with the internalization of the new culture.

The above framework may provide an effective holistic approach towards the creation of the organisational culture necessary for IS.

The work of van Niekerk and von Solms (2005) addresses one of the major issues that the research at hand will be looking at: strengthening the defenses against SE through the knowledge and behaviour of users. The reviewed work provides a solid basis for creating effective non-technical countermeasures and controls.

The paper by **Orgill et al** (2004) titled "The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems" stresses the importance of the human factor in the overall security of an information system, identifies it as the weakest link and relates this weakness to the reality of SE attacks. Brief references to the methods of operation of Social Engineers are made and the merits of the "Approved Social Engineering Audit" (ASEA) as an evaluation tool for determining compliance to security standards and internal security policy are presented in detail.

A case study of an ASEA carried out without notice within an organisation is presented and its results discussed. Certain constraints, prerequisites and the delimitation of such an audit are also examined.

The ASEA was carried out by an auditor assuming the role of a social engineer in order to assist security managers understand the weaknesses in their system and verify that users are following security policies.
A detailed presentation of the audit itself is made and the results of the audit are evaluated and discussed. The effects of this exercise on company policy are briefly discussed and the need for "tailor-made" security education is highlighted. The need for both technical and non-technical controls for SE vulnerabilities is identified.

The value of this paper by Orgill et al (2004) to the research at hand is none other than the very important formal presentation of an audit geared towards identifying SE vulnerabilities and correlating its results to many aspects of an active IS policy. Through this analysis, the value of certain aspects of the audit is made evident and the design of such audits is aided.

Vaughn et al (2003) in the paper titled "Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy" deals with the taxonomy of Information Assurance (IA) metrics. It also summarises the findings of a workshop on the subject that was held in Williamsburg, Virginia, U.S. during the period May 21 through 23, 2001. It begins with the definition of the term "Assurance" as *"an expression of confidence that one has in the strength of mechanisms or countermeasures"*. It identifies the problem of devising metrics that reliably depict the assurance associated with a given Information System. The need for making IS an **integral** component of corporate IT architecture is stressed. The lack of generally accepted, reliable measures for rating IS and security assurance along with inconsistent terminology for IS are highlighted.

The authors then proceed to report on the general findings of the Williamsburg workshop, among which they discuss the confusion related to the nature and value of metrics, the lack of proof of correctness of a measurement procedure, and the non-quantifiable nature of assurance system requirements.

An interesting point made is that the "*Aggregation of various countermeasures may result in an inherently less secure system*", and that (given the complexity and inter-relations of computer systems) this can lead to a false sense of security.

Another point made is that "*We remain reliant on the expertise of our systems administrators or security engineers and their specific knowledge to guarantee the correctness of a system*". Clearly, as "to err is human" this assumption does not provide enough assurance.

Yet another interesting point is that as time progresses, it is easier to mount an attack on a system due to pervasive communications and shared knowledge on the Internet. Attacks need no longer be as labour intensive as they used to be, neither require as high a level of expertise on the part of the attacker as they used to, as strong, automated attack tools are ordinarily created and shared.

As a single homogeneous system of metrics can not address the problem of measuring assurance sufficiently, at the Williamsburg workshop, there were three general categories defined:

• Technical category that includes measures/metrics that are used to describe and/or compare technical objects (e.g., algorithms, products, or designs).

• Organisational category where measures are best applied with respect to processes and programs; and

• Operational category where measures are thought to describe, “as is” systems, operating practices, and specific environments.

Another interesting issue raised is that metrics seem to vary between the government and commercial sectors. In government applications, emphasis is placed on policy and compliance to regulations and directives. In the commercial sector the main issues are driven by economics and interest lies with risk assessment (in financial terms) and the tangible return on the investment in security.

Retaining from the wealth of the paper only those pieces of information that may be of value to the research at hand, in the context of the taxonomy proposed by the authors, the category types of Information Assurance (IA) metrics are defined as: objective/subjective, quantitative/ qualitative, static/dynamic, absolute/relative or direct/indirect. (A discussion is beyond the scope of this summary and the interested reader is referred to the original work). In terms of IA metrics Taxonomy, it is stated that "*the objective of assurance measurement could be grouped into two distinct categories: 1) assessing an organization's IA posture or 2) measuring the IA capabilities of systems or products*". In this sense, there are two groups of metrics defined: a) Metrics for Organizational Security and b) Metrics for Technical Target of Assessment
(TTOA). A further classification appears below:

- Metrics for Organizational Security (measure organizational programs and processes).
  - IA Program Developmental Metrics
    - Policy Management Metrics
    - Process Maturity Metrics
  - Support Metrics
    - Personnel Support Metrics
    - Resource Support Metrics
  - Operational Metrics
    - Operational Readiness Metrics
      - Management Readiness Metrics
      - Technical Readiness Metrics
    - Operational Practice Metrics
    - Operational Environment Metrics
  - Effectiveness Metrics

- Metrics for Technical Target of Assessment (measure the level of assurance provided by a technical object, system or product, in terms of protection, detection and response).
  - Metrics for Strength Assessment

  - Metrics for Features in Normal Circumstances.
  - Metrics for Features in Abnormal Circumstances.
    - Adversary Work Factor Metrics.
    - Survivability Metrics.
- Metrics for Weakness Assessment
  - Risk metrics.
  - Operational limitation metrics.

After recapitulating on the main issues discussed in the paper, the authors conclude by presenting their views on the main qualities of the taxonomy that they propose, which are summarised as:
- The categories must be accompanied by definitions in order for any and all IA metrics to find membership.
- The taxonomy must be made comprehensible and suitable for a general audience.
- The terminology of the taxonomy must be consistent with the established information systems terminology.
- The classification scheme must provide an IS professional with a tool to help consider all areas needing measurement and suggestions for types of measures to employ.

Although not directly aimed at the problem of metrics for SE issues, the principles behind the general discussion of metrics by Vaughn et al (2003) can be of great value to the research. The paper once again stresses the multi-faceted nature of measuring for security and promotes penetration testing (a highly empirical, non-exact and to a large extent non-repeatable method but, nevertheless, a method capable of yielding important results) as a crucial factor for assessing the level of Information Assurance. Furthermore, the insight on the fundamental differences between the security and assurance needs of the private and government sector, provides food for further thought and serves as the foundation of an IS approach that is highly differentiated with respect to the two sectors.

Jelen and Williams (1998) in their paper "A Practical Approach to Measuring Assurance" challenge the traditional definition of assurance as "*the degree of confidence that security needs are satisfied*" and proposes a different conceptual definition of assurance as "*a measure of confidence in the accuracy of a risk or security measurement*". **This makes assurance orthogonal to the measurement of both risk and security**. Using this definition, assurance may be more accurately measured and better communicated. By combining such measurements of assurance w.r.t particular issues from different sources, decisions on security risks can be made more effective due to the better quality of the information that they are based on.

The authors accept that absolute and consistent measurement of assurance is probably unattainable. Instead, they claim that one can take advantage of quantitative risk measurement methodologies that may be employed in a way that yields a rough measure of assurance. This rough measure permits a trade off between seeking more evidence and thus gaining greater assurance on one hand, and employing more safeguards, thus reducing risk on the other. The conclusion of the authors is that although this method does not provide an exact measure of assurance, it does provide a good indication of whether there is enough of it.

The measurement scales associated with the proposed definition of assurance and the resulting measurement methods need not be exact. Scales can employ numeric or fuzzy values and can be relative or absolute. Once a scale has been decided upon, the "security need" can be expressed as a threshold value on that scale. By comparing a measurement of the actual level to the threshold value, it can be deduced whether the need has been satisified. The possibility of uncertainty in the measurement is taken into account.

By keeping the concepts of assurance, risk and security orthogonal, a clear distinction between them is maintained and any confusion caused by the overlap of their meanings is kept to a minimum. While "*high assurance ratings*

have traditionally been associated with high security and low risk", the authors' new approach "*allows high assurance to be associated with low security and high risk as well*".

An example of the above principle presented in the paper is to consider a network component with a large number of security mechanisms, but no information to indicate whether or not they are correctly configured. In a situation like this, it is unclear how the various security mechanisms affect the amount of assurance. Making security orthogonal to and independent of assurance, the sources of added security can be considered separately from sources of added assurance. To raise assurance, it would thus be necessary to first gather more specific information about the configuration of the security mechanisms than to add another such mechanism.

The authors continue by presenting in detail this principle and also provide necessary mathematical models to assess and reduce the uncertainty inherently related to the measurement and assessment methods. They also provide insight on how the proposed assurance evaluation methods can be used to ascertain an organisation's security standing at any given moment, and, based on that information, subsequently plot the appropriate course of corporate action.

As the quantification of risk, security and assurance regarding SE vulnerabilities is very difficult to achieve due to the very nature of these vulnerabilities, the redefinition of assurance presented in this paper by Jelen and Williams (1998) can help address such issues in a non-exact way. This could prove more useful in analysing and assessing the SE problem as well as dealing with it.

This definitive sociology book (originally published in 1966) by **Berger and Luckmann** (1991), titled "The Social Construction of Reality. A Treatise in the Sociology of Knowledge" deals with the sociology of knowledge in society and in particular with what constitutes the reality of everyday life for the average member of society. Berger and Luckmann view society as a dialectical

process between objective and subjective reality. Humans, through knowledge, are thus engaged in a perpetual cycle of creating the objective reality socially and subsequently internalizing these created realities as their own, subjectively. The authors put particular emphasis to the role of knowledge in constructing these objective and subjective realities.
The book is divided into three sections:

a) The foundations of knowledge in everyday life
b) Society as an objective reality construct (i.e. How the objective reality is socially constructed through the mechanisms of institutionalization and legitimation or how social realities hold their own among social groups of people and do not rely on the perceptions of any single individual).
c) Society as Subjective Reality (i.e. how the constructed objective social realities are in turn internalized by individuals as their own subjective realities through primary and secondary socialization processes).

By applying the principles described by Berger and Luckmann (1991) of objective and subjective reality to the constructs of ISMSs, interesting conclusions can be made regarding the social aspects of information security. As the book by Berger and Luckmann and their theory are widely accepted, the application of their principles to IS, may yield some interesting sociological results that may help in explaining several aspects of IS that previously were not considered in depth. Hence, the multidisciplinary character of IS is once again brought to light.

Kevin Mitnick has been called a "cyber-desperado". His unusual abilities with computers led to his conviction and imprisonment on several accounts of computer fraud. After his release from prison in 2000 he has been offering security consulting services. In their book " The art of deception" **Mitnick and Simon** (2002) present a number of attack scenarios, all based on SE methodology. The scenarios are analysed and possible defenses are also discussed. SE methods are dissected and insight necessary to defend against them is presented. Although some of the scenarios do seem too far-fetched to constitute plausible SE attacks, the point is not whether they are true or not. What Mitnick and Simon achieve through accomplished story-telling, is to

raise the average reader's level of awareness against SE. On the practical side, Mitnick proposes a number of countermeasures and practices that should be incorporated in any security policy to better protect against SE.

By studying the analyses that Mitnick and Simon give of a number of SE attack scenarios, the researcher is exposed to most of the common circumstances that may act as SE vulnerabilities. By identifying the relevant risks, efficient measures can be devised to mitigate them to a better extent. Some of the countermeasures presented in this book can be incorporated in the formal description of controls against SE.

In their second book, **Mitnick and Simon** (2005) present a number of attacks carried out through straightforward hacking methods. The discussions of these attacks show that most implemented information systems are running with significant security holes uncovered. This can only be attributed to the increasing complexity of information systems and the complacency of their administrators that may be justified by a false sense of security instilled upon them by the volume of security controls that *are* in place. By going through the various scenarios, Mitnick highlights the risks as well as measures that should be taken to mitigate them. Technical issues aside, the book includes a chapter on SE contributed by Social Psychologist Dr. Brad Sagarin in which the fundamentals of SE methodology is analysed.

Although most of this book by Mitnick and Simon (2005) is not directly related to SE, by studying the analysed scenarios, the SE researcher can quickly see in which ways, seemingly unimportant information can aid the work of the attacker and hence how tempting it is for the attacker to use SE techniques to obtain that information. It is evident that not all hackers possess or can master the necessary skills to carry out a SE attack, but for those who do or can, taking the extra step forward is the obvious solution. An attacker who can use both technical and SE methods against any information system is thus very difficult to fight against.

Dr. **Cialdini** (2001), a professor of Psychology presents in his book "Influence: Science and Practice" the notion of influence in a structured and concise way. Cialdini discusses what he sees as the fundamentals of influence, namely: Reciprocation, Commitment, Consistency, Social Proof, Liking, Authority, Scarcity and Automaticity. The detailed discussion and practical views of these fundamental principles enable the reader to obtain a well-founded insight on them. Furthermore, practical psychological countermeasures against influence are presented in each chapter.

By placing the fundamentals of influence in the context of SE, a structured approach to the methods used by Social Engineers is achieved. By identifying the inner structure of the SE construct, the individual key-components of SE can be singled-out. This, in effect, leads to the breakdown of the SE problem in smaller, more manageable morsels. By devising defense strategies against the smaller issues, the risks stemming from SE may eventually be mitigated to an acceptable level.

The book "Get anyone to do anything" by Dr. **Lieberman** (2000) targets the general audience rather than being a scientific publication per se. Despite the fact that in some cases the book seems to provide oversimplified explanations and guidance on issues of influence, its value can not be underestimated. In many ways it can be viewed as a practical guide on imposing one's will on others and on the other face of the same coin, defend oneself against such attempts by others. Most of the techniques and scenarios examined in this book can be and probably have been) used in SE attacks. Through its easy-going style, this book can serve as a tool in raising awareness regarding SE. Its informal ways and unpretentious language make for easy reading. Material from it could be adapted for use in any security training course, or the whole book could be included as recommended reading.

By applying the information presented by Lieberman (2000) to the principles of SE many valid conclusions can be drawn as most of the techniques used are indeed used in the course of a SE attack. This work supports the more

formal analysis found in the book by Cialdini (2001) and does help in specifying controls against SE attacks.

Max Weber (1864 -1920), a German political economist and sociologist, is considered one of the founders of the modern study of sociology and public administration. As is the case with many of his other works that are famous today, "Economy and Society" (**Weber**, 1978) constitutes a collection of his writings that was revised and published posthumously in 1922. In the first volume of this book, Weber sets the basis for the discussions that are to follow: Basic sociological terms, and definitions of sociological categories, status groups and classes as well as legitimate domination are discussed. A detailed discussion of economy then follows where economy is tied to the social norms and to the relations between organised groups. In the second volume, Weber discusses the legitimacy of domination that is imposed by modern law and state, bureaucracy, traditional domination in the form of patriarchalism, patrimonialism and feudalism, charismatic domination and political domination. Focusing on Weber's study of bureaucracy as presented in "Economy and Society", it is generally accepted that this work constitutes the basis for the "Weberian civil service" generally adopted by European countries. Many aspects of modern public administration go back to the original model presented by Weber that laid the foundation for the vertical, hierarchically organised civil service structure.
Traditional security structures are based on the vertical hierarchical model of Weberian bureaucracy. Consequently, Information Security structures and, to a large extent, ISMSs follow the same principles. When viewed from this angle, shortcomings of modern IS structures that would otherwise go unnoticed are brought to light. When the subject of domination discussed by Weber is transposed to the societal structure supporting the ISMS, the effect that the ensuing power play has on the function of the ISMS, also surfaces. Hence, the social dimension of Information Security is becoming delineated and the foundation is set for a more thorough examination.

In his book "Science in Action: How to Follow Scientists and Engineers Through Society", **Latour** (1987) questions the very essence of the way that

scientists view the world. Scientific process is fundamentally challenged and Latour asks for the re-evaluation "scientific truth". Latour introduces the bipolar principle that on the one hand states that truth is absolute and the scientist is there to explore it, while on the other that facts are actually constructed in the course of scientific work even though they are mostly presented as axiomatic and unquestionable. In this context, "Actor Network Theory" is introduced along with the notions of power struggle and black boxes. In a short, and perhaps oversimplified way, Latour claims that "facts" are not necessarily so but are instead constructed through the social interactions between competing groups of scientists. The opinion of the stronger groups prevails -hence the notion of power is introduced- and the result of the conflict is henceforth considered a fact and rarely challenged. This unchallenged fact, in effect, constitutes a "black box", that encompasses a crystalised opinion which is in turn used as a building block for further construction. Being buried at the "bottom of the pile" the black box remains closed and the notions contained in it are never re-examined. Latour thus claims that although a scientific fact may have reached modern times as neatly packaged and sterile, when its background is examined by going all the way back to the time of its creation (or the instance of closure of the black box) the circumstances that led to the creation may appear tumultuous and full of recriminations between competing groups. In a radical way, Latour proposes the re-opening of black boxes in order to evaluate their contents and hence the paths followed once the black boxes were closed.

As the upholding of security clearly has a social component that may be exploited and used against that objective, it is necessary to examine Information Security from the point of view that Latour proposes. IS is currently built around notions that have remained unchallenged for too long. These may harbor systemic flaws that can go undetected if the black boxes are not re-opened and re-examined. This is the idea behind the re-examination of notions regarding security that are considered indisputable but could be flawed.

Latour (2005) in his book " Reassembling the Social: An introduction to Actor-Network-Theory" once again challenges the existing notions of Science by attempting to re-define the term "Social" that, according to him, has lost its original flexibility as it has become laden with assumptions. Latour thus attempts to re-define "Social" and allow it to resume "the task of tracing associations". This approach of "Sociology of Associations" is the essence of Actor-Network-Theory (ANT). From its original applications in science studies, in this book, ANT is expanded to include many other domains such as health, management, art, religion, law, politics etc. As the author states, the objective of this book is to clarify the ambiguity associated with ANT which is largely due to the vagueness of the word "social". To reach this objective, the author claims that "sociology may be construed as the science of associations and not only as the science of the social".

This work by Latour (2005) gives a better insight on ANT and as such it can make the application of ANT in the study of security structures more accurate. Through the evolution of ANT, new paths can be explored and new results may be obtained with respect to the social construction of security systems.

2.4 Concluding Remarks

This chapter sets the foundation for the following chapters by firmly establishing what the current situation of Social Engineering in the context of Information Security is. Through the presented literature survey the main ideas that helped shape and direct this research are exposed. The multi-disciplinary collection of reviewed sources ranging from Computer Science to Business Process Modelling to Psychology and Sociology show that the solution to the problem of Social Engineering is impossible to be located in a single scientific field. This problem will thus be approached in the course of this work from a multitude of angles (IT Sec, IS, Psychology, Sociology and Metrics) in the chapters that follow.

3. Social Engineering as a backdoor to ITSec and IS infrastructures

3.1 Introduction

The introduction to the current state of things in Information Security (IS) as well as the literature survey presented in previous chapters, set the foundation for the study of Social Engineering (SE) in the current chapter. Here, a discussion of SE is presented with respect to the methods of operation of Social Engineers, and the loopholes in the system that can be exploited.

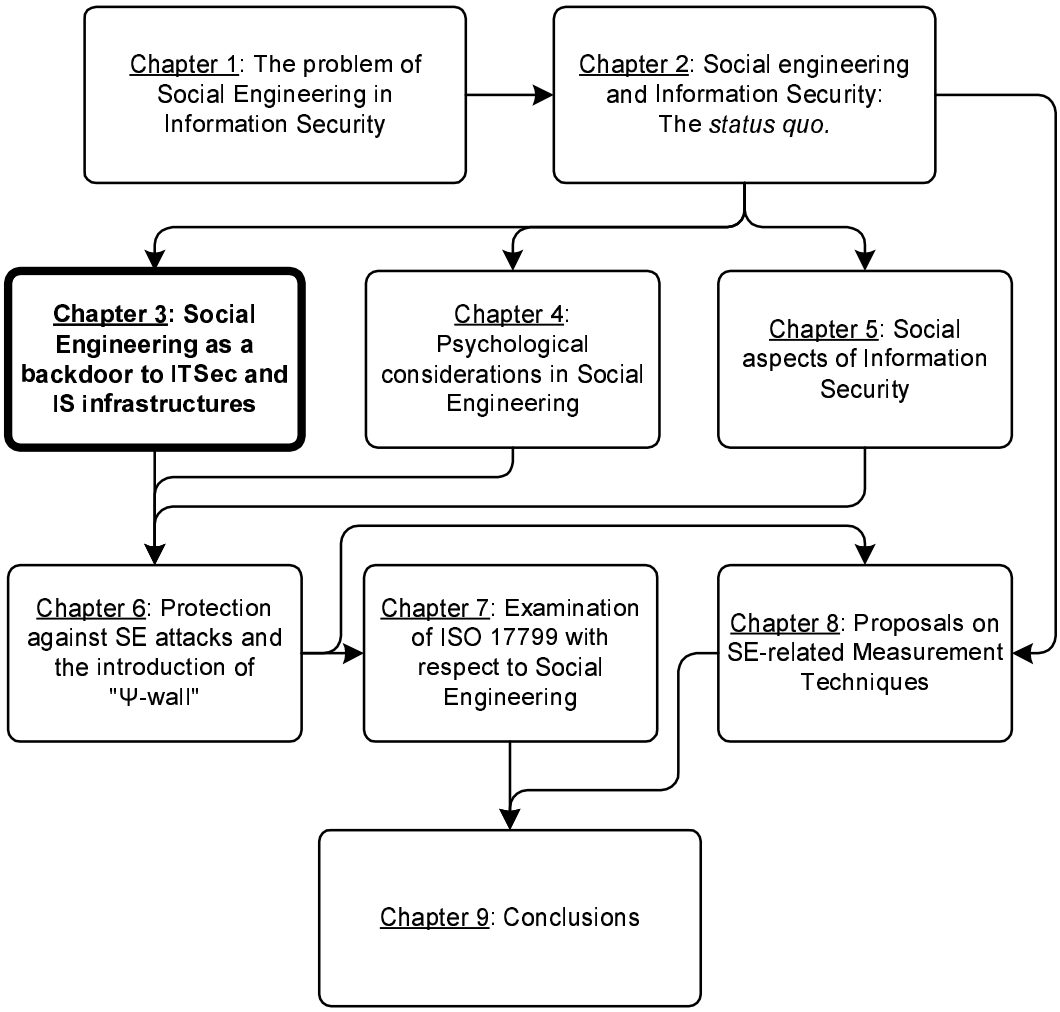

Figure 3.1: Chapter 3 within the context of the overall dissertation structure

This chapter, along with the work that will be presented in the next two chapters on the psychological considerations in SE and on the social aspects of IS, will help in better assessing the controls of the ISO/IEC 17799:2005 security standard (ISO/IEC, 2005a) with respect to SE, in a chapter to follow. Figure 3.1 depicts the role of this chapter within the overall structure of this dissertation.

3.2 Definition of Social Engineering

Security policies are created with the common goal to protect the integrity, confidentiality and availability of information (Pfleeger, 1997, p.4). To this end they try to comprehensively address all security issues and attempt to cover everything from physical security, to electromagnetic emissions control, to personnel certification and authorisation, to user authentication etc. However, one issue that is very difficult to cater for, is that of the exploitation of psychological traits that are inherently present in all humans. By exploiting such human characteristics, an attacker can bypass most (if not all) security rules and directives specified by even the most stringent of security policies and gain access to the sensitive information which is thus only falsely assumed to be safe.

People who employ such methods to circumvent the existing security measures need not necessarily be technological wizards in the sense that hackers are. All they need is good communication skills and the ability to quickly adapt themselves to situations and roles that the ordinary benevolent person can not. These people are commonly described as "Social Engineers" (Mitnick & Simon, 2002, p. 7). The "Engineer" part of the title signifies the attackers' ability to design an attack procedure and successfully carry it out. It equally denotes the ability of the attacker to swiftly adapt to changing situations while interacting with a target (or victim or "Mark"). The term also indicates the possession of problem-solving skills necessary to avoid any pitfalls and through manipulation of the Mark to achieve the desired effect of gaining access to the sensitive information required.

Accordingly, the types of attack that target the human element within a protected system in an indirect and possibly unorthodox way, in order to surpass existing security controls, are generally described by the term "Social Engineering". Those who carry out attacks of this type can successfully apply methods of Social Psychology against other people, with the ultimate goal of gaining access to restricted information. Such attacks call for a high level of preparation and the collection of data that simplifies the attack and makes the claims of the attacker believable.

A formal definition of Social Engineering is found in the Meriam-Webster online dictionary (2004), where it is described as the "*management of human beings in accordance with their place and function in society : applied social science*".

Social Science "*deals with the institutions and functioning of human society and with the interpersonal relationships of individuals as members of society*" (Meriam-Webster, 2004). A Social Engineer will focus on building and exploiting an interpersonal relationship with the Mark. This relationship does not have to be based on a false sense of trust. Alternative routes that are followed by the Social Engineer can be based on psychologically negative principles such as intimidation or fear. Furthermore, the relationship resulting from a SE attack can not always be prescribed, as it is invariably molded by the interaction of the Social Engineer and the Mark. This uncertainty can only be controlled by the skill of the Social Engineer. The Social Engineer's ability to adapt to rapidly changing situations dictates the degree of success of the attack.

As it is clear up to this point, definition-wise, there has been no direct correlation of SE to Computer Systems. This is true because the methods grouped under the term "Social Engineering" are neither particularly related to computer technology, nor are they something new. SE techniques have been used since the birth of mankind to extract information and achieve goals

through the manipulation of unwilling (at least in principle) people. From the ancient art of spying and infiltrating the enemy's ranks to the more modern applied art of advertising, to telephone scams, and pyramid schemes, all fall under -or have a lot in common with- Social Engineering in the sense that they all require considerable skill from the part of the attacker in order to convince the Mark to do something that he/she would not normally do. SE has always been the weapon of choice used to carry out traditional fraud. Hence, the extension of SE practices necessary to take advantage of the opportunities rising from the vast field of computer systems and the information processed through these, is far from unexpected.

Granger (2001) identifies the goals of computer-related SE as being similar to those of hacking in general: "*to gain unauthorised access to systems or information in order to commit fraud, network intrusion, industrial espionage, identity theft, or simply to disrupt the system or network*". This statement formally describes the adaptation of old-fashioned subterfuge to modern technology-oriented reality.

In an effort to better define "Social Engineering" in the context of the computer age, the Hacker's Jargon Lexicon (2004) states: "*Term used among crackers and samurai for cracking techniques that rely on weaknesses in wetware rather than software; the aim is to trick people into revealing passwords or other information that compromises a target system's security*". Note: For clarity, "Wetware" (also known as "Meatware" or "Liveware") according to Hacker's Jargon Lexicon (2004) is defined as: "*1. The human nervous system, as opposed to computer hardware or software. 2. Human beings (programmers, operators, administrators) attached to a computer system, as opposed to the system's hardware or software*".

In the "Complete Social Engineering FAQ" by Bernz (2004) it is stated that "*Hacking takes more advantage of holes in security while social engineering takes advantage of holes in people's common sense*".

Thus, a more precise definition of SE for the special context of computer-related crime would be: **"The subtle psychological and mental manipulation of legitimate users of a computer system, leading to the disclosure of sensitive information that facilitates the attacker to obtain access to that computer system or the data processed on it".** The manipulation has to be subtle because nobody possessing a reasonable level of common sense, will succumb to an unreasonable demand made by the attacker. In this sense, the victim must be manipulated within the scope of his/her everyday tasks and responsibilities. Social engineering does not involve any kind of telepathic mind control and as such can not force actions to be taken by the victim.

3.3 Methods of gathering information

The phase of the SE attack where the attacker actually interacts with the Mark represents the culmination of the attack. At that point the attacker usually adopts an "all or nothing" attitude: either "come up with the goods" or "walk away and close that door for good". In order to launch a successful attack, the interaction phase only follows after careful preparation. Invariably the Social Engineer must present the Mark with enough accurate information to produce the required results. This information may be directly offered, such as quoting names that the Mark is familiar with, or indirectly, for example through the use of specialised terminology or lingo.

Gathering the preliminary information that allows the Social Engineer to make believable claims is paramount to the attack's level of success and takes place in many and frequently unorthodox ways.

In most -if not all- cases, the Social Engineer gathers information by correlating disjointed pieces of data that usually have low or no value on their own. For example, the name, position and internal telephone extension number, of an employee may be casually obtained during different phases of the SE attack and not raise alarms as, on their own, these pieces of

information are not considered sensitive. By combining these with another piece of information, say, when the targeted employee will be out on vacation, the Social Engineer may succeed in impersonating that individual. The special abilities of the Social Engineer have to do with extracting pieces of correlated data from different sources, in order not to raise suspicions, and amalgamating them into a smooth-grained object of value. To accomplish this, the Social Engineer must frequently "fill in the gaps" by, usually, non-factual but truthful-sounding statements, as well as identify problem areas. The objective is to present a well-composed line of statements to the victim of the attack. The problem areas that arise from lack of information (i.e. when the gaps are too difficult to cover for) must at all cost be avoided during the conversation of the Social Engineer with the victim. The confabulation generated by the Social Engineer must thus be carefully steered away from dangerous areas, without tipping the victim to the direction that anything might be out-of-the-ordinary. Any harshness in the verbal manipulation on the part of the Social Engineer or inklings to stupor will most probably trigger the victim's defense mechanisms.

Irrespective of whether the information gathered is "preliminary", to be used in the actual attack, or the main objective of the Social Engineer, the methods used to obtain it demand great levels of ingenuity and lateral thinking on the part of the Social Engineer. The objective of the Social Engineer is to obtain information that would be otherwise near impossible to obtain through traditional technical attacks and hacking.

3.3.1 Dumpster Diving

This technique for gathering information may actually sound worse than it is. It has to do with sifting through discarded documents, magnetic media or hardware in general, with the intention of squeezing out any valuable information from them. Organisations, traditionally, have not been taking care of their garbage. The general tendency is to regard anything that has served

its purpose as useless and, as such, all intrinsic value assigned to it is automatically nullified. This, however, is far from true.

Of all the documents that are being dumped, some may be regarded as less important than others and not compromising to the organisation's security of operations. Although the latest draft report for a revolutionary new product will probably not find its way into the garbage unshredded, the outdated version of the internal phone directory that has just been updated, most certainly will. If a Social Engineer obtains this directory, the internal structure of the organisation becomes apparent. By perusing this directory, the Social Engineer can locate targets, impersonate people of influence, or simply refer to such people in order to clad his/her arguments in a coat of unquestionable authority.

Discarded internal memos and magnetic media that contain truly unimportant information per se can be used to provide information about, e.g., an ongoing project that will help make the Social Engineer's claims believable. Just the internal name of the project may help convince an unsuspecting Mark that the Social Engineer is a person with legitimate claims.

Outdated and old revisions of policy documents, system manuals, surplus workgroup calendar copies including vacations, duty rosters, bad printouts, unwanted excess photocopies etc, can be used by the Social Engineer to find weak spots in the security of the organisation as well as decide on the most appropriate time for the attack when particular people are away from the office.

Discarded hardware can also provide both substantial information as well as morsels thereof that can be interwoven to re-create the "bigger picture". From the extremely obvious hardware pieces such as inoperative hard disks that could be resuscitated for long enough to give up the information they carry, to unfixable fax machines that are being thrown away complete with a thermal

transfer membrane that holds images of the last two hundred incoming fax pages, all can be used by the Social Engineer to extract information.
In another, indirect way, hardware such as discarded networking cards, may provide vital clues to the nature and structure of the organisation's computer network. If the existence of a wireless network is suspected, the Social Engineer could try to pick up the signal by using a notebook computer or PDA from the comfort of his/her car in the visitor parking lot.

Even non-technical material found can be used to allow the Social Engineer physical access to the premises without raising suspicion. Such material could be an old uniform bearing the organisation's emblem, an ID card cut in two that does, however, provide the Social Engineer with invaluable detailed information on the card's appearance, or even, if people are really not careful, blank forms, stationary bearing the organisation's letterhead etc, that can be used to aid the imposter in building the correct image for him/herself.

3.3.2 Physical attacks at the workplace

The Social Engineer will not resort to being physically present at the target location unless it is imperative to do so. Any self-respecting Social Engineer will proceed to such a high-risk operation only after the necessary groundwork and preparation has taken place and, possibly, fake credentials -like ID badges- have been produced through manufacture, alteration or theft.

Even in cases where security is supposed to be high, the Social Engineer can penetrate using a variety of methods that, in general, divert the attention of security officers away from their specified tasks, i.e. ID checking etc. It has been claimed that there is no male security guard who will not help a beautiful female Social Engineer posing as a fresh employee, carrying a large load of documents and at the same time struggling to reach her ID badge to get through the automatic gates, by swiping his own security badge to let her through. This is one of the cases where a little eyelash-batting can get the Social Engineer a long way.

On the other hand, instead of trying to pass for an employee, the Social Engineer may attempt to become one of the "invisible" people who somehow gain an "all access" pass by just being there! These people are couriers of all sorts, delivery persons, gofers etc. It is relatively easy to impersonate a UPS person by just obtaining or making the traditional brown overalls and holding a fake but properly addressed parcel and a barcode scanner / logger. It would be very rare for the UPS person to be stopped at the gate, and even if an attempt to that effect is made, the cunning Social Engineer will definitely find a way to talk himself out of these dire straits by convincing the security personnel that the parcel must be delivered by him, in person, immediately.

A very popular method of gaining access to premises restricted to authorised personnel only, is what is sometimes described as "tail-gating" or "piggy-backing" (Mitnick & Simon, 2002, p.192). This method is used in cases where a badge must be presented to an electronic reader to allow access through a gate etc. What the Social Engineer is counting upon in order to circumvent this security measure, is the fact that people are generally polite, and will not object to someone following them through the security gate that they opened by swiping their personal ID badge. It would be considered impolite to let the person following them to wait for the gate to close, the system re-arm itself and then that person to have to swipe his/her own badge to get through. At large organizations most employees do not know every employee or recognize every face, but are usually more than happy to hold a door for someone, especially if that certain someone is of the sex opposite to theirs and attractive. For the "coup de grace" the Social Engineer may also be brandishing his/her own "badge" (a fake and inoperative one that only *looks* the part), without any intention of using it, to further enhance his/her image and convince the tailgating victim that he/she is also an authorised employee. Once again, subtlety is of the essence.

However, if subtlety can not be used for one reason or another, the Social Engineer may simply opt for the outrageous. With the right approach, an

outrageous attack may simply go unchallenged. The author recalls reading a story about a Social Engineer posing as a company official responsible for the coordination of a fire drill and asking all employees to vacate an office area, in effect leaving behind confidential information at her disposal. Whether this was an actual event or a fictitious scenario has little importance. The point being made is that we are conditioned to accept orders, especially if these are given in an authoritative manner (Cialdini, 2001). Variations on this scheme can simply be achieved by the Social Engineer impersonating any person of authority external to the organisation being targeted, such as a building inspector or a fire department inspector conducting a surprise compliance check. In these cases, the more outrageous the scenario, the higher its rate of success will be.

Another area of physical security that is usually overlooked, is that of contractors who undertake the responsibility of cleaning, maintenance etc. The Social Engineer can pose as a cleaning or maintenance crew member to gain access to the target site. This approach is even more advantageous because access takes place after hours when the field is clear and the Social Engineer can do a lot of work. It would thus be quite feasible for a Social Engineer (normally a highly skilled individual) to actually pursue a job for unskilled personnel with a housekeeping service contractor to get inside the target area. Unskilled personnel, such as those sought out by cleaning contractors, do not have to go through rigorous security checks to get hired. Even if such security checks were in place they would most probably not prevent a Social Engineer from getting the job unless he/she is a known criminal with prior convictions on record. It is obvious that the lack of security criteria alignment in the personnel selection process that by definition exists between the organisation and its service contractors, leaves a lot of room for the Social Engineer to act unchallenged.

Irrespective of the method used to gain access, once inside the target location, the Social Engineer can obtain very sensitive information by removing documents lying on desks or even demand copies of restricted

financial and technical documents be made for him by assuming some position of authority. Just by walking through the office space, the Social Engineer can obtain passwords from sticky notes on monitors, shoulder surfing, and just pretending to be the new, frustrated and helpless guy/girl who is under a lot of pressure to make a good first impression to the boss. The method to be followed is only dictated by the skill and brazenness of the Social Engineer.

Information can also be obtained from workstations that are logged in but whose operators have just left them unattended for "just a moment". Apart from stealing information from an unattended workstation, the Social Engineer can install malicious software on it that will enable him/her to access it remotely through "backdoors". Even if that workstation is not accessible from outside, there are a number of things that the Social Engineer can do on the workstation to make his/her next visit easier and more fruitful, such as creating a personal account, installing a keystroke logging program to obtain valid passwords for connected servers etc.

If the Social Engineer manages to gain access to the site after hours, the main advantage is that he/she can act in a relatively more relaxed way without having people around and access areas and systems that would otherwise be inaccessible. Sensitive information in all forms that was not properly destroyed can be retrieved and perused. Hardware and software can be removed from the premises if that is deemed necessary for the Social Engineer's goals. New hardware can be installed (such as a wireless link to the network or audio/video monitoring equipment). Stationery can be stolen. The list is endless. Furthermore, since information can usually be reproduced, in most cases there is no physical loss to be noticed and thus alarms are not raised, allowing the Social Engineer to return and continue his/her work.
Information security can not exist without an underlying, solid physical security policy in place. Furthermore, it does not suffice to have a physical security policy in place if that security policy is not equipped to deal with the ingenuity of SE attacks. In addition to that, a strict physical security policy at the

perimeter should not provide a false sense of inviolability and lead to complacency as far as physical security at the protected center, the soft underbelly of the organisation, is concerned. At the same time, totalitarian security policies should be avoided because they can only come at the cost of reduced efficiency and the resulting hindrance in everyday operations can be devastating as the concepts of confidentiality and availability are antagonistic to each other (Pfleeger, 1997). Thus, the need for protection of sensitive data must become second nature to all employees so that every action of theirs in the workplace is instinctively governed by safe practice rules. This delicate equilibrium is probably the most difficult goal to achieve because mentalities can not be enforced; they can only be built gradually and methodically.

3.3.3 Attacks over the telephone

Experience shows that people feel deceptively safe behind a phone. They are thus more prone to letting their guard down easily and opening up to total strangers if manipulated correctly. A phone conversation is deprived of most of the defining qualities of a face-to-face conversation.

The subtle facial grimaces, body language, eye movement etc that normally help to set the basis of a trust relationship with an unknown person -even at a subconscious level- are, simply, filtered out in a phone conversation. Furthermore, presentation of hard, physical evidence that backs up the other person's claims is practically impossible over the phone. Hence other methods of "authentication" have to be mutually accepted and these methods are very hard to standardise in our daily dealings over the phone that go beyond the authentication protocol applied by an e-banking teller.

The lack of all of the above qualities -and perhaps more thereof- normally underlying the interaction of two people, when both persons are physically present at the same location, works in two ways, both of which are in favour of the Social Engineer performing the attack. First, as it was already stated, the victim of the attack is more receptive to the Social Engineer's manipulation

and suggestions due to the false sense of security inherent to a telephone coversation. Thus, the victim accepts more easily the "facts" presented by the Social Engineer, directly or indirectly, without really challenging those claims. Second, the Social Engineer can "stretch the limits" by pursuing extravagant goals because he/she knows that if something goes wrong, the interaction can be ended -abruptly if necessary- by simply hanging up the phone, even if this increases the risk of an alarm being raised.

Barring the possibility of the attacker's bluff being called, the above two factors, combined together, can lead to a very successful SE attack with results of very serious proportions.

In conclusion, it can be said that the ethics that govern telephone transactions dictate paradoxical (and very insecure) practices regarding authentication - or more accurately, absence thereof. This "customary" lack of authentication and verification involved in telephone conversations is quite intriguing.

3.3.4 Internet attacks

The Internet is just another means of communication and as such it can also be used to mount SE attacks. Furthermore, due to the convenience and speed of communication over the Internet, we all tend to use it in order to complete business or personal transactions, disregarding, in the process, the fact that communication over the internet is by default insecure and lacks authentication, unless special safeguards are in place.

In the above context, unsolicited (spam) eMail messages coming from strangers are sometimes given more credibility than they actually deserve. Although any Internet-savvy user knows how to deal with spam email, sometimes even the more prudent will be tempted to open such an email item. Furthermore, in the course of a more sophisticated attack, address spoofing can make a fraudulent email message appear as coming from a

trusted source. Hence, generally speaking, unsolicited spam email must be examined in the context of this chapter as a strong tool for SE attacks.

Updated spam email statistics are not easy to be extracted for a number of reasons: First, most statistics are based on the success rate of automatic filters employed on mail exchange servers. As any regular Internet user can testify, the spam email messages that actually get past those filters finding their way into a mailbox are quite a lot. Thus, email messages that are automatically characterised as spam do not account for the real bulk of spam emails sent. Second, statistics based on user reports on spam, such as those found on "Spam Register" (2005) and "Spam Cop" (2005) web sites, are declared to reflect more about those websites' usage patterns than they do about actual spam. Third, spam statistics that are found on commercial "spam-killer" software sites, could be challenged as over-pesimistic to convince site visitors to buy a product.

In an attempt to quantify the amount of spam emails as a percentage of all emails sent, a figure was located on the website of the Wahsington State's Office of the Attorney General of Washington State (2007). There it is stated that "*Almost 45 percent of all email is now spam and that number is growing each year."* Although the page is current, it is not dated. The percentage quoted, however, closely matches the figure given in the "Spam Filter Review" (2006) website, where the statistical analysis regarding spam for 2006 (based on cumulative email usage data from reputable sources for 2005) estimates eMail that is considered spam to represent 40% of all email exchanged. These figures seem rather optimistic as the statistical data obtained from other sources unveil much higher levels of spam.

Novell's "My Real Box" (or MRB) free email service's statistics page (Novell Inc., 2003) quoted on January 26, 2005 that out of 2,104,150 email messages received, 1,805,147 were considered to be spam and, as such, were blocked. This brought the spam percentage reported by Novell on January 2005, to 86%. It could even be argued that as this was the result of automatic filters it

probably yielded results that were lower than the actual ones. The same service, on February 10, 2007, reported that during an up-time of more than 10 days for the MRB server, out of a total of 14,438,749 messages, 12,229,542 of those were blocked as spam, corresponding to a percentage of 84.5%. On January 26, 2005, the quoted real-time 30-day spam statistics index (updated hourly) on the commercial anti-spam software company's "AppRiver" web site (Appriver, 2005), was 82%. On February 10, 2007, the AppRiver site reported the same index in the vicinity of 95%, while its monthly average spam percentage for the period from mid-February 2006 to mid-February 2007, fluctuated between 94% and 96.5%. It is interesting to note that the maximum spam percentage was reached around Christmas of 2006. Although these figures could be challenged on grounds of either being based on inefficient filtering results or serving promotional needs for a commercial product or even being simply arbitrary, this writer's experience strongly corroborates that current spam figures are indeed in the neighborhood of 80-90% of total mail received.

Spam mail could not be used as a Social Engineer attack tool if users simply disregarded it. However, according to a global mail survey carried out by Yahoo! In May and June 2004 (Yahoo, 2004), a considerable percentage of Internet users respond to spam or junk email for various reasons. The percentages of users actually having responded to spam or junk email messages, broken down by country where the survey took place is reported as:

Table 3.1: Response to spam email messages

Country	*Percentage of users having responded to unsolicited email*
UK	18%
France	25%
Germany	16%
Spain	12%
Italy	13%

This shows that roughly 1 out of 5 users actually responded to the spam mail. The main reasons for this response were:

Table 3.2: Reasons for response to spam email messages

Reason for response	*Percentage*
1) To give them a piece of my mind	22%
2) To buy something	7%
3) To unsubscribe	58%
4) Other	13%

By reviewing reasons 1 and 3 above, it can safely be deduced that although this action taken would probably result to more spam coming the user's way, the user was not engaged in a form of voluntary transaction with the spam sender (who could be a Social Engineer). However, reasons 2 and 4 (that amount for 20% of the total) show that the recipient of the spam was somehow convinced to engage in some kind of transaction. Assuming that the spam mail could form the first step of a SE attack, the first line of defense is thus broken. It then rests with the Social Engineer to manipulate the Mark in a way that is clever enough to obtain the desired information.
SE attacks mounted over email are getting more clever by the minute. Under the enticement of free screen savers, free access to sites or anything else that is offered "for free", Internet users execute attachments without hesitation. These attachments could provide "backdoor" access to the Mark's computer, keystroke logging to reveal passwords, false error messages that could make the Mark prone to a reverse SE attack etc.

As Internet users are becoming more aware of such methods and security software finds its way on an increasing number of personal computers, SE attacks mounted over email have become more ingenious. Usually they take the form of an email originating from the administrator of a system the Mark is registered with so that they look like the real thing. Almost invariably these

messages explain that some serious situation has arisen (e.g. suspicious or fraudulent account activity) that requires the Mark's personal details and password to be re-entered (the word "confirmed" is usually used). A link is present "for the convenience of the user" that, if followed, leads the unsuspecting Mark to a carefully constructed web page/entry form that is seemingly authentic. If the Mark makes the mistake to enter his/her details and password(s), his/her account becomes compromised. This type of attack is generally known as "phishing". "Phishing" is defined in the Michigan State Official Web site (2006) as " *the act of tricking someone into giving them confidential information or tricking them into doing something that they normally wouldn't do or shouldn't do. For example: sending an e-mail to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft*".

It should be made clear that in order to make the link presented in the email believable, the lengths to which the Social Engineers go in order to produce whole web sites that look like the real thing but are set up in order to extract sensitive information, have no limit. Apart from building fake web pages that look exactly like the real ones, they also try to imitate the URL by creating URLs that look like the original one. A characteristic example is the case of using "www.paypa1.com" instead of the real "www.paypal.com" URL of the well known online payments' web site, as documented in the "Fight Identity Theft" web site (Fight Identity Theft, 2006). Alternatively, a subdomain address is adopted that refers to the real thing, while in fact it is fraudulent. An example of such a method would be an address of the form: www.paypal.confirm.com. Obviously (but, unfortunately, not to all) this address has nothing to do with the original PayPal domain. It is just a subdomain of some irrelevant "confirm.com" domain (Fraud Watch International, 2007). Other techniques are also used, a prime example of which is the one where a hovering text box is superimposed over the address bar of the visitor's browser. The real URL that the user is being redirected to is

thus masked by projecting over it the proper address that the user expects to see (Fraud Watch International, 2007).

Although fraudulent eMail messages employing "phishing" techniques are usually blindly directed to groups of people (like the customers of an e-banking service or those of an on-line auction house) in an effort to "lure" some of them into revealing sensitive information, there is nothing obstructing a Social Engineer from using such a technique in an attempt to compromise a much more constrained computer system by attacking particular users who are authorised to access it.

Practically all "classic" fraud methods have found new scope in the context of communication via the Internet. Age-old chain-letter/pyramid schemes as well as "get rich quick" schemes have been re-introduced in their e-form reincarnation. Typical examples of the latter are the "Nigerian" scams. These are named after the original scenario of Nigerian state employees trying to export funds from illegal pay-offs with a help of an foreign citizen-turned-victim. Details of pyramid frauds and Nigerian scams are beyond the scope of this work but can be found online (Fraud Watch International, 2005a; 2005b; PopSubCulture, 2005).

Any form of communication over the Internet can be exploited to fuel SE attacks. Internet Relay Chat (IRC) and Instant Messaging (IM) are no exception to this. To protect Internet users from such attacks, CERT has published a relevant Incident note since 2002 (CERT, 2002). According to this note "*Intruders trick unsuspecting users into downloading and executing malicious software, which allows the intruders to use the systems as attack platforms for launching distributed denial-of-service (DDoS) attacks*". The standard method of operation is that automated tools are used to post messages to IRC and IM users, offering to them improved music downloads, protection against computer viruses etc and/or, falsely assuming a position of administrative authority, threatening the user with an impending discontinuation of IRC and IM services if a particular "protection" software is

not immediately downloaded and installed. The downloaded software, when installed, typically functions as spyware, Distributed Denial of Service (DDoS) attack agent or backdoor to relinquish control of the Mark's PC. Thus, the compromised PC can be remotely controlled, private data can be exposed, other malicious software can be installed or propagated, resulting in data loss or tampering. According to CERT, this definitely constitutes a SE attack since its success relies on the decision of the user to follow the instructions put forth in the message.

As reported to NewsFactor Top Tech News (NewsFactor, 2005) by McAfee officials, another interesting approach is to target particular IRC or IM users and in the first phase of the attack flood their mailboxes with unusually large quantities of spam mail. During the second phase, a message is sent with an offer for (free) software that eradicates all spam. Clearly, this software is anything but what it is claimed to be. Although, strictly speaking, this is not a Reverse SE attack in the traditional sense (as discussed in the following section), it can be argued that it is a modern form of the old method. Depending on how well it is planned and executed, it can yield very useful results to the Social Engineer who employs it.

3.3.5 Reverse Social Engineering

Irrespective of which of the above approaches the Social Engineer chooses to mount his/her attack, a very interesting technique that Social Engineers employ is that of a "Reverse Sting". In that case, the Social Engineer causes a problem to manifest itself (or in the lack of a real problem, the Social Engineer somehow convinces the victim that a problem does exist) and then makes him/herself available to eradicate that problem. As expected in any such real-life situation, the Social Engineer is then perceived as a "knight in shining armor", is implicitly trusted and never challenged.

It is remarkable how easy it is to create the underlying situation that will make a Reverse SE attack successful. The possessor of ordinary hacking abilities

can enhance the level of success of his/her attacks by employing SE methods. A compromised system can be made to fail in some pre-determined fashion and the Social Engineer can take advantage of this "mishap" in order to appear (without raising suspicion) and solve the problem, gaining the victims' trust in the process. Furthermore, a subtly compromised system can provide an "error message" that instructs the target of the attack to get in touch with a particular phone number in order to resolve the "error". When the number is dialed, the Social Engineer starts "reeling-in" the victim. Even if it has not been possible for the Social Engineer to gain access to the system, there are ways that the Social Engineer may be able to indirectly convince a victim that a problem exists. If the victim falls for this, the Social Engineer can carry on with the attack.

The above methods are very neatly analysed by Nelson (ca 2000). In his article Nelson identifies three parts to a Reverse SE attack: Sabotage, advertising and assisting.

As shown above, the sabotage can take place in different ways or even be a virtual one. In this phase of the attack an "alarm" somehow goes off, placing the victim in a psychological state that ranges from informed concern to primal fear. The "advertising" phase can precede or follow the sabotage phase or even take place simultaneously with it. In any case, advertising must take place in such a way that the victim's preferred course of action after the alarm goes off, is to contact the Social Engineer rather than anyone else. Finally, the Social Engineer must be able to "assist" by solving the "problem". The Social Engineer can mount the attack either by asking the Mark for sensitive information that supposedly solves the problem, or just solve the problem and use the opportunity as a first step in gaining the victim's trust and thus making the extraction of the sought-after information easier at a later stage.

In the same article by Nelson (ca 2000), an interesting comparison is made between ordinary SE attacks and those based on Reverse SE. The results of this comparison are tabulated in table 3.3 below:

Table 3.3: Social Engineering vs. Reverse Social Engineering

	Social Engineering	**Rev. Social Engineering**
Dependence	The Social Engineer places the call and is dependent on the victim	The victim places the call and is dependent on the Social Engineer
Indebtedness	The victim feels that the Social Engineer is indebted to him/her	The victim feels indebted to the Social Engineer.
Completion	Issues often remain unresolved in the mind of the victim	Most -if not all- issues are resolved, no suspicious loose ends for the victim
Control	The victim has control of the flow of information	Due to the nature of the attack, the Social Engineer has more control in extracting the information
Preparation	Little or no preparation required by the Social Engineer	A significant effort must be made by the Social Engineer into planning the attack and previous access is usually needed

The above table is quite interesting because it begins to show that the psychological mechanisms in action in each of the two techniques of attack are highly disparate. The interaction between the Mark and the Social Engineer takes a totally different form and the outcome of the attack may thus vary. Clearly, the two methods can not be used indifferently by the Social Engineer, but are, instead, chosen according to the particular situation.

3.4 Concluding Remarks

In this chapter the fundamentals of SE were presented. The basic forms of SE attacks were discussed, and the main methods of operation of Social Engineers were accounted for. These can be classified in three primary categories:

- Attacks at the physical level
- Attacks over the telephone
- Attacks over the Internet and email

This categorisation is important and will be used in later chapters of this dissertation.

Even so, the discussion presented in this chapter is by no means sufficient to give the reader an idea of the full extent of the problem at hand. The presentation of the Social Engineer's methods of gathering information, must be combined with a deeper understanding of SE attacks if changes that are effective against SE are to be proposed and implemented in the context of an IS policy.

The required insight will hopefully be provided in the next two chapters that investigate psychological and social issues related to SE and IS. The results of those chapters combined with the analysis of the SE methods of operation presented here will offer a better view of the SE problem.

4. Psychological considerations in Social Engineering

4.1 Introduction

The study of the Social Engineering (SE) methods of operation presented in the previous chapter, showed that a strong element of psychological manipulation and exploitation is always present in all of the SE attacks that require some form of contact between the Social Engineer and the Mark. This chapter will look into the psychology behind SE attacks in an effort to better understand the issues involved and take another step towards building better defenses against SE.

Social Engineering attacks exploit vulnerabilities that are based on principles of human psychology. In conjunction with loopholes in the security structure of the organisation, these attacks can yield results that would be difficult, if not impossible, to obtain through the use of purely technical hacking methods. As SE attacks are based on deception, they are very difficult to categorise. Hence, designing countermeasures for them is even more difficult. Thus, a more fundamental approach is called for, if effective defense methods are to be devised.

In this chapter an attempt is made to identify the methods and techniques used in SE attacks by examining psychological principles as these are applied to the field of Information Security. In a subsequent chapter, psychological countermeasures leading to defense mechanisms will be examined in an effort to provide controls for SE vulnerabilities.

The combination of results from the current chapter, the previous one on SE methods and the next one on the social aspects of Information Security (IS) will ultimately lead to the more accurate assessment of the controls of the ISO/IEC 17799:2005 security standard (ISO/IEC, 2005a) with respect to SE.

The following diagram depicts the role of this chapter within the overall structure of this dissertation.

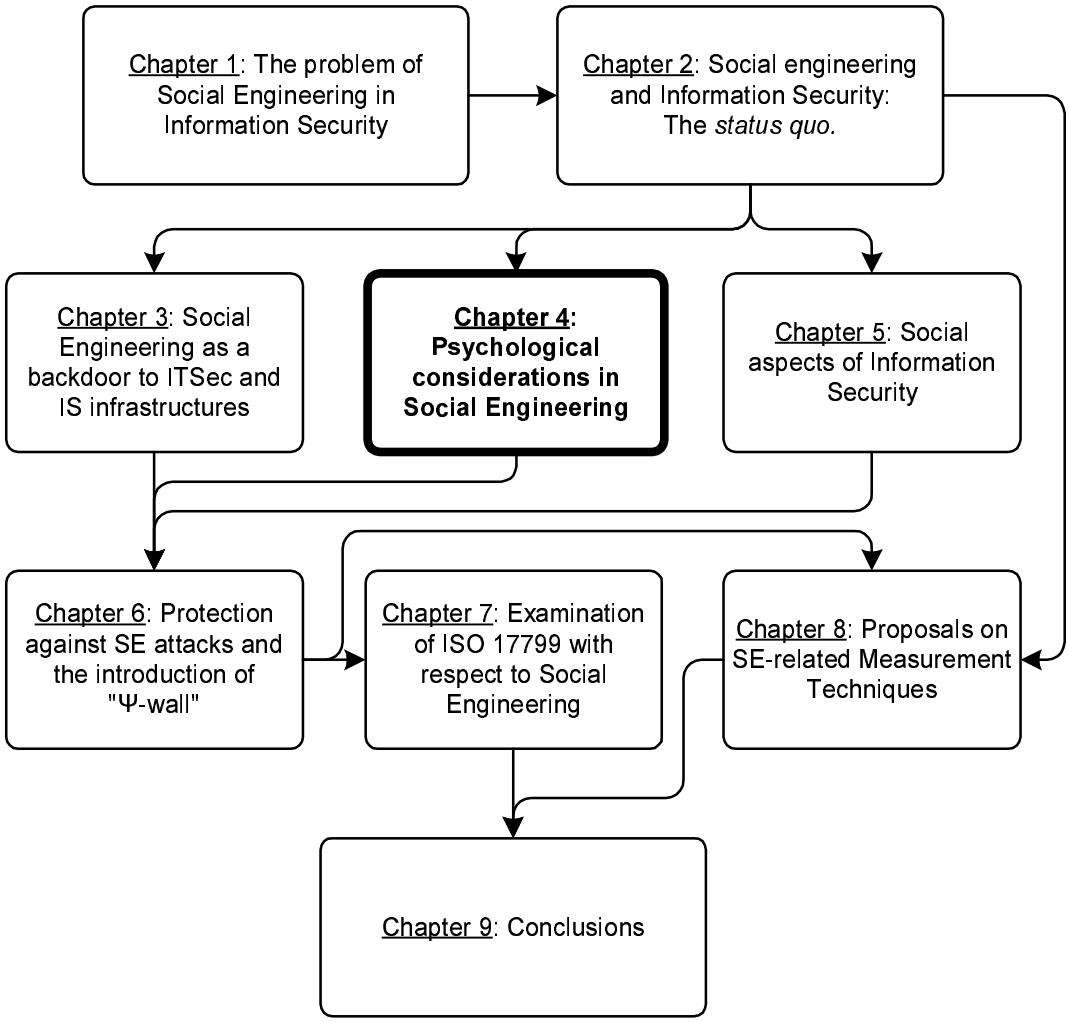

Figure 4.1: Chapter 4 within the context of the overall dissertation structure

4.2 Persuasion - variations on an old theme

Even though the object of this work is Social Engineering and its relation to information systems, the methods and attacks used today in computer-related crime are far from new. They have been in use for at least the past 40-50 years through other standard methods of communication as those were available at the time. For example, telemarketing has been thriving

for many decades in the U.S. over the telephone. Although telemarketing can be (and has been) used in ways ranging from legal to undeniably illegal, it is always based on the power of persuasion the telemarketer has over the prospective client/victim. On the other hand, it has always been a general truth that a good salesman can sell anything. The salesman's abilities are not dependent on the merchandise. Again it is the power of persuasion that comes into play. Con artists have been thriving since the dawn of mankind. Their special ability is their power to influence other people. Politicians and cult leaders have been doing the same thing for thousands of years. Whether used for good or not, in all of the above cases there is a common factor in the methods used: the exploitation of human nature. Irrespective of whether they are used for good or not, influence and persuasion methods have been successful because they exploit the same basic property: human psychology. Thus, the bottom line is that although technology evolves, providing societies with different channels of communication, the basic human psychological characteristics have remained the same as they have been for centuries, if not millenia. Hence, modern SE attacks are based on the same psychological traits that are governed by the very essence of human nature.

4.3 The psychology of physical attacks

Physical presence on the site under attack is, by far, the least attractive method for the Social Engineer. However, there are cases that this can not be avoided. The main method of operation of a Social Engineer mounting a physical attack (usually through impersonation) is to a) blend in with the surroundings and b) use such psychological manipulation techniques that are necessary for the achievement of the goal of the attack.

Carefully orchestrated gestures, facial grimaces and body language are essential before even "first contact" is made. For example, in order to use a tail-gating technique successfully, the Social Engineer must have the

right timing but also the right attitude towards both the person being followed in, as well as the security guard potentially present. Exploiting the natural tendency of people to be nice or the equally normal positive pre-disposition towards handsome people of the opposite sex, the Social Engineer can go a long way. Porting him/herself with the air of authority or, at least, ease, the Social Engineer can surpass most first-contact checks and exploit those mental shortcuts that will allow him/her to move around the target premises unchallenged. If challenged, the Social Engineer will have to be prepared to provide some information (obtained in the earlier phases of the attack) that will back up or explain the reasons for his/her presence on the premises.

There are at least three techniques that can be used efficiently by the Social Engineer in physical attacks:

1. *Exploitation of the human tendency to be helpful*. This natural tendency has already been mentioned in this research but has to be emphasised in this context. A Social Engineer impersonating an employee in a hurry for a meeting who's also carrying a large load, may pretend to be fumbling for his/her badge or authentication token while the security officer instinctively rushes to his/her help. Another, pretending to be a courier for a large company holding a number of boxes, may ask for someone to "hold that door" for him to pass through etc. In most cases, because everyone is conditioned to offer their help to fellow people in need, this conditioned response overrides the call of reason that dictates to carry on with the security check, with obvious results.

2. *False appeal to authority.* All hierarchical structures are based on the authority of higher level personnel upon lower level personnel. Unfortunately, this authority, although originally delegated in order to make the function of the structure possible, is frequently abused to facilitate those possessing it in situations and conditions that they are not supposed to be treated differently from anyone else. It is a very frequent occurrence that VIP members of staff will try to "pull rank" in order not to

have to wait in line to be authenticated or, even worse, to be allowed access when they have forgotten their authentication token (ID card, smart card etc). The lower-ranking personnel responsible for security at points of entry etc, will usually succumb to the minimal of pressure because they are not willing to challenge someone who could get displeased with their "overzealous" behaviour and affect their own standing in the structure. This situation clearly presents an oxymoron since lower-level personnel who are responsible of security are in fact doing nothing more than what is really required of them according to their job description, and should be appraised for that instead of being reprimanded. Such a situation can be exploited by a Social Engineer who can either impersonate someone with authority, or claim to be acting for, or on behalf of, such a person.

3. *Exploitation of "Low Involvement" personnel.* Harl (1997) introduces the idea of "Involvement" as a contributing factor to the success (or not) of a SE attack. People who are highly involved in the system the Social Engineer is trying to compromise (such as administrators, computer security officers, computer technicians and users who are well accustomed to the use of the system) have to have strong arguments presented to them by the attacker in order to be persuaded. Weak arguments act as warning signs to them and may bring the attack to an early and unsuccessful end. On the contrary, night-shift guards, cleaners, or working-hour receptionists at a computer system site are classed as "Low Involvement" employees because they have very low interest in what a Social Engineer may actually ask them to do and weak arguments may actually prove very successful with them. Mitnick and Simon (2002, pp. 150-155) a story is given about a security officer being conned by a teenager whose method of manipulatory attack to convince the guard on the validity of his claims was well thought out, but at the same time was very simple indeed. In similar fashion, a member of the cleaning staff may be persuaded to allow a Social Engineer after-hour access to a site or run an errand for him/her that could well lead to the compromise of information the Social Engineer needs to mount an attack. A receptionist

(a position that requires the employee to be particularly courteous, polite and helpful) may provide the attacking Social Engineer with critical information or even access to restricted areas after some careful manipulation (Mitnick & Simon, 2002, p.162).

In all cases, a physical attack on the target premises requires meticulous preparation. It also demands the attacker to acquire a state of elevated psychological resilience that is necessary to withstand the pressure inherent to such an attempt, as well as the special ability to constantly monitor and actively manipulate the psychological status of the potential challenger to allow the planned attack to unfold. All of the above are not always possible, hence the attacker must also have an escape plan from the premises in case things do not turn out as expected.

It could thus be argued that if strict physical security is applied both on entering as well as leaving an establishment's premises, this could constitute an effective measure towards better control of SE attacks at the physical level.

4.4 Persuasion tactics

SE attacks eventually have to employ persuasion tactics in order to achieve the desired result. There are two routes to persuasion: the Direct or Central Route and the Peripheral Route (Rusch, ca 1999).

The Direct Route is systematic and uses logical arguments in order to stimulate a favourable response from the person being persuaded and / or prompt this person to take the action desired by the persuader. This technique is unfavourable to SE tactics because there simply is no logic behind a request to reveal sensitive information to unauthorised persons.

The Peripheral Route is the tool preferred by Social Engineers who invariably use this technique to misrepresent their objectives. Mental

shortcuts, peripheral cues and distraction techniques are applied in order to trigger acceptance without thinking and reasoning.

In psychological terms, such persuasion can not be considered equivalent to brainwashing. However, strictly speaking, it still is a form of manipulation of a human's mind by another individual in an attempt to achieve an opinion shift, without the manipulated person being aware of what caused his/her opinion shift (Sutphen, nd). Sutphen, in the same article, also argues that the basis of persuasion is always to access one's "Right Brain". In an oversimplified attempt to explore the mechanisms of persuasion, it is stated that while the left half of the human brain is responsible for analysis and logic, the right half is responsible for creativity and imagination. Thus, persuasion techniques attempt to distract and keep busy the left half of the brain in an effort to find a shortcut to accessing the right half. An example of such a technique would be to present the Mark with an arguably dangerous situation that needs to be analysed and assessed by the left half of the brain. This leaves the task of simultaneously processing the main request (that could lead to the disclosure of sensitive information) to the right half of the brain, which is more prone to the suggestion that it would be "ok" to comply with this request. As an example, a Social Engineer posing as an bank IT staff member could call a Mark in the middle of the night and state that unusual activity is being monitored with respect to the Mark's account, with sums of money continually being transferred out of the account. The Social Engineer could then offer to help reverse the transfers and block the account if only the Mark gave him/her the password needed to access the account. At the same time the Social Engineer does not forget to state that it would be irregular to do so and that he/she "is risking his/her job by doing that". While in a state of shock and confusion, the Mark could conceivably fall for such an attack.

Guidelines, for aspiring Social Engineers are provided by Bernz (2004) in the form of a tutorial. Tips and tricks of the trade are given and although this text will definitely not win any literary competitions, it does drive its

main points home rather successfully. Many SE techniques are discussed and almost all of them are based on the application of practical psychology methods in order to persuade the Mark to release sensitive information.

In Grangers' commentary of the above reference (Granger, 2001) there are several persuasion tactics identified:

1. *Impersonation.* This technique can be applied over the phone or in a physical attack. Depending on the type of Mark, different approaches can be taken. Usual roles for impersonation over the phone include an administrator or technician from the company's IT department calling a user, a distressed user calling the company help desk, an executive requesting information or a trusted third party (like the president's secretary) requesting information for the president etc. In physical attacks, the role faked is usually that of an employee, of a person of authority within the organisation or a person acting on behalf of one, a repairman urgently called in to fix a problem, an external IT technician paying a support visit, a delivery person delivering urgent, important or bulky items etc. A good impersonation act combined with other techniques can prove very fruitful for the attacker.

2. *Ingratiation*. If the Mark of the attack is given a good opportunity to gain favour with or be favourably accepted by persons of power within the organisation, he/she will be more willing to go the extra length and do something that he/she is not really supposed to be doing. A Social Engineer posing as a person of importance has a lot to gain by exploiting this principle. If one also considers the opposite side of the coin, which is the fear of the Mark that the person of power asking for the favour will begin harbouring ill feelings for him/her if the request is not granted, it is made even more obvious that the Mark will fairly easily succumb to the Social Engineer's request.

3. *Conformity.* No one likes to be different than everybody else as this could make him/her look out-of-place or even obnoxious. The attacker capitalises on this concept by offering to the Mark those mental shortcuts that justify actions that would seem unreasonable at first. The attacker will let the Mark know that what is being requested of him/her, has already been provided by the Mark's peers or even superiors. The mental shortcut in this case is that if everybody else is doing it, it must be the right thing to do. This information, however, has not been independently acquired by the Mark but it is the product of, usually, indirect hinting on the part of the attacker. A simple, direct statement like: "I have already obtained such information from your colleagues, why don't you give it to me also?" will probably raise an alarm in the Mark's mind. If however this information is indirectly allowed to surface in a way such as: "When I was talking about the same subject to Ms. Smith (the Mark's superior) she let me understand that…", the Mark will feel more at ease and will be more willing to accept that by releasing he requested pieces of information, he/she is only doing what everybody else has already done.

4. *Diffusion of Responsibility.* The attacking Social Engineer will, as a matter of course, ask for sensitive information or require the Mark to perform some kind of action. The Mark will almost certainly hesitate due to the nature of the request, in part because of the responsibility that the Mark feels he/she has to protect the information and/or to uphold certain rules and regulations by **not** taking the requested action. The challenge for the Social Engineer is to alleviate that burden in order to make the Mark feel comfortable with the situation and proceed as it is requested of him/her. The techniques of diffusing the responsibility include elements of the Conformity technique discussed above, as well as tactics based on what the psychological effect of who the Social Engineer **pretends** to be with respect to the Mark's position in the hierarchy. If the Mark is convinced that he/she conversing with the IT manager or one of his/her superiors, the Mark feels less stressed talking about sensitive pieces of data. If the Mark also feels that he/she is doing nothing significantly different than

what peers and colleagues are doing, the personal portion of responsibility that the Mark has, suddenly feels as less of a burden.

5. *Friendliness*. Although friendliness and saying "please" and "thank you" with a smile, does not suffice for a successful SE attack, it is one important component that must not be overlooked. The Mark not only wants to believe the person on the phone and wants to help out, but, also, it is always more difficult to be "sceptical" or "obnoxious" enough to decide to challenge the caller if the caller is really polite, outgoing and open-hearted. ("If the caller is all of the above, then he/she **must** be a good guy/girl!"). Even friendliness though has its limits and a good Social Engineer always knows how to not become unnaturally friendly and when to stop extracting information. Stopping at the right time and perhaps "leaving a door open" for use at a later time is always a good practice during SE attacks. This also forms the basis of a relation-building technique employed by Social Engineers where initial contacts are always friendly and not overly demanding, so that trust is gradually built. This attack culminates when the Social Engineer has become enough of a "phone-pal" with the Mark and is being trusted enough to ask the really important questions that are answered by the Mark without a hint of hesitation.

   In addition to the above tactics, Makosky (1985) suggests the following three persuasion techniques:

6. *Appeal to or creation of needs* according to Maslow's hierarchy of needs (Maslow, 1987): Physiological, Safety, Love and Belonging, Esteem, and Self-actualisation). The attacking Social Engineer will address as many types of the Mark's needs as possible. Flattery may appeal to the Mark's need for Love and Belonging or it will boost the Esteem factor. An urgent phonecall, in the middle of the night, warning of impending financial loss as a consequence of account compromise will definitely strike against the Mark's need for safety, forcing the person under attack to take action while under shock or confusion. Similarly, a request made on behalf of a

potentially very angry supervisor or, worse, employer, will immediately hit on the Mark's physiological needs, as the potential of a reprimand that could eventually lead to job loss, automatically increases.

7. *Social and prestige suggestion*. While social suggestion is almost identical to the Conformity tactic already mentioned, prestige suggestion has to do with a well-known, respected person or a person of authority making a recommendation or request. Common usage of this technique is made by Social Engineers who frequently use the names of respected individuals who are well-known to the Mark, in the "name-dropping" phases of their attack. In the SE scenario, the request does not actually have to come from the well-known individual, it suffices to just let subtle hints surface, suggesting that the respected individual has already complied or is in agreement with the request being presented to the Mark.

8. *Use of loaded words and images*. A word used in the right context can have an expected positive or negative effect. For example, a sentence phrased as "can you **fetch** that document for me" instead of "can you find/bring that document for me" will almost certainly have a negative effect on the Mark on the receiving end of that request. This will put the Mark in a rather defensive state of semi-confusion that could help in making him/her more open to suggestion. A suggestion towards the Mark to visualise an angry boss or another unpleasant situation, could also lead to a state of confusion.

   Finally, Cialdini (2001) presents another persuasion technique with instant persuasion results:

9. *Providing a reason*. As described by the author, the desired effect is obtained through the use of the word "because". I.e. simply providing a reason -any reason- for making a request. Cialdini describes an experiment performed by a Harvard researcher named Ellen Langer who kept trying to bypass the lines at the photocopier machine by phrasing her request in three different ways. The first version was: "*Excuse me, I have*

five pages. May I use the Xerox machine because I'm in a rush?" A legitimate reason was given for this request and the request was successful 94% of the time. In the second version, no reason was given: "*Excuse me, I have five pages. May I use the Xerox machine?*". This request was only successful 60% of the time. One could assume that giving additional information that justifies the request in the form of a reason for it, was responsible for the different success rates. However, the third request formulation was: "*Excuse me, I have five pages. May I use the Xerox machine because I have to make some copies?*" This version of the request had a success rate of 93%. Clearly enough, neither a real reason was given nor additional information presented that justified the request. The "reason" given was simply a statement of the blatantly obvious.

It is concluded that the presence of the word "because" was responsible for triggering the effect of what Cialdini calls "Human Automaticity". The mere use of the word "because" was sufficient to extract a positive response from people and it did not even matter that there was no substantial reason given. In practical terms, this indeed was "instant persuasion". It is also a trick that leaves the victims of SE attacks wandering "what just happened"!

4.5 Influence techniques

Cialdini (2001) identifies six fundamental psychological principles: reciprocation, consistency, social proof, liking, authority and scarcity. As these principles direct human behaviour, they effectively give rise to influence techniques that are being efficiently put to use by "*compliance practitioners*" to power their tactics. (The term "compliance practitioners" is used by Dr. Cialdini to generally identify those people who try to make others comply with their wishes. Clearly, Social Engineers form a subset of this group).

1. *Reciprocation.* One of the basic principles of human society is that if someone gives something to someone else, then the right thing for the recipient to do, is to somehow return the favour. This stems from the reciprocal nature of human society and goes back to the formation of the first human groups. The members of those groups had to share food and skills in order to survive. These basic principles evolved into the interdependencies of modern societies. Clearly, the action of giving and then expecting something in return as well as the other way round, on average, characterises all humans. The ways that this principle can be exploited by Social Engineers are many and range from the basic to the really intricate. "Free" offers on the Internet are very common. Most of the time, offers such as screensavers or background images are given away with the sole intention of persuading the recipient to register an email address in order to receive the free offer. At its most innocent form this technique is used to build up an e-mailing list to be used for promotional material or, worse, to be sold to others for the same use. Apart from the resulting spam mail flooding one's inbox, this type of attack is not very dangerous security-wise and this is the reason behind its popularity and success. Through the use of free email services one can create an address and register as requested, only to abandon the address at a later stage when spam sent to it becomes a nuisance. However, the Social Engineer may introduce a new twist to this story by directing the offer to particular targets and instead of providing just a piece of well-meaning software, entice the Mark to install software that could perform a secondary spying function in addition to its advertised primary function.

   The principle of Reciprocation can also be applied in the already discussed "Reverse SE" attacks. When the Social Engineer solves the problem that torments the Mark, the Mark feels indebted to the Social Engineer and grants the Social Engineer the requested favours.

   In an even more subtle form of reciprocation, the Social Engineer may make an almost unreasonable request, **knowing** that it will not be granted. By then making a lighter and less unreasonable request, the

Social Engineer augments the odds of this second request being granted, compared to the situation where the second request was the only one being made. Although seemingly unreasonable, there is logic behind this sequence. It should be clear that the Social Engineer's target was to **not** have the first request granted. The first request was only made to predispose the Mark according to the Social Engineer's plan. When the first request is turned down, the fact that the Social Engineer continues with a less demanding request, constitutes a concession on the Social Engineer's part. The Mark then feels obliged to **reciprocate** with a concession of his/her own because of the natural tendency to co-operate in the bounds of our societal interaction. This is similar to soliciting for money. A rather high amount of money is first asked for, and after this request is turned down, a second, smaller amount of money is almost certainly guaranteed to end up in the solicitant's money bag.

2. *Commitment and Consistency.* It is a known psychological fact that people are mostly consistent within their words, beliefs, attitudes and actions. This is fueled both by the fact that consistency is a virtue valued by society as well as by the useful shortcuts it provides. These shortcuts make daily life easier in the sense that if one remains consistent with previous choices, the load of re-processing all the data in similar situations as they arise is avoided. One simply sticks to earlier decisions. As far as commitment is concerned, one has to just examine the positive load that the word "committed" carries in everyday conversations. If someone is characterised as "committed", then that someone can implicitly be trusted, is considered to be a person who brings results, is highly dependable etc. (For reasons of clarity and to avoid misconception, another use of the word "committed" is to describe someone who has been admitted to a mental institution. According to Meriam-Webster Online dictionary (Meriam-Webster, 2004) the first two meanings of the verb "commit" are: "***a**: to put into charge or trust : entrust, **b**: to place in a prison or mental institution*". Clearly for the purposes of Cialdini's argument, reference is made to the first of the two meanings).

The Social Engineer makes good use of this principle by subtly manipulating the Mark so that the Mark gradually finds him/herself in such a position that turning down the Social Engineer's request is not an option. This entrapment is based solely on the Mark's previous conduct towards the Social Engineer. In order for the Mark to be consistent towards the Social Engineer, assuming that the Mark has already granted the Social Engineer's inconsequential small favours, the Mark must keep granting the Social Engineer favours that are being gradually built up over many phone calls and an extended period of time. Doing otherwise, will make the Mark look inconsistent with respect to prior behaviour. In this case, the driving force behind the Mark's obsession with consistency is not, so much, what the public reaction would be if the fact that the Mark is inconsistent was brought to light, but rather the fact that if the Mark turns down the Social Engineer's request, this would force the Mark to holistically re-evaluate his/her position and evolved relation with the Social Engineer, since first contact was made. Not only can this make the whole mental-shortcut-based-on-previous-experience structure collapse (Cialdini, 2001), but it really is not an option in the mind of the Mark, since the Mark has to put his/her weight behind previous choices in order to remain psychologically balanced.

This attitude is further enforced by the fact that when person A asks person B for a favour and B grants it, A becomes part of B's personal history of good deeds that contributes to self-esteem. B (who granted the favour) will **have** to like A from that point onwards because B has to justify his/her action by convincing him/herself that this was the right thing to do as A "is a really nice person". It should also be noted that at the time of the favour being granted, B does not have to like A in order to grant the favour, but other reasons may lead B to this decision. Another interesting point is that none of the above necessarily holds true for A. A does not need to like B to ask for the favour, neither B becomes likeable by A after the favour is granted. On the contrary, it is possible for A to develop a dislike for B in order to justify that it was not a favour being granted but that somehow, B being a worse person than A, was obliged to grant A's

request.

All that is required from the Social Engineer in order to "cash in" on such attitudes is careful planning. A commitment in the form of a promise on the part of the Mark (direct, implied or even suggested) may be called upon by the Social Engineer in order to "nudge" the Mark at times of hesitation ("Aaaah… but you promised!").

3. *Social Proof.* According to Cialdini (2001, p.100) *"we determine what is correct by finding out what other people think is correct".* In part, this principle has already been discussed under *Conformity,* above. SE techniques based on the principle of Social Proof are most influential on a Mark, under conditions of either a) uncertainty or b) similarity. In the first case, if the situation is so ambiguous that the Mark does not know what to do, providing information on the actions of others will most certainly turn the Mark in the same direction (see *Conformity* above). In the second case on the other hand, since people are more inclined to follow the lead of others, similar to them, the work of a Social Engineer can be significantly facilitated or significantly impeded.

   In a direct attack, the Mark may hesitate in providing the Social Engineer with the requested information. This hesitation indicates uncertainty and the Social Engineer will provide such conformity-related information to the Mark, that the Mark will be nudged in the desired direction.

   Indirectly, the Social Engineer may benefit by lax security that allows users (i.e. potential targets) to function haphazardly with respect to security measures. This is a regenerative process that is fuelled by similarity and leads to an increasingly insecure work environment as more and more users following the example of others before them, develop disrespect towards security measures. On the other hand, if the proper security policies and directives are applied and the correct incentives are given to workers in order to uphold security and be rewarded for it, the

regenerative effect due to similarity will become positive and lead to augmented security.

4. *Liking.* People tend to respond favourably to other people with whom they share some common interest, hobby, birthplace etc. This natural tendency of ordinary people to like and even to seek out others who are like themselves, arms the Social Engineer with a powerful tactic. That of undertaking the role of a persona that appears more likeable to the Mark by virtue of similarity.

   Generalising, people prefer to respond positively to those who they know and like. It is thus imperative that a Social Engineer become "liked" by the potential Mark. Apart form similarity, the most obvious aspect of all, that of physical beauty, is probably the most important factor for which people like other people. Whether it is conditioning or natural selection, research has shown (Cialdini, 2001) that physical attractiveness has an immediate effect on others, who instantly like those blessed with it. More interestingly though, other qualities of attractive people are further enhanced by the mere fact that their possessors are attractive! Hence, an attractive person will most probably also be considered to be kinder, more intelligent, more talented and, of course, more trustworthy than he/she really is. As a result, attractive people can be more persuasive than others

   Liking can be achieved by familiarity over repeated contact (this was also mentioned under *Friendliness,* above). Also, if the circumstances under which contact takes place are positive rather than negative, liking is much more certain to be achieved sooner than later.

   In SE attacks, these techniques are used to boost the level of liking that the Mark holds for the attacking Social Engineer. In physical attacks, the external appearance of the attacker has a major part in the scenario played out and the success of the attack altogether. In attacks over the phone and the Internet, a deep, resounding voice (natural or filtered through the appropriate voice-changing device) can contribute to the

success of the attack. Additionally, "chatting-up" the Mark in order to establish some common points of reference on which to build a trust relationship can make or break a successful attack. Stretching out the contacts in time can also help a Social Engineer build a trust relationship over the phone with the Mark and use that trust build-up when the attack culminates.

5. *Authority.* It has already been discussed that a false appeal to authority is one of the preferred methods of operation in SE attacks. The reason that such an impersonation is successful, is based on the respect that the average person has for authority. Modern societies systematically employ practices to instill in their members that obedience to legitimate authorities constitutes correct conduct (Cialdini, 2001, ch.6). Furthermore, persons of authority are considered to normally possess high levels of knowledge, wisdom and power. Hence, a mental shortcut can be established by deferring the complexity and responsibility of decision to such persons. This, in effect constitutes an automatic response to persons of authority. Alarmingly, though, as it is also discussed in the above reference, this automatic response tends to be to the **symbols** of authority and not necessarily to its credential-backed substance. Such symbols have been shown by research (Cialdini, 2001, p. 201) to be titles, clothing and automobiles. These symbols, used by the Social Engineer and combined with the right attitude and composure, can effectively project a convincing, albeit false, image of authority that will evoke an automatic response from the targeted Mark. Moreover, due to the automatic nature of the response, the Mark tends to underestimate the effect of authority pressure on his/her behaviour, thus making the attack more difficult to identify and protect against.

6. *Scarcity.* According to this principle, a higher value is assigned to goods and services that become less available. As this happens, their apparent value increases and so does the appreciation of their quality. Additionally, it is argued that as things become less available, our freedoms are effectively curtailed in the sense that we are no longer able to acquire

them as we used to. Psychological Reactance theory dictates that the human response to loss of freedom is to desire them even more strongly (Cialdini, 2001, pp.208-218). Hence, something that becomes scarce also becomes more desirable. (In other words, we appreciate something when we lose it).

Although it is clear that the scarcity principle applies more to deception based on fraudulent on-line auctions, the same principle can be used to enhance the effect of many other types of SE attacks.

For example, in the case of the "well-meaning" e-banking employee who wakes up the Mark in the middle of the night to inform him/her that money is being transferred out of his/her account and subsequently makes a request for the Mark's password to block the transaction, an extra piece of information about how the Social Engineer is risking his/her position in the bank to help the Mark is also usually supplied. Apart from the sense of gratitude that the Social Engineer is trying to conjure, the element of scarcity of the supplied service is also indirectly invoked. The Mark realises that if he/she hesitates to give the requested information to the Social Engineer, the offer may be swiftly withdrawn because of the impending risk of job loss for the bank employee / Social Engineer. This scarcity element makes the quality and sincerity of the offer to appear higher, and thus provides the Mark with a mental shortcut and the Social Engineer with the information he/she is after.

In the case of "phishing" attacks over email, IRC etc, an offer valid "for a limited time only" or "for the first X replies received" may trick the Mark into thoughtlessly and impulsively submitting personal information that will be used to impersonate him/her during a later phase of the SE attack or, even worse, be used to directly gain access to a system.

The above techniques are e-variations on a very old theme. Marketers, politicians, advertisers, sales people and con artists have been using them for ages to convince their Marks to respond positively to their

suggestions. Amazingly, although these methods were identified and brought to light decades ago, they are still very successful and the fact that computer-age Social Engineers use them, is a testament to their effectiveness. The average computer user is thus very vulnerable and the only means of defense is proactive education and distribution of information relevant to these methods of attack.

4.6 Exploitation of attitudes and beliefs

Apart from the tactics of influence and persuasion already discussed, Social Engineers make use of several shortcomings in the function of the systems they target for compromise.

One such shortcoming is the lack of the flow of information about an attack in large, and mostly authoritarian, hierarchies. This is a well-known situation among Social Engineers and attackers who justifiably consider most hierarchies of this type to be governed by what is called in Hacker-jargon the "SNAFU" principle. According to the Hacker's Jargon Lexicon (2004), the acronym originates "*from a WWII Army acronym for 'Situation Normal, All ****ed Up: True communication is possible only between equals, because inferiors are more consistently rewarded for telling their superiors pleasant lies than for telling the truth"*. Despite the annoying vulgarity of the acronym, this principle describes a situation that has definitely been holding true for millenia. It is a well-known fact that military couriers in the times of the ancient Persian empire were either treated as honoured guests when they brought news of victory from the battlefield, or summarily executed if they brought news of defeat. In today's terms, it is not unusual to treat someone who raises an alarm, as if he/she is the **cause** of the alarm! In this most ostrich-like behaviour, ordinarily vigilant employees feel compelled to "turn a blind eye" and ignore the observed signs of a security breach. This is the same type of hierarchy where an impersonation attack by a Social Engineer based on a false appeal to authority, would be more successful. Consequently, the hierarchy's decision-makers become progressively disconnected from reality, leading

to the systemic failure of the hierarchy itself. A term currently gaining acceptance that is used to describe such situations that lead to chaos is "Discordianism". This is actually a recently (1958) created philosophy / religion / joke that has been built to reflect, "formally" describe and discuss the principles of chaos, confusion and disorder in the world (University of Virginia, 2005).

Another attitude exploit stems from the conventional fact that when two parties engage in a transaction or communication, this is done "in good faith", unless, of course, there are serious indications to the contrary. As it holds true in any case of pre-meditated deceit, the deceiver (the Social Engineer for the purposes of this work) has the Mark at a disadvantage. The Mark's attitude of initially acting in good faith by default, effectively delays the triggering of mental alarms and consequently impedes reaction and an efficient response to a SE attack. This is an issue that must be addressed by effective counter-measures that function by making potential targets less naïve and gullible, thus minimising the reaction time to raise alarms.

4.7 Alternative routes

If a Mark can not be persuaded to relinquish the requested data or perform the actions required of him, there always exist harsher ways of getting him/her to comply. Extortion has always been such a way. Although, strictly speaking, extortion is not a SE attack, it is more than just conceivable that sensitive information regarding the Mark can be collected through SE methods and subsequently be used against him/her in an attempt to extort further information. It is no secret that Private Investigators have been using SE tactics to gather information on their subjects, long before the term was coined to describe the principle under which these tactics worked. Regarding the subject of extortion itself, further discussion is beyond the scope of this work.

4.8 Concluding Remarks

In this chapter the fundamental psychological aspects of SE were presented. The common psychological loopholes that Social Engineers exploit as well as the techniques that they use were analysed. This is another necessary step towards building better defenses against SE. Effective controls can only be devised once the problem has been identified as clearly as possible. In this case, the issue has to do with the mind of the attacker against that of his victim. If there is a chance to counter the acts of the Social Engineer, the potential victim must be rendered capable of recognising and resisting the psychological "nudges" of the attacker as well as raising an alarm. In effect the human element becomes the last line of defense in this battle.

In a subsequent chapter, the defenses against SE will be discussed, ultimately leading to the assessment of the ISO/IEC 17799:2005 controls with respect to SE in another chapter. To be able to reach that point though, yet another issue must be first discussed: that of the social aspects of IS. This is the subject of the next chapter.

5. Social aspects of Information Security

5.1 Introduction

As this work deals in principle with issues related to Social Engineering (SE) attacks and their effects on Information Security (IS), it would be unwise to ignore the social elements and social foundations of Information Security.

In previous chapters it has been shown that SE attacks target the human element of IS by exploiting human relations to the maximum. In that context, a discussion of the psychological aspects of SE was presented in hope of better defining the SE problem. However, by ignoring the very nature of social structures that govern all aspects of human relations, fallacious working assumptions can be made, consequently leading to the creation of insufficient controls against the identified Social Engineering threats.

This chapter attempts to strengthen the pursued research by providing a solid foundation for the ensuing detailed analysis of the ISO/IEC 17799:2005 standard with respect to Social Engineering. The diagram of figure 5.1 depicts the role of this chapter within the overall structure of this dissertation.

Social relations between the individuals involved in an Information Security Management System (ISMS) structure, along with the frequently unpredictable fashion that humans act and react to stimuli, provide opportunities that Social Engineers may and do exploit. Although great effort has been invested in forming Information Security standards and procedures, these may prove inadequately equipped to ensure Information Security at the end of the day. 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.

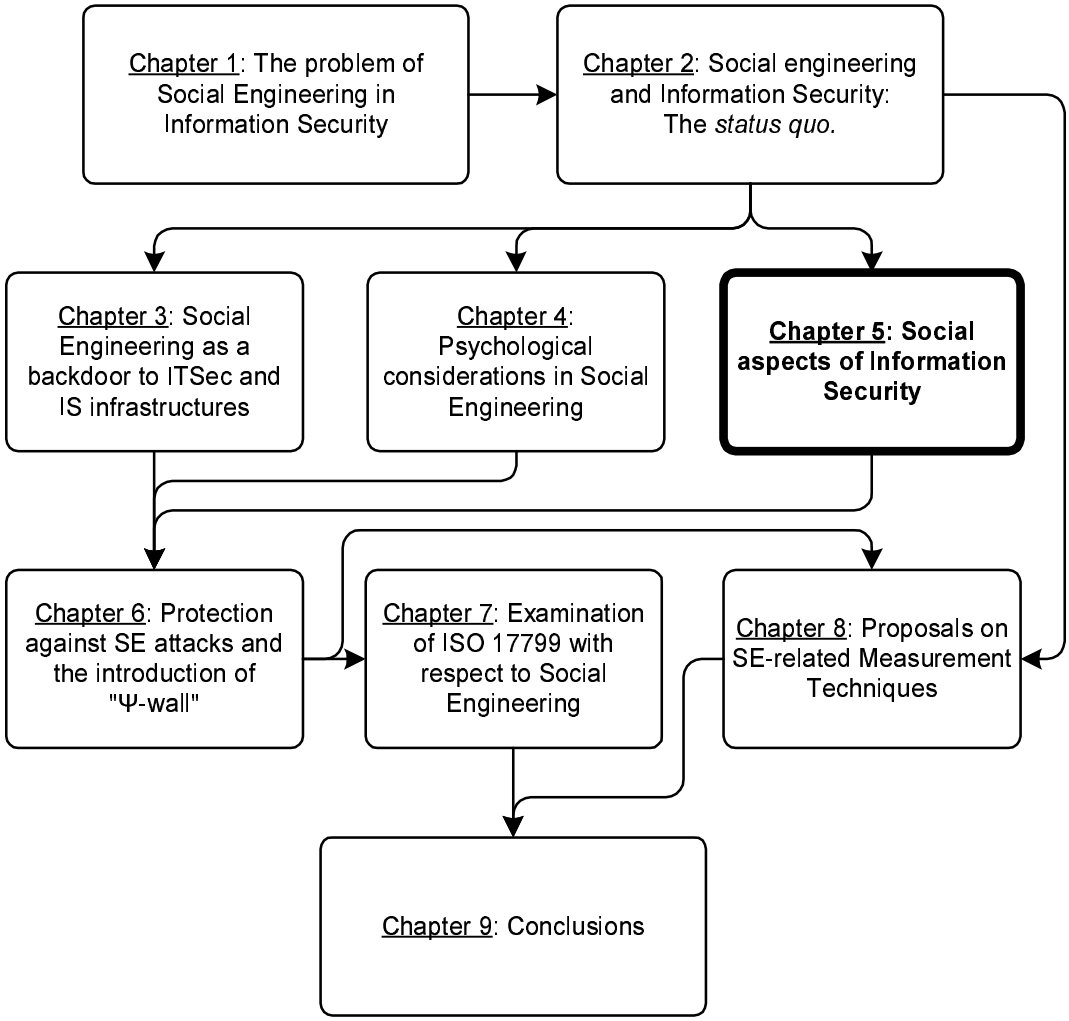

Figure 5.1: Chapter 5 within the context of the overall dissertation structure

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 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 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.

5.2 Current Practice - The Modernist approach to ISMSs

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 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. 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 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.

It does not come as a surprise that these issues are addressed in a default manner in procedures that have to do with the current analysis and design techniques applied in 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 also has to 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.

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:

a) Use of rules and regulations aiming to provide a secure environment.

b) Commitment of everyone involved to a set of prescribed guidelines or policy. This in effect constitutes behaviour control.

c) Use of technical measures for controlling the application of (a) and the upholding of (b) above.

d) Use of non-technical measures to complement (c) above.

e) De facto existence of a technocratic elite of Information Security professionals that oversees the application of (a), (b), (c) and (d) above.

There are three issues that must be brought forward here:

First, the above points are by definition dealt with in ISO/IEC standards 17799:2005 and 27001:2005, proving the modernist character of these standards which may prove to 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 nicely tie in with 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 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.

5.3 The ISMS as a social construct

Bruno Latour, in his two books, "Science on 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 ISMS, comprising both human as well as technological components, is 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 followed in Berger and Luckmann's (1991) book for reasons of proper succession of the principles' applications. Thus the social construct of the ISMS as an objective reality and then as a subjective one, will be discussed in the next two sections.

5.4 The Objective reality of the ISMS

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 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 measures for ensuring it in general, as this has already been discussed. 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 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 17799 (ISO/IEC, 2005a), 27001 (ISO/IEC, 2000b), 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 of formalism in IS management, at the same time bringing forth its bureaucratic nature that is largely based on control and regulation.

Through the above four processes, the social construct of the ISMS as an objective reality is effected.

5.5 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. It is important also to note that formality and anonymity strongly characterise the process of secondary socialisation (Berger & Luckmann, 1991, p.162). A typical example of secondary socialisation is the educational process. A teacher is perceived as an institutional functionary and thus the social interaction between teachers and learners can be formalised. Stemming from this formality, the roles of the teachers and the learners carry a high degree of anonymity. The teachers are entrusted with the particular role of the passing of specific knowledge to the learners. As such they are in principle interchangeable and thus anonymous. (This of course does not come into conflict with the subjective differentiation of teachers with respect to their abilities, stature, performance etc, all of which are qualities that are in principle irrelevant to the formal process of knowledge-passing). As far as the learners are concerned, the learners are also in principle anonymous to the teacher and are strictly viewed as the recipients of specific knowledge.

To shift all this 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 groups have differences in interests, perspectives, goals and agendas. It is these differences that warrant the division into 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 with an ISMS (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 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 scientist who usually fill the ranks of IS professionals. To further aggravate things, when IS professionals have to deal with the inability and, worse, 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 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. This difficulty in common acceptance and internalisation of the security effort by all members of an organisation creates innumerable security holes and provides social engineers with the opportunity for successful attacks.

5.6 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 them.

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, 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 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 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.

5.7 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 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 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. The groups 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 their users that may result in them becoming 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 must have been made clear that Actor-Network Theory, through the use of 'black boxes' comes in direct support of the corollaries of Social Constructionism regarding ISMSs, goes further into providing better understanding of the issues and may even lead the way into devising appropriate solutions.

5.8 Inscription and Translation in ISMSs

The notions of Inscription and Translation certainly help in the formal analysis of phenomena present in ISMSs. It was stated earlier that "Inscription is the process through which a 'pattern of use' or 'action' is 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 the use of strong passwords or, 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, the non-technical measure/artefact/directive regarding use of strong passwords also defines the behaviour of users, but to a different extent. Such directives 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 reports been filed in the case 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 who 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 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. Such a technical measure could very well be the operation of a password-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.

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 assuming 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 is.

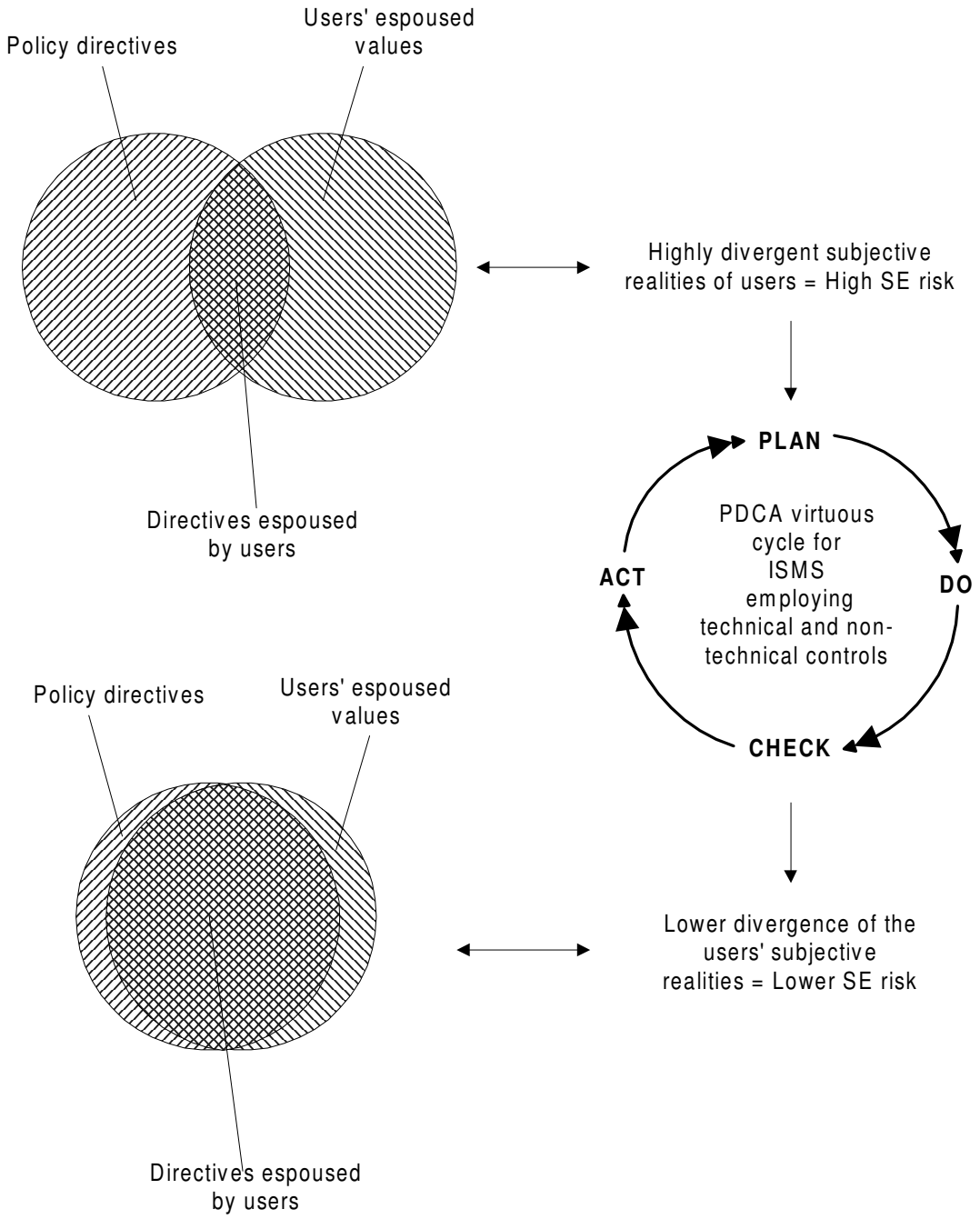

Figure 5.2: Effect of PDCA cycle on users' diverging subjective realities

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 5.2 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.

5.9 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.

"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 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. As it is mentioned elsewhere in this work, this is a fact that is always 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 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 dispenced 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 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.

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

The study presented in this chapter, combined with the analysis of the intricacies of SE and Psychological considerations provide all the necessary information for the study of possible defences against SE. This is the subject of the next chapter and it will pave the way towards the examination of the ISO/IEC 17799:2005 controls with respect to SE that will follow in a subsequent chapter.

6. Protection against SE attacks and the introduction of Ψ-wall

6.1 Introduction

This chapter attempts to combine the results of the previous three chapters on the methodology of Social Engineering (SE), its psychological aspects and the social aspect of Information Security (IS) into devising an effective strategy for strengthening defenses against SE.

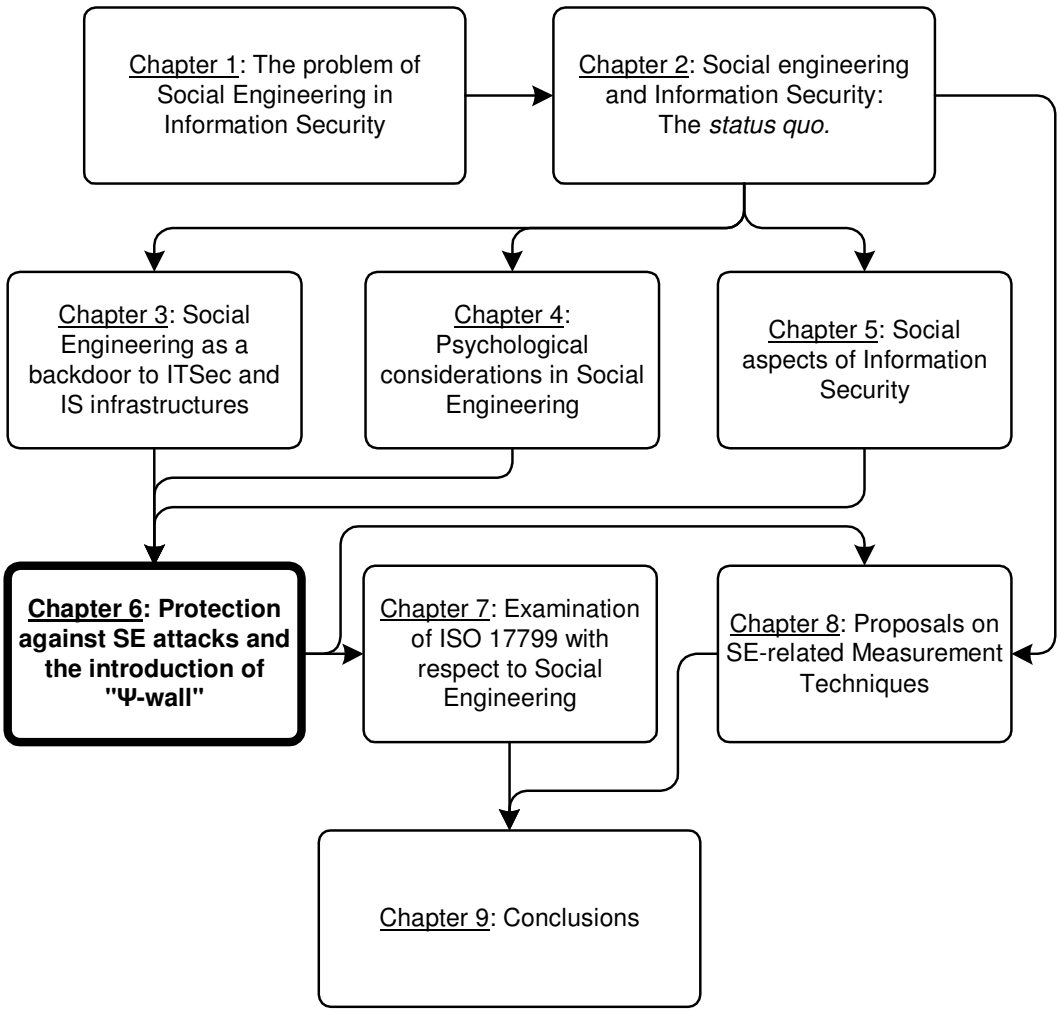

Figure 6.1: Chapter 6 within the context of the overall dissertation structure

The role of this chapter in the overall structure of this dissertation is graphically depicted in figure 6.1.

Through the course of this dissertation so far it has, hopefully, been made clear that when preparing for defense against hackers, the focus should not just be on detailing a firewall policy, adding protection to servers available over the Internet and securing internal network connections and file access. Direct attacks against the people authorised to use these computer systems should be prevented, and this, in effect, is much more difficult to build a firewall for.

As long as people are accessible through a phone line or email, then they are vulnerable to SE attacks. There are many levels of defense against such attacks and they range from creating stronger security policies and implementing controls on physical security and data protection, all the way to increasing awareness regarding SE methods of operation and educating users on how to turn the tables on the attackers. In effect, this constitutes the psychological equivalent of a firewall, or "Ψ-wall" (from the greek letter "Ψ" - correctly pronounced "Psee" but more frequently "Psi"- that serves as an internationally accepted shorthand notation for "psychology", as a quick search on the Internet shows).

6.2 Increasing awareness (through constructive brain-washing?)

Since SE attacks are based on psychological manipulation and influence / persuasion tactics, the only way to block them is to inform the users on applied psychology techniques and alert them to the tricks of the trade as these evolve. As is the usual requirement with all security policies and practices, the responsibility for implementation of such policies lies with the management. A strong commitment to continual research, implementation of new directives and re-evaluation, must precede any related effort if the effort is to bear fruit.

Although security policies must be in place and an incessant cycle of effectiveness measurements and updates must be established, most importantly, it is the Users that must be educated and constantly be re-educated, in order to keep up with the rate of evolution of threats based on SE methods.

Clearly, it is insufficient to just give theoretical lectures on SE methods to groups of bored users. Neither would it suffice to make a one-off impressive presentation and never follow it up. The attack on the problem must be two-fold. First, the issue of security must be presented in such a way that it becomes a very high priority for the average user. Second, after making security "second nature" to the users, the weapons to fight this battle against SE should be handed out in the form of practical tips, tricks and methods designed to nullify the success rate of SE attacks.

One way to direct the attitude change of users towards making security a very high, if not their first, priority, is to "bombard" them with pro-security messages. These messages must be **variations** on the same theme, always urging users to make security their priority. It is common empirical knowledge that the least effective type of message directed to a user is the one appearing everyday on his/her login screen. It was shown by Sears and Freedman (1965) that even if new ideas are not included in a message, the expectancy alone of new ideas in the message, makes the message more persuasive. In practice this means that if security-related messages are re-phrased and re-introduced, they become more persuasive than just re-stating a single message. Thus, the idea of producing and distributing "trinkets" such as catchy mouse pads, coffee mugs, pens, calendars etc, bearing well-designed pro-security messages, should be quite successful in promoting security as a necessity that must be upheld by everybody.

The above method is only the first step in creating an effective Ψ-wall. However, it is a necessary one in getting the message through that all security issues can not be addressed by technical measures alone. The second step

is to make all employees aware of the methods employed by Social Engineers. This can be in the form of short enactment videos in the usual "Discovery channel" hands-on-experience format. The video clips can be distributed over the corporate network or shown in staff meetings and any other gathering opportunity. Although there should be security awareness sessions per se, these airings do not have to be limited to dedicated meetings but should take place as frequently as possible. Such a visually rich method is much more effective than any other kind of textual distribution because, in our day and age, the motto "One picture is worth a thousand words" is stronger than ever.

6.3 Psychological defenses (the brick and mortar of the Ψ-wall)

One of the main targets of the awareness programs discussed above, must clearly be to address techniques against SE attacks exploiting the psychological characteristics of humans as were discussed earlier. A good point to start would be defense recommendations for influence techniques as presented by Cialdini (2001) and appropriately adapted for the scope of this work. Before a defense can be raised, though, the attack must be identified as such.

Despite the nature of the attack (be it physical or over the telephone), when interaction between the Social Engineer and the Mark takes place, there are tell-tale signs that the attacked employee should always be on the lookout for and constantly use as "filters" for any and all claims made by an unknown requester.

These, typically, are:

- Requests of forbidden information
- Refusal to give contact information
- Logical "holes" and small mistakes

- Name-dropping
- Rushing
- Intimidation
- Naivete
- Flattery

Although this is not a complete list of possible signs (no such list could probably be complete), it gives a clear indication of what to look for.

Furthermore, personnel should avoid taking mental shortcuts based on appearances that could help in the success of an impersonation attack: A person wearing a brown uniform with a courier logo stitched on and carrying parcels, does not automatically mean that he/she is working for the courier company. A different person dressed in the typical attire of executive class personnel does not automatically become a trusted person to be obeyed. A technician with tool belt and name-tag arriving in a semi truck during after hours does not necessarily have an assignment to carry out authorised maintenance. Thus, mental shortcuts must consciously be blocked and first impressions must be discredited. It is only the hard facts that must be taken into account and although courtesy should always be in order, proper security procedures must always take precedence.

Having identified the possibility of an SE attack, defenses against influence techniques should be applied:

Reciprocation. When the psychological / social rule of reciprocation is invoked, the attacker has already granted the Mark a favour. The Mark then feels obliged to return this favour or be scorned upon as an ingrate. Usually, the nature of the favour will be such that the favour would not be granted based on the Mark's free will, and this is why some kind of reciprocation must be called upon. So, the dilemma the Mark finds him/herself in is between granting a favour that could lead to security breach or be scorned upon and also have an immediate reduction of his/her self-esteem. The fact that the

reciprocation rule is called upon should be a dead give-away for the possibility of a SE attack. The Mark should realise that the previous favour is actually being used against him/her and thus take steps towards defusing the reciprocation rule.

It would be irrational to reject all genuine favours and all offers. This would quickly become a social problem. Nor is it easy to distinguish between a genuine and a trick offer at the time that it is granted. However, in due course the sincerity of the person making the offer or doing the favour will be proven. At that time, the original offer can be re-evaluated and if found to be insincere (in the context of the favour that is requested in return), the obligations resulting from the reciprocation rule be nullified. In retrospective, it is only genuine offers that should be met with equivalent ones. There is no such rule or obligation for trick favours or offers.

Commitment and Consistency. According to previous discussion, the Social Engineer puts these two principles to use by subtly manipulating the Mark so that the Mark gradually finds him/herself in such a position that turning down the Social Engineer's request is not an option. This entrapment can only be reversed if the Mark pays attention to the "gut feeling" he/she has when faced with the Social Engineers request. To resist the pressure based on Commitment and Consistency, the Mark must develop the ability to continually re-evaluate the initial decision (or chain of decisions) previously made, that lead to commitment and to the situation at hand. The crucial question for the Mark to answer would be "knowing beforehand what I now know, would I have made the same initial commitment that lead to this situation had I been able to reverse the clock?" If the answer is negative, (which in such situations always is), the problem should be addressed directly and it should be explained to the Social Engineer that granting his/her request would be a breach of security and that compliance is not an option.

Social Proof. When the Social Engineer subtly or directly suggest a course of action to the Mark, he/she does so by either providing false data (mr. So-and-

so has already given me this information) or by using a true basis of conformity and at the same time twisting it to serve his/her purpose. In either case, a convenient mental shortcut is forced upon the Mark in order to have him/her comply with the Social Engineer's request. In effect, the Mark is supplied with false social proof data. The only possible defense against this technique is for the Mark to first evaluate the validity of the data presented by the Social Engineer and then take into perspective that even if this data **is** true, the actions of his/her peers simply do not form the only basis for his/her decisions and subsequent actions.

Liking. Social Engineers are willing to spend a lot of effort in building a portrayed persona that is well liked by the Mark in order to befriend the Mark and thus soften the impact of a request and increase the probability of compliance. Thus, the potential victim of such an attack must be aware to the technique and be alert to the potential situation of developing an undue liking for a requester. The potential victim must be sensitive both to the extent of the liking as well as how fast this has come to occur.
Anybody can befriend anyone else very fast under false pretences of similarity, cooperation, association and compliance to the other's whims and desires. Other methods include flattery or, simply, graceful social interaction. Physical appearance also plays a decisive role.
Thus, upon realising that the "liking level" for a requester is unjustifiably high under the circumstances, the Mark must classify that requester as a potential Social Engineer carrying out an attack. The request must then be dissociated from the relation developed with the requester through social interaction. In this state of dissociation, the true nature of the request must be objectively judged and the potential for a breach of security resulting from complying with the request must be identified. If such a security breach is possible, needless to say, the request must be denied.

Authority. It has been analysed, that a Social Engineer's false appeal to authority can bear fruit in the course of an attack. As far as security is concerned, strictly speaking, all claims to authority must be challenged and all

persons must be identified as to who they really are, irrespective of their position in the hierarchy of the organisation. This can be achieved by disregarding the effect of obvious status symbols such as an expensive suit or a company executive car and taking into consideration only hard evidence, like a secure ID badge etc, in order to authenticate the individual. There also exist cases where a true person of authority acts in an unwise manner with respect to security (such as allowing unauthorised personnel on the grounds etc). In this case, the person of authority's knowledge of security procedures, sincerity and trustworthiness must also be challenged. In order to accomplish this inarguably difficult task, the correct procedures must be in place so that employees charged with such tasks can protect themselves against spiteful, retaliatory attacks, by simply sticking to procedures and "going by the book".

Scarcity. The reactions to this psychological principle are difficult to control. This is because these reactions have an element of emotional arousal and while in this state, straight thinking is practically impossible. Perhaps the only means of defense would be to use this emotional arousal as an indication of a possible SE attack. Steps can then be taken to suppress the arousal and attempt to rationalise the situation. If the interaction with the Social Engineer takes place in real time, the element of rushing will also probably be very strongly present. The combination of these two signs put together may help to surely identify and efficiently resist the attack.

6.4 Changing the social model of IS

From the discussion of the social aspects of IS several practical results were obtained than bring to light the gap existing between the expected result of implemented IS policy directives and the actual outcome of its implementation. This discrepancy is largely due to the following issues:

- A gap exists between what the IS professionals perceive as Information Security and what everybody else understands.

- Competition exists between the various groups of an organisation, including but not being limited to Management, IS professionals and Administrative employees.
- Organisation employees who have an IS policy imposed on them but had no involvement in its creation have great difficulty in understanding, accepting and following its directives.
- Barriers are unavoidably raised between the groups of an organisation with the direct consequence that one group does not know how the other groups operate, or worse still, makes erroneous assumptions about this. Thus, when one group is requested to make decisions that affect the other groups as well, the solutions proposed are not optimised for all of the groups.
- The outdated hierarchical structures in today's organisations make the application of IS just another part of them. By nature though, many aspects of IS and especially all that are related to SE can not be forcefully applied through traditionally vertical hierarchical structures but should rather be applied horizontally.
- In the quest for status, groups in the organisation that expect to gain lateral benefits (that are irrelevant to IS) from the application of an IS policy, may promote it more fervently while competing groups will oppose it as a means of denying power to their adversaries.

All of the above prove that an IS policy invariably carries with it political power in the context of the organisation it is being applied to. Needless to say that the larger the organisation, the higher the political power involved in the IS policy.

As it is impossible to change organisational structure and mentalities overnight, it is important to use those measures that will provide the desired effect within the current organisational context.

To begin with, a well-designed security awareness campaign must work in the direction that IS is essential to the well-being of the organisation and the individuals that work for it.

Once the above is accomplished, the procedure of defining or assessing the IS policy and proposing changes to it should be guided by experts but be open for all to contribute and challenge.

To the extent that this is possible IS must be disjointed from the vertical administrative hierarchy. At the same time it must not be enforced in the traditional sense but rather aided to permeate all aspects of the organisation's scope.

What is probably the most difficult challenge is to have IS detached from any power play within the organisation. To accomplish this, the application of IS must not be considered as the privilege of an elite group who controls and enforces it but should rather be entrusted in the care of all employees throughout the breadth and width of the organisational structure as van Niekerk and von Solms (2005) propose. This may indeed sound as a utopian suggestion given the *de facto* creation of a horizontal structure within the organisation, but if the necessary preparation has taken place through security training and awareness, then it might just become plausible.

6.5 Strengthening security policies

Effective IT security is based on solid security policies. Security against SE attacks adds further complications to the creation of security policies because the nature of the attacks is much less pre-determined when compared to that of purely technical vulnerabilities. Hence, apart from the usual measures found in security policies, certain areas of security must be especially strengthened in the particular direction of blocking SE attacks.

The principles presented here for devising controls against SE risks will be further discussed in a subsequent chapter of this work, in the context of the evaluation and strengthening of the ISO/IEC 17799:2005 standard with respect to SE. The inclusion of the present, brief, examination only serves in placing the principles into perspective for the sake of completeness and continuity.

6.5.1 Physical security measures

- In central, controlled entrances and exits to the premises, measures must be taken so that **"tail-gating" or "piggy-backing" is not allowed** by the automated access and logging system. Since it is not practical to have the post's security guard oversee every entry that takes place and efficiently block every attempt to tail-gate, the configuration of the access doors must be such that two people are not allowed to pass through simultaneously. This could be realised by double doors or gates where the outer one has to be closed before the inner one opens. In the space between them, only one person should be allowed to fit. Alternatively, the typical triple-bar access-control turnstiles could be used, one turn of which should be initiated per valid card presentation.

- **Exit from the premises should be controlled** in as an efficient manner as entry to them. This will impede a Social Engineer's attempt to escape from the premises unnoticed. If a person leaving the building is not able to produce the necessary credentials, that person should be held until his/her identity is verified.

- **Access ID tokens should be as secure as possible**, so that a lost or stolen one can not be used by a Social Engineer to gain access. PIN codes should be in use and, as technology progresses, biometrically-protected smartcards to match the card to the owner and ensure the owner's physical presence at the point of access.

- Ideally, all **visitors should be accompanied by staff or personnel** in and out of the premises. As this is not always practical, general visitors should be logged and bear badges indicating their destination. Nevertheless, specialised visitors who must have access to more sensitive areas, such as systems' maintenance technicians from outside vendors, must always be accompanied by the local site administrator (who is supposed to be well known and thus identifiable). In any other case, a procedure should be in place requiring all personnel whose area of responsibility the visitor enters, to call the appropriate site administrator to check if the visitor should really be there. Staff should be **required** to follow this procedure in order to overcome their natural reluctance to do this, as they would feel that it would make them look unfriendly, distrustful or even paranoid if they challenged visitors.

- **Shredders and incinerators** must be used and all data-carrying media that have served their purpose or lifetime must be destroyed (including magnetic media of all types as well as paper-based documents). If a recycling scheme is in place, all material must be thoroughly rendered unusable before placed in the recycling bin. (I.e. paper must be shredded and magnetic media physically destroyed beyond recovery, before being put up for recycling).

- **Garbage should be checked** by assigned personnel for items containing sensitive information. Penalties should be in place for employees who do not follow security procedures.

- In addition to the previous controls, **recycling and garbage bins should rest in a controlled and monitored area** to deter dumpster diving.

- **Physical access to networked computers** should be allowed through the use of secure authentication tokens (such as smartcards) that should remain in place for as long as the workstation is used and be removed when the user leaves the station. As a result, the screen and keyboard should get locked. An interesting development would be the design of a

proximity device that locks unattended workstations and unlocks them while the authorised user is within two meters of his/her station. This could be realised by a two-piece device, one piece remaining permanently connected to the computer and the other one resting in the user's pocket.

- **Employees should be aware of their surroundings** and be especially suspicious of "casual" onlookers who may be on a "shoulder surfing" spree.

- Further to the above measure, specially designated members of the **security staff could make it their job to walk around** the premises/floor/unit with the objective to get to know all employees. If a Social Engineer has managed to penetrate the premises, he/she will be spotted by the special security officer.

- **Contractor personnel**, after being securely authenticated at the point of entry and escorted by staff members to their work area, should be continually monitored by trained security personnel. When their work involves access to computer systems, they should be monitored by designated staff members of the IT department who can evaluate their actions.

- **Reception personnel** should be instructed to only release documents, parcels etc to securely authenticated individuals. Even then, a detailed log of released items must be kept, including the personal identification data of the receivers. Requests for forwarding via fax should also be logged and the requester positively identified.

- All areas containing **network equipment, phone exchange equipment, wiring racks etc should be secured** and access to them should be controlled via ID tokens, logged and recorded.

- The above should hold true for the **mail room** also.

6.5.2 Internet security measures

- Users should be warned not to take part in **unsolicited traditional mail or e-mail surveys** that are not authorised by the organisation. Since this can not be efficiently controlled when the user receives the survey at his/her home address or when he/she has Internet access via his/her home computer, users should be at least forbidden to disclose personal information related to their work. Users should be informed of continually running audits to raise alertness. All mail survey solicitations should be reported to the SE attack coordination centre.

- Users should be alerted to the existence of **fraudulent web sites that require registration with username and password**. Although it is convenient for most users to use the same password or PIN for access to all of the accounts that they have, by using the same identification pair at a compromised site, control of all of the user's other accounts will be relinquished. Users should thus be forbidden to submit the authentication information that they already use to gain access to the organisations' computer network, in registrations to other systems.

- **Under no circumstances should users install software or open attachments** received over the Internet.

- Users need to be aware of **how much the public knows about their position**. In addition, users should be aware of how much information about them is available on the Internet. Social Engineers will conduct searches on the Internet for users' names and attempt to impersonate them once they have gathered enough information.

- **Organisational phone lists should not be published on the Internet** as they can provide a wealth of information to the attacking Social Engineer.

- Users should be suspicious of **windows popping up** while they are working on their computers telling them that the network connection has

been lost and that their user name and password must be re-entered. This can very well be part of computer-based attack that forwards the private data to the Social Engineer

6.5.3 Phone security measures

- If a called party can not securely identify a caller who asks for sensitive information including, but not limited to, personal information about the called party or anyone else, or for information about the corporate computer system, no information should be provided. The called party should insist on **verifying the caller's identity by calling them back at their proper telephone number** as listed in the organisation's official telephone directory. Legitimate activity is not severely hindered by the proposed procedure but SE attacks are effectively blocked.

- **Call forwarding to external lines should not be enabled on dial-up numbers or numbers equipped with a fax machine**. This measure will prevent the Social Engineer from intercepting faxes and / or requesting information to be sent to an internal phone number while the information will actually be forwarded to an external number belonging to the Social Engineer.

- All employees eligible to support via a phone-operated help desk, should be given an **authentication PIN particular to the help-desk service**. Furthermore, help desk personnel can have access to limited personal data on employees so that secure authentication can take place through the combination of a PIN and the correct response to a question pertaining to that data.

6.5.4 General measures

- Any **inquiries made about passwords**, or any other sensitive information should be considered as a SE attack and measures against it be taken including raising an alarm with the appropriate coordination centre, if possible while the attack is in progress.

- **Better protection of personal data** of employees in general, is also of paramount importance. Access to it should be limited in an effort to thwart Social Engineers from gathering enough information to stage an impersonation attack. Such data should be given out on a justified need-to-know basis only and only to authenticated staff members.

- Apart from information related to security that is prepared and presented by the competent directorate within a corporate or organisational structure, **all staff members should actively remain informed on current security issues** and encouraged to make security their priority.

The above list of proposed measures is by no means exhaustive, neither can all of the proposed measures be directly converted to security procedures. They do mark, however, the general direction that the construction of a security policy should be moving in, in order to cater for SE attacks.

6.6 Security compliance measurement

Measuring the degree of effectiveness of any implemented security measure is difficult to begin with. Nevertheless, this constitutes an important factor in the continual re-assessment of the current security policy and a most valuable guide in pinpointing problem issues and addressing them.

In principle, the effect of SE attacks is difficult to operationalise. Collins (2000, p. 68) defines Operationalisation as the process of *transforming a theoretical concept into an empirical variable*, i.e. making the defined concept measurable. Consequently, measuring the effectiveness of a set of countermeasures designed to block SE attacks (the Ψ-wall) is at least as difficult as operationalising the effects of the SE attacks themselves. This is mainly due to the non-descriptive nature of controls against SE that are based on purely psychological techniques.

In short, how can issues like the psychological effect of an awareness campaign on individuals or the actual effect of the psychology-laden process against a potential SE attack be measured?

To operationalise a concept such as the effectiveness of the proposed Ψ-wall (in other words the level of defense against SE attacks), it is imperative to identify all of its dimensions or **indicators,** where *an indicator is an observable measure* (Collins, 2000, p.68). A later chapter of this work deals with the operationalisation in question and hopefully succeeds in proving that operationalisation can indeed be achieved and that the effectiveness of the Ψ-wall may be measurable.

6.7 Audits and Penetration testing

Be it for empirical assessment or exact security compliance measurement, or simply to keep the alertness levels of computer users, and employees in general, high, the combination of internal audits and third-party penetration testing constitutes an indispensable tool for maximising security. Through such methods the shortcomings of any ISMS are brought to light and effectively catered for, thus raising the level of security.

Employees should be alerted to the fact that audits and penetration testing will be carried out at indeterminate points in time. A system of rewards or merit points for blocked attacks could also be established.

In testing for SE attacks, the usual problems regarding the sincerity of the testers, the access limits of the testing, possible liabilities etc that apply for traditional IT penetration testing, do exist. In addition to these, yet another complicating factor comes into play. In applying penetration testing methods to computer networks and computer systems in general, it is argued that a well-trained security engineer is not deficient in knowledge compared to a hacker (Lowery, 2002). As SE attacks constitute a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking

people to break normal security procedures, in testing for vulnerabilities that can be exploited by Social Engineers, the testers have to have honed mental and communications skills (probably on top of engineering skills) in order to duplicate the effect of an attack by a real Social Engineer. Clearly, these abilities can not be taught as part of a course for testers, neither would it be advisable or ethical to employ active Social Engineers or confirmed colleagues of theirs that have supposedly repented or retired. Thus, the selection of testers (either internal or external) may prove to be an arduous task. Although carefully prepared scripts for use by the testers might be helpful, even a half-decent SE attack can not simply rely on scripts.

Another issue is whether the testers are given an advantage over real-life Social Engineers in the form of a copy of the structure's security policy. If they are given such a copy they will know exactly what to look for and where to focus their efforts, something that real attackers will not be able to do as easily. However, the notion of testing for "worst case conditions" is not one without merit.

Ideally, to test for worst case conditions, all of the situations discussed earlier in this chapter -and more- should be examined and the related techniques applied. To this end the paper by Orgill et al (2004) should prove quite helpful. A further complication of testing for SE techniques is that the scope of such an investigation is far greater than that for a straight-forward attempt to e.g. break through the firewall and into the corporate network of the organisation. In the latter case the effort can easily be focused and all attempts be made to bypass countermeasures. While testing for vulnerabilities exploitable through SE attacks, an exhaustive test would involve applying SE techniques on every single employee of the company, simply because the security "chain" is as strong as its weakest link, which in this case is the individual most susceptible to SE attacks (Schneier, 2000). Thus, an exhaustive test would be very difficult to carry out in all but the smaller of organisational structures. However, as the effects of discordianism become more prominent as an organisation augments in size, smaller structures, where interpersonal

relations between employees are more common and stronger, are less prone to successful SE attacks. Hence, for larger structures, the difficulty in carrying out exhaustive tests is very serious.

Random testing in this case does not solve the problem because if penetration was not achieved, all that the subsequent report would state would really apply to the random subset of employees that were actually tested. Since this would be a small part of the whole, the conclusions drawn could be very disputable. In this context, let it not be overlooked that in a real-life attack the Social Engineer will keep carrying out attacks on different employees until the desired information is extracted either in whole or pieced together.

A scheme to efficiently address employees who are more susceptible to SE attacks would be to base the testing on the results drawn from psychological profiling of employees, perhaps in the context of evaluating the efficiency of awareness programs as it has already been discussed. The main difference in the philosophy of the two exercises, though, would be that instead of processing the results of anonymously submitted questionnaires as would be the case of program efficiency evaluations, the profiling should be carried out on individual employees and the results be kept on file. This, in itself would be a very controversial issue.

A defense against the relentless nature of a real-life Social Engineer who will keep carrying out attacks on different employees until the desired information is extracted, might only be possible through reporting and coordination procedures by a central authority in the organisation. Indirectly, the audits and penetration tests should thus also address the effectiveness of such an authority by staging such an attack scenario that would purposely take a number of attacks to be concluded.

All in all, testing for vulnerabilities exploitable by SE attacks is very difficult to orchestrate, extensive preparations need to be made, the people taking up

the role of the attackers should be highly skilled and controversial issues about psychological profiling of employees come into play. Furthermore, every new employee who is hired, forms a new parameter in the security equation that needs to be evaluated and controlled. It has been said that no system can be considered totally secure no matter how well it has been audited and tested. This is even more so when the psychology of individuals becomes a crucial factor. Even after all audits and penetration testing has been carried out, the author believes that there would be no real assurances as to the level of security against SE attacks. The most important contribution of such procedures would probably be the overall raised level of alertness among employees.

6.8 Promotion of higher ethical standards in the workplace

Reekie (2004) introduces the need for the creation of a set of ethical obligations stemming from the organisation's responsibility to the client, as well as its responsibility to itself to protect its interests. Additionally, the need for inclusion of relevant countermeasures in security policy implementation is supported.

In the context of guarding against SE attacks, the promotion of ethical standards in the workplace is of paramount importance. As it has been shown in this chapter, invariably, SE attacks count on some aspect of human psychology to produce results. Whether this aspect is fear of authority, the natural willingness to help, the application of convenient mental shortcuts, the reluctance to become disliked etc, the SE attacks work because people are simply left to their own devices as far as their reaction to an attacking Social Engineer is concerned.

By promoting ethical standards in the workplace, feelings like (but not limited to) fear of powerful people of authority, ingratiation and the feeling of risking being disliked when challenging a fellow employee who might instead be a potential attacker, will be reduced. In a work environment where ethical

standards form the basis for everyday activities, there is no space left for acts of intimidation, coercion or exploitation. Thus, the attacker is faced with a greater challenge than expected or planned for.

Furthermore, in an ethically-bound environment, incident reporting becomes more efficient as the effects of discordianism are reduced and the effectiveness of proper channels of communication between the base of the organisation and its highest levels increases. This invariably leads to better defense against SE attacks.

6.9 Monitoring Social Engineering attempts

The idea of a central point where all reported SE attempts are logged and evaluated and countermeasures coordinated has already been presented elsewhere in this work. Reporting procedures for security incidents as well as the formation of a coordination centre is also prescribed in the directives of the ISO/IEC 17799:2005 standard (ISO/IEC, 2005a). However, in the context of this standard, the coordination centre and reporting procedures may not cater as efficiently as possible for the particular case of SE attacks given that immediate response and even guile are required in order to beat the attacker in his/her own game. The evaluation of the relevant ISO/EC 17799:2005 controls though, is the subject of a later chapter. Ideally, the existence of such a centre will assist in identifying problem areas within the organisation and will also help those responsible for security, **identify the nature** of the attacking Social Engineer's interest. This in itself is of great importance because it can give clear indications regarding what the motives behind the SE attacks are. Concise reports made by the SE attack monitoring authority could give the management information on important issues such as a secret project being compromised or that attempts are made to extract financial information before a takeover etc.

The most difficult part is for personnel to identify a SE attack as one and report it. Ideally, it would also be very useful to let the attack run its course in

an effort to identify its ultimate target. This, however, is clearly beyond the abilities of the average employee. Manipulating the manipulator would be a challenge for even the most cunning expert on counteracting SE attacks.

Thus the most reasonable expectation would just be for the average employee to be able to identify an attack and report it as a result of the whole security education, training and awareness program. The employees manning the monitoring and evaluation centre though, should be highly specialised security professionals who can sift through all the reports, weed out the false ones and extract information of value to the management or the top levels of the hierarchy. Furthermore, they should be able to predict (to some degree) future attacks based on forming patterns and thus call for raised levels of alertness and strengthening of security measures. Most importantly, they would form the mortar holding together the Ψ-wall.

6.10 Concluding Remarks

In this chapter the fundamentals of SE were presented. The basic forms of SE attacks were discussed, backed by a presentation of the most important Persuasion tactics and Influence techniques as modern psychology accepts them.

Due to the complicated and highly non-technical nature of SE attacks, it is argued that in order to defend against them, an organisation must invest upon its human resources and, most importantly, their psychology. Traditional technical measures simply do not offer sufficient provisions to stop non-technical attacks such as SE ones. Thus, a case is presented in support of psychological defenses with the objective of strengthening security policies and improving security mentality and practices in an attempt to provide better protection against SE attacks.

It thus follows that a "psychological Firewall" or "Ψ-wall" must be built mainly through awareness and psychological training programs. The objective of the

programs should be to expose the employees to the reality of SE attacks before they actually have to face one. Mastery of psychological defenses against these attacks can be taught to a certain extent, as is the ability to at least identify them.

The principles governing supporting controls against SE were also specified for inclusion in existing security policies. This discussion sets the foundation for the thorough examination of ISO/IEC 17799:2005 standard (IS/IEC, 2005a) with respect to SE to follow in the next chapter of this dissertation.

The issues of measurement and compliance were addressed through the proposed use of operationalisation methods and the identification of relevant indicators. This direction is further pursued in a subsequent chapter.

It was also maintained that raising ethical standards in the workplace can help against SE attacks as many of the psychological barriers of employees that the Social Engineers thrive upon simply fall apart.

Finally, the importance of auditing and penetration testing was stressed as a means of raising alertness, and the need for a central point of coordination against SE attacks was highlighted.

7. Examination of ISO 17799 with respect to Social Engineering

7.1 Introduction

All of the research carried out so far aimed at providing the necessary background information for the examination of the ISO/IEC 17799:2005 standard (ISO/IEC, 2005a). This chapter deals with the main research question of assessing the standard's directives with respect to Social Engineering (SE). Figure 7.1 depicts the role of this chapter within the overall structure of this dissertation.

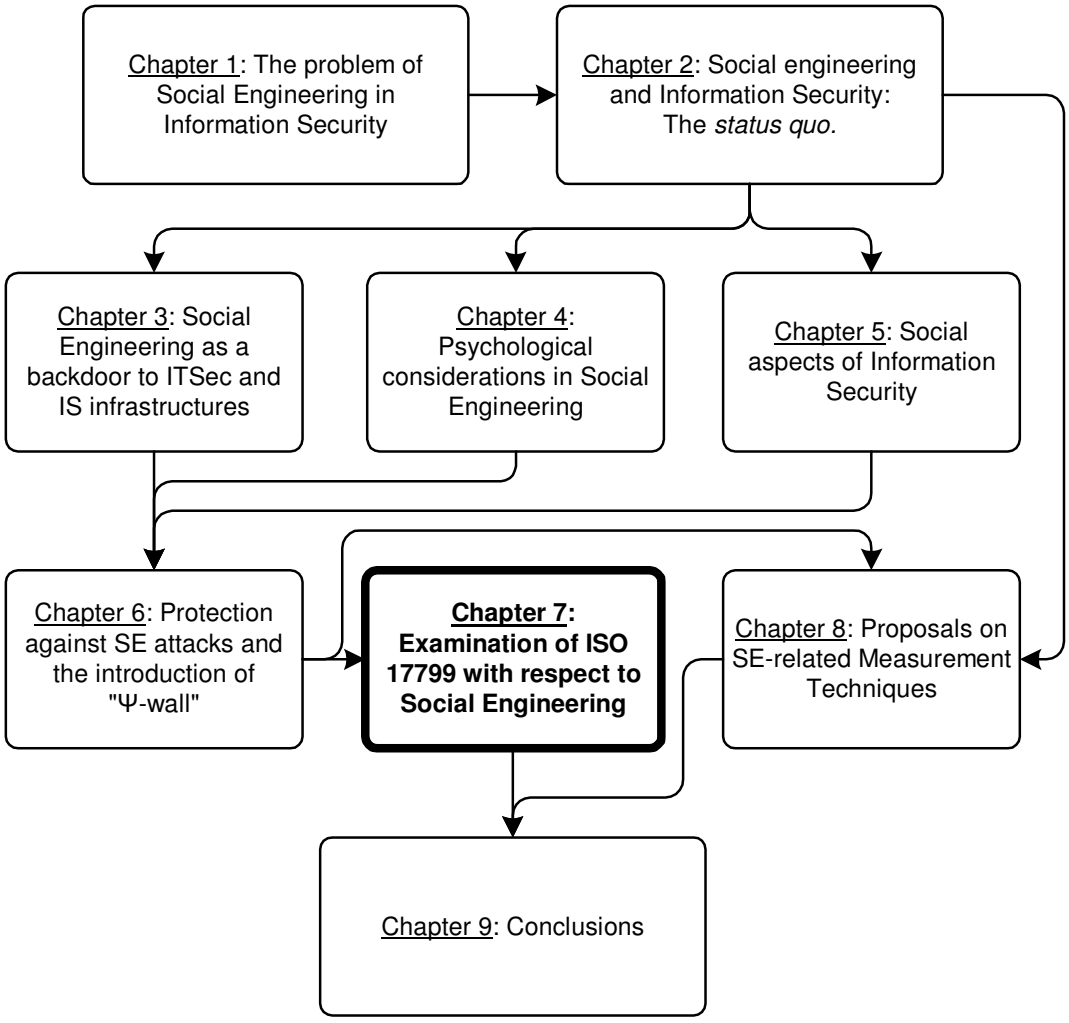

Figure 7.1: Chapter 7 within the context of the overall dissertation structure

(For reasons of simplicity the ISO/IEC 17799:2005 standard will simply be referred to henceforth as "ISO 17799").

As the ISO 17799 currently constitutes the most widely accepted Information Security standard and having already identified the IS issues pertaining to SE attacks and methods thereof, it was deemed essential to examine ISO 17799 under the light of SE. In previous research, (Frangopoulos and Eloff, 2004) the 2000 version of the ISO 17799 (ISO/IEC, 2000a) is compared to other IS standards and practices and the relevant merits, shortcomings and common ground covered are examined. From that examination, ISO/IEC 17799:2000 proved to be the most appropriate standard, in its ability to cover a large variety of risks, that are neither purely technical nor limited to the IT infrastructure of the organisation. In many ways ISO/IEC 17799:2000 also proved to be a "superset" of the other documents. Thus, the results of the current research can easily be correlated back to the other examined standards and practices. Even though this comparison takes place between the 2000 version of ISO 17799 and other material, its results are still valid as the character of ISO 17799 did not change drastically between the 2000 edition and the 2005 revision. For all of the above reasons, it was decided to use ISO 17799 as the subject for assessment with respect to SE. The standard's shortcomings were identified, control elements were proposed and perhaps steps can be taken towards encompassing SE-related issues in a future revision of the standard.

7.2 Structure of the ISO/IEC 17799:2005

The 2005 revision of ISO 17799 comprises 11 security control clauses. Altogether, these clauses contain 39 main security categories. In addition to the above, an introductory clause sets the basis for risk assessment and treatment.

The eleven security control clauses (accompanied by the main security categories included in each clause) are:

1) Section 5. Security Policy
    i. Information security policy
2) Section 6. Organising Information Security
    i. Internal organization
    ii. External parties
3) Section 7. Asset Management
    i. Responsibility for assets
    ii. Information classification
4) Section 8. Human Resources Security
    i. Prior to employment
    ii. During employment
    iii. Termination or change of employment
5) Section 9. Physical and Environmental Security
    i. Secure areas
    ii. Equipment security
6) Section 10. Communications and Operations Management
    i. Operational procedures and responsibilities
    ii. Third party service delivery management
    iii. System planning and acceptance
    iv. Protection against malicious and mobile code
    v. Back-up
    vi. Network security management
    vii. Media handling
    viii. Exchange of information
    ix. Electronic commerce services
    x. Monitoring
7) Section 11. Access Control
    i. Business requirement for access control
    ii. User access management

iii. User responsibilities
iv. Network access control
v. Operating system access control
vi. Application and information access control
vii. Mobile computing and teleworking

8) Section 12. Information Systems Acquisition, Development and Maintenance
i. Security requirements of information systems
ii. Correct processing in applications
iii. Cryptographic controls
iv. Security of system files
v. Security in development and support processes
vi. Technical vulnerability management

9) Section 13. Information Security Incident Management
i. Reporting information security events and weaknesses
ii. Management of information security incidents and improvements

10) Section 14. Business Continuity Management
i. Information security aspects of business continuity management

11) Section 15. Compliance
i. Compliance with legal requirements
ii. Compliance with security policies and standards, and technical compliance
iii. Information systems audit considerations

Insofar the main security categories are concerned, each of those contains:
a) a control objective stating what needs to be achieved, and
b) description(s) of one or more controls that can be applied to achieve the control objective.

A typical control description comprises:
a) a definition of the specific control statement to satisfy the control objective,

b) guidance and information in support of the implementation of the control and how to achieve the control objective,
c) further information, pertinent to the control under examination, such as legal aspects of its implementation and references to related standards.

7.3 Examination of the security control clauses.

Following the structure of ISO 17799 presented above, an attempt was made to view each of the eleven security control clauses under the light of a possible SE attack. Due to the length of the analysis, the detailed results of this effort are included as Appendix C of this work. In that analysis discussions are presented for each of the clauses along with some thoughts on how to further fortify the clauses against SE attacks whenever this is deemed necessary. The results of the examination are summarily presented in the form of the following table. In that table information is given for each of the individual controls regarding its relevance to the defense against SE and whether it needs to be enhanced to serve this role better.

Table 7.1: Examination of ISO 17799 controls with respect to SE

Section	*Relevant to the defense against SE attacks?*	*Needs to be enhanced?*
5 SECURITY POLICY		
5.1 INFORMATION SECURITY POLICY		
5.1.1 Information security policy document	YES	YES
5.1.2 Review of the information security policy	YES	YES
6 ORGANIZATION OF INFORMATION SECURITY		
6.1 INTERNAL ORGANIZATION.	-	-
6.1.1 Management commitment to information security	YES	NO
6.1.2 Information security co-ordination	YES	NO
6.1.3 Allocation of information security responsibilities	YES	YES
6.1.4 Authorization process for information processing facilities	YES	YES

6.1.5 Confidentiality agreements	YES	NO
6.1.6 Contact with authorities	YES	YES
6.1.7 Contact with special interest groups	YES	YES
6.1.8 Independent review of information security	YES	YES
6.2 EXTERNAL PARTIES .	-	-
6.2.1 Identification of risks related to external parties.	YES	YES
6.2.2 Addressing security when dealing with customers .	YES	YES
6.2.3 Addressing security in third party agreements .	YES	YES
7 ASSET MANAGEMENT		
7.1 RESPONSIBILITY FOR ASSETS.	-	-
7.1.1 Inventory of assets	YES(indirectly)	NO
7.1.2 Ownership of assets	YES(indirectly)	NO
7.1.3 Acceptable use of assets.	YES	NO
7.2 INFORMATION CLASSIFICATION.		
7.2.1 Classification guidelines	YES	YES
7.2.2 Information labeling and handling	YES	YES
8 HUMAN RESOURCES SECURITY.		
8.1 PRIOR TO EMPLOYMENT	-	-
8.1.1 Roles and responsibilities .	YES	YES
8.1.2 Screening	YES	YES
8.1.3 Terms and conditions of employment	YES	YES
8.2 DURING EMPLOYMENT	-	-
8.2.1 Management responsibilities	YES	NO
8.2.2 Information security awareness, education, and training	YES	NO
8.2.3 Disciplinary process .	YES	YES
8.3 TERMINATION OR CHANGE OF EMPLOYMENT.	-	-
8.3.1 Termination responsibilities .	YES	NO
8.3.2 Return of assets	YES	NO
8.3.3 Removal of access rights	YES	NO
9 PHYSICAL AND ENVIRONMENTAL SECURITY		
9.1 SECURE AREAS	-	-
9.1.1 Physical security perimeter	YES	YES
9.1.2 Physical entry controls	YES	YES
9.1.3 Securing offices, rooms, and facilities	YES	YES
9.1.4 Protecting against external and environmental threats	YES	YES
9.1.5 Working in secure areas	YES	NO

9.1.6 Public access, delivery, and loading areas	YES	YES
9.2 EQUIPMENT SECURITY.	-	-
9.2.1 Equipment siting and protection	YES	NO
9.2.2 Supporting utilities	YES	YES
9.2.3 Cabling security	YES	YES
9.2.4 Equipment maintenance.	YES	YES
9.2.5 Security of equipment off-premises	YES	YES
9.2.6 Secure disposal or re-use of equipment	YES	YES
9.2.7 Removal of property	YES	NO
10 COMMUNICATIONS AND OPERATIONS MANAGEMENT		
10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES	-	-
10.1.1 Documented operating procedures	YES	NO
10.1.2 Change management	YES	NO
10.1.3 Segregation of duties	YES	NO
10.1.4 Separation of development, test, and operational facilities.	YES	NO
10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT .	-	-
10.2.1 Service delivery	YES	NO
10.2.2 Monitoring and review of third party services.	YES	NO
10.2.3 Managing changes to third party services	YES	NO
10.3 SYSTEM PLANNING AND ACCEPTANCE	-	-
10.3.1 Capacity management .	YES(indirectly)	NO
10.3.2 System acceptance .	YES(indirectly)	NO
10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE	-	-
10.4.1 Controls against malicious code	YES	YES
10.4.2 Controls against mobile code	YES	YES
10.5 BACK-UP .	-	-
10.5.1 Information back-up	YES	NO
10.6 NETWORK SECURITY MANAGEMENT	-	-
10.6.1 Network controls	YES	YES
10.6.2 Security of network services	YES	NO
10.7 MEDIA HANDLING .	-	-
10.7.1 Management of removable media	YES	NO

10.7.2 Disposal of media	YES	NO
10.7.3 Information handling procedures .	YES	NO
10.7.4 Security of system documentation	YES	NO
10.8 EXCHANGE OF INFORMATION	-	-
10.8.1 Information exchange policies and procedures.	YES	YES
10.8.2 Exchange agreements .	YES	NO
10.8.3 Physical media in transit .	YES	NO
10.8.4 Electronic messaging	YES	NO
10.8.5 Business information systems	YES	NO
10.9 ELECTRONIC COMMERCE SERVICES	-	-
10.9.1 Electronic commerce	YES	YES
10.9.2 On-Line Transactions .	YES	YES
10.9.3 Publicly available information	YES	YES
10.10 MONITORING	-	-
10.10.1 Audit logging	NO	NO
10.10.2 Monitoring system use	NO	NO
10.10.3 Protection of log information	NO	NO
10.10.4 Administrator and operator logs .	NO	NO
10.10.5 Fault logging	NO	NO
10.10.6 Clock synchronization	NO	NO
11 ACCESS CONTROL		
11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL .	-	-
11.1.1 Access control policy	YES	YES
11.2 USER ACCESS MANAGEMENT	-	-
11.2.1 User registration	YES	YES
11.2.2 Privilege management .	YES	NO
11.2.3 User password management	YES	YES
11.2.4 Review of user access rights .	YES	YES
11.3 USER RESPONSIBILITIES	-	-
11.3.1 Password use	YES	YES
11.3.2 Unattended user equipment	YES	YES
11.3.3 Clear desk and clear screen policy	YES	NO
11.4 NETWORK ACCESS CONTROL	-	-
11.4.1 Policy on use of network services	NO	NO
11.4.2 User authentication for external connections	NO	NO
11.4.3 Equipment identification in networks .	NO	NO

11.4.4 Remote diagnostic and configuration port protection	NO	NO
11.4.5 Segregation in networks	NO	NO
11.4.6 Network connection control.	NO	NO
11.4.7 Network routing control	NO	NO
11.5 OPERATING SYSTEM ACCESS CONTROL	-	-
11.5.1 Secure log-on procedures	NO	NO
11.5.2 User identification and authentication	NO	NO
11.5.3 Password management system	YES	NO
11.5.4 Use of system utilities	NO	NO
11.5.5 Session time-out.	NO	NO
11.5.6 Limitation of connection time	NO	NO
11.6 APPLICATION AND INFORMATION ACCESS CONTROL .	-	-
11.6.1 Information access restriction	NO	NO
11.6.2 Sensitive system isolation	YES(indirectly)	NO
11.7 MOBILE COMPUTING AND TELEWORKING	-	-
11.7.1 Mobile computing and communications .	YES	YES
11.7.2 Teleworking	YES	YES
12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE		
12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS	-	-
12.1.1 Security requirements analysis and specification	NO	NO
12.2 CORRECT PROCESSING IN APPLICATIONS	-	-
12.2.1 Input data validation	NO	NO
12.2.2 Control of internal processing	NO	NO
12.2.3 Message integrity	NO	NO
12.2.4 Output data validation.	NO	NO
12.3 CRYPTOGRAPHIC CONTROLS	-	-
12.3.1 Policy on the use of cryptographic controls	NO	NO
12.3.2 Key management	NO	NO
12.4 SECURITY OF SYSTEM FILES.	-	-
12.4.1 Control of operational software	YES	YES
12.4.2 Protection of system test data	YES	NO
12.4.3 Access control to program source code	YES(indirectly)	NO
12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES	-	-

12.5.1 Change control procedures .	NO	NO
12.5.2 Technical review of applications after operating system changes	NO	NO
12.5.3 Restrictions on changes to software packages.	NO	NO
12.5.4 Information leakage.	YES	NO
12.5.5 Outsourced software development.	NO	NO
12.6 TECHNICAL VULNERABILITY MANAGEMENT .	-	-
12.6.1 Control of technical vulnerabilities	NO	NO
13 INFORMATION SECURITY INCIDENT MANAGEMENT		
13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES	-	-
13.1.1 Reporting information security events.	YES	NO
13.1.2 Reporting security weaknesses	YES	NO
13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS	-	-
13.2.1 Responsibilities and procedures	YES	NO
13.2.2 Learning from information security incidents	YES	NO
13.2.3 Collection of evidence	YES	YES
14 BUSINESS CONTINUITY MANAGEMENT		
14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT .	-	-
14.1.1 Including information security in the business continuity management process.	NO	NO
14.1.2 Business continuity and risk assessment	YES(indirectly)	YES
14.1.3 Developing and implementing continuity plans including information security	NO	NO
14.1.4 Business continuity planning framework.	NO	NO
14.1.5 Testing, maintaining and re-assessing business continuity plans	NO	NO
15 COMPLIANCE		
15.1 COMPLIANCE WITH LEGAL REQUIREMENTS .	-	-
15.1.1 Identification of applicable legislation	NO	NO
15.1.2 Intellectual property rights (IPR) .	NO	NO
15.1.3 Protection of organizational records.	NO	NO
15.1.4 Data protection and privacy of personal information	NO	NO
15.1.5 Prevention of misuse of information processing facilities	NO	NO

15.1.6 Regulation of cryptographic controls .	NO	NO
15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE	-	-
15.2.1 Compliance with security policies and standards	YES	NO
15.2.2 Technical compliance checking.	NO	NO
15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS .	-	-
15.3.1 Information systems audit controls	NO	NO
15.3.2 Protection of information systems audit tools .	YES	NO

From the examination of the ISO 17799 standard with respect to SE and based on the background provided by the research that led to this examination, several areas were identified where additions must be made to the standard. These are presented in the following section.

7.4 Proposed additions to the standard

Through the examination of the ISO 17799 standard from a Social Engineering point of view, it is made evident that although solid guidelines exist that, by design, promote security in general, there is not much direct reference to Social Engineering.

The standard would thus benefit from the inclusion in each security clause of paragraphs presenting a discussion of the individual controls from a SE point of view. Furthermore the standard could include a separate section on Social Engineering that would attempt to address SE issues. This would not necessarily mean that new controls would be defined, although this is quite possible, but even if existing controls are placed within the SE perspective, the standard would benefit.

The section on Social Engineering should address the main SE methods of attack by classifying them in such a way that the SE concept, which is inherently chaotic, may become structured to the extent necessary that the

security personnel as well as all employees of the organisation are able to understand, follow and implement the proposed guidance. Furthermore, issues pertaining to education, training and awareness-building with respect to SE should be laid out.

One way to categorise controls and guidelines might be with respect to the means that the attacker would use to approach a target. Drawing from the classification of attacks as this was presented earlier in this work, three major areas can be defined: a) SE attacks at the physical level, b) SE attacks over the phone and c) SE attacks over email and the Internet.

At the **physical level**, new controls can be created or existing ones put into the correct context for controlling information leakage in physical form, unauthorised entry to the premises and unauthorised access to sensitive areas. Controls for SE attacks **over the phone** should address the different types of targets. One type of target is the organisation's phone operator / information centre. A second one is the IT help desk and a third type is practically any employee with a phone on his/her desk. SE attacks **over email and the Internet**, must be catered for, both at the user and mail server level.

7.4.1 Physical Level attacks

At this level, and in order to eradicate leakage of information in physical form (documents, magnetic media etc) controls must be geared towards the sanitisation and/or safe disposal of material, garbage inspection and garbage removal area monitoring. This should lead to the minimisation of the effects of a "dumpster diving" attack. Furthermore, creation of significant new controls will not be required as controlled disposal of sensitive material and area monitoring are indeed discussed, primarily in sections 9 and 10.7 of the ISO 17799 standard. However, a useful addition to these controls would be the inclusion of procedures catering for garbage inspections for sensitive material that has been improperly disposed of. The controls of section 9 of ISO 17799

regarding security at a physical level can be boosted according to the discussion found in section 5 of Appendix C and in the previous chapter of this dissertation on protection against SE attacks. This should provide for better physical control against SE attacks and allow only properly authorised personnel to enter the secure perimeter of the organisation. Furthermore, if all areas are continuously monitored for possible intrusions and suspect persons are *de facto* challenged by all employees and not just security personnel, even if a Social Engineer does manage to penetrate the secure perimeter, there should be little chance of successfully carrying out his/her mission. Such a measure, however, requires the existence of a particular mentality and culture that is not possible to instill through directives and policies. To achieve this goal, special education is necessary and this comes in support of the idea that SE-related education should also be discussed in the proposed SE section of ISO 17799. Security education apart, all other controls of the proposed SE section that have to do with physical security will in most cases constitute re-phrased, more detailed and augmented versions of controls already existing in the standard. The content of the "new" controls should follow the discussions of the existing controls already presented and appropriate references to the original structure of the standard will be essential for reasons of clarity.

7.4.2 SE attacks over the phone.

Having identified the three main types of targets, namely, a) the organisation's phone operator / information centre, b) the IT help desk and c) any employee with a phone on his/her desk, the following controls could be considered as effective countermeasures for SE attacks.

1) All employees must be made aware of the danger of SE attacks over the phone through security education and awareness plans (refer to " IS education, training and awareness" subsection).
2) The organisation's phone operators at all levels and the operators at the organisation's information centre must not give out any kind of personal

information of employees to anyone that requests it, neither must they divulge personal phone numbers to people making such requests. The requester can simply be forwarded to the person he/she requested or be given the operator's phone number for the requested individual's department.

3) IT department staff and especially those members of the staff that man the IT help center should explicitly be forbidden to honour requests that are received over the phone for the creation of new accounts or the alteration of access rights, even if the requestor is positively identified. All such requests should be placed in writing and follow proper procedure and authorisation.
4) IT department general staff may be approached with technical support requests. All requestors should be immediately re-directed to the IT help desk that handles support requests. Such an approach may be an attempt on the part of the Social Engineer to bypass security procedures by directly contacting IT members of staff who are not as familiar with the security procedures governing a particular request as their help desk colleagues are.
5) IT help desk staff should positively identify a caller before opening a conversation on any matter. This may require a challenge/response system to be in place and callers be requested to give particular digits of a personal code along with some bits of personal information in order to be positively identified by help desk staff. Alternatively, an infrastructure may be designed for the requests to be received by an application running on a dedicated server. Hence, full user authentication will be necessary for any request to be logged. Such an implementation would relieve help desk staff from the responsibility of carrying out caller authentication and furthermore, the requestor would be called back by the help desk staff on his/her designated number as this would appear on the organisation's official phone list. Caller authentication by IT help desk staff will only be necessary when the local caller is not able to use his/her computer or one nearby to log the request or when a remote caller asks for help. Callback

procedures to the designated phone number should be activated in those cases also.

6) IT help desk employees must not disclose the names of users who have logged a technical support request to IT department outsiders. If a Social Engineer somehow obtains this information, he/she may call the employee who logged the request, pretending that he/she is handling the problem and subsequently launch an attack (Mitnick & Simon, 2002, p. 291).
7) All employees should be warned not to follow orders related to their work that are given over the phone, without first positively identifying the person on the other end of the line and also ascertaining that he/she has the authority and sufficient reason to issue that order.
8) Organisation-wide procedures for positively identifying phone callers should be in place and all organisational units handling incoming phone calls should employ them undeviatingly. As this may involve appropriate infrastructure to be made available to employees, only employees having access to this infrastructure will effectively be able to positively identify callers. All other employees should refer callers to those who have the means to positively identify them.
9) All employees should refuse to enter unknown commands on their workstations, divulge any information that could lead to the compromise of their computer account or the accounts of others, or relay sensitive information over the phone, even when their interlocutor has been positively identified.
10) The contents of the company internal telephone directory must be treated as sensitive material and not be made available to the general public in any form (see section 9.1.3 of ISO 17799). Only numbers for general use (central or departmental operator phone numbers) must be made public for contact purposes and the employees covering those positions must have received proper security education and always be alert to the possibility of a SE attack. Dial-in modem numbers for remote-access users must also be treated as secret and not be divulged over the phone under any circumstances. All reference to these numbers must be strictly made

on a substantiated need-to-know basis and formal procedures for the communication of these numbers be followed.

11) All calls to the organisation's telephone operators (central or departmental) must be recorded for security purposes. All calls to the IT help desk must also be recorded.
12) All employees must easily and inconspicuously be able to contact the appropriate security contact person or security incident management group, or otherwise signal that a SE attack is under way so that the suspicious call is immediately monitored and recorded (according to relevant laws and regulations). Furthermore, suspicious calls must be fully documented for reference purposes and further reporting.
13) All employees should deny to participate in telephone surveys as Social Engineers may pose as legitimate researchers and conceal questions critical to the security of the organisation among other, indifferent, questions. All requests for such surveys should be referred to the appropriate public relations department of the organisation and at the same time be treated as a security incident and reported to the security contact person or security incident management group who should follow up on any and every such request.
14) Even if interlocutors have been positively identified, confidential information should not be discussed over unencrypted telephone connections, especially if the conversation is routed over public telecommunication networks, i.e. if it is taking place between the organisation premises and the outside world. Furthermore, the use of voice or data encryption devices makes it more difficult, if not impossible, for a Social Engineer to mount an attack as, in order to communicate with the target, appropriate encryption equipment will be required.
15) All employees must be alerted to the perils of call-forwarding and the vulnerabilities that may be caused by poor call-forwarding policies. Call-forwarding to numbers external to the organisation must be completely disabled. If a Social Engineer at any point has the opportunity to activate such a forwarding function at an unattended phone set, for instance in a

vacant office, then this internal number can be used for a variety of attacks. The attacker can then call an employee and in the course of the conversation ask him/her to call back at the compromised number. The call will be forwarded to the attacker's own number but at the same time the confidence of the victim in the attacker's claims will be boosted as the number will actually be an internal one. Furthermore, the attacker may ask the target to fax sensitive information to the compromised number. Again, as the number is an internal one, the targeted employee will not be alerted to the fact that the information will be sent outside the controlled perimeter of the organisation and thus classified information may leak.

16) All employees must be made aware of the vulnerabilities introduced by the use of voice-mail. If remote access to the mail-box is allowed by the system, one obvious vulnerability will be that of poor choice of voice-mailbox passwords. As voice-mailbox passwords are usually four-digit numbers, they may be guessed. If simple or default passwords such as "0000" or "1111" are used, then an attacker may compromise the mailbox and obtain useful information that may be used in an attack, by either impersonating the owner of the mailbox or the person leaving the message. There is also a second vulnerability that voice-mail may introduce which is not in the hands of the employees to control but should be analysed in the present context. This vulnerability is a purely technical one as many PBX systems allow "Direct Inward System Access" (DISA) through the voice mailbox menu, either as a feature or as a bug of the system. In the National Institute's for Standards and Technology Special Publication 800-24 (2000) titled "PBX Vulnerability Analysis", even the case of DISA as a **feature** of voice mail is considered a vulnerability and needs to be mitigated. The concept behind the DISA functionality is to allow a remote user to dial in to the PBX system from an outside line and gain access to the usual features of the PBX as if he/she is accessing the PBX from an internal extension. Obviously, an attacker who manages to gain DISA through the voice-mail system, may then be able to gain access to many of the PBX's features and set them up to serve his/her purposes.

These purposes can include (but not be limited to) support for a SE attack, information theft that is not restricted to that contained in the compromised mailbox, use of the PBX as a gateway for long distance calls etc. Hence, one approach would be to not allow remote access to the users' mailboxes altogether. Users should be able to retrieve their messages either only from their own telephone set or any other set within the secure perimeter of the organisation. (It goes without saying that the stand-alone DISA feature should also be entirely disabled). A more relaxed alternative would be to allow access to a user's voice mailbox from particular, pre-defined location(s) that are unique to each user. Such locations could be the user's home telephone or the user's mobile telephone set. Even that policy though may be vulnerable to fake caller-ID attacks. The responsibility for making policy decisions on the use or not of voice-mail and DISA lies with the organisation's administration. In any case, as far as the organisation's employees are concerned, voice mail passwords are more important than the average user assumes and should be treated in the same way and protected to the same extent as any other personal password granting its owner access to a system.

17) Employees must not present information on their daily schedule (routine or otherwise) on the greeting message of their voice mailbox. An attacker may use this information to create a believable scenario in order to deceive other employees (Mitnick & Simon, 2002, p. 317).
18) Employees must alert the appropriate security contact person or security incident management group if previously unheard voice-mail messages are not marked as "new" (Mitnick & Simon, 2002, p. 317). This would obviously indicate that another person who has gained access to the mailbox has already listened to the messages. Employees must also proceed to immediately change their voice-mail password unless otherwise instructed by the security personnel if an attempt to identify the attacker is initiated.
19) Employees should not leave personal or sensitive data in other people's voice mailboxes, even within the same PBX, as those mailboxes can be

compromised and the information obtained from them may subsequently be used in a SE attack.

7.4.3 SE attacks over email and the Internet

Email and the Internet offer the attacking Social Engineer an alternative route to approaching the organisation's employees. Sending emails may be used as a standalone method of approach or in conjunction to any other method already described, in an effort to gain credibility in the eyes of the targeted employee. The following controls may help in mitigating the risk associated with Internet and email-related SE attacks.

1) Employees should not send or request sensitive information over the Internet. Internet is an insecure medium and should be treated as such. If privacy measures are taken such as the establishment of a VPN over the Internet, a formal security assessment must be carried out and the network be appropriately classified prior to any sensitive information being transmitted over it.
2) Passwords for access to any part of the organisation's computer system must not be sent over the Internet.
3) Personal Internet mail addresses of employees must be treated as highly confidential and as such must not be made available to the general public on the organisation's web site or otherwise. For contact purposes, generic departmental email addresses must be posted on the organisation's web site or distributed official documentation.
4) Under no circumstances users may install new software packages on their computers or update already existing ones, especially if the package or update has arrived over email. If such an email message is indeed received, it should be considered as fraudulent and/or malicious and be immediately reported to the appropriate security contact person or security incident management group.

5) All incoming mail messages must be centrally scanned for malicious software threats. If such software is detected, the message carrying it should be deleted and the recipient be notified of this action.
6) If the circumstances demand it, the organisation's security policy may dictate that all attachments of incoming email messages are immediately and automatically deleted by the mail server software and the bodies of messages be scanned for http links or self-executing code.
7) The setup of an automatic forwarding rule that relays incoming internal email messages to an external email address is forbidden. Sensitive internal information may be compromised if this rule is not enforced.
8) Employees must not use their passwords for access to the organisation's computer system in any internet-related activity. Internet passwords can be compromised, effectively leading to the possible compromise of the organisation's computer system.
9) Employees should be aware that they may be targeted by attackers who may offer them over email "free" downloads if only they register at a site. Not only should the employees ignore the message according to rules 4 and 8 above, but they should also report the incident to the appropriate security contact person or security incident management group and provide a copy of the message.
10) Employees should not respond to email messages that ask them to re-confirm their login or personal data by logging in at a particular webpage, even if the message appears to come from the organisation's IT department or any other legitimate source. Such an email constitutes a "phishing" attack and should be immediately reported to the appropriate security contact person or security incident management group and a copy of the message provided.
11) Employees should be aware that personal computers with "always on" connections to the Internet are more vulnerable to attacks. They should thus take all precautions against such attacks by switching off their stations or putting them to hibernation when not needed (in either case with the "wake-on-LAN" feature disabled).

12) If the security requirements demand it, it may be necessary to verify email addresses before receiving from or sending mail to them. There exist cases where mail servers block all incoming messages unless an employee has explicitly requested that messages coming from a particular address be allowed to pass through or has sent an outgoing email message to that address. This measure could appear as an overkill to the problem of receiving spam mail, but many organisations, for example those in the US banking sector, have adopted it already.

7.4.4 IS education, training and awareness

Although IS education, training and awareness are discussed in section 8.2.2 of the ISO 17799 standard, special care must be taken insofar SE issues are concerned. The reason for this is that what is described in section 8.2.2 has to do with solid facts that are well documented and is geared towards informing all parties involved on their obligations and responsibilities stemming from that factual documentation. An approach that will be effective in providing education and raising awareness on SE-related issues must be quite different. The notion of SE can not readily be covered in full by mere reference to relevant documentation nor can it be exhausted in any document. Instead, the personnel receiving the training must be exposed to as many facets of the SE problem as possible, in order to form an esoteric understanding of the issues involved and be able to extrapolate and synthesise in situations of attack. It is this author's opinion that employees should not be given access to the organisation's information system if they have not completed a security education course in addition to the required "basic skills" course needed to operate within the bounds of the organisation's information system. Although this may sound as excessively cautious to the administration's ears given that for the sake of efficiency all new employees must become productive from their first day of employment, it is unarguably impossible for an employee to uphold the security of an information system if that employee is unfamiliar with the operation of the system and/or lacks security education. On the other

hand it should not be considered that by exposing an employee to any single security course the problem of upholding security is resolved. Security education must be continuous and the latest updates must be methodically presented to the employees. This is the only way to achieve the raised level of awareness necessary to effectively withstand and deflect SE attacks. Applied psychology could also be used to raise awareness on SE issues along the lines described previously in this work. This can be accomplished by employing direct and indirect means to psychologically "nudge" the employees in the right direction in the fight against SE. Such an approach may include messages at workstation boot-up, circulars, notices etc. Obviously this is one control that should involve a multi-disciplinary approach to bear fruit.

What should not be overlooked in the context of building security awareness and training for security, is the promotion of ethical standards in the workplace. This should be carried out according to the discussion presented in earlier chapters and follows from the reasoning that in a work environment where the ethical level is high, the circumstances are such that the job of the Social Engineer becomes more difficult. Again, for the promotion of ethical standards to be successful, a multi-disciplinary approach is needed.

7.5 Concluding Remarks

It should be clear by the analysis presented here that the issues pertaining to Social Engineering are not directly covered by the guidelines of the ISO/IEC 17799:2005 information security standard. Furthermore, from the study of the standard it can be deduced -in a qualitative way- that no part of it was written with Social Engineering in mind. Hence, the whole standard is not geared towards dealing with Social Engineering in particular. However, the controls and guidelines presented in the standard, deal with a large part of the types of vulnerabilities stemming from Social Engineering in an effective, albeit indirect, way. By providing subsections in the existing clauses where the SE

aspects of individual controls or control groups are discussed along with adding new sections or clauses containing controls that are specific to the SE methods of attack, the standard will surely benefit. Apart from the introduction of new controls, new sections may even include and/or re-phrase existing controls as it is necessary to place new and existing ideas in the context of SE. If the same attention were placed on the most important issue of security training, education and awareness with respect to SE, then the effectiveness of the standard in building defenses against SE will definitely multiply in strength.

It must be noted that not all of the results of the research presented so far can be coded in the form of new or rephrased controls of the ISO/IEC 17799:2005 standard. The reason for this is that the scope of this standard can, obviously, not include the restructure of organisations or the instillation of the correct attitude towards IS. In the same sense, a policy can not suffice in inculcating the proper IS mentality in people. Hence, the enhancements to ISO 17799 that have been proposed must not be viewed as exhaustive and all-encompassing with respect to SE, although they do help towards acquiring a better level of defense against it.

Having identified the shortcomings of the ISO 17799 standard and having proposed enhancements and additions to it to better cater for risks related to SE methods, the next obvious question is how to assess the level of defenses against SE. The next chapter deals with this issue.

8. Proposals on SE-related Measurement Techniques

8.1 Introduction

In previous chapters, the principles of Social Engineering were examined, as were the social aspects of IS. This two-fold study led to the detailed examination of the IEC/ISO 17799:2005 standard from a Social Engineering point of view. One of the initial questions, however, has not yet been addressed: that of devising SE-related measurement techniques. The current chapter deals with this issue. Figure 8.1 depicts the role of this chapter within the overall structure of this dissertation.

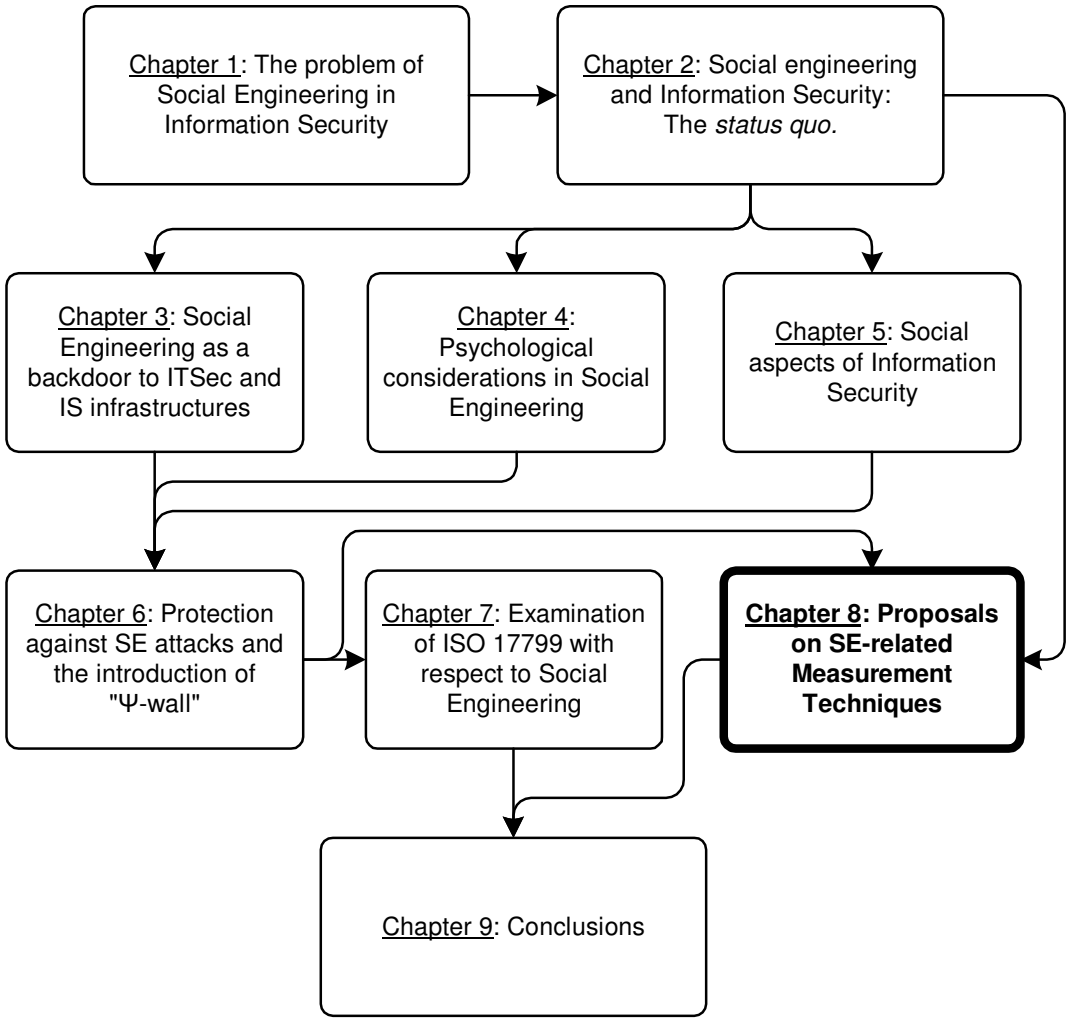

Figure 8.1: Chapter 8 within the context of the overall dissertation structure

The need for metrics related to the Security of Information Systems in general and to the specific aspect of security against SE attacks has already been discussed in earlier chapters of this work.

Given the inherent difficulty of measuring a concept such as Information Security, it becomes much more difficult to produce quantifiable results for an even more obscure aspect of it, namely that which deals with SE.
Despite the degree of difficulty involved, the quantification of the SE aspect of Information Security is essential for the continual re-assessment of any implemented security policy and a most valuable guide in pinpointing problem issues in the defense against SE and in addressing them.

The reason this chapter deals solely with measurement techniques that are related to SE is because in all the IS literature investigated, the SE aspect of IS is inadequately dealt with and material on SE-related measurement is virtually existent, although Information Technology security metrics discussions are becoming more frequent.

Following the analysis that has been presented in the previous chapters regarding SE, this work would be incomplete if an attempt were not made to bring forward the basic principles for SE-specific metrics. This chapter is not meant to exhaustively address the issues pertaining to devising metrics for the performance of security controls against SE threats but hopefully provides a well-laid foundation to build upon in future research.

8.2 Principles of metrics

Prior to examining how SE-specific metrics can be obtained, a brief discussion of the defining qualities of the term "Metrics" is included:

- Metrics must be viewed as tools and yardsticks in the effort to improve an organisation's posture with respect to the examined concept, in our case the efficiency of the organisation's defenses against SE.

- SE-related metrics should address the qualities for the attainment of the set goals and objectives, namely efficient defenses against SE threats.
- Metrics must provide quantified data for the effectiveness of the implementation of controls by assessing the degree to which the goals and objectives for efficient defense against SE threats have been attained.

The very nature of SE threats is a source of major complications when it comes to obtaining the desired metrics. As such, it does not appear possible to obtain a straight-forward and exact metric of security against SE threats. It would thus be more appropriate to try to obtain a measure of the "Assurance" present in a system. "Assurance" is thoroughly discussed by Vaughn et al (2003) who define it as "*an expression of confidence that one has in the strength of mechanisms or Countermeasures*". Assurance is also examined by Jelen and Williams (1998) according to whom assurance is defined as "*the degree of confidence that security needs are satisfied*". Although the two definitions appear to be quite close, there is a subtle difference between them as one is directed towards assessing the quality of the implementation of controls, while the other is directed towards the expected effect of those controls against threats. The two definitions thus have a "cause and effect" relation among them. This relation highlights the fact that although it seems as a small logical step to move from the implementation of controls to the effective mitigation of risk, this may not necessarily be that simple. Thus this gap has to be closely analysed.

Hence, in order to obtain an assurance estimate, the definition of assurance should encompass both of the above notions. Assurance is thus defined in the context of this dissertation as "an expression of confidence that one has in the strength of implemented controls and that security needs are indeed satisfied". In order to obtain the level of assurance with respect to SE, data must be gathered and quantified from a variety of sources that call for different measurement / assessment methods. Furthermore, the results

obtained from various sources must be combined in such a way that an overall result on the level of assurance is extracted.

8.3 Directly measurable aspects of the defense against SE

Some aspects of the defense against SE can be readily measured and, in the worst case, a rough assessment can be provided. (The reader must not forget that it is only the SE aspect of security that is being dealt with here, under the assumption that the original controls of ISO/IEC 17799:2005 are in place as is an ISMS according to the directives of ISO/IEC 27001:2005). An example of a directly measurable aspect of the defense against SE is the level of compliance with the security requirements as these are set forth in the IS policy document. For other aspects of the defense against SE, indirect methods must be employed in order to obtain meaningful results.

The directly "measurable" elements of the defense against SE can be obtained from the assessment of the controls of ISO/IEC 17799:2005 standard presented in the previous chapter, as these were enhanced with respect to SE. By quantifying the level of implementation of the proposed security controls in an organisation, a raw metric can be obtained for single controls or groups of controls. By combining all of the obtained metrics, an aggregate figure can be obtained -perhaps in the form of a percentage- that will give an indication of the status of the security infrastructure of the organisation regarding SE. The reason that this will provide only an indication of the status of the security infrastructure and not an assessment of the degree of satisfaction of the security need against SE threats is due to the vague nature of the concept that is being dealt with. This statement may become clearer with an example. Consider the vulnerability related to hard disk "Mean Time Between Failures" figure (or MTBF): if a control involving backups and related procedures is implemented, then the risk stemming from the actual fact that hard disks do fail eventually, is effectively mitigated. This is a case where an exact metric on a technical control can be obtained and have a value on its own accord as it does give an assessment on the degree to which the goal of protecting the organisation against hard disk failure is

attained. If, on the other hand, the vulnerability of an unauthorised person inside the secure perimeter of the organisation is considered, one of the proposed controls of the previous chapter was to have specially coloured badges worn by visitors so that people not bearing such a badge are immediately challenged by the organisation's employees. The fact that the control is in place has no conceivable way of forcing the organisation's employees to actually challenge individuals who do not carry a badge, thus effectively and definitely mitigating the risk. However, the control *is* in place and this does have to account for something. As long as the control is implemented, a valid metric can and should be obtained. This metric though can not yield conclusive results with respect to the ultimate goal of security need satisfaction with respect to SE, as other conditions must co-exist for the control to be effective. This highlights the qualitative difference between the two examples presented above: in the first case, a technical control (backup technology and procedures) is sufficient to mitigate the risk from a technical vulnerability (hardware failure) and this is quite straightforward in assessing. In the second case, the vulnerability is definitely not technical and has mainly to do with the interaction between humans. Hence, the technical control (issue of specially-coloured badges) must function alongside a non-technical control (the will of an employee to challenge suspicious persons) in order for effective mitigation of the risk involved to take place. This reasoning brings forth the idea that the quantification and measurement of controls against SE only constitute a single component in the formula that will eventually yield the final assessment of the organisation's posture with respect to SE.

However, before moving on to the other components it is necessary to examine the ways that the level of implementation of the proposed security controls against SE can be quantified.

The U.S. National Institute of Standards and Technology in NIST Special Publication 800-55 (2003, section 4.1) presents a procedure for obtaining metrics results using a “Metric Detail Form” for each critical control or group of

controls in the examined context. Although this measurement method is primarily used to address the existing, stable information security processes, the authors state that even measurements attempted on non-existent or unstable information security processes will help pinpoint information security areas that require improvement by returning poor metrics' results. Furthermore, the use of a weighting scale to differentiate the importance of selected metrics in the context of the overall security program is also discussed. Weighting is considered essential in ascertaining that the obtained results accurately reflect the existing security program priorities.

To illustrate the use of Metric Detail Forms, a sample security metric from NIST Special Publication 800-55 (2003, app. A) is reproduced below. This sample metric detail form refers to the "Incident Response Capability" of an organisation and through minimal adaptation could be used in the context of ISO/IEC 17799:2005.

Table 8.1: Sample Metric Detail Form for Incident Response Capability (from NIST sp800-55, 2003, App. A)

A.14 Incident Response Capability	
Critical Element	*14.1 Is there a capability to provide help to users when a security incident occurs in the system?*
Subordinate Question	*14.1.1 Is a formal incident response capability available ?*
Metric	*Percentage of agency components with incident handling and response capability*
Purpose	*To ensure that there is an agency wide incident response capability*
Implementation Evidence	*1. Does your agency component maintain an incident response capability?* *? Yes ? No* *2. If the answer to Question 1 is no, why not?* *? Did not know of requirement ? Lack of resources?*

	Competing priorities *3. Is there a formal process and/or documented incident handling guide that defines "incidents" and describes how to report an incident internally?* *? Yes ? No* *4. Are incidents monitored and tracked until resolved?* *? Yes ? No* *5. Are personnel trained to recognize and handle incidents?* *? Yes ? No* *6. Are alerts and advisories received and responded to?* *? Yes ? No* *7. Number of incidents reported from your agency component during reporting period_____*
Frequency	*Semi-annually*
Formula	*Number of agency components that have incident response capability (tally answers to Question 1 from all components) / Total number of components*
Data Source	*ISSO; NIST SP 800-26 (particularly Items 14.1 and 14.1.1)*
Indicators	*The goal for this metric is 100 percent; an upward trend is necessary to show progress and the continued strength of the IT security program. The ability to report and handle incidents is critical to maintaining an adequate security posture.*
Comments:	*Question 2 is a causation question that indicates why an agency component's incident response capability may be inadequate. If the answer to Question 2 is "Did not know of requirement," it may be necessary to investigate whether a policy is in place requiring an incident response capability, or if guidance is necessary. Other corrective actions will be required if the answer to Question 2 was "Lack of resources" or "Competing priorities."*

	Questions 3 through 6 validate that the essential components of an incident response capability are in place and to what degree. For example, if a guide exists but no training is provided to enable personnel to recognize and report incidents, the capability would not be considered robust. The lack of an element in Questions 3 through 6 indicates weakness in the incident response capability that must be addressed to increase functionality and effectiveness. Question 7 is another validation question. It is unlikely that there will be no incidents reported from an agency component. This number can be compared with agency wide incident reports and correlated with items that would have affected the agency component, to determine whether reporting is occurring as necessary.

Following this example, Metric Detail Forms can be created for any and all of the implemented controls. A critical assumption, though, is that a security policy is in place and general IS controls (the ones prescribed in ISO 17799) have already been implemented. Using that as a starting point, the assessment of the controls specific to SE can begin by creating Metric Detail Forms for the controls prescribed in a SE-enhanced version of ISO 17799. Each of the individual SE-related controls -and even guidelines- discussed in the previous chapter can be examined and relevant, accurate metrics obtained for their implementation. It must be noted that provisions should be made to take into account the interdependencies of controls, as lack of a specific control may render the metrics for other, dependent controls nullified. An (extreme) example of such a situation would be to have users report potential security breaches to appropriate persons serving as a security incident reporting contact points for the departments, but not having the necessary procedures in place for efficient coordination of the departmental contact points and organisation-wide response. Thus, the value of the implemented control of "users reporting to security incident contact person"

would be nullified as the value for the control of "security incident reporting and co-ordination centre" would be very low or zero.

Thus, although results for individual controls can be used to identify the strengths and weaknesses of the defense against SE, a final, aggregate result showing the level of implementation of the controls and guidelines against SE should be based on a weighted average of the results for the individual controls that takes into account control interdependencies. This result, combined with the ones described further on, will eventually lead to the overall assessment of the assurance of the system with respect to SE.

8.4 Operationalisation of the effectiveness of the Ψ-wall.

It was argued in previous chapters that the most effective defense against SE would be decidedly psychological and the notion of building a line of defense based on psychology, dubbed the "Ψ-wall", was presented in a previous chapter. Hence the effort to obtain metrics' results on the assurance of the system with respect to SE is naturally directed to the component qualities of the Ψ-wall as the non-technical, indirect controls against SE stem from it.

In order to obtain metrics for a concept such as Social Engineering, one has to borrow measurement methods from Social Science research. Abstract sociological concepts such as crime can be made measurable in social sciences' terms through the process of "operationalisation". According to Collins et al. (2000, p.68), "operationalisation" is "*the process of transforming a theoretical concept into an empirical variable*", (i.e. making the concept in question, measurable). In principle, crime based on or enhanced by attacks based on Social Engineering methods is difficult to operationalise. Consequently, measuring the effectiveness of a set of psychological countermeasures designed to block SE attacks is even more difficult than operationalising the crime based on the attacks itself. This is because apart from the complexity inherent to the Social Engineering-aided crime, one has

to also take into account the non-descriptive nature of those countermeasures or controls against SE that are based on psychological techniques.

In short, how can the effect of security education on the employees of an organisation be assessed? Surely, this can not be done by an old-school examination process at the end of the training schedule. Furthermore, how can the psychological effect of an awareness campaign on individuals be measured? How can an external observer be sure that the employees of an organisation have internalised the guidance promoting ethical practices in the workplace? Most importantly, how can the actual effect of this psychology-laden process against the potential Social Engineering attack be measured? All of the above observations, and possibly many more, ultimately help in distinguishing all the different aspects of the concept of effective defense against SE. To operationalise a concept, ideally, one must identify all of its measurable dimensions. These dimensions are also known as indicators where an indicator is defined as "an observable measure" by Collins et al. (2000, p.68).

The multi-disciplinary nature of the effort against SE is exhibited once again as it would be most appropriate to ask for the help of a psychology expert who should identify the indicators for the above, multi-part question. However, the author, going out on a limb, believes that some indicators may be readily available.

8.4.1 Effectiveness of security education

As far as the effect of education on security is concerned, the following method should yield an "observable measure" in relative terms:

(It should be noted that security education must not be strictly limited to Information Security as the controls necessary for SE exceed the scope of IS). Assuming, for illustration purposes, that the security education course deals with the subject of "secure practices in the workplace", first of all, a

baseline measurement must be taken at a point in time before the actual education takes place. This measurement can employ various methods, all of which can be carried out internally without the involvement of parties external to the organisation, e.g. external auditors. A (non-exhaustive) list of aspects examined could be:

- Through observation, figures should be obtained for:
  - the percentage of employees who do not abide to physical security practices.
  - the percentage of employees not following a clean-desk practice when they leave their office.
  - the percentage of computer users who keep notes with computer account login information, such as passwords, in insecure and even obvious locations.
  - the percentage of computer users who have login information permanently stored on workstations that allow this.
- Through the use of password strength assessment software the percentage of users who use weak passwords should be identified.
- Through an email message simulating a phishing attack, users should be asked for their user names and passwords, using an excuse such as "re-confirmation of user accounts". A figure should be obtained for the percentage of employees who would unreservedly relinquish their login information.

Obviously, the list can be very long, but these examples suffice in showing the general principle behind obtaining a baseline measurement.

The education and training on security in general and information security in particular can then take place, obviously addressing (among other things) the issues described above.

After the education and training courses are concluded, results on the same aspects as before should be obtained and compared to the original ones. In this fashion, a measurement on the effectiveness of the education will be

established, thus providing one of the sought-after indicators for effective operationalisation.

There are a few points worth noting:

a) The employees that took part in the security education program can be asked (by questionnaire or otherwise) to give their opinion about the value of the education they received. This will help in better assessing the effective level of internalisation of the points made in the course of the education.

b) The results obtained from the measurements before and after the education took place, both have intrinsic values and can definitely be used on their own. Their comparison gives a further measure for the effectiveness of the education.

c) A type of measurement such as the one described above should be considered as an integral part of the education process. There is little point in having security education that is neither assessed nor improved over time to cater for the changing security needs.

d) The fact that education took place, combined with the number of the organisation employees who attended it, is a directly measurable control and should be reflected in the measurement of directly measurable aspects of the defense against SE, previously discussed.

8.4.2 Effectiveness of the security awareness program.

A program designed to increase the security awareness of employees is much subtler than straightforward security education. To all intents and purposes, security education can form only a part of a security awareness program. Security-related messages on notice boards, circulars, welcome screens of computer systems etc, all help in building security awareness in general and with respect to SE in particular. An awareness program is not as

time-specific as a security education course. A security education course has its beginning and end strictly defined in time. The effect that a security education course has on the people that follow it is maximised close to its end. Thus, the long-term effect of the security education course will die out if it is not regularly refreshed and boosted. This is where security awareness programs play a most significant role by constituting the core part of a continual process, the sole aim of which is keeping the teachings of the security education course alive in peoples' minds. Despite the principal differences of security education and security awareness, the results of security awareness can be assessed over time in a similar way as those of security education previously described:

At any given point in time a baseline measurement can be obtained giving an indication of the current level of security awareness in the organisation. The number of aspects covered in the measurement can be increased to include those especially targeted by the security awareness program. Comparative results can yield the measure of success of the awareness program as time progresses and thus an effective indicator for the operationalisation of the effectiveness of the Ψ-wall with respect to SE. Absolute results can also be used as stand-alone metrics on the average level of the security awareness of employees. Another observable measure or indicator can be obtained by establishing what is perceived in theory as a SE threat by the average user in the course of time, assuming that a security awareness program on SE is actively pursued. Such data could be extracted by appropriate questionnaires and/or carefully orchestrated surveys that would be nothing short of full-fledged psychology experiments carried out with the users as subjects.
Yet another indicator could be obtained if the user is presented with multiple scenarios that are known to the user to be SE attacks and is subsequently asked to assign to each one of those a mark corresponding to the gravity of the attack. Interesting deductions can be made if the average user underestimates or grossly overestimates the severity of the attack. It might be

the case that the awareness program will have to be re-assessed and re-formulated in order to address security issues on a more realistic basis.
In parallel to the qualitative deductions regarding the effectiveness of the awareness program, the proposed process will yield the indicators initially required. These indicators will in turn lead to the quantitative assessment of the awareness program's effectiveness with respect to SE, effectively converting this defining quality into a measurable quantity.

8.4.3 Measuring the effects of the psychological process

As far as the question regarding the actual effect of the psychological processes employed against Social Engineering attacks is concerned, the following could function as indicators:

a) Assuming that a security incident reporting and coordination centre has been established and is fully functional according to the provisions of ISO 17799, the percentage of increase in alarms raised against real (not artificially created) Social Engineering attacks after the dispensation of security education courses and as the security awareness campaign progresses, can form a viable indicator. An issue that must be addressed regarding this indicator is that an increase in alarms may result from two distinct conditions. Such an increase may either be caused by the raised awareness of employees who actually perceive SE attacks for what they really are in a way that was not possible before, or by an increased number of attacks that is irrelevant to the education and awareness programs. Additionally, nothing prevents both conditions to occur simultaneously. In order to normalise the results reported by the security incident reporting and coordination centre over time, further observations are necessary.

b) By carrying out penetration testing centred on SE attacks, three immediate benefits may be gained. First, from the number of reports arriving at the security incident reporting and coordination centre in direct relation to the

controlled SE attack, the values obtained in (a) above can be normalised. Second, in absolute terms, the percentage of successful attacks that go unreported in the context of penetration testing will yield another indicator of the effectiveness of the defenses against SE. Third, if the results of the penetration testing are classified according to different types of attacks with different types of goals and targets (some serious, some superficial and many variations in between) the weaker areas of the defense line will be pinpointed.

c) A "post mortem" indicator of successful SE attacks can be obtained from the percentile change of breaches identified after a successful attack has been carried out. For the validity of the result to be ensured, the attack itself should be a straightforward Social Engineering one, or be fairly surely linked to a preceding true Social Engineering attack. (Such a case would be, for example, the penetration into a system using a valid password that had been previously extracted from an authorised user who failed to identify the Social Engineering attack against him/her and thus did not raise an alarm). The obtained result only has to do with those attacks that were successful and were discovered at a later time. As far as the successful attacks that were not discovered are concerned, there is nothing to be said or done as is usually the case with "perfect crimes".

The above indicators effectively lead to the operationalisation of the concepts related to the Ψ-wall. It is by no means claimed that the list of indicators is exhaustive. The interested reader is welcome to suggest additional indicators and methods for obtaining them that will make the operationalisation in question more accurate.

8.5 Presentation of the results

Combining the indicators relevant to the Ψ-wall with the results obtained for the directly measurable aspects of the defense against SE should lead to the establishment of the level of assurance in the system with respect to SE. It is

interesting to note the disparate nature of the results. As a first observation, the results can not be combined in the form of a weighted average. Such an average can not be used in any productive manner and can even be misleading if attempted. There is no useable information in the statement "our system has a 57% assurance with respect to SE". Furthermore, the weight coefficients that have to be used in order to obtain the final result will have to be arbitrary as neither an objective relation between the indicators nor between an indicator and the final assurance value expressed as a percentage, can be established. As a second observation, no indicator may yield useable information on the level of assurance in the system with respect to SE on its own.

To illustrate this point, consider being given just the result (as a percentage) of the level of implementation of controls against SE. This would be inadequate on its own to give an idea about the assurance level with respect to SE. The figure would yield a measure of the theoretical compliance to the security requirements and directives but would lose its meaning in the context of assurance if, for example, the level of security awareness among the organisation's employees is so low that security breaches can not be avoided.
On the other hand, results related to incident reporting would be out of place if the level of implementation of ISO/IEC 17799:2005 controls (general and/or SE-specific) were not furnished. For example, an absolute value for the number of incidents being reported to a co-ordination centre would not mean much if not accompanied by information on the level of implementation of incident-reporting procedures throughout the organisation's structure.
Furthermore, absolute numbers on security education (such as number of participants or education man-hours) would mean very little if not supported by penetration-testing results or actual attack results that help in the assessment of the actual effects of security education.

A way will thus have to be devised to present the results in a form that both retains the values of the individual indicators as well as provides an overview

of their combined values, ultimately offering an indication of the level of assurance in the system with respect to SE.

Ideal to this type of data is the spider chart representation. A spider chart is a specialized type of chart that represents data on a series of radians starting at a single point at the centre of the graph. Each radian forms an axis for each attribute (or quantitative variable) measured. An attribute can be an indicator or a value resulting from a grouping of indicators (if the particular indicators can be grouped). The actual value marked on the radian is the distance from the center of the graph. Spider charts are typically employed to show, in a graphical way, the values of various -and frequently unrelated- organizational performance areas. In our case, the performance areas are related to the assurance of the system with respect to SE. The strong point of the spider chart is that important categories of performance are graphically displayed on the same chart, thus providing a useful overview of performance. A measure of the assurance of the system with respect to SE can thus be obtained by looking at the area covered by the spider web. Furthermore, the examiner can easily visualise concentrations of strengths and weaknesses and subsequently dictate corrective action.

To illustrate the use of a spider chart in this context, let us assume that three subsequent measurements with respect to SE have been taken, separated by six-month periods. The resulting data is then plotted on the spider chart of figure 8.2:

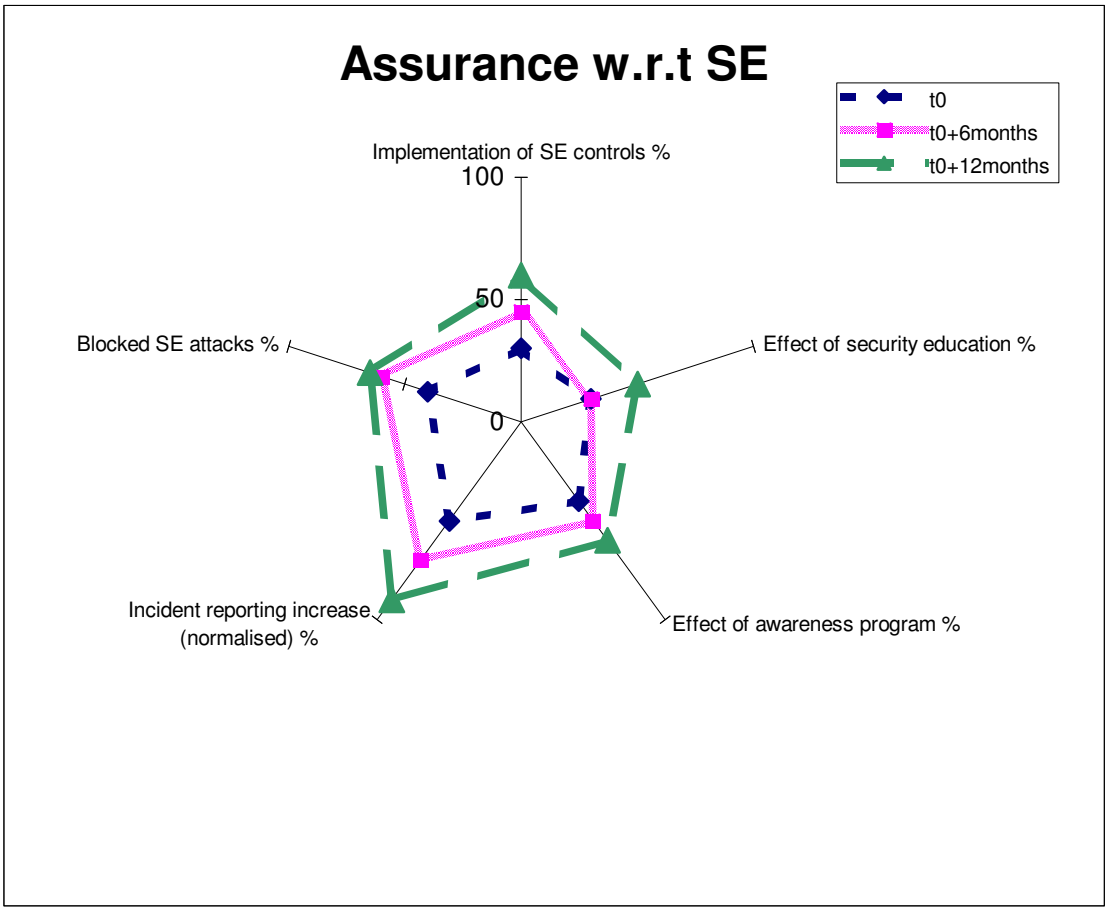

Figure 8.2: Example of organisation assurance over the course of a year

If assurance is represented by the area defined by each line, then the first obvious result is that as time progresses, the assurance rises. Secondary deductions may be that:

a) the security education did not pay off during the first six months,
b) the awareness program did have a uniformly increasing effect over the first year,
c) as more controls get implemented and the effects of security education and awareness increase, so does the incident reporting and the percentage of blocked SE attacks.
d) as the percentile change of incident reporting increases but at the same time the increase in blocked SE attacks does not follow the same rate, this indicates that the number of successful SE attacks in absolute terms was on the rise during the second half of the year.

By comparing charts of the assurance in, e.g. different departments, at the same point in time, weaknesses and strong points can be obtained. Such a spider chart appears on figure 8.3:

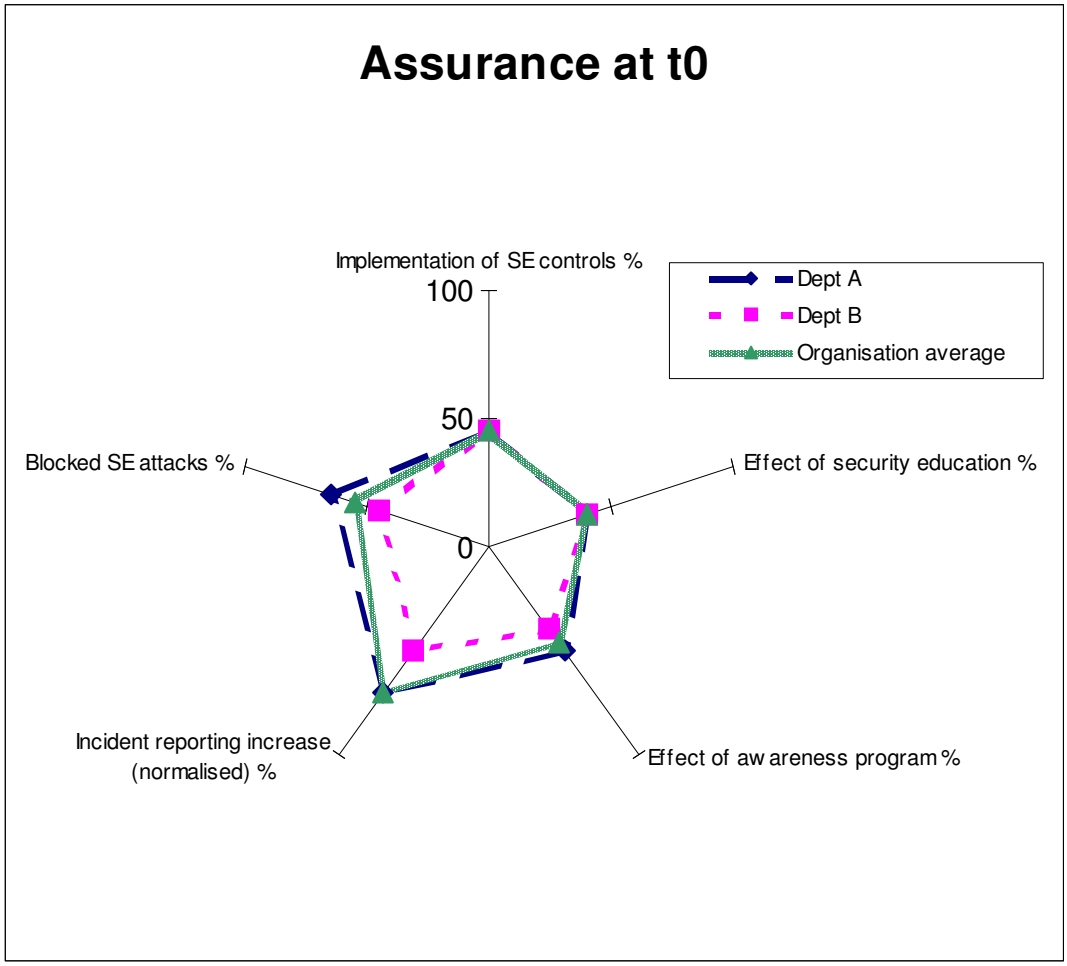

Figure 8.3: Example of departmental assurance at a given time.

In this case, although both departments are assumed to be following the same security policy and the level of implementation of controls is indeed the same, Department B exhibits a clearly lower level of assurance with respect to SE. Furthermore, the employees of Department B seem less capable of identifying SE attacks and thus the overall defense capability is less than what it is for Department A. The deviation from the organisation average is not much for Department A while Department B is definitely lagging behind the rest of the organisation. Such a deviation must be investigated and rectified.

Perhaps this hysteresis is due to a common trait shared among the employees of Department B. Otherwise it may be attributed to poor response on the part of the departmental contact person for security incident reporting. Poor management of the department may also lead to such a situation with the levels of self-esteem and motivation for work of the employees running low at the particular department.

Through the presentation of the above examples, it is hoped that the need for and the advantages of such a measurement approach have been clearly demonstrated. Apart from the assessment of the level of assurance in the organisation with respect to SE, this measurement technique can help in an efficient implementation of the Plan-Do-Check-Act (PDCA) cycle that lies at the foundation of every ISMS implementation. Furthermore, the measurement system itself must have a feedback loop in place if it is to be controlled and adapted to the ever-growing security needs of the organisation. The proposed measurement system does not have to be limited to the SE aspect of security. It can be expanded to encompass all aspects of information security and thus provide an assessment for the assurance of the system with respect to security in general.

8.6 Concluding Remarks

The need for obtaining metrics related to the aspect of security against SE attacks can be satisfied by examining the level of the Assurance of the system with respect to SE. A measure of the assurance with respect to SE can be obtained in the form of a Spider chart where the values of assurance-related performance variables are plotted. By providing a graphic display of these variables that can not be otherwise combined to yield a single numeric result, a useful overview of performance regarding the security against SE is provided. A measure of the assurance of the system with respect to SE can be obtained by examining the area covered by the spider web.

9. Conclusions

In this final chapter, an overview of the achievements and shortcomings of this research are presented and possible directions for future research are highlighted. Figure 9.1 shows the relative position of the current chapter in the context of this dissertation.

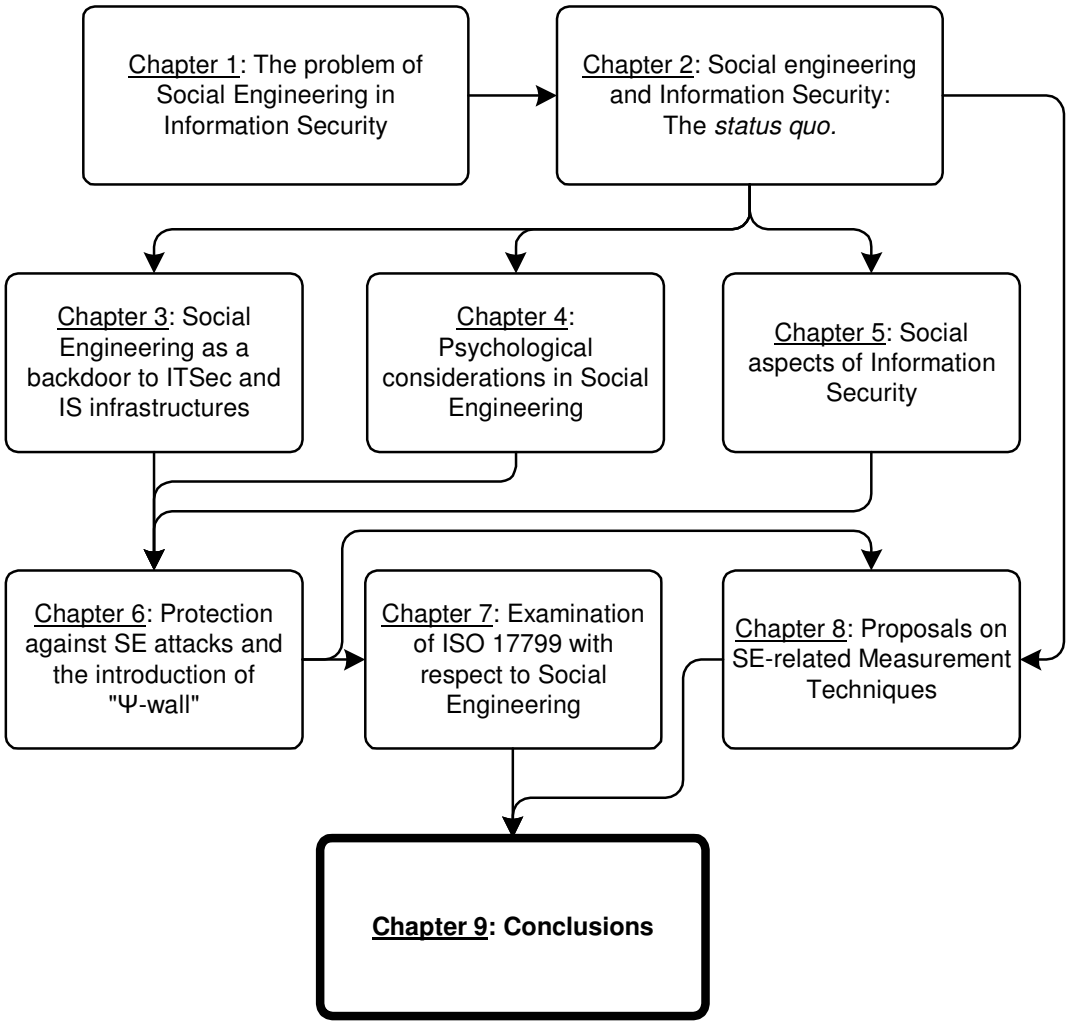

Figure 9.1: Chapter 9 within the context of the overall dissertation structure

The term "Social Engineering" is made out of two words: "Social" and "Engineering". Although this deduction will not win any linguistic prises, by separating its two elements the real value of the term is brought to light. Social Engineering methods can not be successful without the social interaction of humans. As humans are social beings, social interaction between them is unavoidable. For a human being to be 100% insusceptible to

the ways of the Social Engineer that individual should be locked in a dungeon and the key be thrown away. This is comparable to the ultimately secure computer that must be without power and buried under a few metric tons of cement. The "Engineering" element is used in a way that it rather means "manipulation" but at a higher level than usual. This means that the way the Social Engineer approaches a victim resembles an engineering problem. "Engineering" is also used to denote that no problem can remain unsolved if attacked systematically and through the use of a well-founded methodology. By combining all of the above, Social Engineering is nothing more than a discipline that systematically approaches the question of how to manipulate humans and use that manipulation as the means to a goal.

The obvious next question thus becomes: "How can we make sure that our Information Security defenses can withstand the bombardment of Social Engineering?

When the subject of this research was conceived, the obvious first objective was to bring a generally accepted Information Security (IS) standard and the nebulous concept of Social Engineering (SE) together and assess the effectiveness of the former against the latter.

The two-fold research objective thus immediately became:

a) to investigate the effect that attacks of the SE type could have on the existing provisions of IS standards and practices and

b) to devise extra controls for inclusion into standards and practices in order to guard efficiently against SE attacks.

Due to the multitude of available IS standards and practices, a decision was made to chose one representative standard of general acceptance in order to delimit the area of research. A justified decision was thus made to examine the ISO/IEC 17799:2005 standard (ISO/IEC, 2000a) in this context.

In order to address the research questions, it was obviously essential to gather as much information on SE as possible. The first step was to identify the very nature of SE. Almost by definition, SE is difficult to identify as it functions as an "umbrella" concept for any methodology conceivable that takes advantage of one's psychological profile, behaviour or character by exploiting those imperceptible flaws that are inherent to the nature of the human psyche. Thus, from the very early stages of this research, it became evident that in order to obtain valid results, the research would have to systematically address a variety of parameters some of which expanded beyond the strict scope of the Computer Science and Information Systems disciplines. The problem was thus identified as being philosophical in nature to a large extent. If an effective solution to this problem were to be presented, it had to be the outcome of a multi-disciplinary process.

This gave rise to a number of "companion" research subjects the results of which had to precede the main, two-fold research question.

The **first** such subject was **the methodology of SE attacks.** This was studied, analysed and categorised. The four main categories of SE attacks were found to be: physical attacks at the workplace, attacks over the telephone and Internet attacks (all of which require some kind of direct or indirect contact with the targeted employee) and dumpster diving (which does not require contact with employees). During this study, there were also other aspects of SE methodology that were identified and play significant albeit lesser roles in the context of the research.

As research on the methodology of SE progressed, it was made evident that Social Engineers target the human element of Information Systems by using psychological manipulation methodology. Hence, that subject had to be studied also -always in context- if effective assessment of the ISO/IEC 17799:2005 standard with respect to SE were to be made possible.

Hence, the **Psychological Considerations in SE** became the **second** companion subject for research. Through this research the psychology of SE attacks was analysed and the tactics and techniques of Persuasion, Influence and Exploitation of attitudes and beliefs were identified. This provides the basis for IS awareness, education and training plans that will raise the effectiveness of the IS policy against SE attacks.

In the course of the study of psychological considerations for SE, another major issue that heavily affects IS became apparent. That issue had to do with social aspects in the context of IS in general and Information Security Management Systems (ISMS) in particular. It was then realised that an ISMS is a textbook example of a social construct, with all the complications that this involves and -luckily- with all the standard tools that Sociology provides, available for analysis.

The **third** area of prerequisite research was thus focused on the **Social Aspects of IS**. A sociological analysis of IS and the ISMS was carried out. This study on the one hand gave answers to many of the problematic issues that reduce the effectiveness of IS policies and implementations, while on the other it highlighted issues that could be the source of serious but covert problems in upholding IS.

What the study of the Social Aspects of IS also accomplishes is that it lays the foundation for analysing the social character of IS. It provides the means to identify "socially-induced" vulnerabilities and may even help in establishing controls for them. It was demonstrated that the social construct lying at the foundation of any ISMS (in terms of IS hierarchy, individual perceptions and interpersonal relations) severely affects the design, functionality and efficiency of the security policy. As soon as the security policy is in place though, it, too, affects and transforms the dynamic relationships within the social construct of the ISMS. This bi-directional relation between two concepts that function reciprocally as cause and effect can be explosive if left unchecked. Care

should thus be taken for feedback mechanisms to exist in order to ultimately reach an equilibrium point of maximised security efficiency.

Armed with this knowledge, an attempt was made **to devise a protection scheme against SE** that is based heavily on psychological techniques to strengthen the resistance of IS Standards and policies to SE attacks. This became the **fourth** companion research subject. It quickly became evident that to successfully defend an organisation against such attacks, a significant investment must be made on the organisation's human resources through IS awareness and psychological training programs. By exposing employees to SE methodology in a controlled fashion, the most effective defenses -those of a psychological type- can be built against the real danger of SE.

Having laid the necessary foundation by providing a broad overview of Social Engineering, **the main two-fold research question was addressed**. First, an assessment of the degree in which the security clauses and individual controls specified in the ISO/IEC 17799:2005 standard may be affected by SE threats was undertaken. The following three outcomes were obtained upon its completion:

a) It was found that although the set of controls presented in ISO/IEC 17799:2005 is very comprehensive and effective, it was not written with SE in mind.

b) It was deduced that although the controls presented in ISO/IEC 17799:2005 do have the indirect effect of raising the level of security with respect to SE threats, there is still room for improvement and "tuning" of the standard with respect to SE.

c) Through the discussion of the ISO/IEC 17799:2005 controls with respect to their susceptibility to SE threats, the weaker areas of the standard, in this context, were identified.

The third outcome provides the necessary information for the **second part of the main research question** that has to do with the re-design of the standard's controls and/or the introduction of new ones for better protection against SE.

The identified weaker areas of the standard with respect to SE were:

a) physical security where more technical controls need to be introduced to counterbalance the psychological hysteresis of individuals that Social Engineers prey upon,

b) security against SE attacks over the telephone which remains largely untouched in the current version of the standard,

c) security against SE attacks over the Internet and email that needs to be strengthened under the light of emerging SE attacks and most importantly

d) the need for IS training and education related to SE, the promotion of ethical standards in the workplace and IS awareness building (especially where SE is concerned).

With the above points in mind, through a detailed examination of the ISO/IEC 17799:2005 standard, either new controls were devised or the "tuning" of existing controls was proposed so that SE issues are better addressed.

It was also understood beyond doubt that there are many issues of sociological nature that by definition impede the efficiency of any ISMS, such as the vertical nature of hierarchical structures and the struggle for power and status within them. These issues lay clearly outside the scope or context of any IS policy and can not be addressed by any IS standard.

Thus, the "formal analysis of impediments of a sociological nature to IS" may form a prime area for further, interdisciplinary research.

Having identified the core components of the transformation necessary for the ISO/IEC 17799:2005 standard to become better equipped to deal with Social Engineering as well as the limitations of that transformation, it was further considered essential to tackle the issue of measurement of IS with respect to SE. The need for metrics related to the Security of Information Systems in general and to the specific aspect of IS against SE attacks in particular, had been evident since the early stages of this research and is quite important for the fruition of the Plan-Do-Check-Act (PDCA) cycle promoted by the ISO/IEC 27001:2005 standard (ISO/IEC, 2005b). However, given the inherent difficulty of measuring a concept such as Information Security, the task of producing quantifiable results for the Social Engineering aspect of it, seemed daunting at best. It was thus decided to address the level of the **Assurance** of the system with respect to Social Engineering. This eventually led to the formation of the **fifth** companion subject of the main research, that of **SE-related measurement techniques**. Spider charts were employed in an attempt to provide a measure of the assurance with respect to SE. According to this scheme, the values of assurance-related performance variables that can not be otherwise combined to yield a single numeric result are plotted on a spider chart. By providing a graphic display of these variables, a useful overview of performance regarding the security against SE is indeed provided. A measure of the assurance of the system with respect to Social Engineering can thus be obtained by examining the area covered by the spider web. Although the chapter on SE-related metrics is still far from being truly self-sufficient, it does provide firm ground upon which to further build.

Hence, more accurate quantification of SE issues could constitute yet another area of future research.

The provided analysis of the ISO/IEC 17799:2005 standard can also function as a starting point for further work on the assessment with respect to SE of ISMSs that are based on the ISO/IEC 27001:2005 standard.

This work could be of assistance to all involved in designing for IS based on the ISO/IEC 17799:2005 standard, by providing enough insight on how vulnerable systems may be from SE threats. The residual risk due to SE even after the application of the ISO 17799 controls may be quite higher than expected if Social Engineering vulnerabilities are not accounted for and effectively mitigated. Hopefully, this work will result in raising the level of alertness and diminishing the false sense of security that the application of the particular standard may have instilled.

Moreover, this work could provide the basis of a future revision of ISO/IEC 17799:2005 (and even of ISO/IEC 27001:2005) that would cater more effectively for those aspects of Information Security that are related to Social Engineering.

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]

APPRIVER, 2005. *Home page* [online]. Available from URL: http://www.appriver.com [Last access on Feb 10, 2007]

BARCLAYS. 2006. *Telephone Banking* [online]. Available from URL: http://www.personal.barclays.co.uk/BRC1/jsp/brccontrol?task=articleFWgroup&value=8838&target=_self&site=pfs [Last access on Feb 22, 2007]

BERNZ, 2004. *The complete social engineering faq! By Bernz* [online]. Available from URL: http://www.hackpalace.com/hacking/social-engineering/social%20engineering%20faq.txt [Last access on Oct 30, 2004]

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.

BRITISH STANDARDS. 1995. *BS7799: Code of Practice for Information Security Management.* London: British Standards.

BRITISH STANDARDS. 1998. *BS7799-part 2: Information Security Management, Part 2. Specification for Information Security Management Systems*. London: British Standards.

CASTELFRANCHI, C and FALCONE, R. 2001. Social trust: a cognitive approach. In: C. CASTELFRANCHI and Y.-H. TAN, eds. Trust and Deception in Virtual Societies. Norwell, MA: Kluwer Academic Publishers, pp 55-90.

CERT® Coordination Center Web site. 2002. *CERT® Incident Note IN-2002-03 "Social Engineering Attacks via IRC and Instant Messaging"* [online]. Available from URL: http://www.cert.org/incident_notes/IN-2002-03.html [Last access on Dec, 4, 2004]

CIALDINI, R. B. 2001. *Influence: science and practice - 4th ed*. Massachussets: Allyn & Bacon.

COLLINS, K. J. et al. 2000. *Research in the Social Sciences, Only study guide for RSC201-H.* Pretoria: University of South Africa.

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].

DESMAN, M. B. 2001. *Building an Information Security Awareness Program*. Boca Raton, FL: Auerbach Publications (imprint of CRC Press LLC).

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.

EBAY, 2006. *Home page* [online]. Available from URL: http://www.ebay.com [Last access on March 8, 2007]

FBN BANK. 2006. *FBN Bank - Indemnity to FBN Bank (UK) Ltd for fax or telephone instructions from Personal Customers* [online]. Available from URL: http://www.fbnbank.co.uk/forms/Fax_indemnity.pdf [Last access on Feb. 22, 2007]

FIGHT IDENTITY THEFT, 2006. *PayPal Email Scam - Web Form* [online]. Available from URL: http://www.fightidentitytheft.com/paypal_scam_webform.html [Last access on Feb. 22, 2007]

FLETCHER KENNEDY LIMITED. 2007. *Barclays - Instructions transmitted by facsimile indemnity and list of code words* [online]. Available from URL: http://www.fletcherkennedy.com/banking/Fax-Indemnity.pdf [Last access on Feb. 22, 2007]

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

FRANGOPOULOS, E.D. and ELOFF, M.M. 2004. Comparative Study of Standards and Practices Related to Information Security Management. In: *Peer-reviewed Proceedings of the ISSA enabling tomorrow Conference 2004*. ISBN 1-86854-522-9.

FRANGOPOULOS, E.D. and VENTER, L.M. 2004. Biometric protection of smartcards through fingerprint matching: a technological overview and possible directions. In: *Peer-reviewed Proceedings of the ISSA enabling tomorrow Conference 2004*. ISBN 1-86854-522-9.

FRAUD WATCH INTERNATIONAL, 2005a. *Pentagono* [online]. Available from URL: http://www.fraudwatchinternational.com/frauds_and_scams/pentagono.htm [Last access on Jan 15, 2005]

FRAUD WATCH INTERNATIONAL, 2005b. *Nigerian 419 Scams*. [online]. Available from URL: http://www.fraudwatchinternational.com/internetfraud/nigerian419.htm [Last access on Jan 15, 2005]

FRAUD WATCH INTERNATIONAL, 2007. *Phishing Web Site Methods* [online] URL: http://www.fraudwatchinternational.com/phishing-fraud/phishing-web-site-methods/ [Last access on Feb. 22, 2007]

GIDDENS, A. 2001. *Sociology* (4th edition). Oxford: Blackwell Publishing Ltd.

GRANGER, S. 2001. *Social Engineering Fundamentals, Part I: Hacker Tactics* [online]. Available from URL: http://www.securityfocus.com/infocus/1527 [Last access on Oct 10, 2004]

GRANGER, S. 2002. *Social Engineering Fundamentals, Part II: Combat Strategies* [online]. Available from URL: http://www.securityfocus.com/infocus/1533 [Last access on Oct 10, 2004]

HACKER'S JARGON LEXICON. 2004. *Hacker's Jargon Lexicon* [online]. Available from URL: http://www.hack.gr/jargon/html/lexicon.html [Last access on Oct 30, 2004]

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].

HARL, 1997. *People Hacking: The Psychology of Social Engineering* [online]. Available from URL: http://www.noblit.com/docs/people-hacking.pdf [Last access on Oct 14, 2004]

HUMPHREYS, T., 2005. *Revision of ISO/IEC 17799 & New ISMS Developments* [online]. Available from URL: http://www.ewics.org/uploads/attachments/security-subgroup-london-2005/ISO_IEC_17799+ISMS_Developments.pdf [Last access on Aug 18, 2005].

HUMPHREYS, T. 2006. *State-of-the-art information security management systems with ISO/IEC 27001:2005* [online]. Available from URL: http://www.iso.org/iso/en/iso9000-14000/msstandards/pdf/info_2.pdf [Last access on March 3, 2007]

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. 2000a. *International Standard ISO/IEC 17799:2000. Information technology — Code of practice for information security management.* Geneva: ISO Copyright Office.

ISO/IEC. 2000b. *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.

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.

JELEN, G.F. and WILLIAMS, J.R., 1998. A Practical Approach to Measuring Assurance. In: *14th Annual Computer Security Applications Conference (ACSAC '98)*. December 1998. Also [online] available from URL: http://portal.acm.org/dl.cfm

KAJAVA, J. and SIPONEN, M.T. 1997. Effectively Implemented Information Security Awareness. In: *Proceedings of the 13th International Conference on Information Security IFIP-TC11, 13.5.97*. Copenhagen, Denmark

KOKOLAKIS, S.A. et al. 2000. The use of business process modeling in information systems security analysis and design. In: *Information Management & Computer Security*, **8**(3) [2000] 107-116. MCB University Press. ISSN 0968-5227. Also [online] available from URL: http://www.emerald-library.com

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].

LIEBERMAN, D.J., 2000. *Get Anyone to Do Anything*. St. Martin's Griffin, New York, 2000.

LOW, J. et al. 1996. Read this and change the way you feel about software engineering. *Information and Software Technology* 38,77-87.

LOWERY, J. 2002. *Penetration Testing "The Third Party Hacker"* [online]. Available at URL: www.sans.org/rr/whitepapers/testing/264.php [Last access on Jan 15, 2005

MAKOSKY, V. P. 1985. Identifying major techniques of persuasion. In: *Teaching of Psychology*, 12, pp. 42-43

MASLOW, A. 1987. *Motivation and Personality*, 3rd edition. New York: Harper Collins Publishers.

MENDELSSOHN, M. et al. 1989. *Τι είναι Διαφωτισμός;* [Greek] [What is Enlightenment?]. Translated from German by N. M. Skouteropoulos. Athens: Εκδόσεις Κριτική [Kritiki Publications].

MERIAM-WEBSTER, 2004. *Online Dictionary* [online]. Available from URL: http://www.m-w.com [Last access on Oct 30, 2004]

MICHIGAN STATE OFFICIAL WEBSITE. 2006. *Department of Information Technology. Internet Security for Citizens and Government. Definitions* [online]. Available from URL: http://www.michigan.gov/cybersecurity/0,1607,7-217-34415---,00.html [Last access on March 8, 2007]

MITNICK, K. and SIMON, W.L. 2002. *The Art of Deception. Controlling the Human Element of Security.* Indianapolis: Wiley Publishing Inc.

MITNICK, K. and SIMON, W.L. 2005. *The Art of Intrusion.* Indianapolis: Wiley Publishing Inc.

MORGAN, G. 1996. *Images of Organization* (2nd ed.). Thousand Oaks, CA: Sage Publications, Inc.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 1998. *NIST Special Publication 800-16 Information Technology Security Training Requirements: A Role- and Performance-Based Model.* [online]. Available from URL: http://csrc.nist.gov/publications/nistpubs/ [Last access on Jan 15, 2007]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2000. *NIST Special Publication 800-24. PBX Vulnerability Analysis: Finding Holes in Your PBX Before Someone Else Does*. [online]. Available from URL: http://csrc.nist.gov/publications/nistpubs/800-24/sp800-24pbx.pdf [Last access on Jan 15, 2007]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2002. *NIST Special Publication 800-46. Security for Telecommuting and Broadband Communications*. [online]. Available from URL: http://www.csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf [Last access on Jan 15, 2007]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2003. *NIST Special Publication 800-55. Security Metrics Guide for Information Technology Systems* [online]. Available from URL: http://www.csrc.nist.gov/publications/nistpubs/800-55/sp800-55.pdf [Last access on Jan 15, 2007]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2006. *NIST Special Publication 800-88. Guidelines for Media Sanitization* [online]. Available from URL: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf [Last access on March 7, 2007]

NELSON, R. [ca 2000]. *Methods of Hacking: Social Engineering* [online]. Available from URL: http://www.isr.umd.edu/gemstone/infosec/ver2/papers/socialeng.html [Last access on June 14, 2003]. Also available from URL: http://zeth.kodslav.org/security/dokumentation/dokumentation/soceng/socialeng.html [Last access on Nov 3, 2004]

NEWS FACTOR TOP TECH NEWS, 2005. *Social Engineering Spreads New Plague of Web Chat Attacks* [online]. Available from URL: http://www.newsfactor.com/perl/story/16870.html [Last access on Jan 15, 2005]

van NIEKERK, J. and von SOLMS, R., 2005. A Holistic Framework for the Fostering of an Information Security Sub-Culture in Organisations. In: *Peer-reviewed Proceedings of the ISSA 2005 New Knowledge Today Conference*. June 2005. ISBN 1-86854-625-X. Also [online] available from URL: http://www.infosecsa.co.za [Last access Oct 28, 2005]

NOVELL INC., 2003. *My Real Box free email service home page* [online] Available from URL: http://www.myrealbox.com/a?.BQ.EE.Z1QQ.d [Last access on Feb 10, 2007]

OAKES, G. 1998. On the Unity of Max Weber's Methodology. In: *International Journal of Politics, Culture, and Society*. **12**(2) 293-306

ORGILL, G.L., ROMNEY, G.W., BAILEY, M.G., and ORGILL, P.M., 2004. The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In: *Proceedings of the 5th Conference on Information Technology Education*. October 2004. ACM Press.

OSTROFF, F. and SMITH, D. 1992. The Horizontal Organization. *McKinsey Quarterly*. **1** 148-168.

PFLEEGER, C. P. 1997. *Security in Computing*. 2nd Ed., Upper Saddle River, NJ: Prentice-Hall.

POP SUB-CULTURE, 2005. *Nigeria scam* [online]. Available from URL: http://www.popsubculture.com/pop/bio_project/nigeria-fraud.html [Last access on Jan 15, 2005]

REEKIE, C. M. 2004. The emergence of obligation rights in ethical information security awareness. In: *Peer-reviewed Proceedings of the ISSA enabling tomorrow Conference 2004 - Research Papers Section.* June 2004. ISBN 1-86854-522-9 [REE04]

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].

RUSCH, J. J. [ca 1999]. *The "Social Engineering" of Internet Fraud* [online]. Available from URL: http://www.isoc.org/isoc/conferences/inet/99/proceedings/3g/3g_2.htm [Last access on May 25, 2004]

SCHACH, S R. 2005. *Object-oriented and Classical Software Engineering.* 6th ED., McGraw-Hill

SCHLIENGER, T. and TEUFEL, S., 2003. Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture. In: *Proceedings of the 14th International Workshop on Database and Expert Systems Applications 2003* (DEXA'03). IEEE.
Also available from URL: http://computer.org/publications/dlib/ [Last access on Jun 4, 2006]

SCHNEIER, B. 1996. *Applied cryptography. Protocols, algorithms and source code in C*. USA: John Wiley & Sons Inc.

SCHNEIER, B. 2000. *Secrets & Lies*. USA: John Wiley & Sons Inc.

SEARS, D. O. and FREEDMAN, J. L. 1965. Effects of Expected Familiarity with Arguments Upon Opinion Change and Selective Exposure. In: *Journal of Personality and Social Psychology*. **2** (3) 420-426.

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.

SPAM COP, 2005. *Spam Statistics* [online]. Available from URL: http://www.spamcop.net/spamstats.shtml [Last access on Jan 25, 2005]

SPAM FILTER REVIEW. 2006. *Spam statistics 2006* [online]. Available from URL:http://www.spam-filter-review.toptenreviews.com/spam-statistics.html [Last access on Feb 10, 2007]

SPAM REGISTER, 2005. *Statistics* [online]. Available from URL: http://www.spamreg.com/statistics.php [Last access on Jan 25, 2005]

SUN MICROSYSTEMS, 2003. *Datasheet Sun Ray ™ Ultra--Thin Clients* [online]. Available from URL: http://se.sun.com/edu/pdf/sunray.pdf [Last access on March 7, 2007]

SUTPHEN, R. [No date]. *Battle for Your Mind: Introduction* [online]. Available from URL: http://www.sibyllinewicca.org/lib_psychology/lib_p_brain.htm [Last access on Aug 8, 2004]

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

THOMSON, I. 2006. *'Evil twin' Wi-Fi hacks target the rich. Hackers after high net worth individuals in wireless scam* [online]. Available from URL: http://www.airdefense.net/newsandpress/vnunetcom_11_23_06.pdf [Last access on Jan 1, 2007]

TIME MAGAZINE. 2003. *Coolest inventions 2003 - Keeping it safe-Beyond recognition* [online]. Available from URL: http://www.time.com/time/2003/inventions/invshredder.html [Last access on July 7, 2006].

TSUJII, S., 2004. Paradigm of Information Security as Interdisciplinary Comprehensive Science. In: *Proceedings of the 2004 International Conference on Cyberworlds 2004* (CW'04). IEEE.
Also available online from URL: http://computer.org/publications/dlib/ [Last access on May 6, 2005]

TURPEINEN, M. and SAARI, T., 2004. System Architecture for Psychological Customization of Communication Technology. In: *Proceedings of the 37th Annual Hawaii International Conference on System Sciences* (HICSS'04).

U.K. DEPARTMENT OF TRADE & INDUSTRY (DTI), 2006. *Information security breaches survey 2006 - Executive summary* [online]. Available from URL: http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults_execsum06.pdf [Last access on Jan 17, 2007]

UNIVERSITY OF VIRGINIA, 2005. *The Religious Movements Homepage Project - Discordianism* [online]. Available from URL: http://religiousmovements.lib.virginia.edu/nrms/disc.html [Last access on Feb 22, 2007]

VAUGHN, R.B.Jr., HENNING, R. and SIRAJ, A., 2003. Information Assurance Measures and Metrics - State of Practice and Proposed Taxonomy. In: *36th Annual Hawaii International Conference on System Sciences (HICSS'03)* - Track 9. January 2003. IEEE. Also available from URL: http://computer.org/publications/dlib/ [Last access on 27/6/2005].

WASHINGTON STATE, OFFICE OF THE ATTORNEY GENERAL, 2007. *Spam* [online]. Available from URL: http://www.atg.wa.gov/InternetSafety/Spam.aspx [Last access on Feb 10, 2007]

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.

YAHOO, 2004. *Spam Statistics* [online]. Available from URL: http://www.yahooantispam04.com/stats.pdf [Last access on Jan 15, 2005]

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.

Appendix A - IS Terminology

The terminology used to describe the various aspects of the Information Security (IS) concept can in many ways be confusing. It is also not uncommon for similar terms to have different meanings in the context of various IS documents. It was thus deemed necessary to at least clarify how particular terms are used in the context of this work.

This appendix is divided in two sections: The first section provides the definitions necessary for laying the foundation of this work. As such, the definitions are presented in logical rather than alphabetical order. These definitions closely follow the terminology used in the ISO/IEC17799:2005 and ISO/IEC 27001:2005 standards as this work ultimately revolves around them. The second section provides the rest of the general terminology that was used in this work and does not necessarily relay back to the two standards mentioned above. This is sorted alphabetically.

A.1 Foundation terminology

Information Security: ISO/IEC 17799:2005 defines Information security as the "preservation of confidentiality, integrity and availability of information" and goes on to include that "other properties such as authenticity, accountability, non-repudiation and reliability can also be involved".

Information System: ISO/IEC 17799:2005 deals with the notion of an Information System in terms of the complete environment of an organisation within which information is handled. This includes every form of information handling as information can exist on many forms. Thus, an information system includes information handling in any form, building and location issues and all types of assets within the organisation, in addition to its traditionally defined IT systems. An information system can be viewed as encompassing all of the hardware, software, physical, administrative, and organizational issues that are involved in the handling off information within an organisation.

Information Security Management System (ISMS): The ISMS is defined in ISO/IEC 27001:2005 as "that part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security". It is further noted that "The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources".

Risk: In ISO/IEC 17799:2005 risk is defined as the "combination of the probability of an event and its consequence". The risk involved in a highly probable but inconsequential event or in an event of severe consequences but of miniscule probability of ever taking place is thus low. In the context of ISO/IEC 17799:2005 and ISO/IEC 27001:2005, risk has a dynamic quality. It is never assumed constant. It is, by default, assumed to be changing with time (hence the need for the existence of an ISMS).

Risk assessment: In ISO/IEC 17799:2005 risk assessment is defined as the "overall process of risk analysis and risk evaluation". It is considered as one of the foundation elements for the creation of an Information Security system that will provide the correct level of security to every functional aspect of the organisation. Erroneous risk assessment can either lead to an inadequately low level of security, hence making the security system ineffective, while an exceedingly high level of security makes the security system inefficient.

Threat: A threat in the context of any system is the possibility of inflicting damage to the system. In ISO/IEC 17799:2005 it is defined as "a potential cause of an unwanted incident, which may result in harm to a system or organization".

Vulnerability: A vulnerability is defined as a weakness of a system that can be exploited by a threat, with negative effects for the system.

Control: ISO/IEC 17799:2005 defines "control" as the "means of managing risk, including policies, procedures, guidelines, practices or organizational structures, which can be of administrative, technical, management, or legal nature". It is further considered as a synonym of "safeguard" or "countermeasure". ISO/IEC 17799:2005 comprises 11 security control clauses. In total, these 11 clauses contain 39 main security categories. Each security category contains: a) a *control objective* stating what needs to be achieved, and b) *description(s) of one or more controls* that can be applied to achieve the control objective.

Guideline: In the context of this work the term "guideline" is used to describe how to implement a particular control in order to achieve the desired control objective. In ISO/IEC 17799:2005 a typical control description comprises: a) a definition of the specific control statement to satisfy the control objective, b) guidance and information in support of the implementation of the control and how to achieve the control objective, c) further information, pertinent to the control under examination, such as legal aspects of its implementation and references to related standards. It is the guidance presented in (b) above that the term "guideline" refers to.

Plan-Do-Check-Act (PDCA) model: The PDCA model is defined in ISO/IEC 27001:2005. According to this model, a virtuous circle of continual improvement of the ISMS is established. It is assumed that changes in the organisation’s environment occur continually and as a consequence, a monitoring system must be established. The core function of the ISMS is to make new risk assessment, identification of new vulnerabilities and implementation of new controls, as automated a process as possible. Hence, one of the main characteristics of the ISMS which is based on the PDCA model, is that it is “free running” and does not rely on a triggering event of some sort to begin the re-evaluation procedure.

A.2 General terminology

Assurance: an expression of confidence that one has in the strength of implemented controls and that security needs are indeed satisfied.

Phishing: the act of tricking someone into surrendering personal or confidential information or subterfuging that someone into doing something that (s)he normally wouldn't do. Phishing is primarily used as a means to identity theft.

Sanitisation: the general process of removing data from storage media, in such a way that there is reasonable assurance that the data originally contained in the media may not be easily retrieved and reconstructed.

Appendix B - List of abbreviations used

In an effort not to overburden the text of this dissertation, it was decided to use a number of abbreviations for commonly used terms. Although the abbreviations used in this work are the ones generally found in relevant literature, they are included here for reasons of clarity.

ANT: *Actor-Network Theory.*

BPM: *Business Process Modeling.*

IA: *Information Assurance.*

IM: *Instant Messaging*.

IRC: *Internet Relay Chat*.

IS: *Information Security* (this abbreviation is not used in the text to denote "Information System(s)").

ISMS: *Information Security Management System*.

IT: *Information Technology*

ITSec: *Information Technology Security*

MTBF: *Mean Time Between Failures*. A figure giving an indication of the life expectancy of electronic components.

PDCA: *Plan-Do-Check-Act* virtuous cycle. Procedure implemented for the continual re-assessment and improvement of the level of information security.

PBX: industry standard acronym for "*Private Branch eXchange*". Signifies the portion of the telephone system owned by the telco customer. The PBX includes everything at the customer's office up to the point where it connects to the telephone company's lines.

SE: *Social Engineering* (this abbreviation is not used in the text to denote "Social Engineer").

Appendix C - Detailed examination of the ISO/IEC 17799:2005 IS standard with respect to SE

This appendix contains a detailed analysis of the examination of the ISO/IEC 17799:2005 (ISO/IEC, 2005) security controls with respect to Social Engineering.

The ISO/IEC 17799:2005 standard is structured around 11 security control clauses that in turn contain 39 main security categories in total. An introductory clause also exists (section 4), that deals with the very basics of risk assessment and treatment).

The eleven security control clauses and main security categories are:

Table C-1: Structure of the ISO17799:2005 security clauses.

Section 5.	Security Policy	i. Information security policy
Section 6.	Organising Information Security	i. Internal organization ii. External parties
Section 7.	Asset Management	i. Responsibility for assets ii. Information classification
Section 8.	Human Resources Security	i. Prior to employment ii. During employment iii. Termination or change of employment
Section 9.	Physical and Environmental Security	i. Secure areas ii. Equipment security
Section 10.	Communications and Operations Management	i. Operational procedures and responsibilities ii. Third party service delivery management iii. System planning and acceptance iv. Protection against malicious and mobile code v. Back-up vi. Network security management

	vii. Media handling viii. Exchange of information ix. Electronic commerce services x. Monitoring
Section 11. Access Control	i. Business requirement for access control ii. User access management iii. User responsibilities iv. Network access control v. Operating system access control vi. Application and information access control vii. Mobile computing and teleworking
Section 12. Information Systems Acquisition, Development and Maintenance	i. Security requirements of information systems ii. Correct processing in applications iii. Cryptographic controls iv. Security of system files v. Security in development and support processes vi. Technical vulnerability management
Section 13. Information Security Incident Management	i. Reporting information security events and weaknesses ii. Management of information security incidents and improvements
Section 14. Business Continuity Management	i. Information security aspects of business continuity management
Section 15. Compliance	i. Compliance with legal requirements ii. Compliance with security policies and standards, and technical compliance iii. Information systems audit considerations

Furthermore, each of the main security categories contains:

a) a control objective stating what needs to be achieved, and

b) description(s) of one or more controls that can be applied to achieve the control objective,

while a typical control description comprises:

a) a definition of the specific control statement to satisfy the control objective,
b) guidance and information in support of the implementation of the control and how to achieve the control objective,
c) further information, pertinent to the control under examination, such as legal aspects of its implementation and references to related standards.

Following the structure of ISO 17799, each of the eleven security control clauses is examined under the light of a possible SE attack. In this context, discussions are presented for each of the clauses along with some thoughts on how to further fortify the clauses against SE attacks.

C.1. Section 5 - Security Policy

Relevant security category:

- Information security policy

Section 5 of ISO 17799 deals with the cornerstone of security in an organisation. The security policy document is essential in providing management with a set of justified guidelines and support for information security bearing in mind the business requirements at hand, as well as the governing legislation.

At the foundation of the security effort lays the degree of management commitment to the cause. It is stated in ISO 17799, section 5 that:
" Management should set a clear policy direction in line with business objectives and ***demonstrate support for, and commitment to,*** *information security through the issue and maintenance of an information security policy across the organization"*. Also in section 5.1.1 it is stated: "*The information security policy document* ***should state management commitment*** *and set out the organization's approach to managing information security*". In practice, there are examples where management simply accepts a security policy

provided by an external consultant because the organisation needs one. There are cases where members of the management group do not understand -let alone espouse- the security policy document. In such cases, an official endorsement of the policy has very little value and does not promote the policy's acceptance by lower level employees. A typical example of such a situation may arise when a security officer is reprimanded as "overzealous" when he/she attempts to verify the identity of a member of the management group who is not carrying a proper ID token.

Also in section 5.1.1 of ISO 17799, it is stated: "*An information security policy document should be approved by management, and* ***published and communicated to all employees*** *and relevant external parties*" and "*This information security policy* ***should be communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader***". These two statements deal with the very sensitive aspect of how the employees at various levels of the hierarchy understand the policy (if they understand it at all), given all the possible variations in terms of position, job context, knowledge and ability to grasp fine ideas about security. In this sense, the security policy document must be easy and simple to read and not overwhelm the readers either by its volume or by language that is difficult to understand. A complicated security policy or one that takes a lot of effort to read from cover to cover, will not have the desired effect of strengthening security. On the contrary, employees who have been exposed to but have not understood the policy and its directives will definitely be the first ones succumbing to a Social Engineering attack. The justification of this statement is that these users will be lulled to a state of false security by the fact that, for instance, a password system is in place but may end up mishandling their passwords and be persuaded to relinquish them to the attacking Social Engineer.

The point also made in section 5.1.1 about explaining "*security education, training, and awareness requirements*", is one of the most important ones with respect to SE attacks. To define the notion of a "security-aware" employee in

exact terms would be a rather futile exercise. However, security awareness, education and training, if actively pursued, will, in the end, result in raising the degree of understanding security and its implications for the average employee. This will lead to a higher level of resistance against SE attacks and accordingly to a higher level of security. The average person -or employee in our case- can not be expected to automatically become "security-aware" on queue. Similar to the example of WWII England where banners with motos like "Loose Lips Sink Ships" where posted everywhere for everyone to see in order to raise security awareness in the battle against espionage, in addition to proper security training and education, security messages against SE should always be present on monitors, login screens, notepads etc. Even penetration testing should regularly take place, not only to have a continual assessment of the level of security, but to aid in the training of employees against SE attacks. When the average employee is brought to such a level that a potential SE attack is recognised and reported, the required security level, as far as the end-user is concerned, will have been attained.

Remaining in section 5.1.1, the statement "*If the information security policy is distributed outside the organisation, care should be taken not to disclose sensitive information*" should perhaps be more generalised and lead to the protection of the document as a whole. If the current security policy document (or older version thereof) falls into the hands of a Social Engineer, there is a wealth of information that the Social Engineer may use in an attack. From internal directives to security incident reporting procedures, all will be thoroughly studied to yield the best plan of attack that a Social Engineer will follow.

While methods relying on the education of and passing information to users on security issues should indeed be the main tool of building up resistance to SE attacks, the importance of counterincentives against complacency and negligence should not be underestimated. Following this mentality, in section 5.1.1 it is made clear that " *The policy document should contain statements concerning: … (omitted text) … a brief explanation of the security policies,*

principles, standards, and compliance requirements of particular importance to the organization, including: … (omitted text) … consequences of information security policy violations". This, combined with prior proper training, should aid in keeping users alert against possible SE attacks. However, in order to be just in dispensing punishment to users who have failed to uphold the security directives, users must be able to function within a fully operational security infrastructure that protects them. There is little point in identifying users as responsible for a security violation when the security system itself is incomplete or failing. In that case, one would only be looking for scapegoats to take the blame for an inadequate security infrastructure.

Finally, section 5.1.2 "Review of the information security policy" deals with the necessity of keeping the security policy updated. In such reviews and updates it is essential to include all lessons learned from past experience. Thus, if the security policy caters for controls against SE attacks, the review of the policy, if performed according to the ISO 17799 standard, will yield improved defenses against SE attacks.

C.2. Section 6 - Organising Information Security

Relevant security categories:

- Internal organization
- External parties

Section 6 of ISO 17799 deals with both the internal organisation of IS as well as applying IS rules to external, collaborating parties. Management of Information Security within the organisation is effected through the establishment of an appropriate framework that controls the implementation of IS (section 6.1 of ISO 17799). On the other hand, wherever there is a business need for collaboration with external parties, the organisation's security level must be maintained by appropriate controls that are defined in documented agreements with those parties (section 6.2 of ISO 17799).

In the introductory part of section 6.1, among other issues, it is stated that "*a multi-disciplinary approach to information security should be encouraged*". This statement proves once again that IS is not a technical matter alone. As it has already been discussed, defense against SE attacks is more than just technical. Technical controls must be devised and implemented in order to provide a supporting infrastructure against SE attacks, but a large part of the effort -if not the largest part- is definitely non-technical.

In section 6.1.1 "Management commitment to information security" the already familiar notions of Management support of IS, IS policy reviews, resource provision for IS, promotion of security awareness etc are re-iterated. One important notion stated is that "*Management should … ensure that the implementation of information security controls is co-ordinated across the organization*". Lack of such co-ordination may have three immediate effects on the defense against SE attacks: **First**, if the application of IS controls is not homogeneous throughout the organisational structure, users may become confused insofar security practices are concerned. This will both lead to the weakening of the security effort as well as to an increased level of vulnerability of users to SE attacks. **Second**, if there are differences in the application of IS controls between the various components of the organisational structure, the attacking Social Engineer will stand a better chance of successfully gathering the information necessary for mounting an attack, by separately approaching the various organisational components. It has to be noted that Social Engineers, very rarely mount a full-frontal attack to obtain all the necessary information in a single attempt. Their method rather resembles obtaining pieces of the puzzle from different sources and putting them together in order to formulate the larger picture that they are after. **Third**, lack of co-ordination in security incident reporting and response may give the attacking Social Engineer an appropriate window of opportunity to successfully carry out an attack.

In section 6.1.2 "Information security co-ordination", apart from statements regarding the handling of non-compliance, security training, promotion of

security awareness, IS control assessment and implementation, IS incident handling and co-ordination etc, the notion of approved methods for information classification is introduced (and further discussed in detail in section 7.2 of ISO 17799). Although this is changing, the current practice is for the majority of organisations not to have an active information classification policy and most if not all of organisation employees have access to the information, irrespective of their actual need-to-know. This places the burden of securing the handling of information on the shoulders of employees. However, the average employee is not equipped or trained to deal with this. Hence, employees may inadvertently disclose sensitive information during SE attacks as they only have their personal, highly subjective criteria to rely on for determining the nature of the information. If there is no objective classification of the information's sensitivity, employees can not correctly evaluate the seriousness of a possible information leak.

The need-to-know aspect is more important than it first appears, even for information that does not appear very critical at first glance. On the two sides of the SE attack there are a) the attacking Social Engineer and b) the targeted employees. If a "need-to-know" scheme is in place, obviously, the targeted employees can not divulge information they do not possess. Thus, the Social Engineer will have to go to greater lengths in order to locate and attack an employee who actually has the critical information. On the other hand, the Social Engineer's task becomes even more difficult as he/she not only has to gain the confidence of the targeted employee, but also has to prove that his/her need-to-know status is such that the information requested can indeed be provided to him/her according to the organisation's security policy.

Section 6.1.3 of ISO 17799 "Allocation of information security responsibilities" discusses the steps for defining and assigning appropriate security responsibilities to employees according to the directives of the security policy that has been approved and endorsed by Management. The directives presented there lead to the creation of a security hierarchy parallel to the existing hierarchy of the organisation. As some employees will inescapably be

assigned to two positions simultaneously, one in the administrative hierarchy and one in the security hierarchy, conflicts are bound to exist between their two identities. To illustrate this issue, one can imagine the case where a member of the information security hierarchy (e.g. a network administrator) identifies a security incident involving or even incriminating another individual (e.g. a lower member of the management group) who holds a lower position than the network administrator in the security hierarchy or lies completely outside of it. Administratively though, the member of the management group outranks the network administrator and can directly or indirectly affect the network administrator's status in the organisation. The network administrator will certainly be faced with the dilemma of further pursuing the matter or not, as personal loss can result from such action. This conflict reflects the social issues at work in the context of a functioning ISMS and certainly allows a Social Engineer to take advantage of the situation and mount a successful attack by impersonating an individual who holds a high-level position in the administrative hierarchy. It may thus prove imperative to assign the overall control of the IS aspect to a group of people who perform their task of upholding IS, outside the administrative hierarchy. This, however, does not negate the need for employees that lie within the administrative hierarchy to be assigned IS responsibilities in order to protect assets and small-scale security processes within their work space. Whether Management would accept such an "untouchable" IS group, is another issue though!

Section 6.1.4 "Authorization process for information processing facilities" provides implementation directives for new information processing facilities. This includes privately-owned laptops, home-computers etc. From a SE point of view, the introduction of new facilities may provide a window of opportunity during the phase when the capabilities of the newly introduced technologies are not fully understood. A full risk assessment regarding these new technologies can thus not be carried out. Following this, vulnerabilities can not be effectively identified and are thus not efficiently mitigated. Hence, the true extent of the residual risk after vulnerability mitigation can not be safely fathomed. To illustrate this example, one may consider the situation that

arose from the first introduction of wireless networking components in the work environment only a few years ago. In those days that this technology was not fully mature and users and administrators alike had not yet developed sufficient know-how and insight on the technology, there were cases where Social Engineers exploited this fact. Their method of operation was to use mobile wireless-enabled devices outside of or near the organisation premises to gain access to corporate networks. In the rather rare cases in those days that a password was needed, all it took was a little clever manipulation over the phone to have a user or even administrator allow them in. Nowadays that wireless technology is considered mainstream, network administrators have become more cautious in how to deploy and use it. However, according to the executive summary of the "Information security breaches survey 2006" which was carried out by the U.K. Department of Trade & Industry (2006), one out of five authorised wireless networks was still completely unprotected while another one out of five remained unencrypted. This shows that although enough time has passed for the wireless network technology to mature and its security shortcomings to be identified, implementations of this technology still remain vulnerable. Another alarming piece of information is also given in the "Information security breaches survey 2006" (U.K. Department of Trade & Industry, 2006) regarding another type of technology that should be considered mature by now: in 2006 "*Only half of the companies that have implemented Voice over IP telephony evaluated the security risks before doing so*". There is little point in attempting to fully justify such an attitude but it is important to make a note of it. In a nutshell, technologies such as the ones described, are implemented on their merits of convenience, cost-effectiveness etc, while the security factor associated with them seems to pale into insignificance. If one considers currently emerging technologies such as the use of RFIDs, sensor-based smart environment, grid computing, ad hoc networks that join mobile devices, bluetooth-based communication of devices etc, the predictions for the future from a security point of view are anything but auspicious. It should thus also be stressed in the context of section 6.1.4 of ISO 17799, that users and administrators alike, must maintain a high-level of alertness regarding IS during the introductory phase of new information

processing facilities. This high level of alertness should be maintained until all vulnerabilities have been identified through the actual use of the facility and appropriate controls have been implemented.

Section 6.1.5 "Confidentiality agreements" discusses the implementation of controls with a legally binding value, with the objective of securing the organisation's information against leaks. Although the composition and signing of confidentiality agreements is essential, one has to consider that Social Engineers usually manage to extract information from their targets through indirect methods that leave the target thinking that nothing wrong was done. As such, the target will probably not even think of the signed confidentiality agreement while divulging sensitive information during a SE attack.

In section 6.1.6 "Contact with authorities" is discussed. The objective is to maintain contact with relevant authorities so that these can be contacted in an orderly manner when an IS incident demands it. In the context of SE, care must be taken in order to avoid "reverse sting" operations. If such a method is employed by the attacker, the victim of the SE attack may end up calling the Social Engineer for help, while sincerely believing that the call is placed to a legitimate authority. For this reason, liaison with the authorities that may need to be contacted during a crisis situation must be established and maintained long before a crisis arises. It would also be preferable for personal relations to be maintained between the organisation's employee(s) assigned with the task of contacting authorities and the authorities' officers assigned with receiving such calls. Any deviation from the standard procedures such as claims from an unknown individual that he/she is replacing the person usually in charge should be looked upon suspiciously. Furthermore, calls should always originate from the organisation's side. Even when calls are initiated from the authorities' side, the called party within the organisation should hang up and call back the authority's assigned liaison officer at the authority's known telephone number.

For the directives of section 6.1.7 "Contact with special interest groups" an attitude similar to the one described above must be maintained. As advisories, patches and offered executables expected from a special interest group may be spoofed and successfully cloak preparatory stages of a SE attack, all such material must be scrutinised for suspect content. Mechanisms must be in place for confirming the source and validity of all material that is to be incorporated in any form in the production or operational phases of the IT system or relevant procedures.

Regarding section 6.1.8 "Independent review of information security", the reviews must always take into consideration SE methods of operation and help control vulnerabilities related to them. Given the indirect nature of SE, this is not an easy task but it is an essential one nevertheless and ability to identify such problem areas should be included in the list of "*appropriate skills and experience*" of the individuals carrying out the reviews.

In the introductory section 6.2 "External parties", the objective of this security category is stated as: "*To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties*". When a party external to the organisation gains for any reason justified access to the organisation's information facilities or even the information itself, the IS level of the organisation must not be compromised in any way. This category proposes controls for external parties and dealing with customers and also examines appropriate third party agreements.

Insofar SE is concerned, the main issue in all cases is that the organisation no longer has to worry only for SE attacks being mounted against its own employees, but to employees of collaborating parties also. Dealing with the possibility of SE attacks is quite difficult within the organisation. When the security perimeter is expanded to include entities other than the ones immediately and directly controlled, the difficulty augments. As there is no exact yardstick by which to measure the effectiveness of SE controls, it is

practically impossible to ascertain that an external party is at least as effective as the main organisation against SE attacks. Furthermore, it is reasonable to assume that there will be serious impediments in relaying information regarding IS incidents between the external parties and the main organisation. To begin with, the IS incident reporting structures of the main organisation and that of the external party must interface efficiently. This is something that may sound easy in theory and look good on paper but is quite difficult to implement in practice, due to many reasons, most of which are non-technical. If an IS incident that compromises the main organisation's data takes place within the security perimeter controlled by the external party, the external party's response would be to attempt a cover-up rather than admit the compromise and risk losing the benefits of the collaboration with the main organisation. Depending on the gravity and extent of the incident, if the incident is promptly contained and does not get out of control, the external party will not readily admit to the problem. Even if legal clauses are in place to oblige the external party to relay IS incident information, in all but the most extreme cases, the external party can always claim that there was no notice of the incident. In the author's mind there is no solution other than ensuring that external access to information takes place on the strictest need-to-know basis for the external party, their access to the information facilities is as limited as possible, and most importantly that the main organisation receives enough assurances for the level of resistance against SE attacks of the external party. Even if the external party is certified to the strictest of security standards, resistance against SE attacks is not warranted. Applying the controls of sections 6.2.1, 6.2.2 and 6.2.3 is certainly required, but an audit geared towards identifying SE-related vulnerabilities of the external party structure may be called-for prior to any major undertaking that demands access of the external party to the main organisation's sensitive information. In this case, it is only the level of criticality of the information that will ultimately dictate if such an approach is deemed mandatory.

C.3. Section 7 - Asset Management

Relevant security categories:

- Responsibility for assets
- Information classification

Section 7 of ISO 17799 covers the identification and protection of organisational assets (section 7.1 of ISO 17799) and ensures that the level of protection of information is appropriately set (section 7.2 of ISO 17799) through the classification of information.

Sections 7.1.1 "Inventory of assets" and 7.1.2 "Ownership of assets" are not directly related to the effort against SE attacks but are essential in maintaining the overall level of security and indirectly affect the organisation's posture with respect to SE.

Section 7.1.1 deals with the cataloguing of all organisation assets including information assets, software assets, physical assets, service, people and intangible assets. Under the light of SE, some assets readily stand out, including information assets such as "*system documentation, research information, user manuals, training material, operational or support procedures*", and physical assets such as "*computer equipment, communications equipment, removable media*". Regarding information assets, the inventory taken is a very important first step in adequately protecting information that may otherwise be inappropriately disposed of and find its way into the hands of Social Engineers through "dumpster diving" or otherwise. Having accounted for every piece of important information asset, the classification of the asset can then be decided upon, the asset tracked accordingly throughout its useful life and at the end of it be properly disposed of. Even seemingly unimportant information assets such as internal telephone lists, organisation charts and even business calendars should be included in the inventories as these may provide important information for the Social Engineer. As far as physical assets are concerned, cataloguing these provides an essential starting point for their protection. Given the value of the information that is being handled, physical assets can even include floppy disks, recordable or re-writeable optical media etc. In cases where such

media have to be used for the transfer of highly-classified information, these media must definitely be uniquely identified and clearly marked for "classified use only". They must be meticulously tracked, and the information on them must be safely deleted before re-use as required. All this must be carried out throughout their useful, classified life. At their end-of-life they must be "sanitised" whereby sanitisation is defined by the U.S. National Institute of Standards and Technology in NIST Special Publication 800-88 (2006, p. ix) as "*the general process of removing data from storage media, such that there is reasonable assurance that the data may not be easily retrieved and reconstructed*". Following sanitisation, the media may be disposed of according to a specified procedure that leaves no room for a Social Engineer (or any other entity) to take advantage of them.

At first glance, section 7.1.1 seems to have been written with disaster recovery and business continuity in mind. However, the principles of taking inventory of all assets important to the organisation are essential to the day-to-day operation and protection of the organisation. Furthermore, inventory alone does not suffice for adequate protection. Assets must be assigned to individuals or entities that are responsible for their management and security. Also, assets must themselves be classified according to the classification level of the information contained in them. These aspects are covered in sections 7.1.2 and 7.2 of ISO 17799.

In section 7.1.2 "Ownership of assets", the nature of "ownership" of assets is defined, along with the responsibilities of the individual(s) to whom "ownership" is assigned. This does not directly deal with SE, but as assets of importance are assigned to "owners" and custodians who are responsible for their security, it becomes harder for Social Engineers to extract sensitive information from the assets.

Section 7.1.3 "Acceptable use of assets" defines the need for the existence of "*rules for the acceptable use of information and assets associated with information processing facilities*" such as, but not limited to, usage of mobile

devices, electronic mail and the Internet. Once again, such rules may not effectively block a SE attack but may be able to hinder one if guidelines such as "report any attempt of email contact regarding the present status of the IT system or offers for upgrades thereof" are in place.

Section 7.2.1 "Classification guidelines" supplies the basic directives for correctly and consistently classifying information "*in terms of its value, legal requirements, sensitivity, and criticality to the organization*".
Again, whilst classification is not directly associated with the defense against SE, it is an important step in that direction. In association with section 7.2.2 "Information labeling and handling" the classification of information, should clearly appear on physical entities such as documents, CD-ROM disks, hard disks etc in the form of labels, as well as unambiguously accompany all information in electronic form. The combination of these two controls helps the user not to inadvertently mishandle information that ends up in the hands of the Social Engineer. For example, a printed list containing all names, phone numbers and the positions of the Organisation's employees, will find its way with greater difficulty to the dumpster outside the organisation's premises if it is clearly labeled as "confidential" on its cover. Furthermore, if the label "confidential" appears on the top right and bottom left corners of all pages of the list, an employee under attack by a Social Engineer may think twice before relinquishing the telephone numbers of fellow employees to the attacker. A catchphrase warning against SE attacks like "Do you REALLY know who you're giving this information to?" that is printed under the classification label will also help against SE attacks. Hence, although the directives concerning the labeling of classified information, as described in section 7.2.2 of ISO 17799, are technically complete, it might be a good idea to add secondary labeling with phrases against SE or ones that remind users of the proper way to dispose material of that classification, or even that the material has been signed-for and must be returned to its owner.

There are two more issues that need to be discussed while on the subject of classification:

First, in critical environments **all** information-carrying material should bear appropriate labeling, even if that is "Public". This will do away with the risk of a user **forgetting** to add appropriate classification to a document that he/she composes and, subsequently, its recipient assuming that the document is not sensitive as it does not bear a classification label. The proper procedure would thus call for the administrative personnel handling the unlabeled document or its recipient, to assume that the document is by default sensitive, to not process it any further and contact the originator for a corrected version bearing a classification label.

Second, care must be taken not to overclassify information. Although classifying information seemingly provides an easy road to security, this is all but true. Every time a document is overclassified, it puts serious strain on the information-handling system, on both its human and technical components. When wrongly classifying a document that should be Public, automatically, resource-draining procedures for its handling and disposal switch into gear. When a low-classification sensitive document is given a higher-than-should-be classification, the above procedures become by default more stringent and thus require even more resources. This mirrors the continual tug-o-war between security and availability and great care should be taken to have an overall balanced system that serves its purpose without bleeding the resources of the organisation. Furthermore, if classification is unduly used, it looses its meaning and the whole classification scheme becomes transparent in the eyes of the employees, its purpose ultimately forfeited. Such conditions create confusion and lead to a higher probability of successful SE attacks. As it is very difficult to provide an objective yardstick by which to measure the importance of the information and thus provide an accurate and consistent classification assignment, perhaps the most efficient way to control overclassification abuse would be to centrally monitor the classification of documents (through random sampling or otherwise) and issue warnings to documents' originators when such an abuse takes place consistently. Based on the organisation's particular security needs, even quotas and counter-

incentives could be devised to control overclassification abuse.

C.4. Section 8 - Human Resources Security

Relevant security categories:

- Prior to employment
- During employment
- Termination or change of employment

Section 8 of ISO 17799 a) deals with the necessary pre-employment checks of new employees, contractors and third-party users who need to be properly screened, sign appropriate agreements and be assigned security responsibilities (section 8.1 of ISO 17799), b) provides controls to ensure that all of the above entities follow the security directives relevant to their positions (section 8.2 of ISO 17799) and c) provides directives so that the termination or change of employment of the above entities is security-wise managed in an orderly and controlled manner (section 8.3 of ISO 17799). It is also important to note that the term *employment,* in the context of section 8, is meant to: "*cover all of the following different situations: employment of people (temporary or longer lasting), appointment of job roles, changing of job roles, assignment of contracts, and the termination of any of these arrangements*".

The control in section 8.1.1 "Roles and responsibilities" is described as "*Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy*". Furthermore it is stated that these roles and responsibilities should be clearly presented to prospective employees during the pre-employment processes. This in fact "jumpstarts" the candidate's security training and allows the candidate to either accept the responsibilities assigned to him by taking the job or refuse to be part of the rest of the selection process. Although this is not strictly SE-related, it helps by allowing entry only to individuals who have a descent understanding of

security and are thus closer to the goal which is none other than to resist SE attacks.

This control is extended to the employee's of collaborating third-parties. This immediately brings to the surface the inherent difficulty of applying the organisation's security policy and directives to entities foreign to the organisation. This can certainly constitute a problem as it is difficult to have pre-employment processes that are security-wise equivalent among the collaborating parties. The pre-employment process and its security requirements has a lot to do with the job description itself. To illustrate this issue one must consider the real-life situation of an organisation, say a software house, that uses a contractor for cleaning and housekeeping services. There are significant differences between the personnel directly employed by the organisation and the employees of the contractor. The academic level of the people directly employed by the organisation is much higher than that of contractor's employees. Hence, directly-employed personnel are much better adapted to recognise the need for security and thus follow security directives. Additionally, chances are that people who are directly-employed are career-oriented and will take their security responsibilities much more seriously, as their job and future depends on upholding them, than the predominantly unskilled people who work for the contractor. The contractor's employees may be used to moving between jobs often and might even accept the trade-off between being on a continual state of alertness on one hand and risking their employment on the other.
Another issue relevant to SE is that due to the significant differences between the employment processes of organisations and their contractors, an attacker may choose to infiltrate his/her target organisation by getting employed by one of the organisation's contractors.

A possible defense against contractor-related intrusion might be to require the contractor to provide a steady group of employees that handle the organisation's subcontracted affairs. This should be applied in addition to all other directives appearing in 8.1.1 and must not function in the direction of

allowing any other measure to lax. Any changes in the group must be communicated to the organisation and agreed upon in advance and the new member(s) of the group be fully informed on their responsibilities regarding the organisation's security. Furthermore, the organisation should be in a position to demand a person's replacement on security grounds if just cause is presented.

The control presented in section 8.1.2 "Screening" calls for "*Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks*". It is furthermore clarified that the implementation guidance supplied must be extended to include subcontractors and third-party employees. From a SE point of view, and continuing on the discussion of control 8.1.1 above, the screening of contractors and third-party employees, must be ensured to be equivalent to that practiced for direct employees, or else a lateral route to mount an attack against the organisation may indeed be exploited.

Control 8.1.3 " Terms and conditions of employment" asks for signed agreements regarding IS and in particular states: "*As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security*". Although very important and indubitably legally binding, controls based on signed agreements offer little protection against the guile of a Social Engineer. Even though necessary, such a control may only become effective if the signing parties and/or their employees have a solid understanding of the notion of IS and are in a position to identify an attack, not yield to it and, furthermore, raise an alarm. The first condition may be met only through security education and the second through the achievement of a seamless security mentality throughout the collaborating parties. To this effect, efficient

communication paths regarding security must be in place and functioning between the parties. Section 8.2 attempts to address these issues.

The control described in 8.2.1 "Management responsibilities" states that "*Management should require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization*". This calls for security education, definition of security expectations, proper motivation towards applying security, security awareness and application of the defined IS policy. Perhaps the most important aspect of this control regarding SE is offered in the "other information" section of the control where it states that: "*If employees, contractors and third party users are not made aware of their security responsibilities, they can cause considerable damage to an organization. Motivated personnel are likely to be more reliable and cause less information security incidents*". This is indeed the most important statement of the control as it deals with the fact that uninformed or unmotivated personnel with respect to security are more susceptible to SE attacks. Also important is the next paragraph which underlines the role of Management in building the self-esteem of employees as "*Poor management may cause personnel to feel undervalued resulting in a negative security impact to the organisation*". Such negative feelings may well lead to security being neglected and thus making the organisation more vulnerable to SE attacks.

Control 8.2.2 "Information Security awareness, education and training" constitutes, in the mind of the author, the cornerstone of building effective defenses against SE. In this control all the prerequisites for allowing the organisation's employees to stand up against the Social Engineer, exist. It is in the hands of Management to provide training appropriate to the roles and responsibilities of individual employees. Through awareness programs, IS education and training, the self-esteem of employees regarding IS will also rise and combined with hands-on experience and knowledge may make them key contributors to the PDCA cycle.

Working in the same direction as the motivation of employees towards upholding security, counter-incentives such as disciplinary procedures when security breaches occur must be in place. This is dealt with in control 8.2.3 "Disciplinary process". That control states that "*there should be a formal disciplinary process for employees who have committed a security breach*" and goes on to add that "*the disciplinary process should also be used as a deterrent to prevent employees, contractors and third party users in violating organizational security policies and procedures, and any other security breaches*". However, it is the opinion of this author that as far as "defending the perimeter" against SE attacks is concerned, this may work in the opposite direction, such as discouraging employees from coming forth and reporting such an attack. Given the *modus operandi* of Social Engineers, and assuming that an employee has indeed been lulled into a false sense of security and has released sensitive information to the attacker, if the victim later realises what has transpired, he/she may decide not to admit to the inadvertent breach of security out of fear of repercussions. This hesitation, however, may allow the attacker enough space to move on with the next phase of the attack. Hence, as an improvement to this control, provisions must be made so that the victims of SE attacks are not disciplined for reporting the incident, but instead be commended.

The controls of section 8.3 all deal with the orderly management of the termination or change of employment of direct employees and those of subcontractors and third-parties. All three controls described, "Termination responsibilities", "Return of assets" and "Removal of access rights" all have the dual goal of ensuring that departing employees and/or subcontractors a) do not possess information belonging to the organisation or access rights to that information and b) that all specialised know-how held by departing personnel, that is essential for the organisation's business continuation, is properly transferred to the organisation. From a SE point of view, these controls are crucial as Social Engineers may decide to attack the organisation indirectly by targeting personnel members that are known to possess information vital to their goal. As an added measure, the signed confidentiality

agreements between the organisation and its employees, subcontractors or third parties should continue to hold even after the termination of employment. In the case of change of employment, assuming that the sets of terms of the confidentiality agreements are differentiated for the previous and current assignments, it should be obvious that the employee / subcontractor / third-party must continue to be bound by the union of the sets of applicable terms of the previous and current agreements.

One case that must be approached with extreme care is that of terminating disgruntled employees or unilaterally interrupting contracts with subcontractors and third-parties. In that case, extreme measures may have to be taken to ensure that the departing entity may not inflict any damage to the organisation by compromising the confidentiality, integrity and availability of the organisation's information. In order to accomplish such a task, appropriate managerial and technical controls must be in place. These controls must be centrally managed, in order to enable Administration to swiftly sever all contact with the terminated party and deny the party all access to the organisation's information and resources. Physical and remote access to the organisation's installations and information resources must be terminated immediately upon or even prior to the party's notification of termination. All organisation assets (from ID badges to company cars and equipment) must immediately be repossessed by company personnel, even if the terminated party must be accompanied to another location in order to return the asset(s). To this effect, a list of all assets in use of personnel must be kept and continually updated to reflect the current situation. From a SE perspective, any assets or access capability that remain with the disgruntled party may be used by the party to mount an attack that employs SE methods. Such an attack will have a high probability of success as the attacker possesses not only the supporting means to mount it, but also the insider knowledge to successfully carry it out.

C.5. Section 9 - Physical and Environmental Security

Relevant security categories:

- Secure areas
- Equipment security

Section 9 of ISO 17799 deals with the prevention of a) "*unauthorized physical access, damage, and interference to the organization's premises and information*" (section 9.1 of ISO 17799) and b) "*loss, damage, theft or compromise of assets and interruption to the organization's activities*" (section 9.2 of ISO 17799).

Control 9.1.1 "Physical security perimeter" states that "*Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities*". The implementation guidance includes the definition of the security perimeter(s), the use of locks, alarms and other technical measures such as intruder detection systems, as well as considerations regarding the physical location of information processing installations.

In conjunction to control 9.1.1, control 9.1.2 "Physical entry controls" proposes guidelines to ensure that only properly authorised personnel gain access to secure areas, through appropriate entry controls. These guidelines include visitors' entry and departure logging, card readers to allow access to sensitive areas, access logs for auditing purposes, visible identification badges for visitors, restricted access for support personnel etc.

There is certainly no doubt that the guidelines presented in controls 9.1.1 and 9.1.2 will lead to the implementation of a secure perimeter where only authorised individuals will gain access if all the security requirements are always met. However, a Social Engineer does not attempt to forcibly break into the secure perimeter. The Social Engineer will always try to "slide" in by convincing those people controlling the perimeter that entry should rightfully be allowed to him/her. The rich bibliography on the methods employed by Social Engineers to penetrate perimeter security stands as proof that Social

Engineers can indeed bypass security systems by exploiting the human factor. There should thus be two methods to warn-off the danger of a SE attack: a) strengthen the human factor to the point that it is not exploitable or, at least, that it is more difficult to exploit and b) implement such technical measures and practices that even when the human factor is *assumed* to be exploitable, the intrusion of an individual employing SE methods becomes more difficult or is detected as early as possible, at the very least.

"Strengthening of the human factor" with respect to upholding the physical perimeter can only take place through education and controlled exposure to SE threats (via appropriate penetration testing or otherwise) as well as through the implementation of psychological techniques to build defenses against the psychological methods employed by Social Engineers.

Technical measures function better against SE attacks as the human factor is progressively removed from being a pre-requisite for their operation. (Hopefully this will become clearer in the discussion that follows). It is assumed that a system requiring a card/PIN combination for entry and/or access to sensitive areas is already in place, and that security officers are physically present at the main gates. Ways of intrusion that are used to circumvent the existing system (for example, employee in distress, heavily-laden delivery person, following another employee in and others) must thus be efficiently catered-for.

The "*manned reception area*" proposed in guideline 9.1.1(c), will have little effect if the actual entry point is not within a few meters of the reception post. If the distance is not great, the security officer manning the post may efficiently check the identity of the people entering after presenting their badges to a reader. This can only be possible if at the time that a person uses his/her card, a clear facial picture of the authorised card holder appears on the monitor in front of the security officer for comparison.
Furthermore, if in doubt regarding the employee's identity, the security officer must have a means of blocking the entry to the individual before he/she

enters the building. To this end, a two-door scheme may be implemented. In this implementation, the employee should present his/her card to the reader of the first door, enter and then have to pass through a second door a few steps away that would normally simply yield to a push, unless remotely locked by the security officer.

This system may also provide an effective means of preventing "tailgating" or "piggy-backing" (terms used to describe a situation where an unauthorised person follows an authorised employee into the secure perimeter). If tailgating is the only concern, a simpler method of entry control may be implemented through the use of three-bar turnstiles that strictly allow only one person per card presentation to pass.

The security officers manning the reception area must have strict orders to not allow entry to any individual by bypassing the security measures. It could be argued that a solution to this problem might be to have the system not allow a security bypass of the authentication procedure for granting entry. However, in real-world terms, an emergency bypass must be a security officer's prerogative in order to deal with a variety of situations. An attempt should thus be made to diminish the chance of a Social Engineer conning the security officer into initiating a bypass. First of all, emergency bypasses should be identified by the system and logged, preferably with video information also. Such logs should regularly be reviewed and potential threats identified. In order to initiate an emergency bypass, the security officer should have to use his/her own authentication token and PIN code. Furthermore, the procedure could involve a second officer -a supervisor for example- to concur by presenting *his* ID token to the system.

Guideline 9.1.2(c) demands that "*all employees, contractors and third party users and all visitors should be required to wear some form of visible identification and should immediately notify security personnel if they encounter unescorted visitors and anyone not wearing visible identification*". While this may sound very nice in theory, in practice one is dealing with the

deepest folds of the human psyche. People, in their majority, do not like "blowing the whistle" on other people or, worse, challenging them themselves. On the contrary, they want to be liked by and be helpful to others. While special ID cards should indeed be issued to and be worn by visitors, they do not provide much protection in the sense that the ISO 17799 author means them to. The reason for this is that for the scheme to work, the human factor must again be dialed in. Visual confirmation that a visitor is indeed wearing a visitor badge offers to the person making the confirmation nothing more than the assurance that the visitor has been registered at the front desk. Furthermore, low-tech ID badges can easily be counterfeited to at least fool a casual observer. If the average employee finds it difficult to challenge a visitor who is not wearing an ID badge, it will be close to impossible to challenge a visitor on the grounds of the authenticity of the ID badge that the visitor *is* wearing!

In order to remove the human factor from this procedure, technical measures must be employed to confirm that a visitor is where he/she is supposed to be and not elsewhere. This is especially true in those cases where access to the public is essential to the organisation's operation and accompanying visitors is impractical. Such an application of technical measures can be achieved fairly easily by installing a centrally managed access-control system of networked card reader-controlled doors and elevators. Assuming that the building is served by a number of elevators that let people out on a foyer area for each floor, different departments on the floor may have different card reader-controlled entrances. When a visitor presents a valid ID card and states his/her destination at the reception desk, he/she is issued a temporary badge/ID card. With the data presented, the installed access-control system is programmed by the security officer manning the desk, to allow the visitor access to a designated path only that leads to the visitor's destination and back. In that sense, only pre-designated doorways will open following the presentation of the visitor's badge/ID card. Those not designated to open will not do so but, instead, record the attempt and relay it to the central control system. Such events may be used to trigger a warning or alarm at the central

security desk. Accordingly, a token-reader in the elevator will either allow the visitor to press only the floor button relevant to his/her visit, or even automatically make that press for him/her. Furthermore, assuming that the badge/ID card is based around or contains an RFID device, proximity arches along the corridors or at designated (manned or unmanned) checkpoints, may log the route that the visitor is following. This could even provide a countermeasure in case the visitor takes advantage of another elevator passenger's key press to exit the elevator at a non-designated floor. Thus, any deviation from the visitor's pre-designated path or unjustifiable delay during his/her visit may be programmed to trigger an alarm. This alarm combined with the presence of security officers in the building that warrants a prompt response, will give a very small window of opportunity to a potential attacker.

Regarding escorting visitors (a point also made in 9.1.2(c)), this is something that even though constitutes a pre-requisite for any security policy, gets very easily overlooked. This is especially true when the visitor is someone who - without being a contractor and thus not being bound by any relevant agreements- often has a legitimate reason to visit the organisation's premises. After a while employees usually become accustomed to seeing that individual move unescorted. It is exactly that gray area between a one-time visitor that no one recognises and an authorised (and thus screened) collaborating third-party member that may be taken advantage of by a Social Engineer. Again, a logged-access system that covers the whole building such as the one described above, may prove to be a useful tool in the security effort.

Delivery personnel fall under the same general category of unescorted visitors moving inside a secure perimeter. For many reasons, items need to be delivered to the recipient in person and not be left with the security desk. Although stricter delivery procedures may require a security officer to sign for a larger percentage of the incoming items irrespective of who the final recipient is, the problem of a courier insisting on immediate delivery to the recipient will always surface. Tracking the courier using the principles

described above throughout his/her visit to the building may provide a solution. Alternatively, it could be defined that all delivery personnel making deliveries must be escorted, without exceptions, by a security officer, or that the recipients of the items being delivered must always collect them in person from a common area outside the secure perimeter.

Remaining on the issue of "*visible identification*", usually, most badges/ID cards include a picture of their authorised bearer. There is no point of having this picture on the badge if the picture is small, dark, out of focus, badly printed or has faded with time. If an employee must wear spectacles in order to closely examine another employee's badge, then this will simply not happen. Such badges may be sufficient for front-desk identification when the badge must be presented to the security officer performing the control, but are totally insufficient for the casual control that guideline 9.1.2(c) calls for. If the badge photographs are to be of any use in that respect, they must be of good quality and large enough to be clearly recognisable from a distance of 2 meters. As visitors' badges can not have a photograph of the bearer included, colour-coding of the badge may be used to identify which area of the building the visitor is allowed to visit. Furthermore, visitor badges should bear the same colour on both sides. Thus, a badge can not "accidentally" be turned on its neutrally-coloured side to confuse control. Hence, an out-of-place visitor may be swiftly identified and pointed out to security. Such specifications may call for badges/ID cards of a larger format and most probably more expensive to produce, but are essential if the badge characteristics are not to be used as a tool in a SE attack.

Control 9.1.3 "Securing offices, rooms and facilities" provides guidance that is very important in the fight against SE as it attempts to remove those elements that a Social Engineer may use to secure his/her goal. Guideline 9.1.3(b) calls for "*key facilities should be sited to avoid access by the public*". This is very important as the attacker may otherwise pretend to be lost or misdirected if caught. Furthermore, by exhibiting a little well-mannered naivete, the attacker may get away with the attempted breach without raising any alarms. When an

attacker finds him/herself successfully within the secure perimeter he/she must be able to swiftly identify the next target. To this end, any information regarding the "what and where" of the surroundings is essential. By depriving the attacker from such information, more obstacles are placed in the way of a successful SE attack. To this end, guideline 9.1.3(c) can offer significant aid: "*where applicable, buildings should be unobtrusive and give minimum indication of their purpose, with no obvious signs, outside or inside the building identifying the presence of information processing activities*". Indubitably, phone directories can offer a wealth of information to the Social Engineer. Hence, these documents would be something of a prize for the attacker who has already managed to get inside the security perimeter. This is the reason behind guideline 9.1.3(d) that states: "*directories and internal telephone books identifying locations of sensitive information processing facilities should not be readily accessible by the public*". To this guideline one might add that there should not be any unattended telephone sets in publicly accessible places that an attacker might use to extract information from unsuspecting employees. The targeted employees would have no indication whatsoever that the person calling them from a telephone extension from within the organisation is, in reality, an attacker. Another useful addition would be that bulletin and notice boards must not be present in public access areas. As these may carry personal or organisational data, they might provide a Social Engineer with morsels of information that help him/her substantiate his/her claims.

Control 9.1.4 "Protecting against external and environmental threats" deals with physical protection against natural and man-made disasters. Although not directly related to SE attacks, an attacker might intentionally trigger an alarm system in an effort to cause a diversion. This would give the attacker an opportunity to either proceed with his/her plan in vacant offices, or allow him/herself to leave the premises undetected in the general confusion if no other way is safely available, or escape imminent discovery as security personnel will be diverted to co-ordinate the evacuation following an alarm. Hence, in the case of an alarm going off that requires the evacuation of a

building, all occupants must be assembled in a controlled secure area (muster area) at a safe distance from the building and accounted for. (Data from the control access system may help in the accounting of evacuees). Care must be taken not to allow individuals remain behind or re-enter the building, both for their safety and for security reasons. Security must be aware of any individuals leaving the building long after the rest of the people were evacuated. In such an event, the late evacuee must be securely identified and the reasons for his/her delay be fully justified. This event should be dealt with as a potential security breach and logged appropriately at the security incident-reporting center. Following evacuation particular attention must be paid to evacuated visitors who should have their IDs re-confirmed before being allowed to leave the muster area.

Control 9.1.5 "Working in secure areas" calls for physical protection and guidelines for working in secure areas. The guidelines presented here apply to employees, subcontractors and collaborating third-party employees and cover four major areas of security that, although not designed with SE exclusively in mind, may play a major role in relation to SE attacks. Guideline 9.1.5(a) stresses that secure areas and activities related to those areas should be covered by the "need-to-know" principle. This minimises the possibility of information regarding secure areas being disclosed to attackers by unsuspecting employees. Guidelines 9.1.5(b) and 9.1.5(c) respectively suggest that work in secure areas should be supervised and that vacant secure areas should be locked and monitored. If implemented, these two guidelines will definitely place yet more obstacles in the way of the attacker who has already penetrated the outer perimeter. Finally, guideline 9.1.5(d) proposes that recording devices of every form should not be allowed on the premises. Barring such devices from the secure perimeter is quite difficult given the current miniaturisation of such equipment. However, it is very important to attempt to control their use, as video recording devices may very effectively be used in the preparatory phases of a SE attack. Such use could include capturing location data useful for analysis before the major offensive takes place. Even during the offensive, recording devices in mobile phones or

other mobile equipment may be used to store sensitive data and thus smuggle it out of the organisation's premises.

All of the guidelines presented in control 9.1.6 "Public access, delivery, and loading areas" aim at minimising the general risk involved in allowing unauthorised persons to enter the secure perimeter and/or to come in contact with authorised personnel. For SE attackers in particular, this takes away their opportunity to invade the organisation by taking advantage of an area where the security measures are by default relaxed. It is fairly easy to penetrate through such a loading area as the organisation employees working there may assume that the person unknown to them is a member of the delivery company's party and vice-versa. In addition to that, no one will turn down a helping hand when the work is physically intense. To this end, a security officer may be necessary to supervise the procedures and work with the foreman of the delivery party to positively identify all members of the delivery crew.

Control 9.2.1 "Equipment siting and protection" states that "*Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access*". With regards to SE, guidelines 9.2.1(a) "*equipment should be sited to minimize unnecessary access into work areas*" and 9.2.1(b) "*information processing facilities handling sensitive data should be positioned and the viewing angle restricted to reduce the risk of information being viewed by unauthorized persons during their use, and storage facilities secured to avoid unauthorized access*" should be able on their own to ward off the SE technique of "shoulder surfing". Through careful placement of equipment and by being aware of their surroundings, employees at work may thus effectively prevent an attacker from casually observing their monitors and keyboards. Technical measures can also be employed such as special filters that limit the viewing angle of computer monitors. The rest of the guidance in this section mostly deals with the physical protection of equipment and there is also one last guideline to

avoid interception of sensitive information due to equipment emanations (electromagnetic or other).

Control 9.2.2 "Supporting utilities" deals with the necessity of protecting equipment against failures in supporting utilities. To the guidance presented in this section it should be added that the supporting utilities should themselves be well protected against intrusion to the maximum extent. If the installations of the supporting utilities are not within the secure perimeter, they may be targeted by a Social Engineer, in an attempt either to cause a diversion by means of the ensuing disorder or to mount a "sting" operation in which the attacked will turn to the attacker for help and support.

Control 9.2.3 "Cabling security" continues in the same mentality as 9.2.1 and 9.2.2 by offering adequate protection for cables of all sorts and types. Regarding SE attacks, unprotected cabling can be interfered with to mount a "sting" operation or attach devices in critical points to eavesdrop or inject modified signals to serve the attacker's purpose.

Control 9.2.4 "Equipment maintenance" ensures the equipment's uninterrupted availability and integrity. It is of paramount importance to ascertain that only previously screened and authorised personnel, either internal or external to the organisation, holding appropriate security clearance is allowed to carry out maintenance tasks. By implementing such controls, it will be virtually impossible for a Social Engineer to present all proper credentials and impersonate an authorised maintenance person.

Control 9.2.5 "Security of equipment off-premises" deals with maintaining information security when equipment is taken outside the secure and controlled perimeter of the organisation.

It goes without saying that when the object dealt with in the organisation calls for extremely sensitive information to be handled, the risk of taking and/or using equipment off-site can not be fully mitigated. For this purpose, classified

equipment must not be taken off-site for any reason except appropriately authorised official transportation and even in that case all necessary precautions must be taken to avoid loss of or damage to the equipment. Additionally, remotely working with highly classified data should be considered unacceptable unless through risk assessment and vulnerability mitigation has been carried out.

For the majority of the cases though, where working outside the organisation's premises is allowed, official equipment may well be targeted by individuals seeking to gain access to the organisation's information. Equipment may be stolen and "shoulder surfing" in an unprotected, open to the public, environment is quite easy. When equipment is stolen, the material loss can be significant but even more important is the compromise of the information contained within the stolen equipment. Even that is relative though. If the theft is a random incident, then there is a chance that the information per se will not appear as valuable to the thief who will swiftly try to get rid of the hot property in his/her possession. In that case, the hard disk containing information will be re-formatted at some point and the original information cleared. In most cases, the person on the receiving end of the stolen equipment will neither have knowledge of the nature of information previously contained, nor attempt to reclaim it by using specialised software. There are cases though when the thief will try to extract personal sensitive information, such as credit card data etc, from the equipment. The worst case scenario though would be for the theft to not have occurred randomly but after careful planning, with the ultimate goal of gathering enough information from the stolen equipment to mount an attack against the organisation. In order to protect information from unauthorised access in cases where equipment is stolen -or even lost- there is only one way to do so and that is through the application of password protection and encryption techniques on critical data. Fortunately, there are many applications supporting such solutions available on the market today and even custom ones could be created if there is a justified need. Encryption techniques should thus be added to the guidelines of control 9.2.5 as an extra

measure capable of protecting information if the equipment falls into the wrong hands.

When working in public areas, the user must be on the lookout for vulnerabilities that may compromise the security of the organisations' information. The user's choice of a location to work on a portable computer or even his/her posture while working may have a definite and significant effect on a potential attack attempt. Furthermore, resources that are available on that location, such as WiFi hotspots etc, should not be trusted. It is only recently that a new method of operation, which is now officially classified as a Social Engineering *modus operandi*, was identified (Thomson, 2006). The "Evil Twin" method as it was dubbed, uses fake wireless access points to steal personal information from unsuspecting users. The fake wireless access point is placed near a commercial hotspot and is given the same name as the original hotspot. Thinking that the original hotspot is serving him/her, the unsuspecting user logs-on to the fake hotspot. Subsequently, the generated traffic is monitored and recorded to extract personal information. Such installations were found in international airport lounges and there have even been reports of the victims' computers being remotely hacked. This is obviously a threat that would be rather difficult to implement within a secure perimeter but quite feasible to realise in a more security-wise relaxed environment. This proves that users can not be complacent regarding the secure use of their equipment. What can be a secure practice in one environment may prove to be quite the opposite in another.

Control 9.2.6 "Secure disposal or re-use of equipment" enforces removal or safe-deletion of sensitive data and software contained in equipment that is to be disposed of or re-used. It is imperative to sanitise equipment for disposal or use a secure deletion method for re-use as the data contained in the equipment may easily end up in the hands of a Social Engineer via the organisation's dumpster or through a recycling facility. To take things one step further, perhaps garbage or material for recycling should even be checked for security issues before being dumped. This should not apply to disposed

equipment only but to documents and anything else that might carry sensitive information. Re-use holds its own dangers as, after sanitisation, once classified equipment may be de-classified and put to good use in another part of the organisation where the classification of information and the level of security are lower. If sanitisation has not been carried out properly, sensitive data may eventually leak through unclassified channels.

Control 9.2.7 "Removal of property" should logically precede control 9.2.5, as it defines under what circumstances, equipment, information or software should be taken off-site. By following precise procedures for removal of the above assets by positively identified and authorised personnel, a Social Engineer has fewer chances of getting away with removing such assets or convincing an employee to do this for him/her. Hence, this control is another step in the right direction in the fight against SE.

C.6. Section 10 - Communications and Operations Management

Relevant security categories:

- Operational procedures and responsibilities
- Third party service delivery management
- System planning and acceptance
- Protection against malicious and mobile code
- Back-up
- Network security management
- Media handling
- Exchange of information
- Electronic commerce services
- Monitoring

Section 10 of ISO 17799 deals with a) the "*correct and secure operation of information processing facilities*" (section 10.1 of ISO 17799), b) the implementation and maintainance of the "*appropriate level of information*

security and service delivery in line with third party service delivery agreements" (section 10.2 of ISO 17799), c) minimising the risk of system failures (section 10.3 of ISO 17799), d) protecting the integrity of software and information (section 10.4 of ISO 17799), e) maintaining "*the integrity and availability of information and information processing facilities*" (section 10.5 of ISO 17799), e) ensuring the "*protection of information in networks and the protection of the supporting infrastructure*" (section 10.6 of ISO 17799), f) preventing "*unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities*" (section 10.7 of ISO 17799), g) maintaining the "*security of information and software exchanged within an organization and with any external entity*" (section 10.8 of ISO 17799), h) ensuring the "*security of electronic commerce services, and their secure use*" (section 10.9 of ISO 17799) and i) detecting "*unauthorized information processing activities*" (section 10.10 of ISO 17799).

Control 10.1.1 "Documented operating procedures" calls for common procedures that are comprehended and followed by the employees involved in them. Obviously, documented procedures offer an elevated degree of protection from internal as well as external dangers and are thus indirectly related to SE attacks, but there are a few finer aspects described in the guidance offered in 10.1.1 that bear direct relation to SE. First, "*mail handling management*" is mentioned as being one of the procedures that need to be documented. This is important as a Social Engineer may target the mail room to remove mail items, insert new mail items or intercept and alter mail items. Organisation stationery can be stolen for later use, messages may be inserted to prepare the ground for the main attack etc. In guideline 10.1.1(e) it is stated that operating procedures should include "*special output and media handling instructions, such as the use of special stationery or the management of confidential output including procedures for secure disposal of output from failed jobs*". Failed job outputs that are not disposed of properly according to security regulations and the level of confidentiality of the information that they contain, may end up in the hands of the Social Engineer during "dumpster diving" missions. Even fragments of jobs that only contain partial information

can be of value in the context of a SE attack. Again, the matter of security-wise control of disposed materials, would add to the level of protection of information. 10.1.1(e) asks for the documentation of the procedure for contacting support in case of unexpected operational or technical difficulties. This is very important in order to prevent "reverse sting" operations.

Control 10.1.2 "Change management" speaks of the need for controlling any changes to information processing facilities and systems. If there is lack of such strict control, malicious software created by a hacker may find itself installed in an operational system. This can be accomplished in the context of a SE attack whereby the administrator/supervisor -or even a simple user in some cases- is convinced to install the software as a necessary patch, problem-solving solution etc.

Through the "Segregation of duties" described in control 10.1.3, the risk of deliberate or accidental system misuse and/or compromise of information is reduced by ensuring that no single person can actually affect information assets. As such, the Social Engineer's work instantly becomes more difficult as there are more than one employees that need to be targeted and convinced to act in a way that will eventually lead to a successful attack.

By the "Separation of development, test, and operational facilities" described in control 10.1.4, the chances of the operational facility being compromised as a result of a SE attack, are reduced during the development of a new system. As many individuals, external to the organisation, unavoidably find themselves involved with various aspects of a system in development, it is by definition more difficult to uphold the required level of security in relation to the system being developed. Hence, a Social Engineer may target the system under development in order to gain access to the operational system. This becomes more difficult through the separation of the two systems.

Section 10.2 "Third party service delivery management" ensures that third parties continue to uphold the terms of their agreements in terms of service

and information security. It could be argued that the controls presented in this section do not have a direct relation to SE attacks in particular. However, these controls help in seamlessly interfacing the organisation's security policy to those of the collaborating third-parties. Effectively, having an as common as possible security policy, will help in countering SE attacks. Most importantly, guideline 10.2.2(c) "*provide information about information security incidents and review of this information by the third party and the organization as required by the agreements and any supporting guidelines and procedures*" effectively ascertains that a security incident caused by a SE attack that targeted the third party in an attempt to compromise the security of the organisation's information, will raise all necessary alarms, both within the organisation and the third-party structures, in an attempt to block any further phases of the attack.

Section 10.3 "System planning and acceptance" offers guidance in order to minimise the risk of system failures through sound capacity management and system acceptance practices. Though not directly related to SE, it helps avoid emergency situations that well-informed Social Engineers may benefit from.

The controls of section 10.4 "Protection against malicious and mobile code" serve the obvious cause of protecting the integrity of system, software and information against malware. Through a repertoire of attack types, Social Engineers may convince a targeted employee into installing a piece of software on the system, thus compromising system security. Hence, the directives of controls 10.4.1 "Controls against malicious code" and 10.4.2 "Controls against mobile code" do indeed create a line of defense against such threats. There are however issues with the guidelines as, for instance, guideline 10.4.1(c): "conducting regular reviews of the software and data content of systems supporting critical business processes; the presence of any unapproved files or unauthorized amendments should be formally investigated". Taking into consideration the thousands of files installed on a single system, that are necessary to support a large number of applications from different developers and vendors, it is probably futile to attempt to

identify every single file and verify its function. In theory, it might be helpful to try and locate suspicious files but in practice even this is becoming increasingly difficult. Further on, it is stated that "*The use of two or more software products protecting against malicious code across the information processing environment from different vendors can improve the effectiveness of malicious code protection*". It is well known that antivirus and "internet security" software products from different vendors are rather intolerable of one another and most even ask the person performing the installation to remove other software of the same type before proceeding. Even false alarms and lockups can take place if more than one such products co-exist on the same system. Hence, this guideline should be taken with a grain of salt. Two (or more) pieces of protection software could co-exist on the same network provided that they do not execute on the same processor. This arrangement could possibly result in the benefits described in control 10.4.1 but the effort in keeping two or more such products updated may not be worth it. This is especially true if the products execute within the confines of a network that has no Internet connections for security reasons.

There is a further complication regarding the use of commercial software to control malicious and mobile code and that stems from its limitations. The very nature of common computer virii, worms, malicious Java scripts etc is such that they all constitute malware which propagates indiscriminately, infesting any unprotected system. Hence, when a new virus is located, the antivirus software houses identify its characteristics and add it to the list of mitigated threats. This list then is passed on to the antivirus software users through a mechanism of updates. However, when a particular organisation (or even individual) is targeted by a Social Engineer, chances are that the malware implanted in the system through SE techniques will be a new and unknown piece of software that will never become "mainstream" enough to cause the attention of the antivirus software houses. Even though antivirus and related software do use heuristic methods to identify misbehaving pieces of software that are unknown to them, this offers little protection as there exist programming tricks that can be employed by the malware author to avoid

detection of the malicious code. Furthermore, a clever attacker would implant a low-profile piece of software that silently works in the background without being detected. This is quite different from the "show-off*ish*" behaviour of mainstream malware. Hence, although the use of antivirus and anti-malware software is essential, it does not solve the full extent of the problem. Thus, it is once more proven that steps must be taken in the direction of building up psychological user defenses against SE attacks, rather than trying to identify and rectify the problems caused by a successful one. This, however, does not devaluate in the least the need for protection against malware.

Control 10.5.1 "Information back-up" provides guidelines for effective and secure back-up procedures. Especially guideline 10.5.1(h) that calls for encryption of back-ups when the backed-up data is classified, helps secure the data carried on a back-up set if the set is stolen. As backup sets are always high on the list of infiltrators since they contain the most important data in a space-efficient way, rendering them useless is very important.

Section 10.6 "Network security management" provides guidance for ensuring the protection of information in networks as well as that of the supporting infrastructure. As is true for most security controls, the ones presented here do not have a direct relation to the issues involved in SE. Control 10.6.1 "Network controls" could benefit from the addition of guidelines stating: "Networks must be classified according to the classification of information passing over them" and: "Networks providing Internet access to users should be classified at the lowest level".

Regarding connections between networks there must be at least two guidelines: "Routing equipment must only be used to connect networks of the same classification" and: "Connections between networks of different classifications must be established only if business processes demand it and only through appropriate Firewall equipment". An exclusion from the above guideline would be: "When the level of classification of a network demands it,

the network should be physically isolated from other networks of lower classification (even connection through Firewall equipment is not allowed)".

Furthermore: "Only equipment of classification equivalent to that of a network can be connected to that network" and: "Computer equipment in general and workstations in particular, must not be physically connected to more than one networks at any time. Moving the physical network connection of equipment from one network to another is forbidden. Firewall and routing equipment is excluded from the above directives". A connection established in defiance of the above directives would function as an unauthorised bridge between the two networks and must not be allowed. If there is a general need that has been properly justified for users' workstations to be simultaneously connected to two different networks and the classifications of the two networks allow it, then the bridging must take place at a central level using proper router and firewall equipment. Such an implementation must first undergo a full security examination to identify and mitigate relevant risks.

Finally, a guideline concerning network outlets should be added: "Measures must be taken to ensure that network outlets are protected against unauthorised use by centrally deactivating unused outlets and by locking active outlets to the authorised equipment that uses them.

Perhaps the reason that networks have not received much attention regarding their classification is that until recently, it was not financially sound or even feasible for an organisation to install and maintain a number of different network backbones, each classified at a different level. By realising the severity of the threats to the network that could materialise through a single networked user's connection to the Internet, an increasing number of organisations opt for physical separation between backbones. This requirement becomes more prominent as the classification level of information transmitted on the network, rises. In this case, it is not just the Internet that constitutes a potential threat but rather the potential of unauthorised access form within the organisation becomes a calculable risk. The concern is such

that in some cases (Government services, for example) even VPN realisations may seem inadequate. Hence, physical separation may prove to be the only solution. This physical separation should not be compromised by PCs or other equipment connected to more than one networks (simultaneously or not) that could act as an uncontrollable bridge between them. Apart from the danger of creating a transfer path for common malware between the two networks, if the PC is simultaneously connected to the two networks, using two network interfaces, real-time bridging may occur. If there is only one network interface on the PC and the PC is connected to the two networks at different times, delayed-action information leaks may take place by first obtaining data from one network and then passing it on to the other network when the physical connection is switched. Through the use of DHCP, such a scenario would not require much effort on the part of the attacker. It is conceivable that a legitimate user could be persuaded to do such things by a manipulative Social Engineer posing, for instance, as a help desk member.

Section 10.6.2 "Security of network services" is necessary to ascertain the level of security offered by network service providers. As network service security is tightened, the Social Engineer has fewer opportunities to strike.

Section 10.7 "Media handling" provides precise guidance for ensuring that information-bearing assets should not be disclosed, modified, removed, or destroyed in an unauthorised way and that business activities should not be interrupted. If the proposed controls are in place, a SE attack targeting media or system documentation will most probably not succeed.

Section 10.8 "Exchange of information" provides controls for maintaining the security of information exchanged within an organisation as well as with any external entity. By specifying policies and procedures to protect the exchange of information through any and all communication channels available, including physical transfer, and by applying the need-to-know principle to the bulk of the information being exchanged, the possibility of information leakage in general or -more specifically- as a result of a SE attack, is minimised.

Regarding the use of fax machines in particular, one should always bear in mind that a fax-id may be faked and that there is no automatic acknowledgement system in place. The "OK" indication received at the end of the transmission does not automatically mean that the designated recipient has already read and properly processed the faxed message. In addition to all the precautions outlined throughout the controls of section 10.8, vocal communication and confirmation at pre-designated telephone numbers should follow either the transmission or the reception of significant documents. Even in that case a faxed copy is not considered a legally-binding document in most parts of the world. At least, though, a Social Engineer's attempt to impersonate the other party in communication by fax will have failed. A partial solution to the problems associated with faxed documents may be achieved through the use of dedicated encrypting equipment. Such encryptors are connected between a standard fax machine and the PSTN telephone line and are pre-set to communicate in a secure manner, only with equivalent setups in other locations. Through the use of shared keys, no outsiders may intercept transmitted documents or inject fabricated ones into this secure ring. Despite the obvious drawbacks that have to do with key creation and distribution, increased cost of equipment acquisition and maintenance and the fact that secure communication is limited to a specific number of destinations, such a system can be considered quite secure from a SE point of view. The aspect of availability does suffer and makes the system impossible to view as a universal solution, but otherwise, this encryptor-based system does uphold the confidentiality, integrity and non-repudiation aspects of security.

Sections 10.9 "Electronic commerce services" views the problem of security from the side of the organisation implementing the electronic commerce (section 10.9.1) and On-line services (section 10.9.2). However, the risk here is no longer associated only with the organisation side. Through SE methods over email or otherwise, key-loggers may be installed on the client's side to record and transmit keystrokes that reveal passwords, personal information etc. Furthermore, another very popular SE technique, "phishing" can be very

successful in extracting personal information, passwords etc and may potentially lead to full-fledged identity theft. The organisation involved with providing electronic commerce and on-line services may not be held directly or legally responsible as there is no way of controlling what types of malware are being executed on the client's PC or to which SE attacks the client may have succumbed. However, it is imperative that all organisations dealing on-line with their business partners or the general public, take all precautions to help uphold the security of both ends of the communication line. Such precautions may include splash screens with warnings about spyware and instructions on how to uphold the security of the transaction through SSL, the use of on-screen "soft" keyboards for sensitive data entry that can not be logged by the key-logging routines of spyware, the issue of One-Time Password (OTP) devices to be used by registered clients (for web banking services, for instance), directed emails about fraud on the Web and phishing attempts, the use of asymmetric cryptographic keys for encrypted point-to-point communications etc.

Section 10.9.3 deals with the integrity of publicly available information. If a Social Engineer manages to modify such information, he/she may then use it as a confidence-building tool in an attack targeted towards another Mark. For example a victim could easily be fooled by being told by the Social Engineer to address a reply containing sensitive information to " mr. So-and-So whose name and telephone number appear on the organisation's official web page". If the page has already been compromised to reflect the Social Engineer's preferred phone number or email address, the attack is more than likely to be successful.

Section 10.10 "Monitoring" is only indirectly related to SE. Even in that case its value is limited to a "post mortem" analysis of what has transpired in the course of SE attack. This section stresses the need for logging user activities, system use, system administrator and system operator activities, faults and information security events with as much detail as possible. Furthermore, all systems should be synchronised so that their logs are synchronised too and

log files should be adequately protected against tampering. Clearly, if the logs are to be of any value, their integrity must be ascertained. If log entries are deleted, modified or added, it may be feasible that the real guilty party gets away with the crime and an innocent individual takes the blame. Hence, log integrity is of paramount importance. By regularly examining log files with the use of specialised software, secure system operation may be warranted to an acceptable degree and perhaps attacks in progress may be identified and interrupted. Even if this is not the case, the sooner the problem is identified, the better the chances of containing the damage are.

C.7. Section 11 - Access Control

Relevant security categories:

- Business requirement for access control
- User access management
- User responsibilities
- Network access control
- Operating system access control
- Application and information access control
- Mobile computing and teleworking

Section 11 deals with a) the creation of an access control policy which is based on business and security requirements for access (section 11.1 of ISO 17799), b) ensuring authorised user access to information systems and preventing unauthorized access to them (section 11.2 of ISO 17799), c) the prevention of unauthorized user access to the information system and the upholding of information security by assigning responsibilities to users (section 11.3 of ISO 17799), d) the prevention of unauthorized access to networked services (section 11.4 of ISO 17799), e) the prevention of unauthorized access to operating systems (section 11.5 of ISO 17799), f) the prevention of unauthorized access to information held in application systems (section 11.6 of ISO 17799), g) the upholding of the level of information

security dictated by the security policy when mobile computing and teleworking facilities are used (section 11.7 of ISO 17799).

Before proceeding with the discussion of the individual controls presented in this section, the reader needs to be reminded that Social Engineering methods aim to provide the attacker with authorised access to a system through a manipulated legitimate user rather than bypassing the enforced access control measures.

The control discussed in 11.1.1 "Access control policy" aims at creating an access control policy that serves as a rule-book for dispensing access rights to users, depending on business and security requirements. The policy must be kept current with frequent reviews in order to reflect the true needs of the organisation.

Especially guidelines 11.1.1(h) and 11.1.1(i) may help to fend-off a Social Engineer seeking authorised access to the system. In particular, by segregating the roles of access request, authorisation and administration, it becomes difficult for the SE to successfully carry out attacks against all of the role bearers in order to gain authorised access to the system. In conjunction with the segregation of roles, if the requirements for "*formal authorisation of access requests"* are defined and upheld under all circumstances, a Social Engineer's attempt to exercise pressure or otherwise convince an administrator to grant him/her access will be doomed to failure as such action on the part of the administrator will simply not be prescribed in the formal procedures. Although an approach based on the attacker's impersonation of a legitimate user who needs access to a system is thus effectively mitigated, other, rather indirect attacks that aim in making the person responsible for controlling access to the system yield to the attacker's demands, are still quite possible. The exercise of authority, for example, and possibly intimidation, may bend the resistance of an employee fearing for his/her future in the organisation. If such is the case, the whole system of controls will, in fact, collapse. Thus, as it has already been mentioned, the main line of defense

against such SE approaches rests solely on the existence of a sound security mentality within the organisation, one, though, that does not turn into an obsession with security as this will, in itself, ultimately lead to extreme situations.

Section 11.2 deals with "User access management", i.e. ensuring that authorised users are granted access to the information system and preventing unauthorised users from gaining access to it.

In particular, control 11.2.1 governs the procedures of registration and de-registration of users. Most importantly, guideline 11.2.1(a) provides for the assignment of responsibility to the users for their actions. This is accomplished through the creation of personal, unique and non-re-useable accounts. Hence, solid, auditing trails can be obtained and non-repudiation issues can be automatically resolved. One issue of the same guideline that generates some reason for concern, is the creation of group IDs and passwords. This potentially constitutes a major vulnerability as by sharing a common account and password, the responsibility for malevolent actions through that account is diffused to more than one individuals. If a security breach does take place under such conditions, it is always a major source of anxiety for all members of the group. Also, the larger the group, the more difficult it is to pinpoint the guilty member(s). In guideline 11.2.3(a) users are prompted to "*… keep group passwords solely within the members of the group; …*". In the mind of the author, it is futile to have such a statement, as a group member who, for any reason, has compromised the group password, can easily deny the fact, given that the account details are common knowledge among a number of people. The age-old truth about shared secrets not being secrets, definitely holds strong in this case. Allowing for some rather specialised forms of support and maintenance structures, as far as ordinary users are concerned, there is no need whatsoever for shared, group passwords. Given the abilities of modern authentication systems, each group member can have a personal (truly secret) password and be assigned individual and group rights and responsibilities upon login. The complications

of having group passwords do not end here, as such passwords have to be reset when a group member leaves the group for any reason. Such a reset will involve the formal notification of all group members and will also call for acknowledgements to be returned that must also be administratively processed, i.e. logged, securely archived etc. It can thus be seen that from a purely administrative point of view, such action may become very quickly, very complicated. Administrative difficulties put aside, a Social Engineer can more easily persuade a target to disclose a group password than a personal one as the sense of ownership of a group password is weaker than that of a personal one. Furthermore, the password of a group of which the target is no longer a member, may seem to the target as of a security-wise lesser value and be given out with fewer reservations.

Guidance 11.2.1(b) that calls for separate authorisations from the system owner as well as Management in order to be granted access to the system may impede an SE attack, as multiple targets create a greater chance of failure.

Directives 11.2.1(d) and (e) regarding issuing written statements to the users outlining their access rights and requiring them to sign appropriate documents, assists in creating and maintaining a security culture. By following directives 11.2.1(h-j) and controlling redundant accounts and IDs, "loose ends" do not exist for a Social Engineer to take advantage of. Dormant accounts are always targeted by Social Engineers and hackers alike, as they are not regularly monitored -if monitored at all- and can provide an efficient back door to the secure perimeter. Disgruntled employees may use their own accounts that were not deactivated upon their departure themselves or unreservedly release that information to a Social Engineer that approaches them. Even more seriously, if the disgruntled employee used to have high-level access to the information system, he/she may have succeeded in creating supplementary accounts for him/herself that remained unused, just in case of such an eventuality. This is another major issue that dictates the segregation of system administration duties which has already been

discussed. If such segregation exists, then no individual can act uncontrolled and single-handedly create accounts.

Section 11.2.2 concerns "Privilege management" and attempts to minimise the need for privileged users on the system. In directives 11.2.2(d) and (e) a prime example of technical controls that effectively mitigate a non-technical vulnerability is given. This is achieved through a) the implementation of system routines that help avoid granting privileges to users and b) the use of programs that avoid the need to run with privileges. Thus as the need for privileged use of the system is minimised, a Social Engineer may not take advantage of such privileges to compromise the security of the system.

Control 11.2.3 provides directives for "User password management". Apart from the references to group passwords that are made in 11.2.3(a) and which have already been discussed, the remainder of the section's directives provide a very solid foundation for the protection of passwords. Especially important is guidance 11.2.3(c) that calls for established procedures for verifying the user's ID in cases of requests for new or temporary passwords. It effectively deals with a very common method of SE attack whereby the attacker attempts to prove his/her ID through references to other employees or by bringing up facts and details internal to the organisation, or even by persuading another employee to vouch for him/her. A solid identification procedure eliminates such risk. As an addition to the directives presented in this section and in the context of building psychological controls against SE attacks, apart from the official exchange of signed statements and agreements regarding passwords, users should also be given informative material on the importance of keeping passwords secret. This should include guidance on how to defend themselves against SE attacks, preferably through discussed examples of such attacks. This should only be the first step in building the necessary security culture.

If the guidance of control 11.2.4 "Review of user access rights" is followed, then it should be made reasonably certain that the rights and privileges of

users do in fact remain current and are solely dictated by the needs of the users' assignments. If obsolete user rights and privileges remain active, they may indeed be discovered by attackers by means and in ways that have already been discussed.

Section 11.3 "User responsibilities" makes clear that the co-operation of authorised users is essential if the security of the information is to be upheld.

In 11.3.1 "Password use" a set of instructions for the secure use of passwords is presented. Directives 11.3.1(b): "*avoid keeping a record (e.g. paper, software file or hand-held device) of passwords, unless this can be stored securely and the method of storing has been approved*" and 11.3.1(g): "*(do) not include passwords in any automated log-on process, e.g. stored in a macro or function key*" in particular, if implemented will impede the work of a Social Engineer who has entered the security perimeter. If there is neither a written record of the password, nor has the password been saved in the form of a macro etc, then the attacker can not make use of e.g. an unattended workstation to gain access to the system. Directive 11.3.1(e) calls for the "*change passwords at regular intervals or based on the number of accesses (passwords for privileged accounts should be changed more frequently than normal passwords)…*". Apart from its obvious value in upholding the security of a system by regularly resetting compromised passwords, this guideline should be extended to call for the automatic and system-wide disablement of passwords of dormant accounts. Although dormant accounts should not really exist in a well looked-after system, there is always a chance that such a case may occur as people sometimes make use of long-term leaves of absence etc. If passwords are disabled after a reasonable time of account inactivity, the dormant accounts are effectively locked down and thus made unavailable to attackers. The authorised user may at any given time, upon his/her return, re-apply for a new password to his/her account and go through any authentication processes that are deemed necessary. Although the proposed scheme may sound as a "belt-and-braces" solution, it is easy enough to implement in any modern information system and the benefits from its

application should be evident. Another very important directive is 11.3.1(i) that dictates to "*not use the same password for business and non-business purposes*". If the same password is used on multiple systems by a user, then the security of that password is only as good as the weakest system the password is used on. If one system is compromised and the password falls into the hands of an attacker, then access to the other systems may be gained, leading to the compromise of their security. Especially passwords used on the Internet should never be used on classified networks. As users tend to want to remember one simple password for all cases where login is essential, an interesting form of attack has been appearing through email "spam". Although not exactly "Phishing", whereby the target is fooled into entering his/her login information to a replica site pretending to be a valid one of which the target is an authorised user, this attack lures unsuspecting users by promising free software, screensavers, MP3s etc. The only prerequisite for the free download, is that the user first has to create a personal account with a user name and password. Although the free downloads do not carry a malicious payload, this form of attack can be very dangerous as it is built around one purpose: to have the visitor register and provide a username and password that might match those used on a business system. Obviously, this method would not be effective if the original emails were blindly sent to random recipients. However, if the attacker is targeting the Information System infrastructure of a particular organisation and finds him/herself in need of a user name and password, then the method's virtues become apparent. All that the attacker needs to do is to target the employees of the organisation via email. Chances then are that in a very short time a valid pair of user name and password entries would be produced that would enable the progress of the attack.

Control 11.3.2 deals with the issue of "Unattended user equipment". Assuming that an attacker has managed to break into the secure perimeter of the organisation, his/her next target would be to gain access to the system. Unattended equipment, especially equipment in the middle of a process that requires privileged access to the system would give the attacker ample

opportunity to carry out the goal of creating a secret, privileged account on the system and/or install software appropriate to his rather special needs. The guidance presented in this control is sound and the control can be further enhanced by technical controls as they appear on the market. One solution is provided by smart-card controlled Ultra-Thin Client equipment (Sun Microsystems, 2003). These work on a principle that requires the user to insert a cryptographically-protected smartcard (Schneier, 1996; Frangopoulos & Venter, 2004) that is uniquely encoded for him/her and further protected by a PIN. When the card is presented to the reader on the Ultra-Thin Client equipment, the client first has to check the validity of the card in order to allow the user to then go through the authentication process. If all is well, a session is created for the user on a special server that serves the Ultra-Thin Clients. When the user leaves the Ultra-Thin Client he/she may choose to leave the session running. All that needs to be done is to remove the user's smartcard from the Ultra-Thin Client reader. As the Ultra-Thin Client equipment is virtually stateless, the client is released for the next user while the original user's session is kept running on the well-protected server. As soon as the original user inserts his/her card on any other Ultra-Thin Client, the original session is brought to that client. This "session-mobility" feature makes the Ultra-Thin Client especially safe when it comes to SE attacks as, in order for the equipment to be used in *any* way, a valid smartcard must be inserted in the Client along with its authorised user's PIN. As the Ultra-Thin Client has no local storage space in the form of a hard disk or otherwise, even in the improbable event that an attacker does gain access to it or disconnects and steals it (!) there is no information on it that can be compromised. Thus, clearly, such an implementation provides a very effective control against a critical phase of a type of SE attacks. Another technical measure for the rather non-technical issue of the absent-mindedness of users can be implemented through the use of proximity devices that lock the PC equipment when the authorised user is more than a few meters away. This device is made up of a cryptographically authenticated pair of transmitter - receiver. The receiver is always connected to the PC and controls access to it through secure authentication, cryptography, and/or other methods. If the receiver is not

connected to the PC or when the transmitter is not within a specified range of the PC/receiver, the PC and its contents are locked down and are rendered totally inaccessible. When the authorised user of the PC returns within range, he/she can continue working after providing a personal password to the system. Such a system provides an extra safeguard in case the user forgets to secure his/her PC before leaving for a short period of time. Thus, the window of opportunity for an attacker to take advantage of unattended equipment is greatly reduced if not nullified.

Control 11.3.3 "Clear desk and clear screen policy" calls for the adoption of a clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities. If this is upheld, not much -if any- information will be compromised in the event of a physical intrusion. The directive about not leaving sensitive information unattended on printers is very useful as is the proposition of having access control by PIN, installed on all network printers. Such a provision makes the physical presence of the job owner in the immediate vicinity of the printer essential in order to receive the output. The output can not be released to anyone without the PIN of the print job owner.

Sections 11.4, 11.5 and 11.6 deal respectively with "Network access control", "Operating system access control" and " Application and information access control". The controls presented in these sections are quite detailed and cover a wide variety of network and OS access-related threats in a quite efficient manner. These controls should be adequate to ward-off most if not all attempts by a hacker to gain access to the network, the operating systems it supports and the applications running on it. However, it must be taken into consideration that a Social Engineer would most probably use a lateral method of operation. A Social Engineer would choose to pose as a) an authorised user to administrators, b) an administrator to users or c) a maintenance or support person to either users or administrators. If the controls of section 11.4 are in place and no shortcuts are taken in securely identifying the caller as being who he/she claims he/she is, then the attack will

almost definitely come to an abrupt end. However, the alternative method that the Social Engineer will use in an attack, would most probably be to convince an authorised user / administrator / maintenance person to do the job for him/her. As organisations are re-enforcing their defenses, the SE attacks no longer target the organisations themselves, but rather the users of the organisations. Hence, the users must be exposed to SE methodology if they are expected to recognise SE attacks and efficiently defend themselves and the organisation against them. Users should be trained to avoid any unusual requests that involve relinquishing their system access privileges to *any* other person. Thus, users should be trained to think in a lateral way similar to the one used by the attacker. In such a context, the question of whether the user will outsmart the attacker or vice-versa may arise. If "smartness" were to be measured in terms of IQ or otherwise, then it might be argued that a Social Engineer who is smarter than the average person, would in practice be invincible. This would lead to the question of how to devise a viable defense scheme to outsmart such a person. To answer this question it suffices to consider that the Social Engineer must go to extreme lengths to produce a viable and believable scenario. On the other hand, the person in defense only has to identify those telltale signs that accompany a SE attack and simply raise the alarm. This can only be accomplished through the existence of solid procedures and the education of users on SE methods of operation. Organisation employees should systematically be exposed to the persuasion techniques used by Social Engineers in an attempt to build defenses. To illustrate this, the reader should consider a simple example: A Social Engineer could easily show up at a remotely connected location of the organisation, pretending to have arrived from the central offices on assignment or otherwise, begin chatting with the person at the reception in a confidence-building attempt and eventually -when it would be considered appropriate to do so- ask for access to the organisation's network using the local person's account. In such a case, the fact that another person asked for the use of the receptionist's account -one of the telltale signs of a SE attack- the person manning the reception desk should immediately deny any co-operation and log this as an attack with the appropriate co-ordination security response

office of the organisation. It is hence made evident that although sound and complete, the controls described here do not directly cope with the SE threat.

Section 11.7 approaches the very sensitive issues of "Mobile computing and teleworking". As it has already been discussed, working outside the controlled perimeter of the organisation poses tremendous security risks for the information handled within the organisation's scope. Furthermore, data that may be obtained directly or indirectly through the use of mobile or remote equipment can be used to compromise the very existence of the organisation. The control described in 11.7.1 "*Mobile computing and communications*" attempts to mitigate the obvious risks involved with mobile computing and there is no doubt that it would succeed in achieving this end if its directives are properly implemented. The real issue though is how to establish for a fact that the guidelines are upheld and that the control does indeed function as designed. In this author's mind this is impossible to do as the control deals with locations outside the secure perimeter of the organisation. Hence, by the control's very nature, it is the end user who is ultimately responsible for its implementation, in circumstances that can neither be monitored nor centrally controlled.

The advent of cutting edge technologies such as wireless networks that are swiftly embraced by users and organisations alike, has the potential to create many vulnerabilities. The operational incorporation of new technologies by organisations, in many cases before a scrupulous assessment of the level of security that these technologies provide is even made possible, brings forth many new threats, including those stemming from Social Engineering. The reader is reminded of the "Evil twin" threat that has already been discussed in this context. This is a typical example of the inability of the organisation to centrally control all segments of a communication channel. Even though not directly implemented by the organisation, the incorporation of any wireless network in its operations is indirectly endorsed if access to an internal network of operational significance is allowed to the organisation's users over the Internet. The average user can not really be held responsible for using a

technology that is available to him/her, especially if there is no contra-indication to its use. Before the "Evil twin" method, no one would have thought of the possibility of such a threat. Even before that, the security level of wireless access points had been repeatedly thought of as adequate, then challenged and subsequently upgraded many times. The result can be seen in the number of successive standards concerning the level of security of wireless connections. The same holds true for mobile telephony. A long distance has been covered in terms of security since the days of analogue mobile communications in North America until present day digital mobile systems where complicated encryption schemes are employed and are continually being challenged and upgraded. Through the use of SSL and VPN technologies, it is arguably true that any insecure channel can be used for secure communication. However, as these technologies are primarily based on asymmetric cryptography, their effectiveness is constantly being challenged. Furthermore according to the UK's Department of Trade and Industry Information security breaches survey (2006), in 2006 40% of the companies that allow staff to connect via pubic wireless hotspots do not encrypt the transmissions. Whether this lack of encryption is due to unavailability of funds, incomplete security policy or lack of in-house know-how is irrelevant. The "bottom line" is that information is handled over insecure networks that the end-user can not control and, under the circumstances, can not be held responsible for.

Control 11.7.2 "Teleworking" deals with the necessary policy, plans and procedures that must be in place to allow security to be upheld while personnel members are working remotely from a fixed location outside of the organisation. All of the guidelines presented in this section deal with physical security, access to the equipment, antivirus protection, the restrictions and provisions of home equipment, backups, business continuity etc. However one issue is not sufficiently addressed, and it has to do with the technological infrastructure that has made teleworking as we perceive it today, possible. It is the proliferation of high-speed connections at home as well as at the workplace that has made teleworking a viable method of working for a

continually increasing number of employees. In the past, teleworking was indeed possible, but the nature of work being done was dictated by the telecommunication equipment and channel limitations. Teleworking used to be ideal for business fields where live information was not essential. For instance, a translation company teleworking employee could send and receive assignments through a direct connection to a company Bulletin Board System (BBS) via modem. With the proliferation of the Internet, email replaced the BBS. Again though, the exchange of information was more or less time-limited to the beginning and the end of the work transaction. Today, broadband connections allow users to communicate from home via voice and live video-conferencing, as well as have an uninterrupted bi-directional high-speed flow of data between their location and the organisation's head offices. Technical methods can also ensure the security of the exchanged data. Hence the security issue is shifted to the employee's remote workplace. This can make the employee's home-office the target of the Social Engineer who regards it as the "soft underbelly" of the organisation. Interestingly, there is no mention of Social Engineering attacks or appropriate countermeasures in section 11.7.2 and the control would greatly benefit from such an inclusion.

Additionally, broadband Internet connections can both be considered as a blessing and a curse. A blessing because of the new horizons that such fast connections allow the user to explore and a curse because of the vulnerabilities they may carry, many of which can certainly be related to SE. In the National Institute's of Standards and Technology Special Publication 800-46 (2002), a 113-page publication solely dedicated to the "S*ecurity of telecommuting and broadband communications*", the increased risk of broadband connections is attributed mainly to the increased duration of the connection when compared to simple dial-up connections and to the semi-permanent and static IP addresses that some broadband services provide on demand from their users for activities such as on-line gaming and web server hosting. A static IP may allow an attacker to target a specific user, aiming at gaining access to the organisation the user is teleworking at. A Social Engineer can launch a phishing attack that is custom-made to compromise

the specific target's personal information by imitating the look of official login pages etc. Such a phishing attack will be virtually undetectable by security software as such software needs to be alerted to the existence of the attack before including its signature to the list of threats it protects against. This is impossible for a one-off case. When the IP address is dynamically allocated, one might assume that a specific attack is not possible, which is largely true. The threat in that case comes from random attacks and simply stems from the fact that the computer will stay turned on, using the same IP address, on average for longer periods of time than what would be the case for a computer with a dial-up connection. Even worse, the computer might be left connected and unattended for long periods of time, either in an idle state or during download of large files. The random attacker thus has ample opportunity to compromise the targeted computer.

During the past decade, emerging technologies in the field have had mainly to do with mobile computing and communications techniques and equipment, and have enabled communication in all forms to become faster, cheaper, richer in content and to an increasing extent released from location constraints. This rapid emergence, caused and fueled by the innate need of our race to communicate with one another, has changed the way we view the concept of work. This change has generated significant societal and economic repercussions, the long-term effects of which we are just beginning to fathom. Users are free to roam the globe and still be in touch with the organisation's headquarters as well as friends and family. This is exactly where the contradiction in security terms begins. Users have a tendency to combine official and personal information on the same device and use that same device for both purposes when they are on the move, simply because it is convenient. Strangely enough, all the controls regarding the classification of equipment as well as the directives for physical separation of equipment of different classification seem to fall apart when a user is on the move. Although it is rarely openly admitted, requests for sending sensitive information over insecure channels take place all the time. This is one case where technology is not able to provide solutions that are simple and secure enough and at the

same time warrant the unimpeded upholding of the security policy when users become mobile. This is clearly a case where the availability of information is challenged if its confidentiality is to be upheld and when this happens, the globe-roaming executive will usually prefer availability over security. We have not yet reached a state where all of the security measures seamlessly integrate with our customary notion of working and communicating. The plethora of applied privacy and security standards, acronyms, emerging security techniques, new threats to security and the like, are clearly capable of perplexing even experts in the field. How will the average, non-expert user be able to make sense of all this and decide upon a course of action when the need arises? It is exactly this uncertainty that the Social Engineer uses as a tool in targeting not the organisation, but its users instead. To help reduce the uncertainty, the guidelines of controls 11.7.1 and 11.7.2 should stress the duality of a successful defense. On one hand, there are the purely technical measures that must be implemented in order to create the infrastructure for attaining the desired security level. On the other hand, there are the users' actions that ensure the upholding of security. The second part is the most difficult to strengthen and this can only be done through the education of users and awareness programs. Exact and structured directions can and must be given to users so that they can block SE attacks. However, this is definitely not going to work 100% of the time. Defending against SE is not an exact science. Neither can the ingenious attack of tomorrow be fully anticipated today. The Social Engineer has his mind and ingenuity to rely upon and the only real weapon against those is also a human mind; the mind of the potential target who now finds himself on the first line of defense in a never-ending battle. Hence, the users' minds must be exercised to recognise any uncharted new attack through exposure to data gathered from previous or hypothetical attacks.

C.8. Section 12 - Information Systems Acquisition, Development and Maintenance

Relevant security categories:

- Security requirements of information systems
- Correct processing in applications
- Cryptographic controls
- Security of system files
- Security in development and support processes
- Technical vulnerability management

Section 12 deals with a) the security requirements of information systems
In order to ensure that security is an integral part of information systems (section 12.1 of ISO17799), b) preventing errors, loss, unauthorized modification or misuse of information in applications (section 12.2 of ISO17799), c) protecting the security of information through cryptographic
Means (section 12.3 of ISO17799), d) ensuring the security of system files (section 12.4 of ISO17799), e) securing the development and support processes in order to maintain the security of application system software and information (section 12.5 of ISO17799) and f) managing technical vulnerabilities in order to mitigate the risk that may result from the exploitation of published technical vulnerabilities.

As it stands, section 12 is not directly related to the mitigation of risks stemming from possible SE attacks. A small number of issues do arise in certain parts of the text but most have already been thoroughly examined in the context of previous sections of the ISO 17799 standard. Nevertheless, these will be pinpointed and briefly placed in the context of this section.
One of the guidelines of the control described in 12.4.1 reads "*Software patches should be applied when they can help to remove or reduce security weaknesses*". It probably should be added that "**patches should come from a verified and authorised source to avoid the risk of introducing fake patches to the system that could lead to its compromise**". This may come as an effective control for a "sting" operation orchestrated by a Social Engineer and also applies to section 12.6.1.

Another guideline of control 12.4.1 states: "*Physical or logical access should only be given to suppliers for support purposes when necessary, and with management approval. The supplier's activities should be monitored*". Although identification of collaborating third-party personnel has been dealt with extensively in previous sections, it might be worthwhile to add here: "**Supplier personnel should be positively identified and if necessary be previously classified according to their intended purpose and access**". Hence a Social Engineer will not be able to walk thorough to the heart of the organisation pretending to be a member of a supplier's personnel.

In control 12.4.2 that offers guidelines for the protection of system test data, it should be added that "**depending on the sensitivity of the information normally carried by the system and its classification, test output should be treated in the same manner as operational output and be subjected to the same sanitisation or controlled destruction procedures**". This way neither actual information may inadvertently leak, nor information about the output format or other detail internal to the system may be compromised.

The guidelines offered in control 12.5.4 regarding information leakage, may help in halting the result of a SE attack that was successful in planting of covert channel software or other spyware.

C.9. Section 13 - Information Security Incident Management

Relevant security categories:

- Reporting information security events and weaknesses
- Management of information security incidents and improvements

Section 13 of ISO 17799 is probably one of the most important sections of the standard insofar SE is concerned. A solid security incident management infrastructure is essential in providing effective defense against SE attacks. Section 13 deals with a) formal procedures of reporting information security events and weaknesses in a manner that allows prompt corrective action to

be taken (section 13.1 of ISO17799) and b) ways of providing consistent and effective management of IS incidents.

Control 13.1.1 deals with "Reporting information security events" (section 13.1.1). The guidelines presented there, offer a solid foundation for a reporting procedure that is necessary for successful response to IS events. The point made about making all people involved in the operation of the organisation aware of reporting procedures for security events and points of contact is very important. During a SE attack, there is usually very little time to either go through the hierarchy in order to file a report or waste precious time in trying to locate the person responsible for receiving that report. This corroborates the argument for a hierarchy of IS professionals that must be independent of and deployed in parallel to the administrative hierarchy of the organisation. Furthermore, guideline 13.1.1(c) is definitely along the right track with respect to SE attacks as it provides for immediately reporting to the Information Systems security contact person without having to fill out any paperwork. "Duress alarms" are also mentioned and this too is a measure that should be considered in the context of SE attacks. Assuming that user training and security awareness schemes have been successful in giving employees the necessary edge on SE attacks, a targeted employee may indeed realise at some point that he/she is under attack by a Social Engineer. If the attack is taking place over the phone, the employee may put the attacker briefly on hold in order to notify the appropriate security contact person. If the attack is taking place with the attacker "in situ" then a coded phone call for e.g. request "for stationery with the organisation's logo in French" to the security contact person, should set the defense mechanism in motion in order to locate and apprehend the attacker.

Control 13.2.1, "Responsibilities and procedures", outlines the procedures that should be in place so that the response to IS security incidents is most effective. In guideline 13.2.1(c) the need for audit trails is emphasised. In the case of SE attacks these can include video footage or recorded telephone conversations. For such evidence to be admissible in court, it must be made

certain that it is collected in a proper manner according to legislation and the principle of protection of personal rights. Control 13.2.3 deals with the matter of evidence collection in general, but not with the recording of either phone conversations or video in particular. Provision should perhaps be made for this aspect of evidence collection also.

According to control 13.2.2 "Learning from information security incidents" there is a need for quantifying and monitoring the types, volumes, and cost of IS incidents. If this is also applied to SE attack-related incidents, then a measure of success of security-related training and awareness schemes with respect to SE can be indirectly obtained. This is very important due to the inherent difficulty in obtaining direct measurements regarding SE attacks. Hence, if there is a chance of obtaining real-life SE-related metrics, this can be made possible through the existence and consistent operation of an IS security incident reporting mechanism.

Returning to control 13.2.3, on the issue of evidence trail establishment in the case of information on computer media, it is stated that mirror images of media should be securely obtained and kept. While this may be fairly easily possible for most of PC systems, when it comes to creating a mirror image of the hard disk of a server or of any other mission-critical piece of hardware, the process may not be that simple. In order to protect the state of the system as it was during or shortly after the incident, the attacked system must be taken off-line and mirror images be obtained. This is never an easy or fast process and what this means in practice is that the system must *stay* off-line for a significant amount of time or else contamination or even loss of the evidence may occur. It can thus be argued that an extreme form of Denial-of-Service attack could be initiated simply by creating the false idea that the system is under attack and cause it to be taken off-line. All it would take to bring down the system could, in theory, be a couple of carefully placed phone calls to trigger the IS incident response mechanism.

As the uncertainty of whether the system is under attack or not rises, it is much more difficult to identify and counter the attack. This is something that could be used by the Social Engineer in an attempt to work around the IS incident response mechanism. By frequently creating small and insignificant IS discrepancies, these would initially be treated as IS incidents and result in the mobilisation of the response mechanism, but would, after a while, tend to be ignored. When this point is reached, the real attack can take place and have a greater possibility of success.

C.10. Section 14 - Business Continuity Management

Relevant security categories:

- Information security aspects of business continuity management

The objective of section 14 of ISO 17799 is described as "*to counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption*". Hence, the controls of this section can not be directly related to the notion of SE. One issue though that has to do with the control of sub-section 14.1.2 "Business continuity and risk assessment" is that every effort should be made to consider the SE attacks and their effects in the risk assessment procedure. In order to do so, it would be helpful if SE vulnerabilities and threats could be reduced to quantifiable entities.

C.11. Section 15 - Compliance

Relevant security categories:

- Compliance with legal requirements
- Compliance with security policies and standards, and technical compliance
- Information systems audit considerations

The objective of section 15 of ISO 17799 is "*to avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements*". As such, most of the controls of this section are not directly related to SE. Control 15.2.1 "Compliance with security policies and

standards" is obviously important as is control 15.3.2 "Protection of information systems audit tools", given that any self-respecting attacker, Social Engineer or otherwise, would attempt to render the audit tools unusable if possible, to make any trail that has been left behind, difficult or impossible to follow.

C.12. References

FRANGOPOULOS, E.D. and VENTER, L.M. 2004. Biometric protection of smartcards through fingerprint matching: a technological overview and possible directions. In: *Peer-reviewed Proceedings of the ISSA enabling tomorrow Conference 2004*. ISBN 1-86854-522-9.

ISO/IEC. 2005. *International Standard ISO/IEC 17799:2005. Information technology -- Security techniques -- Code of practice for information security management.* Geneva: ISO Copyright Office.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2002. *NIST Special Publication 800-46. Security for Telecommuting and Broadband Communications*. [online]. Available from URL: http://www.csrc.nist.gov/publications/nistpubs/800-46/sp800-46.pdf [Last access on Jan 15, 2007]

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. 2006. *NIST Special Publication 800-88. Guidelines for Media Sanitization* [online]. Available from URL: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf [Last access on March 7, 2007]

SCHNEIER, B. 1996. *Applied cryptography. Protocols, algorithms and source code in C*. USA: John Wiley & Sons Inc.

SUN MICROSYSTEMS, 2003. *Datasheet Sun Ray ™ Ultra--Thin Clients* [online]. Available from URL: http://se.sun.com/edu/pdf/sunray.pdf [Last access on March 7, 2007]

THOMSON, I. 2006. *'Evil twin' Wi-Fi hacks target the rich. Hackers after high net worth individuals in wireless scam* [online]. Available from URL: http://www.airdefense.net/newsandpress/vnunetcom_11_23_06.pdf [Last access on Jan 1, 2007]

U.K. DEPARTMENT OF TRADE & INDUSTRY (DTI), 2006. *Information security breaches survey 2006 - Executive summary* [online]. Available from URL: http://www.pwc.com/uk/eng/ins-sol/publ/pwc_dti-fullsurveyresults_execsum06.pdf [Last access on Jan 17, 2007]