# INFORMATION SECURITY AWARENESS: AN INNOVATION APPROACH

Carlos Orozco Corona

Technical Report
RHUL-MA-2009-03
16th February 2009


Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX, England
http://www.rhul.ac.uk/mathematics/techreports

2008

Royal Holloway
University of London

# Information Security Awareness: An Innovation Approach

Royal Holloway
University of London


**Orozco Corona, Carlos**

Student Number:
**100579890**

Supervisor:
**John Austen**

Department of Mathematics
Royal Holloway, University of London

Egham, Surrey TW20 0EX, England

# Information Security Awareness:

# An Innovation Approach


## Orozco Corona, Carlos

Student Number:

**100579890**

Supervisor:

## John Austen


Submitted as part of the requirements for the award of the

**MSc in Information Security**

at Royal Holloway, University of London.

I declare that this assignment is all my own work and that I have acknowledged all quotations from the published or unpublished works of other people. I declare that I have also read the statements on plagiarism in Section 1 of the Regulations Governing Examination and Assessment Offences and in accordance with it I submit this project report as my own work.

Signature: Date: **21st August 2008**

# Acknowledgements

*I would like to dedicate the effort imprinted in this dissertation project, to those persons who suffered my absence while I was writing it; my son and my daughter. I am especially grateful for the support that I received from my wife, who made this adventure possible.*

# Information Security Awareness: An Innovation Approach

## Table of Contents

# List of Figures

# List of Tables

# List of Acronyms

List of acronyms used in this dissertation:

**CERT:** Computer Emergency Response Team

**DoI**: Diffusion of Innovations

**E-CMC:** Extended Convergence Model of Communication

**E-mail**: Electronic mail

**FBI**: Federal Bureau of Investigation

**FIRA:** Fideicomisos Instituidos en Relación con la Agricultura

**IDP**: Innovation-decision process

**IMP**: Incident Management Process

**IS**: Information Security

**ISA**: Information Security Awareness

**ISAC**: Information Security Awareness Campaign

**ISAP**: Information Security Awareness Program

**ISF**: Information Security Forum

**ISG**: Information Security Governance

**ISP:** Information Security Policy

**ISKC**: Information Security Knowledge Campaign

**ISPC**: Information Security Persuasion Campaign

**ISCC**: Information Security Confirmation Campaign

**IT**: Information Technology

**SN**: Social Networks

**SNA**: Social Network Analysis

**S/R**: Stimulus / Response

# Executive Summary

Scholars and security practitioners seem to converge in the understanding that *Information Security* is in great part a problem about people; hence the need for a more holistic approach in order to understand human behaviour in the *Information Security* field which requires a multidisciplinary approach. Recent events such as the "Interdisciplinary Workshop on Security and Human Behaviour" hosted in Boston, Massachusetts in June 2008, are considering this approach and they have conveyed a multidisciplinary teamwork, composed by computer security researchers, psychologists, behavioural economists, sociologists, philosophers, among others, to address and understand the human side of security. This dissertation represents one of these efforts in approaching *Information Security* from different perspectives. A holistic approach would enable security practitioners to understand the human side of security and as a result be more effective on reaching the pursued security objectives. However, this approach may pose additional challenges, not just in the research field by conveying and reaching consensus among multiple disciplines, but at the organisational level.

The proposed dissertation project aims to produce an *Information Security Awareness* framework based on Innovation theory that contributes to the active participation and behavioural change of an individual towards the acceptance and compliance of the Information Security Policies within an organisation using viral marketing techniques and alternative methods for the delivery of the security message over pre-established social networks. Prior to these proposed innovations, this dissertation examines at length *Information Security Awareness* from the perspectives of: management (chapter 2), psychology (chapter 3) and social networking (chapter 4) to give a balanced view of a solution to these issues.

CHAPTER

# 1

# Introduction

Serious *Information Security* (IS) incidents are still occurring despite the existence of the *security* procedures that are meant to counter or minimize their negative effects. During the last and present year several information security incidents were registered, some of them of significant severity and some of them with consequences that are still being estimated due to their severe potential negative impact against a considerable part of the population.

The possible causes might be several and varied, for example, employees that are not following the established information security procedures because they are not familiarized enough with them or not aware at all about the security procedures that they must follow under determined circumstances or for the execution of a determined task. Moreover, the lax application of the security procedures, the lack of security procedures under determined circumstances or for the execution of a determined task, the lack of mechanisms to review the effectiveness of the Information Security Awareness Program (ISAP), they all may lead to undesired results with unexpected consequences.

In general it can be argued that these causes are in part the result of poor ISA at different levels. Either the cause is a procedure which may reflect a low perception of the risk under a given context by a security practitioner or the lax application of a given security procedure by employees. Current security awareness practices are not being effective in achieving their objectives, as evidence from international security surveys conducted in 2007 suggests, particularly regarding the cultural change within the organisation that would help to reduce the risks associated with the human factor or minimize the negative effects of information security incidents.

## Contents

A recent study conducted by the University of Oulu identified 59 different ISA approaches from both the academic and private sector. This study remarks that only a small number of those approaches count with a theoretical foundation. This means that only a minority of the current ISA approaches are able to provide a certain degree of assurance in the achievement of the expected results. Particularly there are two approaches based on theoretical backgrounds that treat the behavioural change of the individual from two different perspectives. These two perspectives facilitate the understanding of the underlying process that takes place when an individual decides to behave in a determined manner.

Although the behavioural change of the individual remains to be the heart of an ISA, evidence suggests that there are still efforts to be done to achieve this objective. Since the expected behavioural change might not be evident, the mechanisms to measure the ISA effectiveness are subjective and difficult to get right.

Even though current ISA approaches try to address from different angles the issue of behavioural change, none of the 59 ISA approaches explicitly takes advantage of the underlying social networks (SN) that co-exists along with the official communication network imposed by the organisation's hierarchical structure and the impact they have on the individual's behaviour. The non-official communication networks can be determined by performing a Social Network Analysis.

The Social Network Analysis (SNA) unveils a set of key individuals that play an important role in the flow of information within an organisation. These sets of people, generally recognised and respected by their peers frequently exert some influence on the behaviour of their peers. Presumably, evidence suggests that there is a disproportion between the number of employees and the number of these key individuals. That is, that just a small percentage of the population of an organisation plays one of these roles, following *Pareto's law* commonly referred to as the *80/20 principle*, which shall not be taken literally, but as a manner to point out such disproportion.

In addition, the delivery methodology followed in these approaches do not take advantage of these key individuals who could help influence their peers toward a positive perception of the information security policies and initiatives. It was noted that 1 out of the 59 approaches uses some elements of the Diffusion of Innovation (DoI) theory, which takes in consideration to a certain extent some influential people within the organisation commonly referred to as opinion leaders; nonetheless, it does not provide any further insights, since there are more than just opinion leaders playing decisive roles in the diffusion process, such as opinion formers, mavens, connectors and salesmen.

Apart from this approach, it seems that the DoI theory has been left aside by the rest of the ISA approaches, neglecting the possibility of gaining additional knowledge of the underlying process that takes place every time a new product, idea, or service is launched and how the diffusion process could be influenced to increase the rate of adoption of a determined innovation. Additionally, despite the fact that Viral Marketing is regarded as a controversial topic in the current marketing environment, the essential principles can be used to aid in the achievement of the ISA objective, since these marketing techniques accelerate the spreading rate of a given message.

## 1.1 Purpose of this Dissertation

The proposed dissertation project aims to produce an ISA framework based on Innovation theory that contributes to the active participation and behavioural change of an individual towards the acceptance and compliance of the Information Security Policies within an organisation using viral marketing techniques and alternative methods for the delivery of the security message over pre-established social networks.

## 1.2 Objectives

The main objectives of this dissertation project are:

1. Base the ISA on the DoI theory.
2. Apply marketing principles to the ISA framework.
3. Address common problems which result from the poor delivery of an ISA program.
4. Identify and exploit SN as an alternative channel to deliver the security message.
5. Apply Viral Marketing techniques to the delivery phase of the ISA program to reinforce and maximize the impact of the security message.
6. Provide an alternative method to deliver an ISA program under the perspective of the 80/20 principle.
7. Provide an alternative method that copes with the acceptance of a changing environment.

## 1.3 Scope

The scope of this thesis is to propose an alternative method to conduct an ISAP, based on the DoI theory. The implementation of an ISA with an Innovation approach is beyond the scope of this thesis.

## 1.4 Research Strategy

The literature review made in this dissertation uses material obtained from different electronic sources such as *Web of Science, Elsevier's ScienceDirect, JSTOR, Business Source Complete, IEEE Computer Society Digital Library, ACM Digital Library* and also the content of several relevant books was explored; some of these books were obtained directly from RHUL library, other from the *InforM25* (the union catalogue of all the academic libraries within the M25 Consortium) and some others through *Inter Library Loans.* In addition several international surveys in the field of *Information Security* were analysed to provide the current state of ISA. Finally, two interviews with information security practitioners and lecturers were conducted.

## 1.5 Structure of the Dissertation

This dissertation is organised as follows:

The purpose of chapter two of this dissertation is to introduce ISA and to discuss its origin and context as the result of the responsibilities and practices exercised by the board of directors and executive management towards the implementation of an Information Security Governance strategy. Once the need for ISA is explored, the importance and the concept of ISA are explored along with a critical analysis of the current relevant approaches. Then several recognised international surveys are analysed to determine the current status of ISA in the enterprise environment and comment on some current initiatives taken by some governments towards the successful and effective implementation and management of an ISAP. Lastly, a case study is revised in this chapter, with the purpose of identifying and analysing the factors that prevented the achievement of the ISA objectives.

In chapter three, the results of these surveys are put into context by determining the roots of these failures, which lead us to the real objective of the ISA, the achievement of cultural and behavioural change on the employee. Several theoretical approaches aiding behavioural change are explored. In this chapter, a combined approached is proposed to understand the underlying process of the perception of reality of an individual and offer a manner in which this perception can be affected; as a consequence the typical individual's response to a given security event would be modified.

Once knowledge is gained on the manner in which an individual responds to a set of stimuli, in chapter four we explore how the individual is exposed to multiple stimuli when interacting in both official networks and social networks and how this affects their perception of reality and as a consequence their behaviour toward the acceptance of security policies. In order to determine an individual's SN, a SNA is

conducted. As a result, not just the individual's SN emerges, but also the presence of key individuals in such networks is unveiled. Several alternatives are explored to conduct the SNA and discuss the importance of these key individuals and their roles in the SN. Lastly, an example of a viral marketing email is presented to illustrate the points involved in this chapter.

The purpose of chapter five is to introduce the DoI Theory, its main elements and how it can be used for ISA initiatives. In this chapter it is discussed how the DoI theory uses SN as communication channels and key individuals to increase the rate of adoption of the innovation. A suggested ISAP model based on DoI theory using viral marketing techniques over SN is proposed. The model comprises two broad phases; the first phase involves one campaign called *information security knowledge campaign* (ISKC) and the second phase involves two campaigns, an *information security persuasion campaign* (ISPC) and an *information security confirmation campaign* (ISCC). An *initialisation* stage is conducted for the model such as performing the SNA, determining the key individuals, designing viral marketing content for the campaign's materials and planning an alternative 80/20 delivery method for the ISA material. In addition, this chapter shows how the model can be adapted to any existing model, making it complimentary to existing ones.

# The Need for ISA

CHAPTER

2

## 2.1 Introduction

The purpose of this chapter is to contextualise the ISA initiative by exploring the need for ISA, the reasons for which it should be regarded as a governance issue and consequently be supported by the board of directors and executive management. Then, a definition of ISA is provided and an analysis of the current ISA approaches that results relevant to this definition are also discussed along with their objectives and requirements, examining the reasons for which current approaches seems to fail in achieving them. These are essentially the main motivations that this thesis aims to address. A case study is mentioned to illustrate this position and it is further supported by the analysis and discussion, of the results of relevant IS surveys, that provide us with the current state of ISA.

## Contents

## 2.2 IT, a business enabler and a source of risks

Modern organisations reflect, in their business operations and production models the impact of technological breakthroughs which resulted in response to the new market context. The new context demands from organisations to respond faster to the market needs and to adapt themselves to a changing environment. These demands imply the reduction of costs of operation, costs of production and improving the time of delivery of the product or service. Hence, collaboration between organisations and automation in the operation and production process are the tools that aid organisations in the achievement of these objectives and remain competitive in this new and dynamic context [2].

Collaboration and particularly *automation* are supported by *Information Technology* (IT) [3]. It can be noted that over the past 20 years, increasingly, organisations have been adopting IT solutions for the automation of some of their processes in order to satisfy the demands of the current market and facilitate the achievement of its objectives, trusting IT to support the core business process. Arguably, this could be the reason for which IT is regarded as a business enabler issue [4]. However, the consequence of the indiscriminate adoption of IT [5], is that organisations are becoming highly dependent on IT systems as evidence suggested in [6], where it reports that 84% of the surveyed companies in the United Kingdom are precisely in this situation, which is translated into additional risks, that is, at the time IT solutions are incorporated into the business environment, additional operational business risks are introduced as well [3].

In order to analyse how technology introduces new risks, it is necessary to discuss the technology lifecycle. Consider for instance the life cycle of technology as the diffusion of an innovation [7]; that is, mapping the technology lifecycle with the rate of adoption of an innovation following an S-shaped diffusion curve as shown in Figure 2.1. Before going further in this point, it is worth noting that an innovation is not necessarily a synonym of technology. An innovation can be a piece of technology, but not necessarily vice versa. Everett Rogers in [8, p. 12-13] defines innovation as "*an idea, practice or object that is perceived as new by an individual or other unit of adoption*" (see Chapter 5).

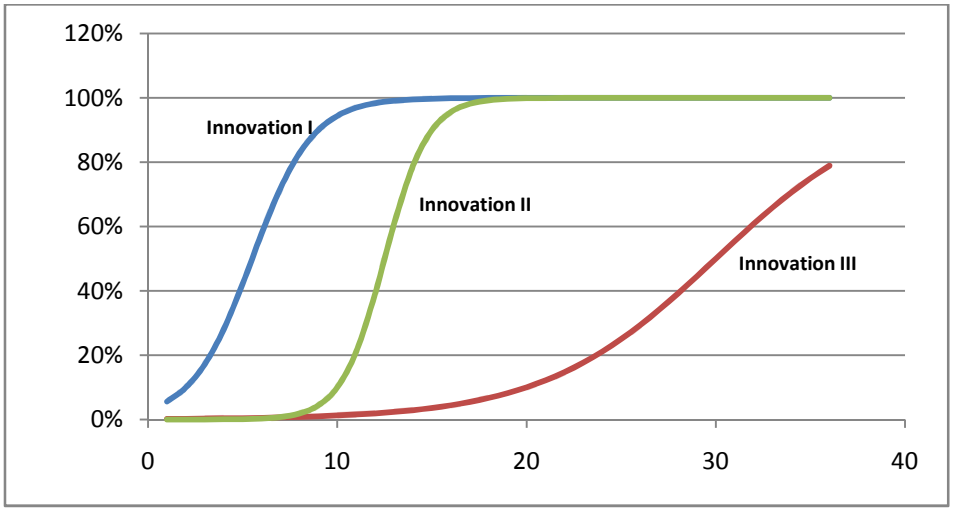



**Figure 2.1** The S-Shaped diffusion curve represents the cumulative adoption rate of an innovation over a period of time [7].

Figure 2.1 shows 3 different innovations that illustrate the common pattern of the S-shaped curve over a time period; that is, the beginning of the curve represents the introduction of the innovation, since there are just a few people adopting that innovation, the adoption rate rises slowly, then it follows almost an exponential growing behaviour, which usually happens when more people are aware of it and is influenced by their peers when adopting that innovation, and finally, the adoption rate decreases as less people remain to adopt the innovation [8], [9].

The same stages can be mapped into the technology life cycle, for example, the first stage involves the introduction of the technological innovation developed by manufacturers to the market; that is, a new IT solution which can aid the collaboration or automation in support of a business process within the organisation. The Second stage involves testing the IT solution as a proof of concept in order to evaluate its usability within an operating environment [3]. Since a new concept is being introduced to the market, there are few people aware of the existence and functionality of that innovation; hence the rate of adoption is slow at first. The third stage involves the "large-scale deployment" [3] of the technological innovation when the IT solution is made available to a great number of potential adopter in the market. During this period the actual diffusion of the innovation takes place; as more people become aware of it, the adoption rate grows rapidly. The fourth stage involves a maintenance period, when few organisations remain left to adopt the technological innovation or the adoption rate has reached its maximum value. It is worth noting that it is very likely that during this fourth stage other innovation technologies might already have been adopted and others are being introduced or are planning to be adopted. The point here is that complexity begins to emerge as a consequence of overlapping the adoption of several technological innovations [3].

Since technological innovations or IT solutions are being adopted to support business processes, the need to protect those IT solutions arises with its adoption [10]. When security is not considered in the design and development of the technological innovation such protection is often available through technical means; that is, with another technological innovation or IT solution specially manufactured for that purpose [3, 11]. Not surprisingly, security technological innovations follow the same cycle as technological innovations and they often appear after the adoption of an IT solution, as the technology has to be assimilated and analysed to identify its vulnerabilities and be able to manufacture the appropriate countermeasure [4]. For example, consider innovations in Figure 2.1 as technological innovations and the time periods plotted on the X-axis as months. *Innovation I* is introduced into the market and then it is rapidly adopted, following the technological life cycle. However, the security technology innovation, that is, *Innovation II* which is the technology capable to protect *Innovation I* has not been developed yet. Furthermore, whenever *Innovation II* appears in the market it might not be immediately adopted as it needs to go through the technological life cycle; hence *Innovation I* is regarded to be secure nearly at the end of stage 4 of its technology life cycle. As a consequence a risk gap is opened between the introduction of *Innovation I* and the development and adoption of *Innovation II*. In a real business environment there might be several technological innovations being adopted and as a consequence several risk gaps being opened, some of these risks are in part due to the resultant complexity of the IT infrastructure.

Note that security technological innovations may introduce their own risks and become complex as well, violating the principle of *Economy of Mechanism* proposed by Saltzer and Schroeder in [12], which states, regarding a security mechanism, to "*Keep the design as simple and small as possible*"; that is, that the more complex the security mechanisms are, the less assurance can be achieved in their correctness. This is mainly the reason why organisations that are highly dependent on IT are more exposed and vulnerable to security threats [4], as they have to cope with a wide range of new operational risks introduced by an indiscriminate adoption of IT [5].

## 2.3 The need for ISA

It might be important to note that a deep understanding of IT is required in order to identify its risks and be able to manage them appropriately [13]. As a consequence, the organisation is not solely dependent on IT, but also becomes highly dependent on the personnel managing the IT infrastructure, more specifically, on the specialised skills of the individual that manages the adopted IT solutions. This is very important to remark, since a human factor becomes decisively in the reliability of the information managed by the IT infrastructure [13]. Hence, the lack of the appropriate skills,

training and security awareness of the technology being managed constitutes one of the biggest threats that an organisation faces against its business information.

The scenario becomes more complicated when some technological innovations are adopted and are made available to individuals with insufficient technological skills and without a clear understanding of the underlying risks of the technology they are using, resulting in additional business risks that the organisation has to manage [14]. The administration of these risks implies that the executive management is aware of the risks introduced by IT. Therefore awareness at this level is paramount, as the lack of awareness could result in failing to prevent serious damages to the business information assets of the organisation. The *SANS Institute* (SysAdmin, Audit, Network, Security) in [15] suggests a roadmap to conduct an ISA at the senior management level.

In general, it could be said that the problem being discussed has two faces and a common element. One face involves the lack of awareness at different levels about the risks introduced by technological innovations [3], namely, at the board of directors and executive management level, at the Information security management level and at the end-user level. The second face involves the absence or weak mitigation actions taken upon the risks encountered. Both faces of this problem share a common element, namely, the human element. This situation, where awareness is not always followed by the appropriate actions is reflected in the survey's results reported in [6], where it shows that 81% of the respondents "believe that their board gives a high or very high priority to information security". However, only 55% "have a documented security policy".

Since people represent one of the biggest threats for the business information [16], the less trusted people involved in security decisions, the better, because the more trusted people is involved in security decisions, the more weak the system becomes [17]. Evidently, organisations still need to rely on people to conduct their business and trust that they will take the appropriate security decisions; however, when no ISA initiative is in place, it would be difficult for organisations to obtain the assurance that the correct decisions are being taken and also for employees, it would be difficult for them to know for instance what a security threat is and what they are expected to do in the face of it; therefore the need for security awareness regarding information systems shall become a high priority for the organisation. The executive summary in [6], suggests to "integrate security into normal business behaviour, through clear policy and staff education" in order to protect organisations in this new dynamic context. In [1], McLean points out that by appropriately conducting an ISA the risks introduced by IT could be mitigated and in the event of a security incident their negative impacts could be minimized.

Nonetheless, this initiative needs to be supported by the highest level of management in the organisation. Moreover, responsibilities and roles must be assigned in order to effectively address these risks. Otherwise the objectives of ISA might not be successfully achieved. This is one of the reasons why ISA should be treated as an Information Security Governance issue.

## 2.4 ISA, a governance issue

Nowadays, for many organisations, business information is considered a critical business asset and as valuable as their supporting systems, processes and networks [18-21]. Hence, information needs to be protected in terms of its:

- **Confidentiality**. The Information is protected against unauthorised disclosure at the moment it is used or accessed through Information Systems or network communication systems.

- **Integrity**. The Information is protected against unauthorised alteration or modification, and ensures that information has been preserved in its original state since it was last accessed or altered by an authorised subject.

- **Availability**. Information is available and usable at the moment that it is required, preventing unauthorised denial of use and improving the mean time between failures.

Confidentiality, integrity and availability are the fundamental tasks in Information Security [22] and they result essential for maintaining competitiveness, profitability, legal compliance and commercial image of the organisation, among others [23-25].

The value of information seems to be clear for some companies, using it strategically as a business enabler [21, 26]; since it is perceived as a critical asset for the business, its protection initiatives appear to be supported by all levels of management and are far from being a negotiable issue [27]. As a result, the IS function emerges from the need to preserve the secure state of information that aids the executive management to accomplish the mission of the organisation. Unfortunately, for many other companies, this is not the case. Surveys such as [6, 28, 29] and others, show that there is a great percentage of organisations aware of the need for IS but a considerable less percentage of those organisations are actually doing something in this respect. It could be said that the value of information is not perceived clearly, and is relegated and treated as a pure technological issue at best, which might explain why

Information Security lacks of the appropriate executive management attention [18]. In addition, the initiatives towards IS activities tends to be cumbersome, because of the constant negotiations towards the provision of sufficient resources to protect the business information assets. It is true that every security initiative that requires resources from the organisation has to be fully justified [27], but that is a different issue from having to persuade every time the executive management for the need to protect business information assets.

The challenge is how to make these organisations aware of the business information risks that the organisation as a whole is exposed to and once aware ensure that the IS initiatives will count with the commitment and support from all levels of management in order to effectively achieve the expected results. The first part of this problem shows the need for an initial ISA at the top management levels (see sections 2.2 and 2.3) while the second part involves the need to treat IS as a *governance* issue [20].

Recognising the value of information might require from organisations to change their current paradigms towards the protection of information, such as migrating the IS function from the technological realm to become a strategic and management issue [22]. It could be said that such migration is possible if the need for IS is addressed from a governance point of view in order to ensure that the initiatives will count with the management commitment and support at all levels; and responsibilities, roles and tasks are defined to ensure the achievement of objectives. In other words, treating IS as a governance issue, results in the instantiation of the *Information Security Governance* (ISG) strategy.

According to the IT Governance Institute in [27, p.11], Governance is defined as:

> *"...the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly"*,

Punctually, the responsibilities of the executive management are:

- To protect the critical assets of the organisation.
- To ascertain that risks are managed appropriately.
- Verify that resources are being used responsibly.

Since information is a critical business asset, the executive management is then the ultimate responsible of ensuring that the appropriate measures are taken to protect it. In addition, the executive must ensure that risks against the business information are appropriately managed. Furthermore, the executive must ensure that employees account with the sufficient skills to preserve the secure state of the information resources that they operate [27].

For those organisations that must comply with legal and regulatory requirements, the executive management could result liable and be charged of negligence by failing to protect the business information. Therefore, the executive management needs to ensure and eventually show evidence that due care towards the protection of information is being practiced. Particularly, regarding ISA, the executive management must verify that an ISA program is in place and its objectives are achieved by ensuring that it provides not just security awareness on security policies and guidelines, but security education and training as well. Otherwise, the charge of negligence is possible against the executive as he or she would fail to practice due care towards the protection of the enterprise's critical business information resources [19]. This is the reason why ISA shall be regarded as a governance issue, particularly as an ISG issue.

By extension, the IT Governance Institute defines ISG in [27, p. 17] as:

> *"...a subset of enterprise governance that provides strategic direction, ensures that objectives are achieved, manages risks appropriately, uses organisational resources responsibly, and monitors the success or failure of the enterprise security programme"*

A complementary view is provided by the *Information Systems Audit and Control Association* (ISACA) that aids to show evidence that due care towards the protection of information is being applied, that is to:

> *"Establish and maintain a framework to provide assurance that information security strategies are aligned with business objectives and consistent with applicable laws and regulations"*

The recommendation to establish such framework is to adopt known IS *best practices* such as the international standard *ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems - Requirements*. According to [6], the adoption of this standard has been increasing in the last two years, resulting in a greater number of security specialists that know, understand and

are familiarised with this framework, which guarantees to a certain extent an effective implementation of the standard. In addition, organisations can use this standard for legal compliance purposes, reducing the potential liabilities caused by failing to protect the critical assets of the organisation.

Although, an organisation could prevent charges of negligence by adopting an international standard that helps towards legal compliance and satisfy regulatory and contractual requirements, the protection of information goes beyond, by addressing specific business risks that can endanger the competitiveness of the organisation in the market [30]. In an interview to Julia Allen, a senior researcher at CERT (*Computer Emergency Response Team*) conducted by the *CERT Executive Podcast Series* [31], comments on a common methodology that she has been using to introduce this topic at the top level of management. In this set of questions, the executive management is prompted to assess the impact of various scenarios where the organisation image could be damaged; confidential information could be disclosed or stolen; the core business information systems were not available and so forth. These questions are used to draw attention of the executive management about the business information risks that should be addressed, which goes beyond the merely legal compliance.

In the best of the cases the need for IS should arise as a result of an initial ISA where the value of business information is clarified and executive management recognises the nature of the risks against the business information. However, if the need for protecting information arises from compliance to legal, regulatory or contractual requirements, the result could be a partial implementation of the IS function, that may not be thoroughly supported by all levels of management and not seriously taken by the rest of the employees. And as a result, limiting the benefits of putting IS in place [30].

Having set the scene and identified the importance of ISA as a governance issue, the following section moves on into analysing the common understanding of ISA, along with the requirements and objectives that are typically pursued in its implementation.

## 2.5 ISA, requirements and objectives

More often than not, in the literature, the term *ISA* has come to be used in a broad sense to refer to a *training* program, or an *education scheme* or simply used to denote the systematic provision of security-related information. Furthermore, sometimes it is used as a term that encompasses all these three; *awareness, training and education*. For example, this broad use of the term ISA is typically found in titles of IS research articles, such as "*Information Security Awareness: Selling the Cause*" found in [1], "*A User's Guide: How to Raise Information Security Awareness*" found in [32], "*A*

*prototype for assessing information security awareness*" found in [33] and even in IS initiatives such as the "*Information Security Awareness Forum*" where the authors of these research articles or the members of these organisms are in fact treating with issues more than simply *awareness*. Hence, the need to clarify exactly what is meant by *awareness, training and education*.

For instance, according to a definition provided by the Oxford English Dictionary [34] *awareness* is:

> *"The quality or state of being aware; consciousness"*

And *being aware* is defined as:

> *"Informed, cognizant, conscious, sensible. To be aware (of, that): to have cognizance, to know"*

*Consciousness* and *awareness* are considered synonyms by [34].

From this perspective, it could be argued that Information Security *Awareness* is solely concerned with informing employees about relevant security issues in order to promote a security conscience. However, a serious weakness of this conception is that this would be a limited and an inefficient manner of trying to achieve a *behavioural change* regarding IS issues. Nonetheless, it is the first step towards this objective [1].

In the definition provided by the ISF in [35, p. 6], the ISF reflects this position:

> *"Information security awareness is the degree or extent to which every member of staff understands the importance of information security, the levels of information security appropriate to the organisation, their individual security responsibilities, and acts accordingly."*

It shall be noted that this definition involves a decision making process where employees are expected to act according to the security knowledge they possess after an ISAC. More than just making the employee aware of the threats and vulnerabilities associated with IT, they are expected to make the correct decisions on how to protect information and IT assets [36].

The terms *education* and *training* are defined by [34] as:

*Education*:

> *"The systematic instruction, schooling or training given to the young in preparation for the work of life; by extension, similar instruction or training obtained in adult age. Also, the whole course of scholastic instruction which a person has received. Often with limiting words denoting the nature*

> *or the predominant subject of the instruction or kind of life for which it prepares, as classical, legal, medical, technical, commercial, art education."*

*Training:*

> *"To instruct and discipline in or for some particular art, profession, occupation, or practice; to exercise, practise, drill; to make proficient by such instruction and practice"*

It can be noticed, that there are significant differences among these three concepts. Firstly, a*wareness* is concerned on making individuals more conscious about a topic by providing relevant information using different channels and mediums. In an IS context the *awareness* would be targeted to all employees within the organisation [2]. Secondly, e*ducation* is concerned with the *systematic instruction* about a topic, where *systematic* involves the development of knowledge and understanding given in several levels that may lead to a specialisation on the topic in question. Lastly, *training* involves a notion of *practicing* or *exercising* the acquired knowledge or skills [13]. In an IS context different *education* and *training* would be required by determined job functions [2] that might require the development of specific knowledge and skills. For example, while all employees should be aware of the threats posed by leaving their workstation unattended and be trained on how to control that risks, only few people should be trained on how to protect the e-mail server of the organisation.

In addition, it is also necessary to clarify what is meant by the terms *Program* and *Campaign* within the ISA context. These are defined by [34] as:

*Campaign:*

> *"Applied to any course of action analogous to a military campaign, either in having a distinct period of activity, or in being of the nature of a struggle, or of an organized attempt aiming at a definite result"*

*Program:*

> *"a plan or scheme of any intended proceedings (whether in writing or not); an outline or abstract of something to be done. Also: a planned series of activities or events; an itinerary"*

*Information Security Awareness Campaign* (ISAC) is a concept that involves targeted efforts towards the achievement of specific information security objectives over a determined period of time. According to Rogers in [8] effective *campaigns* strategies consist of:

1) **Formative research**. Where the intended audiences are analysed and the content of the messages are planned accordingly.
2) **Definition of campaign goals**. Where the purposes of the campaign are defined as detailed and specific as possible.
3) **Audience segmentation**. Where employees are logically divided into groups with relative homogeneous characteristics.
4) **Design of campaign's mass messages**. Where a set of activities and messages are expected to be designed in such manner that they can "trigger interpersonal network communication among members of the intended audience" [2, 8, 13].

For example, assume that the results of a *formative research* may report the need to protect the business information of an organisation against the threats posed by having employees opening *unsolicited* e-mails (formative research). Hence, an ISAC would have the purpose of minimising the negative effects caused by unsolicited e-mails in a time period of six months (definition of campaign goals), by informing the employees (awareness through *campaign's mass messages*) who interact with parties outside the organisation (audience segmentation) about this threat and also prepare them on how to behave when faced to that risk through pre established training sessions (education and training through *campaign's mass messages and activities*).

It may be noted that *awareness*, *education* and *training* are in their own complete phases that may happen at different points in time. However, it is expected to have *education* and *training* preceded by *awareness* in order to ensure a deeper understanding and reinforcement of the IS messages.

*Information Security Awareness Program* (ISAP) is a concept frequently used in the literature that encompasses the sum of all efforts towards the nurturing of a security-minded culture (from the definition above) by *planning a series of security activities or events*; the efforts that are expected to appear in a regular basis such as *awareness*, *education*, *training* and *campaigns* all form part of the overall ISAP [35] which is undertaken regularly either to achieve a new IS objective or reinforce existing ones, as illustrated in Figure 2.2.

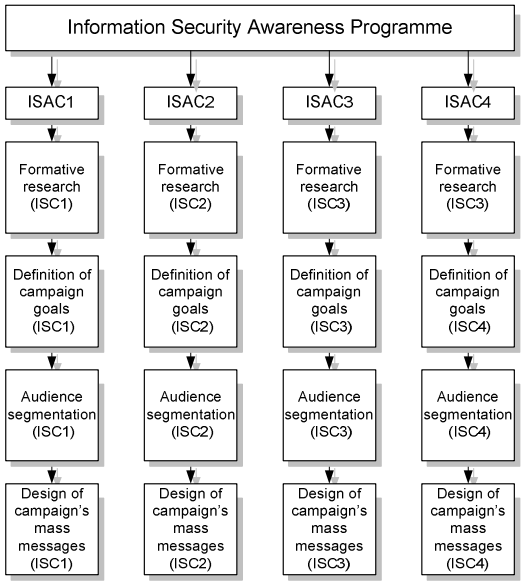



**Figure 2.2** Model for an ISAP [35].

One of the main objectives of ISA is to decrease the level of risk against IT systems by informing the employees about the risks associated with the technology they are operating, which may result in a decrease in the number of security incidents [1]. However, in [37], Parker questions whether the risk approach is the best option in which ISAP should be based, arguing that risk cannot be objectively measured. In addition he suggests a positive approach for ISAP instead, which main focus would be that of *due diligence* towards the business information and information systems as well.

Another motivation for implementing ISA might be compliance to legal, regulatory or contractual requirements as a mechanism to prevent legal charges against the executive management [19]. However, this approach might not be able to guarantee an objective positive effect in the employee behaviour, since an ISAP requires a continuous effort [35].

Although, having employees educated and trained to be aware of the security policies, standards and guidelines might be important ISA objectives to pursue [19], it can be argued that behavioural change is one of the most important and one of the most difficult objectives to achieve [8]. This is the reason of why the word *nurture* is used in the ISAP definition; it has the purpose of emphasizing that supplying information regarding IS issues is not enough to cause a behavioural change; conversely, what is needed is a more holistic approach that enables employees to develop a security-minded culture and stimulates the required security response [1].

In general anyone within the organisation that operates any form of IT services and manages business information in any form should receive enough information to learn about their associated threats and how they can be countered [5]. Since in modern

organisations the majority of employees fall in this category, the achievement of the ISA objectives will be determined not just by the number of employees reached through the ISAP, but also in the manner the messages stimulates employees to learn more about IS issues and interact with their peers [13]. Furthermore, in [36] it is suggested that even those employees not using any form of IT shall be "security aware".

## 2.6 Effectiveness of current ISA approaches

In general, it could be said that the effectiveness of a project is commonly measured according to the extent that the pursued objectives are achieved. From this perspective the effectiveness of an ISAP would be determined according to the extent in which behavioural change is achieved. However, as it was previously argued, this objective is not easily achieved nor easily measured. Therefore qualitative and quantitative methods need to be used in this regard in order to obtain an objective approximation of the effectiveness of additional factors that influence the success of this objective [33, 38].

### 2.6.1 Measurement approaches

For instance, in [38], *PriceWaterHouseCooopers* identifies a set of methods commonly followed by organisations to measure the effectiveness of the ISA approaches. These are basically four:

1. **Process Improvement**. This approach is concerned in assessing the surrounding issues of the ISA process itself and the elements that support it. It is not concerned with issues such as if the security level was improved or not. For example the performance indicators that this approach could assess include among others:

    a. *The correctness* of the security message and guidelines, by assessing the extent that the security message and guidelines are addressing the business risks.
    b. *The delivery method,* by estimating the number of people that were reached by the security message.
    c. The *freshness* of the security message, by measuring the frequency in which the security message is updated.
    d. The *deployment* method by measuring how many employees are aware of the security message and guidelines.

Advantages:

- The performance indicators described above can easily be defined and collected.
- The performance indicators a) and c) can be reassessed before the end of the ISAC, enabling the ISA manager to adjust the process accordingly.
- Returns useful information that can allow the ISA process to be improved.

Disadvantages:

- This approach is not concerned on measuring whether the security level was improved or not.
- Cannot provide the assurance that the ISA objectives are being achieved.
- Some measures depend on the feedback provided by employees which may be subjective.

2. **Attack resistance.** This approach is concerned on measuring how prepared employees are at the moment of facing a security attack. For example the performance indicators that this approach could assess among others include:

   a. The number of attacks employees can recognise. For example, asking employees to answer an online quiz or a survey.
   b. The number of successful attacks. For example if employees are persuaded to disclose their password.

   Advantages:

   - This approach shows some of the results achieved by the ISAP.
   - Since these results are commonly positive, they can be used to convince the executive management of increasing the budget for ISA activities.
   - Since employees are directly targeted on security issues, the interest in security issues might increase.

   Disadvantages:

   - There could be a considerable number of attack scenarios and the attack scenario to be tested tends to be very specific.

- An interactive attack scenario could result in being costly and cumbersome to manage in large organisations.

3. **Efficiency and effectiveness.** This approach is concerned with the nature of security incidents involving human behaviour. For example the performance indicators that this approach could assess among others include:

   a. The number of security incidents due to human errors.
   b. The amount of downtime due to human behaviour.
   c. The number of incidents due to human errors that caused severe impact in the organisation.

   Advantages:

   - These measures could be easily implemented by the *incident management process* (IMP).
   - The measures obtained may result of interest for the executive management.
   - The statistics may reveal tendencies and areas where ISA should be targeted, improving the overall ISAP.
   - It enables the possibility to report how much it costs to the organisation the lack of awareness.

   Disadvantages:

   - Since not all employees might be reporting the security incidents, the statistics provided by the IMP may not reflect the current state of security awareness within the organisation.
   - In order to conduct an accurate collection of incidents resulting from ISA, the helpdesk staff would need to be trained to distinguish between regular incidents and incidents resulting from human errors.

4. **Internal protections.** This approach is concerned in assessing the extent to which the individual has assimilated the security messages and guidelines in order to apply those principles in their day-to-day activities; that is, the extent that their behaviour has been affected. For example the performance indicators that this approach could assess among others include:

   a. The number of viruses that their computers have been infected with.
   b. The manner in which they protect sensitive data.

c. The number of unauthorised content and software installations onto their computers.

Advantages:

- The approach could provide objective measurements of the effect of the ISAC.
- Internal or external audits may provide valuable feedback on the effectiveness of the ISAC.

Disadvantages:

- Any given measure would be specific to the behaviour that is being measured.
- Behavioural change is a complex issue (more on this in chapter 3) difficult achieve and difficult to measure.
- The measurements are on specific behaviours, while the ultimate objective is to conduct any activity with security in mind.

Far from being an exhaustive list, this is just a generalisation of the methods identified in [38]. In real operating environments, organisations would use a wider variety of methods or combine several of these approaches with a set of additional and more descriptive metrics for a more accurate measurement of the effectiveness of their ISAP.

According to [38], the order in which these approaches are used by respondents starting from the most popular approaches are:

1. ***internal protection*** is used approximately *by* ***two thirds*** of respondents
2. ***efficiency and effectiveness*** is used approximately by **over half** of the respondents
3. ***attack resistance*** is used approximately by **one quarter** of the respondents
4. ***Process improvement*** is used by a small number of the respondents.

The methodology for assessing the ISA proposed by Kruger in [33] uses 3 dimensions: *knowledge*, *attitude* and *behaviour*; that is, these dimensions asses what employees know about the topic, whether employees have a positive or negative attitude towards IS issues, and assess employees security behaviour in the face of a security threat respectively. Additionally, each dimension considers 6 focus areas, namely *adherence to company policies, secrecy of passwords, careful use of the Internet and e-*

*mail, careful use of mobile equipment, report security incidents, actions-consequence awareness.* Kruger remarks the last focus area as the most important in his model. Hence, Kruger's model could be classified as a combination of the *attack resistance* and *internal protection* approaches.

As it can be noted, the effectiveness of an ISAP could be measured from different angles, but researchers remark one out of the rest, which is regarded as one of the most important to measure, the one that measures the extent to which the behaviour of the individual was affected by the ISAC.

### 2.6.2 The state of ISA

As IT risks are addressed by developing the correspondent security countermeasures, ISA aims in the same sense to develop a security-minded culture as a countermeasure against the risks posed by human factors [37]. As evidence shows, this countermeasure is not easy to get right.

According to the Information Security Status Survey [35] conducted by the *Information Security Forum* (ISF), the majority of the respondents believe that their ISA programs are not being effective, as they have not achieved their objectives and behavioural changes are not clearly perceived. Furthermore, the majority of the respondents admitted that the awareness initiatives are not sufficiently supported in terms of time, efforts and resources in general.

Moreover, the Security Awareness Index Report [36] conducted by Pentasafe Security Technologies, is a survey undertaken among 583 organisations worldwide which reports that two thirds of the respondents feel that their ISAP is "either inadequate or dangerously inadequate", particularly in financial institutions, healthcare and public and government agencies.

### 2.6.3 Common ISA problems

According to [35] the ISF identified 7 key issues that contribute to the unsatisfactory results of ISA initiatives:

1. **Informal ISA management framework.**

   Consequences:

   a. Awareness activities might be relegated and incorrectly prioritized.
   b. The ISAP might not be conducted appropriately due to a lack of commitment and meet projected deadlines.

According to the *Information Security Status Survey* [35] more than a half of respondents are using an informal ISA management framework; a programme that lacks of the appropriate structure that could enable the overall program to achieve its objectives. Even though the ISF does not mention it, informal ISA programmes could also result in negative attitudes by employees towards security issues.

2. **Unclear reasons for the need of ISA.**

   Consequences:

   a. Difficulties to justify before the executive management the need for resources to conduct an ISA
   b. Difficulties to measure accurately the effectiveness of an awareness activity.

   According to [35], the general perception is that the majority of the respondents believe that ISA needs to be raised because it is a good practice rather than a clear understanding of how they can contribute towards the overall reduction of business information risks. This problem reflects a situation where the value of information is not perceived clearly within the organisation.

3. **Lack of a formal and documented objective.**

   Consequences:

   a. The overall ISAP would suffer of permanent insufficiency because of ineffective activities and the waste of time, efforts and resources.
   b. Difficulties to evaluate if a determined awareness activity succeeded or not.
   c. Difficulties to obtain an accurate financial cost of the ISA activities.
   d. Employees might get confused on what is expected from them because of inconsistent security initiatives.

   According to the *Information Security Status Survey* [35] less than 10% count with a documented ISA objective.

4. **Lack of top management support.**

   Consequences:

   a. Poor cooperative actions from management toward the development of a mature ISAP.
   b. Lack of credibility and commitment from employees towards the awareness initiatives.

c. Poor appreciation from employees of the importance of security to their roles.
d. A behavioural change is unlikely to be achieved due to the lack of the influence of the top management sponsorship.

The *Standard of Good Practice for Information Security* [39], produced by the *ISF,* recommends that ISA initiatives shall be based on formal programmes and supported by a top management executive. The same position is appreciated in the international standard *ISO/IEC 27001:2005.* The *Information Security Status Survey* [35] reports that only 33% of the awareness activities are sponsored by the senior business management.

**5. Failure to use specialised awareness materials.**

Consequences:

a. Unclear and repetitive security messages might be ignored by employees that have heard similar messages and rather than reinforcing the expected behaviour, employees might lose interest.
b. Employees might fail to adopt the desired behaviour since it is not clear what is expected from them.

By specialised awareness materials the *ISF* refers to brochures, posters, reference cards, electronic documents, etc. According to the *Information Security Status Survey* [35], it is very common to deliver repetitive security messages using non-specialised awareness materials in approximately half of the awareness activities.

**6. Measuring knowledge of employees rather than measuring the effectiveness of the ISAC.**

Consequences:

a. False feeling of security. Since measuring *awareness* could show that employees might know about a determined security issue, measuring *effectiveness* proves whether the security message changed the behaviour of the employee.
b. Difficulties to measure the success of the ISAC because of the lack of a mechanism to measure effectiveness.

According to the *Information Security Status Survey* [35], the methods for measuring effectiveness followed by the respondents might be subjective. In addition, the ISF reports that even though the respondents may assess the success of awareness activities in some form, the majority do not count with a formal method to measure the effectiveness of the ISA activities.

**7. Lack of sufficient resources to maintain an ISAP.**

Consequences:

a. ISAP might not receive the appropriate treatment and commitment from the security management team, hence failing to achieve the overall ISAP objectives.
b. Resources might be in the form of time, efforts, money and support. According to the ISF in [35], four out of five member organisations feel that they have not committed sufficient time to the development and implementation of the awareness activities.

Turning to the survey results provided by Pentasafe Security Technologies [36], the reasons of why organisations are obtaining such unsatisfactory results seem to be involved with:

- Flaws in the implementation of the basic ISA best practices, such as data classification and measurement systems.

  According to [36], more than half of the respondents do not provide sufficient guidance on how to protect information resources. Moreover, approximately two thirds of the respondents do not track if employees have read the security policies.

- Lack of formal security awareness training.

  According to [36], almost a half of the respondents have not received formal security awareness training. Moreover, less than one fifth have received security awareness training in the past six months.

According to [28] human error is the first cause of failures; therefore security awareness initiatives are the top priorities of management. In this survey Deloitte identifies the following most common security vulnerabilities posed by human factors:

- Email attacks (SPAM)
- Virus and worms outbreaks
- Phishing/pharming
- Employees misconduct (intentional)
- Spyware
- Social engineering

Whereas the *CSI* (Computer Security Institute) survey [29] reports that the top three attack types are:

- Insider abuse of NetAccess
- Viruses
- Laptop / mobile device theft

The results reported by these surveys indicate that the human factor is still the main cause of major failures. Since ISA aims to mitigate the risks posed by human factors, the ISA approaches being used seem to be not as effective as expected.

Apparently, the financial losses associated with security incidents involving human causes have dropped in respect to past years. According to [6], the total cost of security incidents dropped a third in respect to the results obtained in 2006. Moreover, the CSI in [29] reports that the overall financial losses have dropped nearly a half compared with the results obtained in 2006. One question that needs to be asked, however, is whether these results in fact represent that financial losses are being dropped due to effective security measures or not.

The reality is that in both surveys there are additional factors apart from possible effective security measures that influenced the drop of financial losses. For instance, the CSI in the survey [29], reports that many organisations were reluctant to share details about their financial losses; therefore a considerable number of respondents did not answer this question of the survey and as a result the overall amount of financial losses dropped. Although in the survey [6], PriceWaterHouseCoopers and associates do not mention explicitly that there were fewer respondents regarding this issue, they pointed out that there are a lot of security incidents that are not reported and hence their associated financial losses not disclosed as well.

Nonetheless, it shall be considered that some of the implemented security measures might be working successfully. In the survey of 2006 conducted by the CSI in cooperation with the FBI (Federal Bureau of Investigation) [40], reported that *virus contamination* was the most common security incident whereas in the 2007 survey [29] the CSI reports that this type of attack as the second most common which might indicate an improvement in this type of security measures. Similar results were obtained in 2007 in the survey [6], while in 2006 virus infection was the most common cause of security incidents, in 2008 virus infection dropped to be in the fourth place.

The results obtained in [28] by Deloitte, in [36] by Pentasafe Security Technologies and in [6] by PriceWaterHouseCoopers and associates, reveal that the financial services industry is the sector that appears to spend most on security, and particularly in ISA initiatives. These results are significant, since the financial sector seems to be highly concerned on IS issues and probably more receptive to ISA initiatives.

### 2.6.4 Case study: ISA initiative in FIRA

FIRA (Fideicomisos Instituidos en Relación con la Agricultura) is a Mexican financial institution whose mission is to create value in the productive networks of the rural and phishing sectors with efficiency and profitability criteria, through the development of the financial, technological and service markets.

In December 2003 the institution, through an outsourced service provided by a third party, designed the content of an ISAP according to the needs of the institution. One of the top management directors was involved in this initiative.

Three ISAC was designed, intended to be delivered in three phases: 1) Introductive, 2) Informative and 3) Reinforcement under some marketing concepts and methods such as the *target audience* which was the entire number of employees in FIRA, the *product* which was the ISAP itself and the *objective* which aimed to achieve an understanding and a behavioural change on the employees regarding IS issues through the use of attractive visual aids.

The objective of the *Introductive* phase was to obtain the attention of employees and generate and maintain their interest on IS issues. The communication strategy in this regard was striking visual aids and short but meaningful messages. The communication channels used in this phase were official institutional channels, lectures and training sessions that were designed for targeted audiences. Additionally, the channels used for general audiences included animated spots sent via e-mail, intranet web page. The time estimated for delivering the content of this phase was 4 weeks.

The objective of the *Informative* phase was to deliver the information security policy, the security requirements and the behaviour that is expected from them using similar methods, materials and communication channels.

The objective of the *Reinforcement* phase was to reinforced the acquired knowledge, communicate any changes made to the information security policy, and maintain a short but continuous delivery of the content of the information security policy according to the relevant audiences.

In general the first phase was the awareness itself, and the following phases involved training and education strategies to reinforce the security messages and to aid a behavioural change on the employees. The overall design and activities seemed to be plausible and promising but unfortunately the ISA initiative undertook by the institution failed, barely concluding phase 1.

From the point of view of the results of Pentasafe Security Technologies in [36] the ISA initiative involving these three phases was attempting to implement the basic ISA best

practices, such as data classification, a tracking mechanism and a system to measure the results. Additionally in the second and third phase a formal security awareness education and training was considered not just to raise the level of security awareness but an attempt to affect employees' behaviour.

From the point of view of the *key issues for security awareness* identified by the ISF in [35] :

1. The ISA initiative did have a formal structure and a formal ISA framework, since there was enough documentation, formal deadlines and was initially prioritised as an institutional concern (*key issue 1*).

2. The security management team had clear and documented reasons of why information security awareness had to be raised (*key issue 2*).

3. The ISA initiative had formal and documented objectives in each of the planned phases which were revised with the top management. Additionally the costs associated with the ISA activities were correctly budgeted (*key issue 3*).

4. Initially, one of the top management directors was involved in the ISA initiative, sponsoring the project and providing his support, but unfortunately, though the ISAP had a formal structure, the IS framework that was intended to be created within the organisation could not be officialised, causing the initiative to eventually be relegated and inappropriately prioritised. The fact that the programme was not supported by an official IS framework as it was initially intended, shows a lack of sufficient top management support (key issue 4).

5. The ISAP design considered appropriate specialised awareness materials. Furthermore, some material was targeted to specific audiences in order to facilitate the understanding of the security message and the behaviour expected from employees (key issue 5).

6. The proposed ISAP design considered a form for assessing the awareness activities effectiveness, according to section 2.6.1, this is a combination of a *process improvement* and *internal protection* approaches (key issue 6).

7. Since not all levels of management echoed the support for the initiative and additionally the implicit lack of top management support, the resources to fund the ISA activities were eventually insufficient. The commitment of the security management team was scarce because they were under pressure from carry on with other activities. Since it was not supported by an official business unit,

economical resources were retired or not considered anymore for these activities (key issue 7).

**Table 2.1** Case Study – factors influencing the unsatisfactory results of the ISAP in FIRA.

| FIRA – ISAP | | |
|---|---|---|
| **ISF – 7 key issues for ISA** | **Pentasafe critical factors** | **Measurement approaches** |
| ☑ Informal ISA management framework. | ☑ Flaws in the implementation of the basic ISA best practices, such as data classification and measurement systems. | ☑ Process Improvement |
| ☑ Unclear reasons for the need of ISA. | ☑ Lack of formal security awareness training. | ☒ Attack resistance. |
| ☑ Lack of a formal and documented objective. | | ☒ Efficiency and effectiveness. |
| ☒ Lack of top management support. | | ☑ Internal protections. |
| ☑ Failure to use specialised awareness materials. | | |
| ☑ Measuring knowledge of employees rather than measuring the effectiveness of the ISAC. | | |
| ☒ Lack of sufficient resources to maintain an ISAP. | | |

The overall results of this ISA initiative:

- People ignoring further security messages from the IT department.
- Behavioural change could not be achieved, as security incidents involving human errors, addressed by the ISAP, were still being reported.
- Poor appreciation from employees of the importance of security to their roles.
- Credibility and commitment affected from employees towards the awareness initiatives.
- Since the ISAP was not an institutional concern until 2008, all the security incidents caused by human errors are unlikely to be quantified, hence the inability of the institution to prevent and estimate its financial losses caused by this issue.

## 2.7 Summary

In this chapter it has been discussed how the adoption of IT introduces additional risks that have to be addressed in some form. These solutions are typically found in the form of other IT solutions which essentially follows the same risk pattern. The more the organisation adopts IT solutions (whether they are secure IT infrastructure to secure other IT solutions or not), the more the organisation become dependent on people and their technical skills. IT became ubiquitous within the organisations, therefore any person dealing in some manner with IT and business information must receive proper awareness, training and education. The security awareness initiatives must be fully supported by the top management and form part of an official IS framework, this is only possible if ISA is derived from an *Information Security Governance* strategy undertaken by the executive management and board of directors. Since the ultimate objective of ISA is to achieve a behavioural change on those individuals interacting with the information resources of the organisation, awareness is not enough, but a combination of awareness, education and training can aid in the achievement of this goal based on behavioural theories. Several methods are used nowadays to measure the effectiveness of the ISAP mostly combining several approaches to obtain a more accurate result. Additionally, key issues identified by the *ISF* and *Pentasafe Security Technologies* that are involved in the unsatisfactory results of current ISA approaches, were used in a case study of a financial institution that helped us explore the causes of its failure.

# Beyond Awareness

## *When Awareness is not enough*

CHAPTER

3

## Contents



## 3.1 Introduction

The purpose of this chapter is to explore some approaches of social psychology which have been used by researchers who have aimed to achieve a change in attitude and behaviour on individuals towards IS issues. Additionally, to explore popular trends that can also be considered such as the *viral marketing* principles. Lastly, a combined approach is proposed to be used as the base of the overall proposed framework in this dissertation.

## 3.2 The ultimate goals of ISA

As mentioned earlier in Chapter 2, section 2.5 *"ISA, requirements and objectives"* the ISA definition borrowed from the ISF involves a *decision making process* where employees are expected to *act* according to the security knowledge that they posses after an ISAC is delivered. The word *act* and *behave* can be used interchangeably in this definition as it can be appreciated in [35]. It could be argued that ISA may have several objectives such as reducing the number of security incidents or reducing the risks posed by human failures in IT systems [1], for example; nonetheless, the ultimate goals ISA pursues are to achieve a change in the *attitude* and *behaviour* of people [41, 42]. In this dissertation the term *attitude* is going to be used to refer to the negative or positive position that a person adopts toward a determined issue [43].

As it has been discussed earlier, *awareness* by its own would not be sufficient to achieve such behavioural change; what is needed, apart from initial *security awareness*, is a method to affect the mechanism of the individual's *decision making process* [1]. It is by using the appropriate psychological techniques that this mechanism can be affected and as a consequence influence people's attitudes and behaviours [42]. Unfortunately, these principles seem to be ignored by security professionals when designing the ISAP [41].

For instance, in [44] Puhakainen reports 59 different ISA approaches found in the academic and industrial environments that aims a behavioural change on the individual. However, the study reports only 2 ISA approaches that employ social psychology [41, 42] as a means to influence people's attitudes and behaviour, and 1 ISA approach using the stimulus-response model (see [45]). In addition there are at least 2 ISA approaches that Puhakainen's study did not consider and the author offers no explanation for its exclusion. One of them conducted by Leach [14] uses a combination of the stimulus-response model and cognitive processes. The second approach produced by the ISF uses the *Force Field Analysis* technique developed by Kurt Lewin [35], to achieve a *behavioural change* on employees. These two approaches are discussed further in this chapter.

## 3.3 The Behaviorist approach

The behaviourist approach aims to explain and measure the human behaviour displayed in response to a stimulus. In the literature this is known as the stimulus-response or S/R model [1]. According to Skinner [45], a *stimulus* is produced by a variation in the environment affecting the organism and the correspondent part of the displayed behaviour to this *stimulus* is properly the *response*. For example executing a new program in a computer system; that is, manipulating the current state of the

environment would be the *stimulus* and the corresponding consumption of computer resources observed such as memory and processor time would be the *response* or displayed behaviour.

In [45], Skinner points out that even though it might be unlikely to demonstrate that a displayed behaviour could be the result of the stimulating environment as a whole, he asserts that it is possible to induce *part* of the displayed behaviour according to certain laws. For instance, ISA aims to obtain as a response a positive attitude from employees towards IS issues in such a manner that they observe the ISP and act accordingly to protect the business information and IT systems being under their custody. However, the expected behaviour might be inhibited due to a set of conflicting stimuli such as unclear and undocumented ISA objectives, informal ISA management framework, failure to use specialised materials to deliver the content of the security message or in general all those tasks that employees are asked to perform that overrides the priority of IS issues or overlook the IS concerns that shall be considered in their day-to-day activities.

### 3.3.1 The static laws of the reflex

According to Skinner [45], there are a number of laws that might make possible to induce a part of behaviour, he calls these "*the static laws of the reflex";* the term *reflex is used* to refer to the observed relation between a stimulus and a response [45, pp. 12-14].

#### 3.3.1.1 The law of threshold:

> *"The intensity of the stimulus must reach or exceed a certain critical value (called the threshold) in order to elicit a response"* [45, p. 12].

This law refers to the degree that the individual possess to resist external forces, particularly if these forces are not intense enough. The individual would be affected only when the external forces exceed the individual's degree of resistance [45].

For example, according to this law if the security message (*stimulus*) is not meaningful to employees then the desired *response* is unlikely to appear; that is, to engage the employee's interests in IS issues.

3.3.1.2 The law of latency

> "*An interval of time (called the latency) elapses between the beginning of the stimulus and the beginning of the response*" [45, p. 12].

The individual do not respond immediately to a *stimulus*; moreover, the time taken to respond to a determined stimulus will vary from individual to individual. Furthermore, the latency is determined by the strength of the stimulus, the stronger the stimulus the shorter the latency [45].

For example, according to this law if the sponsorship and support from all levels of management in favour of ISA initiatives are visible to all employees within the organisation (*high intense stimulus*), the adoption of the ISP is likely to occur within a reasonable short amount of time (*low latency*). On the other hand, if the employees do not perceive such top management support and are simply required to comply with the new organisational policies (*weak stimulus*), the rate of adoption of such policies is likely to be slower (*high latency*) than if top management support were visible.

3.3.1.3 The law of the magnitude of the response:

> *"The magnitude of the response is a function of the intensity of the stimulus"* [45, p. 13].

The more intense the stimulus, the stronger is the response; this is known as the S/R ratio. Moreover, the response is likely to be drawn only if it meets the law of threshold [45].

For example, according to this law if the sponsorship and support from all levels of management in favour of ISA initiatives are visible to all employees within the organisation (*high intense stimulus*), a high rate of adoption of the ISP is likely to occur (*strong response*) within a reasonable short amount of time as a consequence (*low latency*).

3.3.1.4 The law of after-discharge

> *"The response may persist for some time after the cessation of the stimulus"* [45, p. 13].

This law not just refers to the time the response persists after the stimulus, but also refers to the activity during this time. The more intense the stimulus, the more the time and activity increases [45].

For example, assume that the security message meets the law of threshold and carries a highly impacting security message that can engage the interest of employees (*intense stimulus*) then according to this law after the security message is delivered employees would be interested in IS issues and willing to comply with the ISP. However, this response would not last for an indefinite amount of time; it would need to be reinforced to maintain the interest of employees. Otherwise, eventually, such response would disappear.

3.3.1.5 The law of temporal summation

> *"Prolongation of a stimulus or repetitive presentation within certain limiting rates has the same effect as increasing the intensity"* [45, p. 13].

This law refers to those stimuli that are not intense enough to meet the law of threshold; however, summation and prolonged repetitive presentation of weak stimulus that do not surpass the threshold value, may elicit a response if such stimulus is presented at regular times and at regular rates [45].

For example, according to this law the design of the security message may not necessarily satisfy the demands and requirements of each employee within the organisation (*sub-threshold stimulus*) but if a set of security messages (*summation of sub-threshold stimulus*) are being sent in a determined regular basis at the appropriate time, the overall ISA initiative would raise in intensity, causing a high rate of adoption of the ISP (*strong response*) that would last for a determined period of time (*after-discharge*).

The term *static* is used here by the author to distinguish this set of laws from others that deal with a change in the observed behaviour when a reflex is repeatedly elicited, which he calls *"The dynamic laws of reflex".*

### 3.3.2 Dynamic laws of reflex strength

3.3.2.1 The law of reflex fatigue:

> *"The strength of a reflex declines during repeated elicitation and returns to its former value during subsequent inactivity"* [45, p. 16].

When a reflex is repeatedly elicited a degree of tolerance seems to be developed in the individual; according to Sherrington [46], several laws are affected. The *law of threshold* is affected by increasing the *threshold* value; the *law of latency is affected* by increasing the *latency* value; the *law of after-discharge* is affected by reducing the

amount of time and the activity taking place once the response is elicited and the *law of the magnitude of the response* is affected as well by decreasing the magnitudes in the relation S/R [45].

For example, according to this law, if an individual's attitude towards IS issues presents a low threshold value to respond negatively to ISA initiatives, and the latency value in which the individual decides to discard the security messages is short, and the individual's response after receiving the security message takes a long time to appear to follow the security guidelines, then by repeatedly eliciting such negative reflex, the static properties of the individual are likely to be affected and develop a certain degree of tolerance; in other words, the threshold value to respond negatively would raise [45, 46], hence reducing the negative response against the security message and eventually eliciting a positive response. The latency value in which the negative response used to appear would rise [45, 46], delaying its appearance and allowing the individual to be exposed more time to the security message in order to be able for the individual to assimilate it. Moreover, the *after-discharge* and S/R ratio value would be reduced as well [45, 46]. This means that the negative position against IS issues taken by the individual would not last and eventually the negative response would disappear or be at minimum, as the stimulus is less negative each time (*weak stimulus*); therefore the negative response would be weaker each time as well.

### 3.3.2.2 The law of facilitation

> *"The strength of a reflex may be increased through presentation of a second stimulus which does not itself elicit the response"* [45, p. 16].

This law takes into account additional stimuli that by themselves are unable to elicit the desired response; however, if the reflex is already present but the response is weak, the additional stimulus may facilitate the reflex to elicit the desired response [45].

For example, according to this law, for those cases where employees are in the process of changing their behaviour (*reflex*), they may remain in that state for a prolonged period of time unless they start seeing their workmates adopting the security guidelines delivered through the ISAC (*sub-threshold stimulus*) whereas the mere observation of others complying with the ISP might not elicit the desired response by itself (unless the model they are watching is an influential individual, but for the purpose of this example this is not the case, more on this in chapter 5).

3.3.2.3 The law of Inhibition

> *"The strength of a reflex may be decreased through presentation of a second stimulus which has no other relation to the effector involved"* [45, p. 17].

This law is essentially the same as *the law of facilitation* except for the sign. Whereas the *law of facilitation* increases or aids the appearance of a determined response, the *law of inhibition* aids to degrade a response [45].

For example, according to this law, the adoption of the desired security behaviour would be inhibited or may never appear (*reflex*) if employees see their line manager not complying with the ISP or not following the security guidelines deployed during the ISAC (*additional stimulus*).

### 3.3.3 Operant Behavior

In [45, p. 20], Skinner uses the term *operant to* refer to that behaviour for which the response is not previously correlated with its eliciting stimulus. He refers to the process of conditioning an *operant* behaviour as Type R, in order to distinguish it from the process of conditioning that type of behaviour for which the eliciting stimulus is correlated with its correspondent response which he refers to as Type S. For example, if an employee spontaneously decides to help her/his workmates regarding IS issues, the behaviour is catalogued as *an operant* since the eliciting stimulus might be unknown.

3.3.3.1 The law of conditioning of type R:

> *"If the occurrence of an operant is followed by the presentation of a reinforcing stimulus, the strength is increased"* [45, p. 21].

For example, according to this law, an employee might decide to report security incidents as the result of an apparent "spontaneous" decision (*operant*); since this represents a desired behaviour, it then should be reinforced in order to strength the response and ensure its recurrence. The reinforcing stimulus could be in the form of a reward upon the displayed behaviour [45].

According to Peter and Nord [47], nowadays psychologists consider operant conditioning and the S/R theory as two separate approaches. Moreover, Peter and Nord [47] state that operant conditioning do not fall under the S/R model but under a *response-reinforcement* model, since the focus of operant conditioning is to reinforce a determined response regardless of the stimuli that occurred. In addition, operant

conditioning is not concerned with learning, but on seeking the recurrence of a determined behaviour.

### 3.3.3.2 The law of extinction of type R

> *"If the occurrence of an operant already strengthened through conditioning is not followed by the reinforcing stimulus, the strength is decreased"* [45, p. 21].

For example, according to this law, if an employee is already displaying the desired security behaviour intended by the ISAP (*operant*), the lack of any reinforcing stimulus (in the form of a reward, for example) would cause eventually the behaviour to disappear [45].

According to Skinner [45], the strength of the operant is a function of the rate of occurrence. This means, that the more frequent the individual's security behaviour is reinforced, the longer it would take for this behaviour to disappear. Conversely, the more the individual's security behaviour is required to be displayed without any form of rewards, the more likely is the security behaviour to disappear.

These are the laws that to a certain extent capture the essence of behaviourism upon which further behavioural theories were founded and others such as *constructivism,* which adopts a cognitive approach, emerged as a result from the strong criticism against behaviourism [48].

Although Skinner acknowledges the existence of studies where several scholars attempted to demonstrate the *deterministic nature* of behaviour (where for all type of behaviour there was a stimulus-response correlation, hence arguing a deterministic nature), he contends that this assumption is an "unsatisfactory appeal to ignorance" and points out that there exist a wide range of behaviour for which no stimulus is known, that he calls *operant* [45, pp. 19-20].

Perhaps the major criticism against behaviourism that has been pointed out by scholars, according to Peel [48], is that behaviourism attempts to explain any resulting behaviour from the perspective of a pure stimulus-response perspective without considering the individual's previous knowledge or cognitive psychological processes that play a role in the resulting behaviour.

Nevertheless, in [48, p. 21] Peel contends that some of the behaviourism principles should not be discarded without a studied consideration since they could be ignored as a result of a common assumption of being flawed. Moreover, he suggests an

integrative approach by combining different behavioural theories as the theoretical base for learning theories, that is, for example by combining behaviourist principles (which do consider cognitive aspects) with constructivist principles as the foundation for effective learning theories.

An example of an ISA approach that uses the stimulus-response model of behaviourism is proposed by McLean in [1]. In this approach the author uses the S/R model to explain how different and conflicting stimuli can negatively affect the behaviour of the users towards the compliance of ISP (*the law of inhibition*). For example, the ISAC may be stimulating the employees' environment in order to obtain a positive response and act according to the IS guidelines; however, conflicting stimuli reaching employees, such as project deadlines that overrides pre-established security priorities will inhibit the appearance of the desired security behaviour.

Additionally, in [1], McLean explores the possibility of applying conditioning techniques (*the law of conditioning of Type R*) used in some marketing principles where employees are treated as *consumers* and *security messages and guidelines* as the marketed product. Moreover, in [1], McLean combines the S/R model with the diffusion of innovations theory which essentially explains the underlying process that takes place when an individual adopts an innovation or in this case, a *new* idea. As a result McLean produces an eclectic model upon which his ISA approach is based [1].

## 3.4 Behavioral change using social psychology

According to Faris [58, p. 422] *Social Psychology* (SP) is "*the science of human nature in interaction*". SP studies both the collective behaviour of individuals within a group and the individual's character and personality that result from the frequent human interaction within that group. In [58], Faris identifies social influences as a determinant variable on the individual's learned behaviour. Therefore, researchers in the field of ISA [1, 14, 41, 42] and others have used SP techniques to achieve a change on the individual's attitudes, beliefs and behaviour in order to improve the compliance towards the organisation's ISP, obey the security advices given through the ISAC and nurture a security-consciousness that enable employees to make the appropriate decisions in the face of a security threat [1, 41, 42].

In [49], Lindesmith seems to agree that there is no distinction whether the one who learns is a human or an animal. This might be one of the reasons for which the *static* and *dynamic laws* described in the previous section that are used by behaviourists to study how in general an organism learns and consequently behave in a determined manner, are borrowed by *social psychologists* to study specifically how humans achieve a learned behaviour [49].

### 3.4.1 The perception of the reality

From the point of view of social psychology the displayed behaviour is the result of a cognitive process involving the individual's ideas, attitudes, beliefs, knowledge, affective responses and behaviour intentions [43], [42]. It could be said that these are the elements involved in the *decision making* process that needs to be affected in some manner in order to achieve the desired change on the individuals' attitudes and consequently in their behaviour. In [43], Zimbardo identifies this set of elements as the *attitude system* which helps to explain the displayed behaviour by an individual under determined circumstances and conditions. In [50], Schneier identifies these elements in two parts: one as the *feeling* based on intuition and other as a *model* based on reason pertaining to the individual who uses it to perceive reality. In [41], Kabay identifies this set of elements as the *schema* which is described as a mechanism under which individuals perceive reality and make decisions based on this perception.

Clearly, if individuals make decisions based on their perception of reality, then the individual's schema should become the ISAC's target [41]. This argument is paramount and central to what it is proposed in this dissertation, since it would affect the overall ISAP design and at the same time provide a roadmap to develop the ISAC based on this approach.

Nevertheless it should be pointed out that the perception of reality or schema does not necessarily match with reality because an individuals' schema is limited by the amount of knowledge and the inherent cognitive biases to the human nature [50]. Hence one of the tasks of the security practitioners should be to help an individual alter her or his schema in order to provide a closer perception of the reality regarding IS issues.

An example of a schema not matching reality can be found in a scenario where the current employees' perception of the risks against the business information ignores the reality of internal threats. In this scenario, employees' schemata may be formed by a common belief probably obtained from the news media, TV shows or movies where hackers are portrayed as the only and most dangerous threat against the business information but not their workmates who have a limited knowledge in IT and security issues. This schema might lead employees ignoring internal threats. According to the *Information Security Breaches* survey [6, p. 23] almost two thirds of the respondents reported that the worst security incident had an internal cause particularly *staff misuse of information systems* (47%) in large business. These results are consistent with what is observed in other surveys. For example, according to the CSI survey [29, p. 13] the top three types of attacks detected in 2007 were *insider abuse of Net access* (59%) and *Virus* (52%) and *Laptop/Mobile device theft* (50%).

The problem with this schema is probably a lack of sufficient information that could enable the employee to understand the threats associated with their operating environment. If this schema is modified; that is, if employees knows and understands the security threats, then a change of attitude would be expected to arise and consequently be reflected in a behavioural change.

In addition, according to Kabay [41, p. 35-4], many employees' schemata may be in conflict with the ISP. For example, in the ISAC launched by FIRA (institution previously introduced in chapter II) they implemented what they called the "10 Maxims of Information Security". One of the maxims involves *information security incidents* where employees are encouraged to report flagrant security incidents; this implies reporting their workmates committing a security violation. The conflicting schema is that employees are taught to maintain a polite and harmonious working environment and collaborate among themselves to get their job done. If the ISP is not implemented appropriately, it might represent not just a direct outrage against the employees' working environment but an ISP difficult to comply with, since employees would be reluctant to report one of their friends. For instance, this type of security policies should consider some psychological aspects of the employees in order to have an accurate expectation of the results such as personality issues that might arise when trying to comply with the ISP since some compliance problems could be rooted in personality styles rather than in bad attitude towards IS [41].

Having said this, it could be argued that one of the objectives of ISA is to change employees' perception of reality regarding IS issues, in other words, affect their current security schema and bring it as near as possible to match it with the security reality [41].

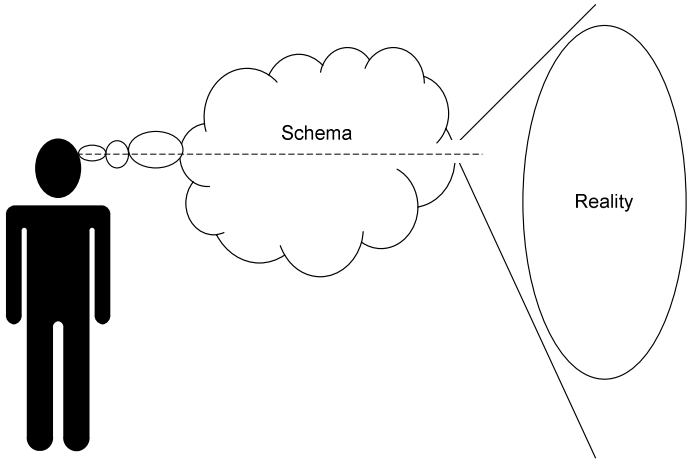



**Figure 3.1** The perception of reality.

Now the question is how to affect this schema to obtain the desired change in attitude and behaviour. By *attitude*, as mentioned earlier in this chapter, the term is going to be used to refer to the negative/positive or favourable/unfavourable position that a person adopts toward a determined issue; regarding the IS context, is the negative or positive attitude that an employee adopts towards IS issues. This position, according to Zimbardo [43], is the result of evaluating the different responses to a set of interrelated elements that he calls *attitude system.* Figure 3.2 shows an *attitude system* example.

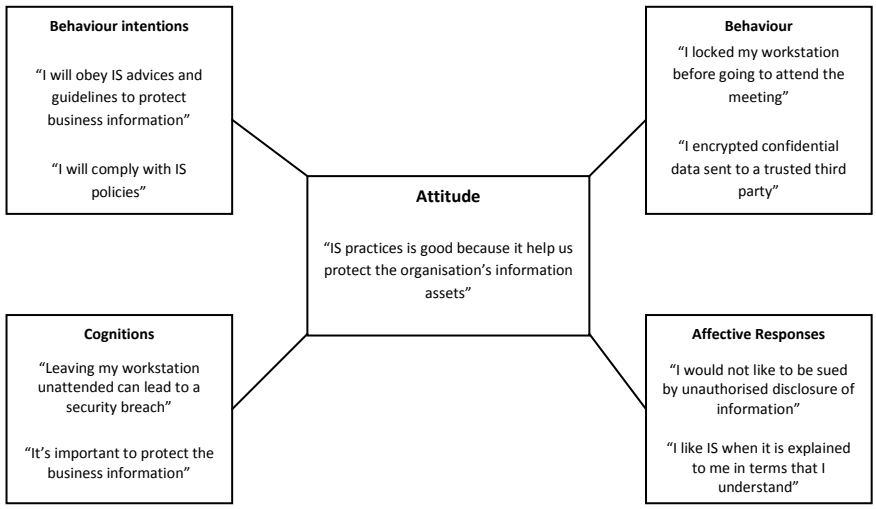



**Figure 3.2** The Attitude System [43].

As it can be seen from Figure 3.2, central to the *attitude system* is *attitude* itself, representing the overall evaluation of the system. The interrelated elements that influence the overall evaluation are the *behaviour*, the *behaviour intentions*, the *cognitions* and the *affective responses* [43, p. 32-33].

**Behaviour intentions.** Refers to the manner in which an individual plans to behave under determined circumstances and conditions.

**Behaviour**. Refers to the observable *action* performed by an individual which may not be the same as the intended behaviour.

**Cognitions.** Refer to the set of ideas and beliefs, knowledge and the notion of the expected behaviour in a determined situation.

**Affective responses.** It involves sensations, emotions and "gut feelings" in general that an individual presents as a response to a determined issue.

As it can be appreciated from the *attitude system* shown in Figure 3.2, all these elements are interrelated. Hence a variation in any of those elements will affect the

rest of them, causing to eventually change the attitude and consequently the displayed behaviour.

According to von Solms [42], there are three particular methods to achieve a behavioural change:

1. Affecting the individual's behaviour.
2. Influencing attitudes through behavioural change.
3. Influencing attitudes through persuasion.

The first method, ***affecting the individual's behaviour***, is what behaviourism attempts to do; it tries to change the behaviour of an individual regardless of any previous knowledge, ideas, beliefs, affective responses and attitudes. Von Solms [42, p. 169] identifies 6 methods falling in this category, however, only those relevant for this dissertation are going to be mentioned:

**Instrumental learning.** Instrumental learning uses two techniques: *operant learning* which is essentially *the law of conditioning of type R* and *Shaping.* The latter is basically operant learning but conducted in increasingly steps of complexity [43], [42].

For example, if an employee starts showing a positive attitude towards IS issues, then that employee could be initially rewarded. Next time, only when that employee shows more than a positive attitude and starts showing a part of the desired behaviour, then the employee is rewarded again. This process continues until rewards are more difficult to obtain and the required behaviour is closer to the expected one.

**Social learning.** This is one of the techniques that are going to be used in this dissertation and it will be explored in more detail in the following chapters. This method considers how an individual is influenced by his/her fellow workers to adopt a determined behaviour as a consequence of pertaining to the same social network [42].

For example, consider an ISP that requires from employees to build a password of at least 8 characters according to password complexity requirements (built with numbers, lower-case/upper-case letters and punctuation marks) and from Systems Administrators (sysadmin) to build at least a 14 character password with complexity requirements. The sysadmin's friends (who are not sysadmins) would be influenced by this practice and the displayed security-minded behaviour and consequently start building their own passwords with these higher security requirements even though they are not obliged to do so (this is a real example extracted from a case study conducted in FIRA).

In general, this technique resembles *the law of facilitation* stated by Skinner in [45], as there is an additional stimulus which by itself is not sufficient to elicit a response; that

is, just by observing the sysadmin complying with the password complexity requirements is not a stimulus with enough intensity that by itself cause his friends to change their passwords in the same manner. However, it may facilitate the sysadmin's friends to comply with such ISP.

**Conformity.** This technique is a special case of the previous one and is involved with group pressure [42]. Within a group, according to Skinner [51], each member is considered a source of stimuli.

For example, consider the scenario of the previous example, but this time the sysadmin's friends are other sysadmins. If one of them has not change his/her password according to the password ISP then this sysadmin would start experiencing group pressure as the displayed behaviour and ideas does not harmonise with those of the rest of the group. Eventually, this sysadmin would adapt his/her behaviour to the one expected by the group.

This technique could be explained from *the law of reflex fatigue's* point of view stated by Skinner in [45]. Since the reflex of a negative response against complying with the ISP is repeatedly elicited by each of the group's members, eventually, the *law of threshold* is affected by increasing the *threshold* value of the sysadmin's negative attitude against ISP ; the *law of latency is affected* by increasing the *latency* value which delays the sysadmin's negative response; the *law of after-discharge* is affected by reducing the amount of time and the activity taking place once the response is elicited, and the *law of the magnitude of the response* is affected as well by decreasing the magnitudes in the relation S/R, that is, the sysadmin's negative response begins to fade, allowing to emerge the desired positive response.

The second method, ***influencing attitudes through behavioural change,*** aims to change the individual's attitudes which ultimately result in a long lasting behavioural change [42]. Von Solms [42, p. 169] identifies 3 methods falling in this category, however, only 2 of them are found relevant for this dissertation:

**Self-persuasion.** This technique requires from the individual to temporarily play a determined role and then the individual is prompted to find arguments to support the underlying point of view of that role. Typically this role would be one that is contrary to the individual's attitudes, ideas and beliefs [42], [43].

For example, this technique would be addressed to those individuals that are reluctant to comply with the ISP. They would be prompted to adopt the role of an *information security specialist* and then be asked to justify a determined ISP or ISA initiative in general. Social psychology research has found that this is one of the most effective techniques to achieve a change in the individual's attitude.

This technique involves some form of *the law of inhibition* stated by Skinner in [45]. Where the role played by the employee which is contrary to his/her ideas and beliefs act as a stimulus that aids to degrade the employee's negative response towards the ISP or the ISA initiative .

**Dissonance.** This technique exploits a natural need for cognitive consistency; that is, any displayed behaviour by the individual contrary to any of his/her beliefs, ideas or attitudes would induce a cognitive inconsistency which in turn would lead to an uncomfortable state that the individual would try to overcome by modifying existing beliefs, ideas and attitudes [43].

For example, consider the case of an employee who does not lock his workstation. By presenting different real cases to that employee showing the consequences of leaving his computer logged on and unattended would cause a dissonance between his current behaviour and the unwanted consequences of leaving his workstation unattended. Hence, in order to alleviate that cognitive dissonance (uncomfortable state) he would adopt the security guidelines that advice him to lock his workstation any time he leaves his workplace.

These techniques involve some form of *the law of inhibition* stated by Skinner in [45]. Where the role played by the employee which is contrary to his/her ideas and beliefs or the cognitive inconsistency that is induced, act as a stimulus that aids to degrade the employee's negative response towards the ISP or the ISA initiative .

A technique which is not mentioned in [42] is the *force field analysis* technique, which could be classified in this second method as it aims to change the individual's attitude [52].

**Force Field Analysis.** Refers to a social psychology technique developed by Kurt Lewin, which is based on *field theory* [53]. According to Hewston *et al* [52], *field theory* considers the individual as a part of a larger system where social forces exert influence on the individual's behaviour. This technique sees the behavioural change as the result of the alteration in the equilibrium held by two opposite forces (see Figure 3.3); namely the *driving* and *resisting* forces [35, p. 23-25]. The *driving forces* are those that aim to achieve a change in respect from the current situation. Whereas the *resisting forces,* restrain those driving forces, preventing such change from happening.

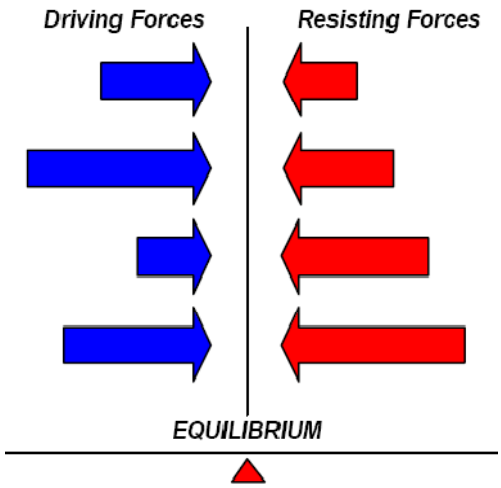



**Figure 3.3** Force field analysis model [35].

For example, a positive attitude towards a behavioural change can be achieved if the *driving forces* are greater than the *resisting forces* (Figure 3.4). Conversely, if the *resisting forces* are greater than the *driving forces* then a negative attitude against a behavioural change would be achieved instead (Figure 3.5).

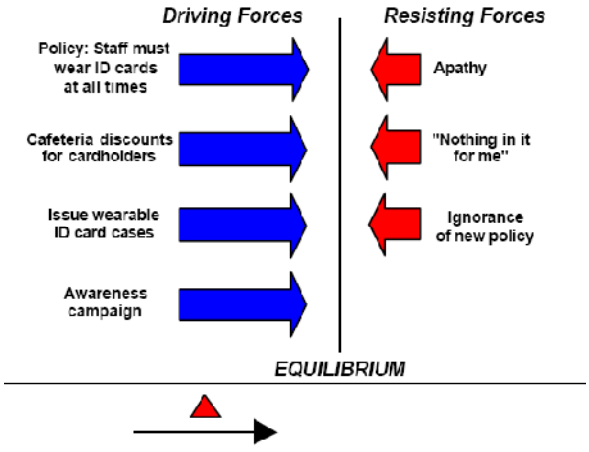



**Figure 3.4** A positive attitude towards a behavioural change can be achieved if the driving forces are greater than the resisting forces in number or strength [35].

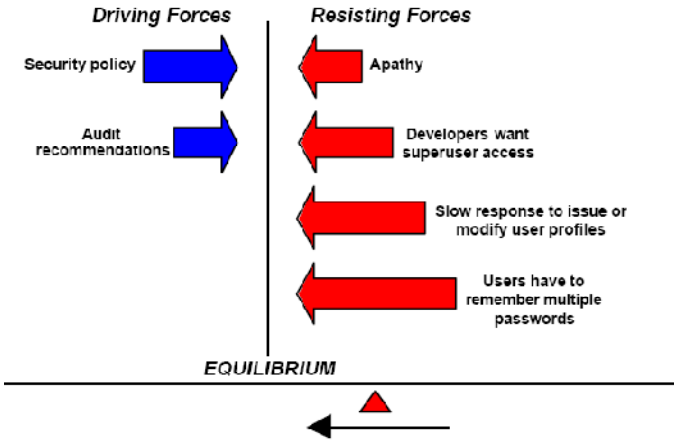



**Figure 3.5** In this example resisting forces are greater than the driving forces then a negative attitude against a behavioural change would be achieved [35].

One interesting aspect of this technique is that it provides a mechanism to *unfreeze* the existing behaviour, manipulate the *driving* and *resisting forces* to induce a behavioural change and then *refreeze* the balance once the desired behaviour has been achieved [35].

For example, before the ISAC, the *driving* and *resisting forces* are balanced, and the current behaviour is *frozen.* Nonetheless, once the ISAC for locking workstations is launched, additional *driving forces* are added to the current situation and *resisting forces* emerges as well, such as apathy, ignorance of the ISP, etc. In this moment the behaviour is unfrozen. Then the behavioural change would be achieved if the value of the diving forces exceeds the value of the resisting forces. In order to ensure a behavioural change, each resisting force would need to be effectively addressed. Once the desired behaviour is achieved, mechanisms for evaluating the new behaviour would help to refreeze the achieved behaviour.

The third method, ***influencing attitudes through persuasion***, aims to cause a permanent change on the individual's behaviour by persuading individuals to change their current attitudes [42]. This involves a more conscious decision by the individual about the future behaviour, which instead of being induced, the expected behaviour is explained and exposed. Von Solms [42, p. 171] identifies 5 prerequisites which need to be satisfied in order to attempt to persuade an individual:

> **Exposure.** If the security message is delivered in a written form, the security practitioner has to ensure that the entire security message is read by the employee; else if the security message is in an audible form the security practitioner has to ensure that the entire message was listened by the employee [42].

For example, in FIRA, the IT department deploys in a monthly basis via e-mail a technological bulletin aimed to inform employees about relevant IT issues and help them to solve common IT problems and reduce to a certain extent the incidents reported to the help desk. However, even though the bulleting was delivered to the entire organisations, it was found that just few employees opened the e-mail and read it thoroughly.

**Attention.** According to dissonance theory, the more dissonance the message, the less attention would be attracted from employees. In order to grab the attention of an audience, *consonant* (opposite to dissonance) messages need to be communicated; that is, messages that harmonise with employee's ideas and beliefs [42].

For example, if employees are explained that from the point of view of security, virtually every human makes security trade-offs in a daily basis [17], then employees would eventually appreciate that information security is not that different or that complicated than what they thought it was going to be. This would be a *consonant* message which to a certain extent agrees with employees' beliefs and ideas.

**Comprehension.** The audience needs to be able to understand the security message that is being communicated. Hence depending on the complexity of the message, the medium over which the message is communicated would facilitate such understanding [42].

For example, consider the "10 Maxims of Information Security" used by FIRA in its ISAC. FIRA decided to deliver to all employees, calendars with the "10 Maxims of Information Security" printed on it, facilitating their understanding and retention to employees. Whereas if these calendars would not been available in this form but just as part of the introductory IS session, it would have been unlikely to achieve the desired understanding and retention of the security message that employees have today after this ISAC.

**Acceptance.** The next step in persuasion is the acceptance of the security message. A form to increase the acceptance rate is to find as many arguments against the security message as possible before it is delivered; then address each argument and find the appropriate counter-argument. According to von Solms [42], the arguments presented by an expert are more likely to be accepted by the audience.

**Retention.** Finally, the last step in attempting to persuade an individual is to ensure a long lasting attitude change. According to [43], there are different techniques to ensure the retention of attitudes, some of them involves some form of repetition, but among the most effective ones are those resulting from an active participation of the individual such as in the case of *self-persuasion* (commented above in this chapter).

The most recent ISA approaches use one or a combination of the previous social psychology techniques. For example, the ISF's ISA approach [35, p. 22-29] uses the *Force Field Analysis* technique developed by Kurt Lewin. Kabay [41] and von Solms [42] both use several SP techniques to improve employees' compliance towards ISP which have been discussed in this chapter.

The ISA approach proposed by Leach in [14], in its structure resembles the S/R model proposed by Skinner in [45]; nonetheless, cognitive psychological processes are actually involved in the resulting behaviour. The ISA approach combines several SP techniques in order to improve the user's security behaviour. For example, Leach divides the factors that influence the user's behaviour into two groups. The first group comprises a set of "stimuli" that forms the employee's perception of the security behaviour that is expected from them, such as the security behaviour they are required to show, the actual behaviour perceived by the employee from the rest of the employees and previous knowledge gained by decisions from the past. The second group comprises a set of "stimuli" that make employees feel committed to comply with the ISP such as their personal code of conduct, the level of commitment they feel towards the organisation and the difficulty that they find in complying with the ISP (Figure 3.6). From these two groups Leach [14] points out three key factors as the most influential, the security behaviour showed by their workmates and senior management, the employee's decision making skills and the level of commitment towards the organisation [14]. According to the techniques presented in this section, Leach's ISA approach aims to affect directly the individual's behaviour by using *operant learning, social learning and conformity* techniques.

A recent ISA approach developed by Pahnila et al [54] combines several theories to produce their model, such as General Deterrence Theory, Protection Motivation Theory, the Theory of Reasoned Action, Information Systems Success and the Theory of Reasoned Action. These theories are related to some of the SP techniques previously mentioned, but used in a particular form. The results of this combination is a model where the most important factors that need to be influenced are the individual's attitude towards compliance, the individual's intentions to comply and the actual compliance with the ISP.

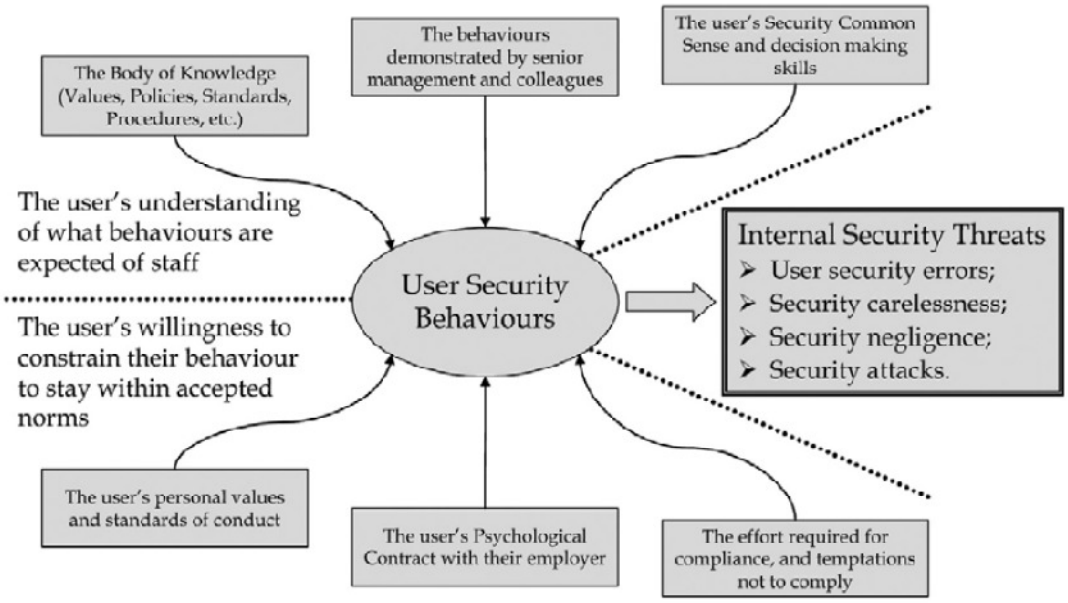



**Figure 3.6** Factors that influence the employee's security behaviour [13].

In general, the techniques discussed in this section can be applied to make any ISAP more effective. As pointed out by Skinner [45, p. 9] when he comments that it might not be possible to obtain the complete desired behaviour from an individual by stimulating their environment; nonetheless, at least part of the individual's displayed behaviour can be induced.

## 3.5 Conditioning Principles in Marketing

According to McLean [1], employees could be treated as "*consumers*" and the "*product*" could be an idea. Thus the ISP, security messages and guidelines would become the *product* of the ISAC under a marketing perspective. However, these conditioning principles must be considered cautiously, since operant conditioning is not concerned with learning but with reinforcing a determined displayed behaviour. Therefore, it should form part of a larger model where learning theories are involved as well [47].

An application of *operant conditioning* could be appreciated in the field of marketing. Since an ISAC can be treated as a product under a marketing perspective, operant conditioning principles used in marketing can be used to promote such *product* among the *customers*. The following are typical conditioning campaign phases that introduce a new product to the market, namely *initial conditioning campaign, behavioural change campaign, point of delivery messages campaign and branding campaign.*

### 3.5.1 Phase I. Initial Conditioning Campaign

Typically the marketing industry uses operant conditioning in advertising in order to create a positive association between the product and the individual's attitudes and beliefs [55], [1]. According to McLean, in this initial phase no active participation of the individual is required. This could be regarded as a preparatory phase which purpose is to decrease the strength of any *dissonance* factors between the individual's attitude and beliefs, and the product, in order ensure its acceptance.

For example, consider an organisational campaign promoting the organisation's purpose to comply with data protection laws, regulatory requirements, as well as the benefits to the organisation as a whole of being compliant, but without any allusion to the participation of the employees yet in this phase. The purpose is to implant in the mind of the employees the overall objective of the organisation and the benefits of being compliant, seeking to obtain later a positive attitude in further initiatives in this regard.

### 3.5.2 Phase II. Behavioral Change Campaign

After the initial conditioning campaign is launched, another campaign seeking to persuade individuals to change their behaviour is launched. In this phase additional stimulus are used whether to *facilitate* the appearance of the desired response or to *inhibit* the appearance of a determined response by associating a positive stimulus or a negative one respectively (according to *the law of facilitation* and *the law of inhibition*). According to McLean [1], in this phase the individual's active participation is required.

Continuing the previous example, in this phase the organisation's campaign would remarkably allude to the employees' participation as the utmost critical factor to achieve such organisational compliance. In addition, the campaign would show the support of all levels of management and through themselves also the security behaviour that would be expected from the rest of the employees (additional *stimuli* that would facilitate the appearance of the desired response).

### 3.5.3 Phase III. Point of delivery Campaign

This campaign involves a set of messages that are meaningful for the individual only if *the initial conditioning* (phase I) and *behavioural change* (phase II) *campaigns* were previously conducted. According to McLean [1], the reason is that the effectiveness of this type of messages (short and specific messages that McLean identifies as *point of delivery messages* or *delivery of instruction*) depends on the linkage established between them and the *initial conditioning* and *behavioural change* campaigns. The

main purpose of the *point of delivery messages* is to remind the individuals the behaviour expected from them before they act or offer a clear message of the consequences if they do not behave as expected.

For example, *points of delivery messages* could be those posted on the organisation's notice board stating "You are the key to good security" or those slogans stickered on each toilet of the organisation stating "Look who is responsible for protecting the information of our organisation".

### 3.5.4 Phase IV. Branding Campaign

The purpose of *branding* is to associate a determined slogan, image, logo or a symbol in general with the product [1]. According to Stuart [55], this is commonly referred to as *conditioned response*. The result would be that if previous campaigns achieved a positive attitude towards the product, then just by observing the brand itself, similar attitudinal responses would be elicited toward the brand [55].

For example, at the beginning of the *initial conditioning campaign* a slogan stating "You are the key to good security" could be used throughout the ISAC. After each training session, at the end of each security message, video clip, email and any other security related material the slogan would appear attached; establishing in this manner the association between the product and the brand. Henceforth, the brand alone would elicit the individual's attitudinal response which could ultimately result in the desired behaviour.

## 3.6 Summary

Behaviourism is a psychological stream which has been strongly criticised by scholars; nevertheless, its laws still stand along with other theories to understand and induce at least part of the displayed behaviour of an individual. The schema is a biased *filter* that determines how individuals perceive reality and make security decisions based on this perception. The target of the ISAC now becomes the employees' schemata, with a particular focus on their attitudes, since behaviour is a consequence of a change in attitude. Unfortunately, even though there is an increasing interest by researchers in using these techniques in the field of ISA [41, 42, 44] and many others, these techniques seem to be ignored by security practitioners [41].

# Social Networks and Behavioral Change

CHAPTER

4

## Contents



## 4.1 Introduction

The present chapter is in some form a continuation of the social psychology techniques discussed in the previous chapter. The purpose here is to analyse the manner in which *social networks* influence the behaviour of its members and explore some mechanisms frequently used to discover the underlying *social networks* existing along with the official communication network within an organisation and how *social networks* become the medium to cause a viral behaviour.

## 4.2 Communication Networks

Over the past 50 years, several *models of communications* have been proposed by scholars to create a model of behavioural change in social systems [56]. However, Rogers & Kinkaid [56] point out that most of the proposed communication models, linear models in its majority, have failed to consider the underlying semantics and subjectivity present in human communications, where a message issued by the sender may have a different meaning for the recipient.

A linear model is considered as such, because the interacting elements of those models operate in a linear fashion, where most of the times the sender aims to affect the behaviour of a passive receiver. For example the model proposed by Shannon and Weaver [57, p. 4] comprises essentially six elements, namely the *information source* which is the entity that creates the *message* intended to be sent to the receiver; the *transmitter* which is a device that converts the message into a suitable form (*signal*) to be sent over the communication channel; the *channel* which is the medium used to deliver the message to the receiver; the *noise source* which is an element considered in the model to refer to those potential alterations in the original signal while it is transmitted over the communication channel towards the receiver; the *receiver* which is a device that converts the receiving signal into the correspondent message and the *destination* which is the intended recipient of the message [57]. These components are arranged in a linear sequence where the communication of information flows from left to right (Figure 4.1).

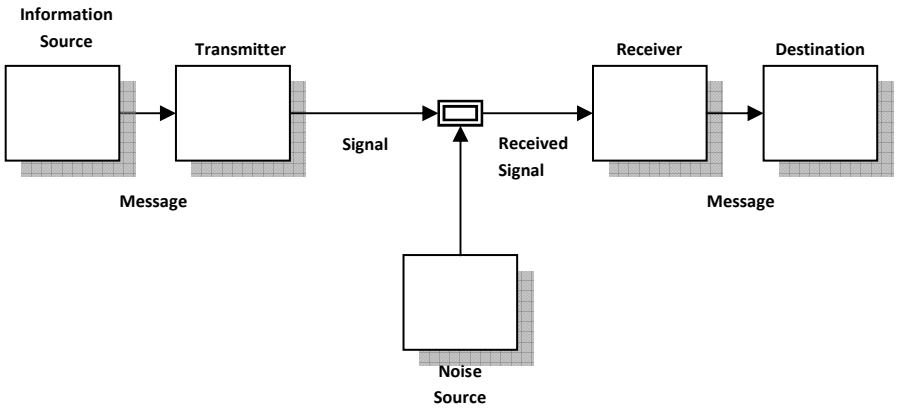



**Figure 4.1** Shannon and Weaver's Linear Model of Communication [56].

Nevertheless, Rogers and Kinkaid [56] remark that the most important contribution of the model proposed by Shannon and Weaver in [57] is the introduction of their concept of *information* that refers to the reduction of uncertainty when there is a choice between two alternatives, and that became fundamental to any

communication model and further for *communication* or *social networks* [56]. According to a definition provided by Rogers and Kinkaid in [56], the *Communication* process involves two or more entities in a continuous information exchange with the purpose of achieving a *mutual understanding* not of the *physical reality*, which may not be accessible for both entities, but of the reality perceived through different sets of information that moulds the individual's *schema*. It shall be remarked that it is a continuous information exchange because *mutual understanding* can only be achieved in a certain degree, when individuals *converge* it means that sufficient feedback was exchanged between one and other to move towards a common point of interest [56].

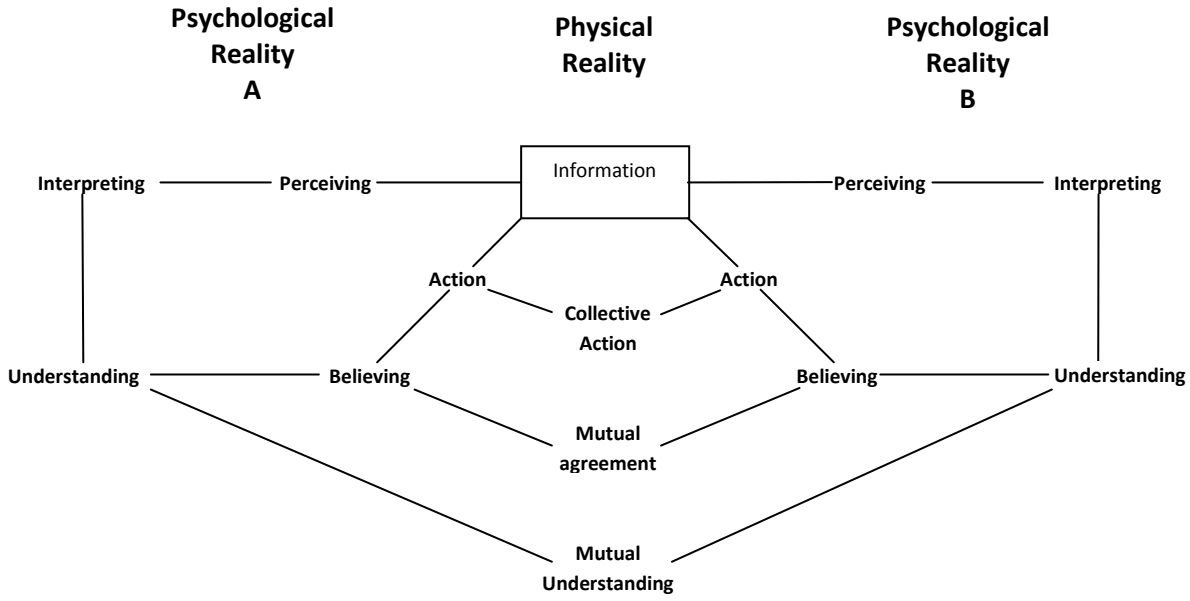



**Figure 4.2** Components of the Convergence Model of Communication [56].

Figure 4.2 shows the *Convergence Model of Communication* proposed in [56] (p. 55) (Figure 4.2). The model considers *information* and *mutual understanding* as its central components in a *dyadic communication*; that is, two connected individuals communicating over a communication channel [56] (p. 142). The model aims to portray the dynamic process of communication, which main purpose is *mutual understanding* as it affects the attitudes of the participating entities and ultimately leads to collective action. In addition, this model considers that individuals can not just reach a mutual understanding, but also they could reach a mutual misunderstanding, and instead of converging they could diverge and never reach a mutual agreement leading to a conflictive behaviour instead [56, p. 56].

This model involves individuals being exposed to three different abstractions of reality, namely, the *psychological reality* of each participating entity which is subjective and biased due to the information (ideas, beliefs, knowledge and attitudes -

see *attitude system* in chapter 3) that the individual posses in respect to a particular issue; the *social reality* which is achieved through the continuous exchange of information and feedback between the participating entities until their understanding converges in a common point, creating additional information about physical reality in which their actions or behaviour would later rely on; and the *physical reality* to which access is mediated by information that individuals have created by themselves or shared with other entities.

According to Rogers and Kinkaid [56, p. 71], the *convergence model of communication considers:* the effects of communication on the participating entities and other entities no directly involved in the communication process; the effects of the subjective interpretation of information and the effects of a behavioural change presented by any of the entities directly involved in the communication process. It worth be noted that this model considers the co-lateral effects of communication on the individual's environment, or more properly, on those individuals that are closed to the individuals directly participating in the communication process.

For example, consider an ISAC targeted to *sysadmins* to raise the awareness on password policies. This campaign could be seen as a source transmitting a message over a channel (such as email, leaflets, videos, etc.) targeted to a determined group of individuals (sysadmins). Nonetheless, this would be only the *linear model of communication's* view. Under the *convergence* view, the effects of such campaign would consider not just the *sysadmins* as the recipients of this information, but additional variables from the individual's environment, such as the effect of this communication on the security practitioners responsible for the ISAC, on the sysadmins' friends, on the security practitioner's friends, on the interpretation of information by sysadmins, on what sysadmins say between each other about the ISP. Co-lateral effects are important variables that should not be ignored, since they generate additional information that ultimately influences the attitudes and behaviour of the individual.

The information-processing in this model is similar to that previously discussed in the *attitude system*; furthermore, it could be argued that the *attitude system* model and the *convergence model of communication* complement each other in order to explain the behavioural change in social systems. The former considers *behaviour intentions* and *affective responses* that are not considered by the latter. On the other hand the *convergence* model provides a communication approach model that puts the individual's behaviour in the context of a social system. If these two models are merged, a deeper insight could be gained to explain and induce a behavioural change in a social system (Figure 4.3).

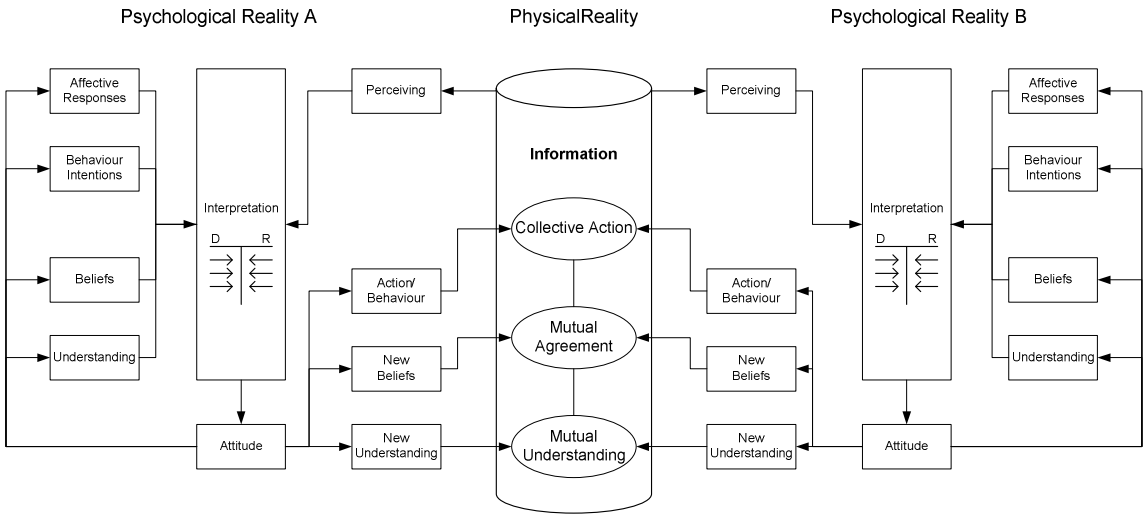



**Figure 4.3** Extended Convergence Model of Communication.

## 4.3 A combined approach

According to Peel [48], a combined approached to aim a behavioural change is more likely to succeed than just utilizing one technique alone. Moreover, he asserts that the combined techniques shall consider behaviourists and cognitive principles, beliefs, previous knowledge, attitudes and affective responses.

Figure 4.3 shows a combined approach that merges the *attitude system* (covered in Chapter 3) and the *convergence model of communication.* The resultant model is called by the author of this dissertation, *the extended convergence model of communication* (E-CMC). The E-CMC involves aspects of *social psychology* (behaviourism applied in social learning [49, p. 272]), *cognitivism* (which considers beliefs, knowledge, feelings and attitudes [48, p. 22]) and *Lewin's force field analysis model*.

The E-CMC model considers individuals participating actively in turns in a continuous process of communication and acting on the same information until a *mutual understanding* is achieved that leads to *common agreement* and ultimately to *collective action*. Any of the two entities, *A* or *B,* can create information. Consider a piece of information sent from *B* to *A*. The information that is shared is first *perceived* according to the psychological reality of individual *A* and then enters a personal (subjective and biased) interpretation process. The *interpretation* process is influenced by *prior conditions* comprising *cognitive psychological processes*, *affective responses, behaviour intentions, beliefs* and *knowledge.* The *interpretation* process measures all these inputs in terms of *driving forces* and *resisting forces,* according to *Lewin's force field analysis model*. The *disequilibrium* caused by a difference in these forces will lead to a negative or positive *attitude* towards the piece of information

being shared. The resulting *attitude* feeds-back the *prior conditions,* which mean that additional *beliefs*, *knowledge* and *understanding* are gained and will influence future interpretations. If additional *understanding* is gained then additional *information* is gained by that individual and it can be shared with the counterpart. Individual *B* performs exactly the same process and return information to the counterpart until they gradually reach a *mutual understanding* (or misunderstanding), which may lead to a *mutual agreement* (or disagreement) and ultimately to *collective action.* The main differences compared with the *convergence model of communication* are that the E-CMC model involves additional *cognitive psychological processes,* such as *prior conditions*, *affective responses*, *intentions* and *attitudes.* The E-CMC model offers a deeper insight on how a behavioural change in a social system could be influenced.

For example, consider an ISP that prohibits the sharing of passwords. The *change agent* is involved in the communication process with an employee. The *change agent* provides *information* about the ISP, such as the reasons of why passwords should not be shared and what the alternatives are to this *"need"* [58], [5]. The employee receives this information via email as the *communication channel* and *perceives* it according to the psychological reality of the employee and then is *interpreted*. This *interpretation* is affected by other cognitive psychological process. The employee may have an *affective response* towards this piece of information, such as "*I don't like these policies*, *because I need to share my password when I am on holiday!*" and may also have *intentions* to *behave* in a determined manner "*I will comply with this policy, but I will also ask for a temporal account to overcome this problem!*", moreover, the employee may have particular *beliefs* and *understanding* in this particular respect "*sharing my password to someone I trust might not be that bad! In any case, my workmate hardly knows about computers!, so there is no such threats*". The individual interprets all these inputs, represented by *Lewin's force field analysis* model:

Driving forces:

1. Security policies
2. Offering temporary accounts
3. Audits

Resisting forces

1. Apathy
2. Ignorance of new policy
3. Problems if my account is not available when I'm holiday
4. Conflicting schema "He is my friend, and I am asked to trust nobody!"

For this example, as there are more resisting forces than driving forces (assuming that resisting forces are not just greater in number, but in strength), the *equilibrium* point shifts towards a bad attitude regarding this ISP. Although the employee's intentions were to comply, this is not necessarily the ultimate result. In this case, the employee would present resistance to change her security behaviour as she perceives (in her psychological reality) more "disadvantages" on adopting the required behaviour than in the one the ISP intends to supersede. If this *understanding* is shared with the *change agent,* the latter will process the incoming information and in return the *change agent* can attempt to add more *driving forces*, and more information about the risks involved in sharing passwords. Eventually, as the *driving forces* over number the resisting forces in number and strength, the employee is more likely to gain deeper understanding on the risks involved in sharing passwords, reaching a *mutual agreement* and finally adopting the required security behaviour.

There are some important points to remark in this example; first, in order to achieve a behavioural change, the communication process must be active in both directions; that is, employees are enabled with the opportunity to give feedback. Second, a behavioural change can be attempted from different angles. In this example, it was by adding driving forces and affecting beliefs, but there are more options as those mentioned in Chapter 3. Third, the *change agent* needs to consider the perception of the potential adopters in order to be more effective in the *diffusion process.* Fourth, *behaviour intentions* might not be the ultimate behaviour; nonetheless, it affects the ultimate attitude. Fifth, perfect mutual understanding might never be reached, but sufficient mutual understanding is possible; therefore tolerance to errors and slow compliance shall be approached from this perspective. After all, there are different realities, the physical reality, to which we may not have access but through the information we have about it; the psychological reality of the individual, subjective and biased according to prior conditions; and the *social reality*, gained through *mutual understanding* and *mutual agreement.* The job of the *change agent* is in great part to provide further information about the *physical* reality of IS as to affect the employee's schema, bringing as close as possible both perception and reality.

This shows a need to be explicit about exactly what is meant when we refer to a *social system*, *communication network* and *social network*. The term *social system* is defined by Rogers in [15, p. 23] as "*the set of interrelated units engaged in joint problem solving to accomplish a common goal*", for example the members of an organisation compose a *social system* since they all have a common goal or mission. The terms *communication networks* and *social networks* seems to have come to be used almost indistinctly. For example, according to Rogers and Kincaid [56, p. 95] "John Barnes defines *social networks* as "*a set of points joined by lines... which indicate which people interact with each other*" and Rogers [15, p. 27] defines *Communication network* as a set of "*interconnected individuals who are linked by patterned flows of*

*information*". In both definitions the common element is communication; for the first concept communication is in the form of *interaction* and for the second communication is in the form of *flow of information*. Therefore, in this dissertation these terms are going to be used indistinctly.

## 4.4 Communication in Organizations

When looking at an organisation chart for example, its different organisational units and subsystems within the organisational system as a whole could be appreciated, this is commonly referred to as *structure* [59, p. 77]. The purpose of the formal structure commonly imprinted in an organisation chart is to provide *regularity, predictability and stability* to the relationships of the organisational units and subsystems in order to achieve the organisation's goals [59]. As a consequence the individual's behaviour within the organisation is in part determined by the formal structure [59]. From the perspective of the *extended convergence model of communication,* when a new employee is hired, the communication process takes place; engaged in a continuous exchange of information until a mutual understanding is reached between the organisation and the new employee. In part, this mutual understanding leads to a mutual agreement of the expected behaviour from the new employee within the organisation. Moreover, the expected behaviour in turn, shall reflect the patterned communication flows and formal relationships intended by the organisation chart, job functions and corporate policies in general [59].

According to Rogers and Agarwala-Rogers in [59], along with the formal structure and as a result of the frequent interaction of individuals an *informal structure* emerges within the organisation. Both structures complement each other, being the latter an inherent part of any social system where human interaction is present, even in the most rigid social systems [59]. Moreover, informal communications play an important role in determining employee productivity [60], they may use the same communication channels and in some cases the formal and informal communications might overlap [59]. In [59], Rogers asserts that the degree to which the informal and formal structures overlap, serves as an indicator of the extent to which the formal structure and formal communications are considered appropriate for the current organisational context (Figure 4.4).

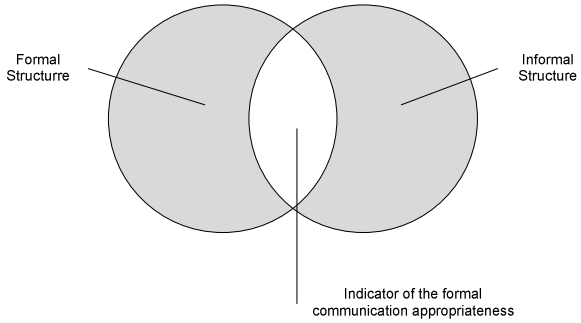



**Figure 4.4** Indicator of the extent to which the formal structure and formal communication structure are considered appropriate for the current organisational context [59].

In addition, informal structures are important from the managerial point of view, because they constitute alternative channels that employees use to communicate with each other more rapidly and more efficiently, as they typically do not use the same communication channels as those used in formal communications [61]. According to Rogers in [59], vertical flows of information are not as common as horizontal flows in organisations due to the issue that employees might feel more confident in establishing an informal communication relationship with other employees at the same hierarchical level than with employees at higher positions, which is probably one of the main reasons for such efficiency [59]. In addition, this is congruent with the *extended convergence model of communication* since a mutual understanding is more likely to occur with employees at the same hierarchical level because of a similar perception of reality, established by common ideas, beliefs, intentions, affective responses, attitudes and information. This is fertile ground for *rumours,* which are just one form of informal communications and according to some researchers a practice that should be encouraged and even cultivated for the benefit of the organisation towards the achievement of its goals [59].

The consequences of this type of communication among employees, when considered in a mass scale, involve a continuous exchange of information where ideas, beliefs, knowledge, attitudes and ultimately behaviours could be affected. Informal structures are an inherent part of formal structures, they are simply a consequence of human interaction and if not managed appropriately or at least acknowledged, they could pose a real threat instead, where malicious individuals could take advantage of this type of communication and use it against the organisation. Consider the case for example, in which a malicious employee deliberately aims to raise negative attitudes against determined corporate policies within the organisation using rumours. This action could result not just in employees' negative attitudes towards the corporate policies in question, but in undesired behaviours attempting against the organisation's objectives.

Informal structures within an organisation could be seen as the informal communication networks that emerge as the result of the frequent interaction among the members of the organisation. They are typically formed during those lapses of time where official communications are temporally put aside or decreased at a point where informal communication and open human interaction takes place. Consider for example the organisation's social events, induction training sessions, lunch breaks, off-site meetings, etc. It would be impracticable to maintain a workplace where the only form of communication permitted among employees was official communications; that would result in a very strange working environment and human behaviour as a consequence, where even at lunch time, for example, employees would not be allowed to talk to anyone that was not part of the same organisational unit to whom a relationship was considered official or where such communication was not enabled by the organisation chart. Apart from the impracticable issue in this example, alienation, monotony, general employee dissatisfaction, among others, would result from such a working environment (see "*Alienation on the assembly line*" case in [59, p. 87]). In the practice, it could be said that informal communications, are to a certain extent encouraged by organisations, when nurturing a friendly working place in which politeness is the principle rule or when organising social events dedicated for employees and so forth. However, according to the *Employment in Europe Report 2007* [62], monotony and consequently employee job dissatisfaction are still the problems in large and highly structured organisations.

Although, one of the objectives of the organisation chart is to predict the communication behaviour of employees, the objective could be regarded as achieved only to a certain extent. Evidence about this is the existence of the informal structure itself, where the majority type of communication taking place in the organisation is informal communication [60]. Interestingly, despite the apparent unpredictability and spontaneity, informal communications are a determinant factor in the effectiveness of an organisation for achieving its goals. Additionally, they tend to be autonomous and 'fault-tolerant', in the sense that they are not ruled or influenced by the top management and they are not affected by problems in the official communication channels [59].

## 4.5 The Meta-Matrix of Networks

According to what is has been discussed so far in this chapter, an organisation could be seen from two different perspectives; the formal organisational structure perspective, where the required communication relationships among all the organisational units have been determined according to the organisation's needs to achieve its goals; and the informal organisation structure perspective, where the

"*real*" organisation as a whole appears as an entity composed by a set of small interconnected communication networks [59]. Additionally, the relationships among these small communication networks are changing continuously over time, thus an individual is immerged in a complex dynamic social-technical system [63]. In this regard, Carley *et al* [63] and [64] assert that the network dynamics in which the individuals are immerged involve not just their social networks, but a set of additional networks that in conjunction they call the *meta-matrix of networks* (Table 4.1).

Each type of *network* in the *meta-matrix* serves a particular purpose and can be used to analyse at a particular level the relationships of a group of individuals or the organisation as a whole [65]. These network of relations involves people (or agents), knowledge, resources, tasks- events, locations, organisations, roles and attributes; nonetheless, only those networks involving people, knowledge and tasks are relevant from the security point of view [63].

According to Carley [64, p. 2], the 6 matrices relevant to information security are formed considering the following elements:

**A** as the number of *agents* or *people* in the network,

**K** as the number identifiable pieces of *knowledge*, and

**T** as the number of different *tasks*.

**Table 4.1** Meta-matrix of the 6 relevant networks for addressing information security, linking agents (A), knowledge (K) and tasks (T) [64].

| | Agent | Knowledge | Tasks |
|---|---|---|---|
| Agent | **AxA** | **AxK** | **AxT** |
| Knowledge | | **KxK** | **KxT** |
| Tasks | | | **TxT** |

The resulting *networks* according to the *meta-matrix* shown in Table 4.1, are:

**AxA – Social networks:** when linking *people* with *people* (that is, Agents x Agents or AxA) the resultant network is a *social network*, which essentially shows *who "talks to whom"* [64, p. 2]. In a broadly sense, this network is particularly useful for identifying key employees and isolates (people apparently not connected with other people, Figure 4.8 shows a couple of isolate dyads, one is formed by individuals #13-#14 and the second is formed by individuals #15-#16) [64, p. 2]. This type of *social networks* can be approached at different levels [59]:

- ***System network*:** refers to the social network of a whole system, such as an organisation. The number of elements in a *system network* is the number of elements interacting in the whole system. For an organisation the number of individuals involved in the system network may range from several hundreds to several thousands of persons (Figure 4.5).

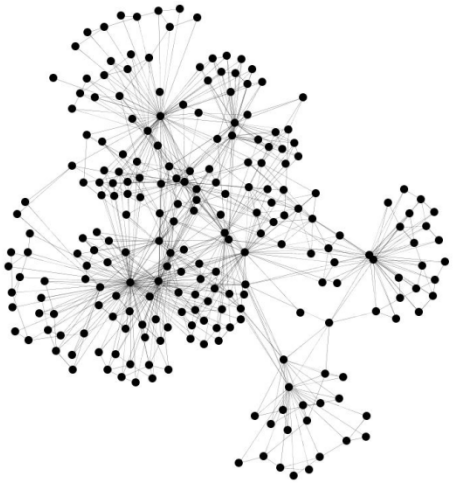


**Figure 4.5** System Network

- ***Clique:*** refers to a more compact type of social network involving a small number of individuals (ranging from 5 to 25 in average) communicating more frequently among each other than with the rest of the system. *Cliques* (and their interconnection among its members and other cliques) could be regarded as the building blocks of the *system network* (Figure 4.6 example from [59, p. 129]).

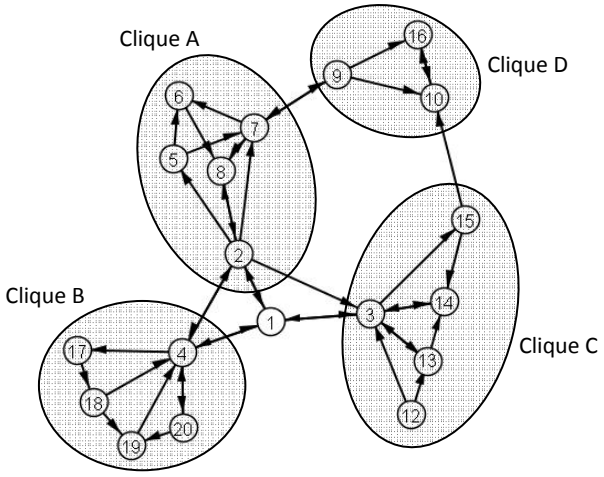



**Figure 4.6** Sociogram of four communication cliques [59].

- ***Personal network:*** Also called *egocentric networks* [56, p. 134], refers to the communication network that a particular individual possesses within a social system. For example, within an organisation each employee is interconnected with a set of other employees. Figure 4.7 shows the personal network for employee #11 which comprises individuals: #1, #3, #4, #5, #9 and #10.

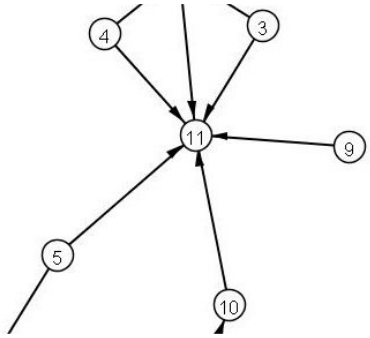



**Figure 4.7** Personal Network for employee #11.

Particularly, in *social networks,* the communication relationships are generally motivated and maintained by three common factors; by a common concern in achieving the goals of a determined task; by the affinity among the members of the network or by a common interest in determined topics [59].

**AxK – Knowledge network:** when linking *people* with *knowledge* (that is, Agents x Knowledge or AxK) the resultant network is a *knowledge network*, which essentially shows *who "knows what"* [64, p. 2]. In a broadly sense, this network is particularly useful for identifying key employees regarding a particular piece of knowledge [64]. These employees may be seen as *opinion leaders* (see section 4.6) in a particular topic (RN – Diffusion of innovations).

**AxT – Assignment network:** when linking *people* with *tasks* (that is, Agents x Tasks or AxT) the resultant network is an *assignment network,* which essentially shows *"who does what"* [64, p. 2]. In a broadly sense, this network is particularly useful for identifying redundancy of tasks and key employees regarding a particular task [64].

**KxK – Information network:** when linking knowledge with *knowledge* (that is, Knowledge x Knowledge or KxK) the resultant network is an *information network,* which essentially shows what piece of knowledge is related to what [64]. In a broadly sense, this network is particularly useful for identifying missing information links [64].

**KxT – Needs network:** when linking *knowledge* with *tasks* (that is, Knowledge x Tasks or KxT) the resultant network is a *needs network,* which essentially shows what piece of knowledge is needed to perform a particular task [64, p. 2]. In a broadly sense, this network is particularly useful for identifying information redundancy and security critical points [64].

**TxT – Task-precedence network:** when linking *tasks* with *tasks* (that is, Tasks x Tasks or TxT) the resultant network is a *task-precedence network,* which essentially shows what particular task should be executed before another [64, p. 2]. In a broadly sense, this network is particularly useful for determining the order in which a set of tasks shall be executed to achieve a desired result [64].

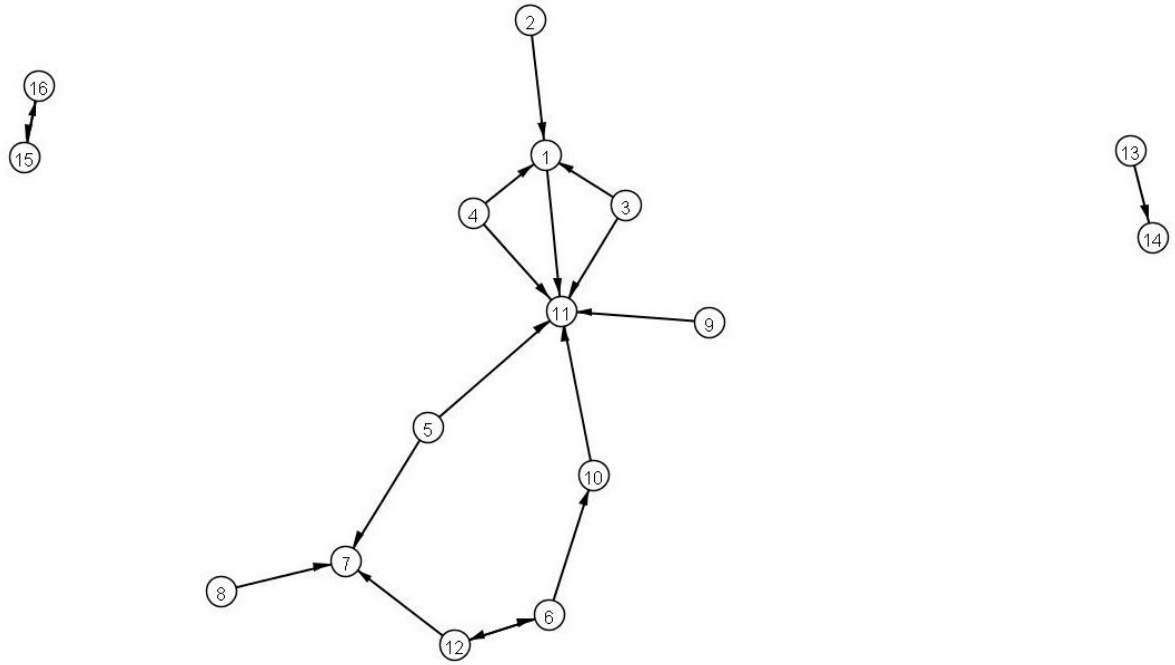



**Figure 4.8** Sociogram, a graphical representation of a social network.

Figure 4.8 shows a graphical representation of a *network*, which could be of type AxA, AxK, AxT, KxK, KxT or TxT (this holds if only the networks relevant to IS are considered), where the nodes represent either *agents*, *knowledge* or *tasks*. The edges, sometimes represented as arrows to be explicit about the direction of the flow of information, represent the connections or interactions of those particular nodes. For example, consider Figure 4.8 as if it was a *knowledge network* (AxK), individual #11 appears to be very influential since individuals #1, #3, #4, #5, #9 and #10 seek for his or her advice on a particular topic. In addition, the proximity of individuals #3 and #4 indicates a more likely similar knowledge than individuals #5 and #10 which appear slightly more separated, indicating a lower degree of similarity.

For the purpose of this dissertation the relevant networks are the *social network* (AxA) and the *knowledge network* (AxK). These networks could aid in the process of propagating the security message at the *informal communication* level, in order to stimulate a mutual influence towards compliance of the ISP, by attempting to identify key employees that holds the sufficient information security knowledge that could enable them to influence their peers [59], [64], [66]. The social network in its own might not be sufficient to influence and obtain the desired behaviour [67]; additionally, the key employees are required to be perceived within their social network as knowledgeable individuals in a determined topic in order to be able to influence their peers, this type of individuals are commonly refer to as *opinion leaders* [8, p. 27].

Targeting *opinion leaders* to aid the rapid propagation of an innovation is not knew, several scholars ([8, 66-70] and many others) have been developing algorithms, frameworks and methodologies on how to identify *opinion leaders* and how to use them to spread a piece of information as fast as possible through a social network. However, this approach seems to be ignored by security practitioners in the IS context, particularly in the ISA context, where to the knowledge of the author of this dissertation, only one ISA approach ([1]) has as its theoretical base the DoI theory and only covered to a certain extent, not including the characteristics that the *change agent* (or the security practitioner manager of the ISA) must have in order to expect positive results of the overall diffusion, the characteristics of social system and psychological issues that have been mentioned in this dissertation, which plays a determinant role to achieve the desired results.

It is evident the need for a more holistic approach to understand human behaviour in the IS field, which requires a multidisciplinary approach. For example, a recent event, “Interdisciplinary Workshop on Security and Human Behaviour” held in Boston, Massachusetts, from the 30th of June to the 1st of July 1, 2008, considered this approach, where they conveyed a multidisciplinary teamwork, composed by computer security researchers, psychologists, behavioural economists, sociologists, and philosophers, among others, to address and understand the human side of security. This dissertation represents one of these efforts in approaching IS from different perspectives; that is, from a managerial (chapter 2), psychological (chapter 3) and social networking perspective (chapter 4) to offer a balanced solution. A holistic approach would enable security practitioners to understand the human side of security and as a result be more effective on reaching the pursued security objectives. However, this may pose additional challenges, not just in the research field by conveying and reaching consensus among multiple disciplines, but at the organisational level. In this respect, a multidisciplinary approach is more likely to thrive in the academic arena rather than in the operating environment of an organisation; probably the multidisciplinary approach to address IS would thrive only if

it is supported and maintained under an *information security governance strategy* which would ensure the participation of the different business units of the organisation.

By analysing a *personal network* (a subset of AxA), it could be inferred from the graphical representation of the social network, which individuals are more likely to exert a degree of influence on the behaviour of another individual [59], hence by analysing the behaviour of the individual's friends (the word "friend" is used to indicate frequent communication with another individual), the individual's behaviour could be explained to a certain extent [59]. For example, Figure 4.8 shows the personal network of individual #11 whose behaviour is influenced by individuals #1, #3, #4, #5, #9 and #10. These effects on an individual's behaviour caused by others are commonly referred to as *system effects* [59, p. 111].

The *personal network* of individual #11 has additional characteristics. For instance, note the group formed by individuals #1, #3 and #4, and the group formed by individuals #5 and #10. The first group is commonly referred to as an *interlocking network*, where all the members of the group are friends of each other. The second group is commonly referred to as *radial network*, where those individuals are not friends of each other or where both individuals have individual #11 as a common friend. Thus the personal network of individual #11 is interlocking and radial. In addition, *interlocking networks* are more *integrated* than *radial networks*. Integration is a measure where the number of connections is divided by the possible number of connections among the members of the personal network, this measure indicates the degree in which the members of the personal network of an individual is interconnected among each other [56]. Hence, the number of connections within interlocking networks is greater than those of the radial networks, which means that interlocking networks are more integrated than radial networks.

This is important for our purposes, since a new piece of information (or an *innovation*) is more likely to spread faster over radial networks, reaching a greater number of individuals than if it were spread over members of interlocking networks [56], in other words, an innovation would spread more efficiently over interlocking cliques [59] (Figure 4.6). The innovation diffuses hoping from clique to clique through the linkages established by a group of *homophilous* individuals (individuals who are similar in several attributes such as beliefs, ideas, social status, education and the like [8]) that play an informal role in the communication process, liaisons, bridges and *opinion leaders* [56, p. 135-136] (Figure 4.11).

## 4.6 Informal Communication Roles and the 80 / 20 Principle

There are several informal communication roles which are not officialised [59] such as *gatekeepers, liaisons, bridges, opinion leaders and cosmopolites*; nonetheless, their existence might be evident once the social network emerges after performing a *social network analysis* which main purpose is to identify the communication networks that exist in a social system. In [71, p. 70] Gladwell refer to these roles as *connectors*, *mavens* and *salesmen.*

**Gatekeepers.** According to Rogers [59], another function of the organisation chart is to restrict and discourage some communication flows in order to prevent information overload of determined positions. For example, one of the functions of the immediate boss is to mediate direct access to the boss's boss from subordinates by reducing direct information flows, preventing in this manner *information overload,* which is a common organisational problem. This role is commonly known as gatekeeper (see Figure 4.9). This role is important to consider during the design of the ISAP, as *gatekeepers* control access to determined resources (including other social networks) which could affect in a given moment the flow of information.

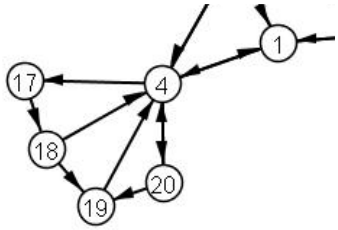



**Figure 4.9** Individual #4 is Gatekeeper as it restricts direct access from individuals #17, #18, #19, #20 to individual #1.

**Cosmopolites.** Within the organisational context, refers to those individuals that provides openness to the organisation by maintaining a continuous exchange of information with the organisation's environment [59], [56] (Figure 4.10). Typically these roles are more likely to be found at the top and at the bottom of the organisation hierarchy. This is because at the top organisational level, executives maintain continuous communication with entities outside the organisation, exchanging ideas and information in general. And at the bottom of the organisation hierarchy, employees deal with a relatively more operating environment which requires constant communication with external suppliers or third parties, opening the organisation to new ideas and exchange of information in general [59]. This information is what maintains an organisation aware of its environment and to a certain extent it could be said that this information obtained by *cosmopolites* provides

strategic direction for the organisation as a whole. As it will be mentioned, *cosmopoliteness* is an important part of *opinion leaders*.

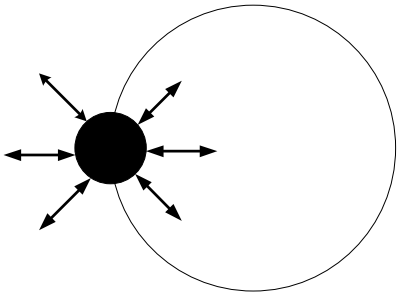


**Figure 4.10** Cosmopolite, provides openness to the organisation by maintaining a continuous exchange of information with the organisation's environment [59].

Similarly, *cosmopolite communication channels* refer to those communication channels that link an individual to resources outside the organisation [8, p. 207]. For example, mass communication media such as radio or television are regarded as *cosmopolite communication channels* [8, p. 207]. This characteristic is important for the purposes of this dissertation, because it can aid in making a clear distinction between the communication channels needed to spread a determined piece of information as fast as possible and the channels needed for persuasion. The characteristics of *cosmopolite communication channels* are more suitable for reaching massive audiences than for persuasion, whereas *localite channels* (opposite to cosmopolite channels) are more suitable for persuasion than for reaching massive audiences [8]. This means, that *cosmopolite communication channels* are more suitable for conducting awareness campaigns, whereas *localite channels* are more suitable for launching a behavioural change campaign.

**Liaisons and bridges.** *Liaisons* are those individuals that links two or more different cliques without himself pertaining to any of these cliques, whereas the individual acting as a *bridge* pertains to one of these cliques [56] (see Figure 4.11). Gladwell [71] does not make this distinction and simply calls these individuals *connectors.* These individuals are very important for the social system, as their main function is to maintain together the rest of the cliques and makes possible the flow of information along the social system. If they were removed arbitrarily, the system as a whole could suffer from communication problems which might lead to communication inefficiency [59, p. 135]. Liaisons and bridges (*connectors*) represent points of failure for the communication networks within the social system; hence organisations should acknowledge their presence in order to prevent the negative effects caused by blind decisions when moving (or removing) employees arbitrarily [59]. These roles are

important for the purposes of this dissertation because these individuals are who make possible for a piece of information to be spread rapidly within the organisation. For this purpose, AxA *networks* are suitable to identify *liaisons* and *bridges*.

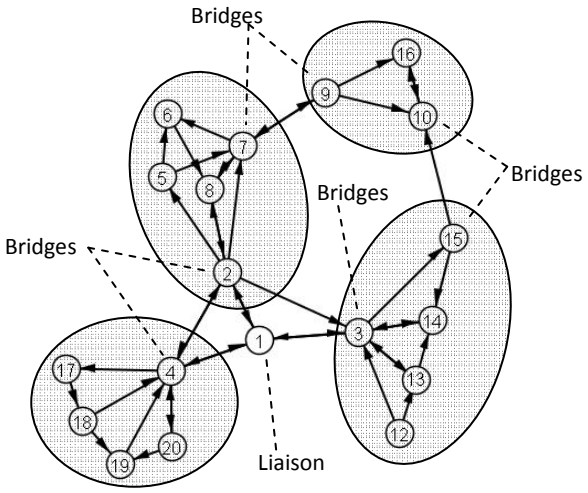



**Figure 4.11** Sociogram of four communication cliques, showing liaison and bridges individuals [59].

**Opinion Leaders.** Refers to those individuals with the capacity to informally influence the attitudes or behaviour of their peers (these peers are going to be referred as *followers* in order to clarify the concepts) [56, p. 123]. Gladwell [71] refers to them as *salesmen*, because of their abilities to persuade and influence individuals to behave in a desired manner. As an informal role, opinion leadership is neither a property nor a function determined by the organisation chart; *opinion leaders* are perceived as such by their *followers* because of their evident expertise, knowledge, social accessibility and their willingness to observe the organisational policies [8]. This perception suggests that *opinion leadership* is a property that could be lost or degraded if the perception of the followers about their *opinion leader* is affected in any form; on the other hand, it is also a perception that could be nurtured and maintained [8, p. 27, 325]. In this regard, in [72], Miha suggests developing a reward system in which these key employees were recognised.

*Opinion leaders* are typically the targets of *change agents* (refers to the individual who seeks the adoption of an innovation; in the IS context would be the security practitioner conducting the ISAP) to accelerate the *diffusion* of an *innovation* [73, p. 57-58], [69]. According to Rogers [8, p. 27], *opinion leaders* main characteristics are their relatively degree of *cosmopoliteness*, their higher socio-economical status (compared to that of their peers), their *innovativeness* (the degree to which individuals easily adopts an innovation at an early stage compared to the rest of the

individuals in the social system [8, p. 22]) and their position in their communication structure which enables them to exert influence to the rest of the members of their communication network [8, p. 27] (Figure 4.12).

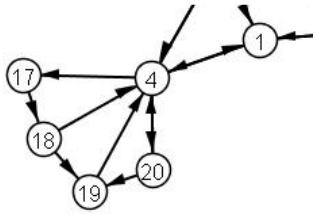



**Figure 4.12** Individual #4 is an opinion leader in clique B.

It worth be noted that *opinion leaders* are regarded as such for their knowledge in one or more particular topics [8, p. 314]; nonetheless, for the same communication network several *opinion leaders* may exist [73, p. 64], [74, p. 84]. For example, the *knowledge network* (AxK) regarding IS issues is very likely to be different from a *knowledge network* regarding IT issues; since there might be an IT specialist and a security specialist in the same communication network, each of them would be perceived as an opinion leader, one in IS issues and the second in IT issues. Therefore it is reasonable to expect several opinion leaders to emerge in the same communication network, where the network would be determined by the piece of knowledge in question [73]. For this purpose AxK *networks* would be suitable to identify *opinion leaders*.

According to Rogers [8, p. 388], the employment of *opinion leaders* can be beneficial to an organisation, not just in successfully diffusing a desired innovation, but in terms of saving economic resources as well. The change agent could secure the success of a campaign or achieve the adoption of a determined innovation if the influence of the opinion leaders is employed correctly. As a consequence, by using the influence of opinion leaders, approximately 80% of employees could be reached and influenced, with the effort of only that 20% of key employees, which implies the reduction of the required resources that are needed to reach and persuade each employee individually. As it can be noted, the efforts of the change agent are maximized when opinion leaders are involved. In addition, the ideas promoted by the change agent are more likely to be accepted if they are transmitted through opinion leaders, as they are regarded as coming from a *credible* source, from the point of view of the *followers*.

However, in order to achieve and use such advantages, a close interaction between the change agent and the opinion leader is required. The problem is that the constant interaction between the change agent and the opinion leader could lead to undesired outcomes, such as losing credibility and consequently the influence of the opinion leader when this ability is overused. Therefore, the change agent should work closely

with opinion leaders in the measure that their capacities are not affected by this constant interaction [75]. In addition, the motivations that opinion leaders may have to remain in such position are an issue that seems to be ignored by researchers [76]. Added responsibility and dissatisfaction could be issues affecting the motivation of those individuals once they realize that they play an important part in the diffusion process [73].

## 4.7 Pareto's Law

Between 1896 and 1897, Vilfredo Pareto, in an attempt to explain the income inequality at his time, created a mathematical formula derived from empirical evidence. Interestingly, the same pattern described by his formula was found in further empirical studies. Despite the fact that Pareto's law has been strongly criticised and attacked by economists because of its vagueness among other issues, after 1930 Paretian thinking resurge and Pareto's law started to be intensively considered and applied in different areas [77]. "*The Principle of Least Effort*" by Harvard professor of philosophy, George K. Zipf and US engineer Joseph Moses Juran with his rule of "*Vital Few and Trivial Many*" reflect the rediscovery of Pareto's law. The pattern described by the formula is almost a constant unbalance between two sets of statistical data in a *disproportion* of 80%/20%. For example, in his time, Pareto related two sets of data, one set was the total income in the country and the second set of data was the population. The results obtained using his formula was that approximately 80 percent of the income in the country was produced by approximately 20 percent of the population [78, p. 276]. When this formula was applied to other sets of data, the same unbalance appeared. This inequality described in Pareto's law is commonly referred to as the *80/20 principle.* Pareto's law has been used in several areas such as economics, business, marketing, networking [59], software development [79], [73], among many others.

According to Koch [78], a generalisation of Pareto's law indicates that:

- 20% of the inputs correspond to 80% of the outputs.
- 20% of the causes are responsible for the 80% of the consequences.
- 20% of the efforts account for the 80% of the results.

Pareto's law should be considered cautiously, it should not be interpreted literally, that is, the 80% or 20% are approximations and ultimately what this law points out is that the expected pattern is an unbalance in a greater or lesser measure when relating two sets of data, but rarely correlated in a 50/50 proportion [78, p. 23-24].

Having made this observation, it could be anticipated that according to Pareto's law, "20%" of the employees (liaisons/bridges) are responsible for the "80%" of the information flowing through informal communication channels. Similarly, "20%" of

the employees (*opinion leaders* or mavens/salesmen) are perceived as opinion leaders by the "80%" of the employees within the organisation. There is evidence supporting these assertions. Rogers [59] reports the results of an investigation carried out by Keith Davis, where 10% of executives from 67 companies were liaisons [59, p. 137]. Moreover, Rogers [59] reports the results of another investigation carried out by Donald F. Schwartz, where the results indicated that 15% of 142 professors from the College of Education at Michigan State University, were identified as liaisons [59, p. 137]. Rogers [59, p. 137] conclude that "Most networks analyses find that from 5 to 20 percent of an organisation's members are liaisons". Moreover, in their method for accelerating the diffusion of innovations using opinion leaders, Valente and Davis [73, p. 61] propose to designate the 10% of the individuals as a threshold to recruit opinion leaders. Moreover, Rogers [8, p. 312] points out the unbalance in the distribution of opinion leadership within a social system, remarking that only few individuals account for this quality, whereas the majority either lacks of it or is not present sufficiently. Although, neither Rogers [59] nor Valente and Davis [73] allude to Pareto's law or to the 80/20 principle, the so commented unbalance is reported in the expected *disproportion* in these examples. Therefore, when seeking these key employees the 20% approximation serves as a threshold to know when the analysis has reached enough opinion leaders to influence approximately 80% of the organisation.

## 4.8 Communication Network Analysis

Also known as social network analysis (SNA) is defined as "a method of research for identifying the communication structure in a system, in which socio-metric data about communication flows or patterns are analysed by utilizing interpersonal relationships as the units of analysis." [56, p. 82]. SNA consist of a set of quantitative and qualitative socio-metric measures [80, p. 3] which values are then used to create a graphical representation of the relationships among the units encountered after the data is analysed [81]. Within the context of an organisation, the purpose of conducting a SNA is, on one hand to identify the informal communication roles and on the other hand to determine to what extent the informal communication structure corresponds to the formal communication structure of the organisation [59].

The SNA can be performed at several levels depending on the unit of analysis. The units of analysis can be: individuals, personal communication networks, dyads, cliques, or system networks [56, p. 123]. Particularly, this dissertation will consider individuals and personal networks as the unit of analysis, with the purpose of finding the informal communication roles and informal communication networks, where these roles are immerged within the context of an organisation; that is, perform a SNA to obtain the AxA and AxK *networks* which are intended to be used during the ISAC.

There are several methods to measure *opinion leadership* (AxK *network*) as a network-type variable in a given system. One of the most common methods is inviting members of a social system to nominate opinion leaders [73], [56], [82]. This method is used because individuals who receive the most nominations by their peers reflect a level of influence. In addition, this method is used because it overcomes most of the disadvantages posed by other methods, such as hidden agendas in self-designated methods [83], or those methods where project staff selects their leaders who might not possess the sufficient knowledge and the influence required to obtain the advantages of using opinion leaders, among other methods [73].

In [73], Valente and Davis used the *nomination approach* to identify opinion leaders in a simulated network, reporting considerable improvements in the diffusion process, compared to those approaches where *persons* were selected at random and those who received the fewest nominations. Similarly, in [72], Miha uses the same approach by asking employees of the organisation whom they learn the most from. In this study the author found that the individuals with the most nominations were the persons with the most experience. In this regard, Miha [72, p. 9] proposes that "the greater the experience of the employee in a certain field, the bigger the probability that co-workers will seek to learn from this person", which directly alludes to the influence exerted by opinion leaders.

It worth be noting that the majority of methods for identifying *opinion leaders* involve some form of manual inspection, this is in part because the socio-metric data that needs to be analysed involve qualitative and subjective issues about the particular perception of a given individual about another such as asking "Who would you turn to for advice on this topic?". Moreover, cultural issues contribute to subjectivity when identifying *opinion leaders,* because for a determined cultural background certain aspects result more important than for other cultural backgrounds which ultimately affect the perception of who is or who is not perceived as an *opinion leader* [75]. Nonetheless, research has been made for the automation in the discovery of the most influential individuals and the underlying informal communication network (AxA network) within an organisation through the processing of email server logs, emails messages (email archives), instant messaging systems and web sites logs [84], [82], [70], [85], [86], [87], [88], [65] among others. Particularly, email processing methods for performing SNA seems to be one of the most frequently method used by researchers, as it is regarded as an indicator of collaboration offering a vast amount of information in electronic form that could be analysed relatively *easily* [82].

Mining the email server logs is to a certain extent the more *intuitive* option to perform a SNA within an organisation rather than instant messaging systems or web server logs, because of the intensive and ubiquitous use of email applications (Figure 4.13). The information needed for extracting the informal communication network (AxA

network) is already stored on the email server logs in the fields “From:”, “To:” and the message’s timestamp “Received:” and “Sent:”, needed to plot the graphical representation of the AxA network (*Sociogram*), where a node in the resulting graph is a person who sent or received an email and the arc linking any two nodes denotes a message sent from that one node to the other (Figure 4.8), and then proceed to perform the correspondent socio-metric measures.

A generalisation of the common procedure that researchers follow to mine social networks from email logs or archives are:

a) Identification of communities within the organisation by applying a clustering algorithm.
b) Identification of informal communication roles and informal communication networks.
c) Measurement of socio-metric data.

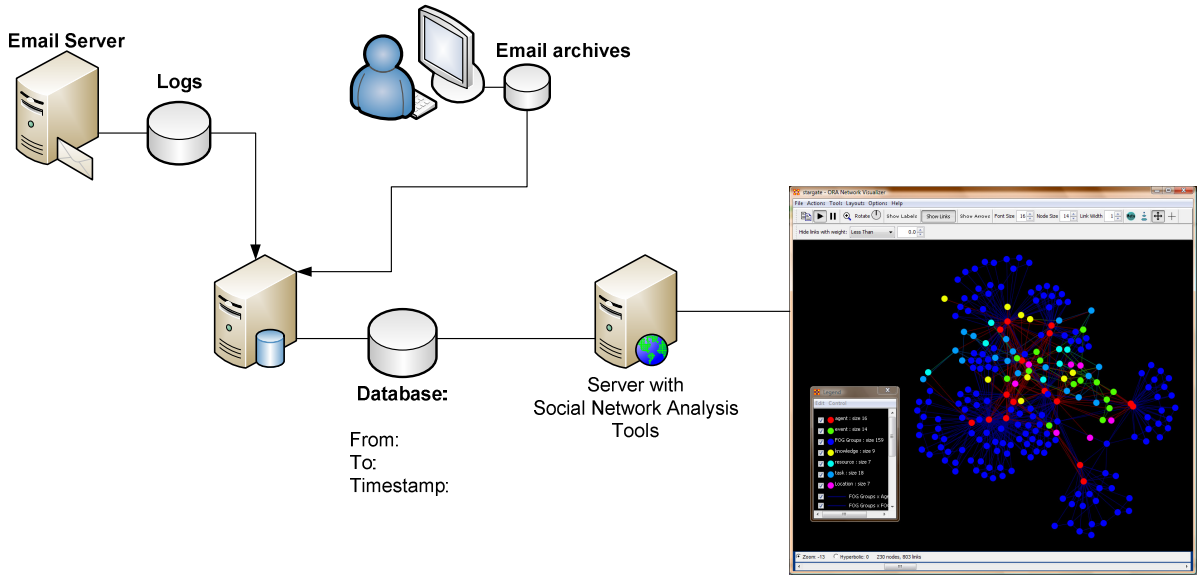



**Figure 4.13** General procedure for mining social networks from email server logs or email archives (similar scheme in [85]).

In [82], Tyler et al propose a method for the automatic identification of communities by processing the organisation’s email server logs. Their aim is to find the informal communication network and also identify informal communication roles, particularly those involving any form of leadership. They claim that their method fully automates the identification of both the informal communication network and “leadership” within the identified communities. Their results indicate a successful identification of communities that they further corroborate with a set of interviews with members of the identified communities.

In [85], Gloor et al propose a similar method, but instead of analysing the email server logs they analyse the email messages archive. The email archive is parsed in order to extract the fields “From:”, “To:”, timestamps and the content of the messages and the obtained data is stored in a Database Management System (DBMS). Then a Graphical User Interface (GUI) developed in JAVA access the DBMS to extract the parsed information, so the data is able to be analysed and consequently plotted accordingly. The authors claim that their SNA tool is able to identify leaders in what they call Collaborative Innovation Networks (COINs). A measure that they use is the number of messages sent minus the messages received divided by the total number of messages sent and received. The authors identify leaders as those individuals whose communication is balanced or close to 0 [85, p. 5].

In [86], Culotta et al implement the approach taken by [82] et al and integrate it to a more comprehensive application, integrating the individual’s address book and their identity that might exist on the internet on a personal web page. The authors recognise that trying to automatically find communities could be regarded as a very subjective task. Not surprisingly, the authors found that highly connected individuals that were in the address book did not appear in their email archive. This is because their personal relationships are not determined by email exchange.

In [70], Bird et al propose a similar approach as that of Gloor et al [85], they parse the email archives and extract the fields “From:”, “To:” and the timestamp of each message. They extract successfully the AxA network; however, the author recognises that the exchange of email is just one aspect of the communication’s structure which implies that more data would be needed in order to effectively determine the individual’s position in the social network. That is the extent to which an individual may be perceived as an influential or not.

In a recent study [87], Carvalho et al attempt to indentify “leadership roles” directly from the emails exchanged in a teamwork context. The procedure used to extract the AxA from email archives is essentially the same as in the previous studies. The authors claim that they could accurately predict, based on the email traffic and the content of the email messages, leadership roles within the team with up to 95% of certainty. Furthermore, they point out that the study conducted by Tyler et al [82] was more subjective than theirs, which implies, that their study is to a certain extent subjective as well. The authors point out that broadcast messages could provide a notion of what a leader’s behaviour looks like.

There is an alternative attempt to model as accurate as possible an AxA and AxK networks. The approach proposed by Choudhury and Pentland [89] involves a wearable electronic device that the authors call “the sociometer” that individuals of the target system carry at all times during a determined period of time in order to allow the device to model their social network by registering the devices of the people

with whom they interacted. The advantage of this approach is that the social network of an individual could be modelled almost regardless of the environment. However, its application would be considerably limited. For instance, for an organisation would not scale well, considering an organisation geographically spread in the world with thousands of employees. Moreover, updates to the social network would be cumbersome and would depend on the availability of the individuals to continue wearing the device at the required moment.

The literature reviewed so far in this section, regarding mining the email logs or email archives has the purpose of pointing out that the term *leader* is somewhat ambiguous and misleading in these studies. At best, some authors provides a notion of what a leader's behaviour might look like [87], but the majority do not define what they mean by *leadership* and seems to refer to *leadership* as a measure of connectedness which is not necessarily what an opinion leader is. Therefore, it could argue that the individuals with the *leadership* that these studies aim to identify are not the same as the individuals that this dissertation has pointed out as *opinion leaders*. The author of this dissertation contends that the measure of connectedness in these studies for example, do not necessarily mean *opinion leadership* since not all human relationships are bound to email messages, despite the fact of the popularity of email applications [86], there could still exist *opinion leaders* who might neither appear as highly connected nodes nor plotted in the mined *sociogram*. Research Scientist at the Center for Collective Intelligence at MIT's Sloan School of Management, Peter A. Gloor was contacted by the author of this dissertation to comment on this respect:

> "*...the contribution index gives a good indication of influentials, also the "galaxies", in "don't be a star, be a galaxy". So, the short answer is, the social network position is a good predictor, but to be certain, there is no substitute for interviews.*" – Peter A. Gloor.

Nonetheless, what these studies do successfully achieve is the mining of the AxA network either from email server logs or email archives which enable to effectively identify liaisons and bridges, those informal communication roles that enable the fast spread of information within the organisation. There are several socio-metric measurements that can be performed in *network analysis,* for the purpose of this dissertation the author is going to focus in those socio-metric measurements that make possible the identification of well-connected nodes, that is, liaisons and bridges [86], [59].

It worth be noting that network scholars refer to the *indices of communication network* (socio-metric measurements) in different forms, for example, Gloor et al [85, p. 4] provides a definition for *centrality* which is the same definition for *individual connectedness* provided by Rogers and Kinkaid [56, p. 178, 183]. The author of this dissertation will adopt the definitions by Rogers and Kinkaid [56] because they provide a deeper description on which measurements are more likely to be useful to identify the informal communication roles.

Typical socio-metric measurements can be performed at the personal, clique and system level, depending on the aims of the analysis. Particularly, to identify well-connected nodes, the typical measurements, according to Rogers and Kinkaid [56, p. 178, 183] are:

**Individual connectedness:** This index is computed by taking into account the number of present arcs that a particular member has, divided by the number of possible arcs in the graph; that is N-1, where N is the number of members of the network. Hence the minimum *individual connectedness* value is 0 and the maximum is 1. This measurement provides the degree of linkage of a particular member. This index could be useful in determining the extent to which a particularly member is influenced by the system [56, p. 178].

**Individual integration:** This index is computed by taking into account the number of connections among the members of the communication network divided by the possible number of connections. This measure indicates the degree in which the members of the personal network of an individual are interconnected among each other. As it was mentioned before, this index indicates to what extent a personal network is *radial* or *interlocking*. In the former network this index tends to zero, whereas in the latter network, the index tends to 1. Additionally, this index could be particularly helpful in finding at least two of the informal communication roles. Since *bridges* are linking two or more *cliques,* the *individual integration* index is expected to be low. Moreover, *liaisons* are expected to have this index even lower than *bridges* [56, p. 179, 180].

**System connectedness:** This index is computed by taking into account the number of connections among the cliques of the whole system. This index indicates the degree in which the cliques of a given social system are interconnected among each other. This index is particularly useful to assess the extent in which innovations are expected to be efficiently diffused within the organisation [59]. The more connected the system, the more efficient the communication network is.

## 4.9 Viral Marketing and the impact on the individual's behavior

This topic is included in this chapter because v*iral marketing* can only be explained through the intervention of the informal communication roles that exist within an informal communication network.

*Viral Marketing* is a term frequently used in the marketing field, but to date there seems to be no consensus about its definition [90, p. 334], [91]. Leskovec et al [92, p. 4] describe it in terms of the diffusion of an innovation: "*viral marketing … diffusion of information about the product and its adoption over the network*". Modzelewski [91] argues that viral marketing is not the same as word-of-mouth (where customers share information about a product with other customers). He goes further by stating that "*True viral marketing differs from word-of-mouth in that the value of the virus to the original customer is directly related to the number of other users it attracts. That is, the originator of each branch of the virus has a unique and vested interest in recruiting people to the network*". For Phelps et al [90, p. 334], the concept involves the use of electronic communication tools where individuals voluntarily pass along emails. Regardless of the particular conception of this term by researchers in the marking industry, researchers Steve Jurvetson and Tim Draper coined the term *viral marketing* in 1998 [93] to refer to the epidemiological behaviour in the adoption of a particular innovation through the customer's personal communication network. Viral Marketing is an example of how informal communication networks can be exploited to spread information about an innovation as fast as possible (typically based on email communication tools), at the same time that the message requests to the recipients to act accordingly and forward the message to their *friends* [94], [95]. By forwarding the message, *viral marketing* successfully achieves its primary goal, eliciting the desired response on the targeted individuals by passing along email.

### 4.9.1 Motivations

Nowadays, the majority of marketing campaigns involves launching massive amount of sales messages to potential customers. While this technique is effective for *innovation awareness* on potential adopters, the side effects of such overwhelming amount of messages is a general apathy to advertising [96], [97], that is, potential customers are ignoring sales messages and the marketing campaigns encounter serious problems in achieving its objective of influencing people's behaviour favourably to their marketed product. This is one of the reasons why *viral marketing* has emerged as an alternative to classical marketing techniques, to engage the interest of potential customers back into their products. When using *viral marketing* techniques, messages received by potential customers are not directly from companies, but from *credible sources* such as friends, who recommend the use of a

determined product or service [98], [90]. In general, individuals are more likely to pay attention to any message coming from their personal communication network than a message coming directly from a company [94]. Thus, *viral marketing* techniques emerge as a response to a generalised apathy towards massive marketing sale messages [94].

Although, the problem in organisations might not be massive marketing sales messages, the outcome could be the same; that is, the problem is very likely to be apathy towards IT and security guidelines messages. Consider for example the IT department of the financial institution from the case study in Chapter 2. FIRA promotes monthly an electronic bulletin called "**InfoBIT",** in which topics such as general IT advises, IT articles, security guidelines, promotion of IT services among others, are delivered via the email service to all the employees in the organisation as an effort to increase the awareness on *relevant* topics. However, during a training programme for administrative employees, more than 90% of the administrative assistants of the institution, recognised not to have even opened those emails, allegedly because the content was neither "*relevant*" for their functions nor "*interesting at all*". Additionally, since these messages were *informational,* administrative assistants decided to ignore them, knowing that such action would not represent any *harm* against their jobs.

Apathy towards this type of *informational* messages could be addressed with *viral marketing* techniques. In addition, certain types of *official* messages could also be treated with *viral marketing* techniques, such as the *security* messages of the ISAC. This is because the desired outcome is a positive change in attitude that would not be achieved by imposing a new behaviour. The aim is to enable employees to make decisions with security in mind, to nurture a security minded culture, whereas an imposed behaviour is very likely to raise a "*do the least, sufficient to comply*" attitude that would eventually result in severe security breaches. The problem with "**InfoBIT"** is that it is indiscriminately addressed to all employees within the organisation. As a result, the message is read by a minority of employees, sufficiently curious to see what have arrived to their mail boxes, but the majority ignoring the email at best, or delete it at worst, without eliciting any favourable response towards the messages contained on the bulletin.

Arguably, the aim of *viral marketing* could be regarded as being the same as biological virus, or computer virus, that is to "*survive and to reproduce*" [99, p. 4]. According to what it has been discussed in this Chapter, in order to achieve a higher rate of employees reading the bulletin, the email should be sent by *opinion leaders* [100] (instead of the IT department whose image within the same organisation is typically not the best in most of the cases) to their *followers* (Figure 4.14)*;* perhaps with a personal note that the opinion leader might consider appropriate, which could be of

particular interest for the members of their network (*survive*), at the same time that the *opinion leader* asks the recipients to *spread the word* to their contacts regarding the content of the email (*reproduce*). Thus, *viral marketing* is used in this case, by employing *opinion leaders* and prompting the members of their informal communication network to promote and distribute the message contained on the bulletin [100]; in this form, v*iral marketing* becomes a tool that could be used by *opinion leaders* to exert their influence over their followers, by exploiting the informal communication network.

It has been widely commented in this dissertation that the individual's personal communication network directly affects the individual's behaviour, by exerting a certain degree of influence towards the adoption of a determined innovation [100], [95], [92], [94], [101], among many others. In this regard, by using viral marketing techniques three of the steps towards persuasion are made (see Chapter 3), by increasing the exposure, attention and acceptance of the security message simply by receiving the email through a *credible source*. In addition, the delivery of such messages over informal communication networks would also serve as the first step for a marketing conditioning campaign (see Chapter 3). As it has been mentioned in Chapter 3, this would eventually lead to a change of attitude and ultimately to a behavioural change regarding IS issues.

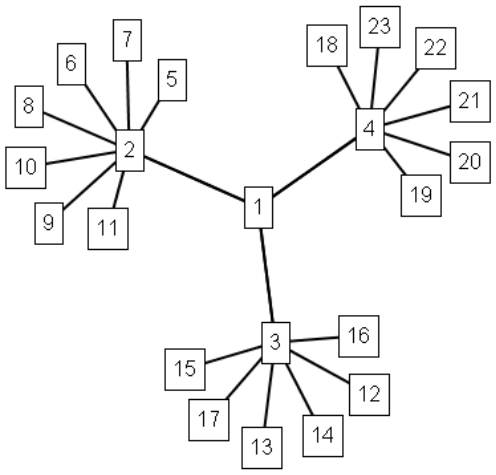



**Figure 4.14** Change agent (#1), communicating to the rest of members of the social system through opinion leaders, individuals #2, #3 and #4.

### 4.9.2 Advantages and Disadvantages

The uses of *viral marketing* techniques present both advantages and disadvantages in its use. For instance, information spread via *viral marketing* is relatively fast and most of all un-expensive [100], [98]. *Viral marketing* is regarded as an effective tool for launching innovations since awareness of the innovation is spread rapidly through

informal communication networks. Additionally, sharing information about the innovation is effortless when it is delivered through email communication tools and the message is to a certain extent immune to apathy as a consequence of having the message sent from a *credible source* [96], since this type of communications from individual-to-individual are regarded as open, honest and motivated by the individual's willingness to educate and help [90].

However, the ultimate results could be positive and/or negative [100], where negative worth-of-moth could spread even more rapidly than positive word-of-mouth [90]. Since the content of the message is under control of the recipient, the received message is prone to be filtered, incomplete or even biased [100], potentially every time the message is forwarded. According to Phelps et al [90], approximately one third of the messages were forwarded with a personalised note. One important aspect that must be considered when designing a *viral marketing* campaign is that *marketers* must also consider the worst scenario, this is, where a negative word-of-mouth is spread instead [98]. Another disadvantage is that *viral marketing* is not entirely a controllable issue; once it has started and has reached a determined number of targets, the *diffusion* might not be able to be stopped; regardless if what it is being spread is a negative or positive word-of-mouth [8]. Hence, if not managed appropriately, viral marketing could result in unfavourable attitudes towards the innovation [92]. As a countermeasure in this regard, a reward program for opinion leaders could be implemented, to reward those who effectively exert their influence and achieve in their followers the intended behaviour described by the original security message [90].

According to a viral marketing study conducted by Phelps et al [90, p. 341], found that women were involved in a higher degree in pass-along emails than men. The most common attachments were ".jpg" files and ".gif" files. Approximately one third of the messages were forwarded with a personalised note [90, p. 342]. Women were more likely to write personalised notes [90, p. 342]. The top five motives for sending pass-along email was because they were *fun*, *enjoyable*, *entertaining*, *to help others*, and *to have a good time* (in general enjoyment and entertainment) [90, p. 343]. According to the results obtained in this study, most of the emails that were forwarded involved some form of free stuff and helpful tips [90, p. 345].

According to [102], another viral marketing report, where 3500 customers were surveyed, found that a 36% of the respondents do forward emails to some extent [102, p. 4]. Interestingly, this report confirms that women are more likely to pass-along email compared to men in a proportion of 38% to 33% [102, p. 5]. Moreover, 27% of the people forward email to between 1 and 5 people in average, which practically follows Pareto's law discussed in a previous section. This particular result indicates that if a message is forwarded by 27% of the people, virtually half of the

social system in question would be aware of the contents of that message, in other words, only 4 messages in average would be needed by the 27% of people who forwards email to deliver the message to the 100% of the members of a social system. Lastly and worth noting is the correlation between the type of content and the messages that were forwarded; the majority again, include some type of humour (jokes, funny videos and pictures) [102, p. 8].

### 4.9.3 General characteristics of viral marketing messages

- **Engage the interest of the recipient.** According to the results previously commented, the message must include some form of humorous content and helpful tips [90], or intrigue the reader to engage their interest [98]. This aspect will determine to a certain extent the *survival* of the message.

- **Associated with a credible source**. The recipients must associate the message with a *credible source,* otherwise the resulting effects might not be the ones expected [98].

- **Elicits or encourage the response of sharing the message**. The message must prompt the recipient to forward the message to the members of his or her personal communication network and particularly to those who do not know about the message [98]. This aspect is what actually would cause the "buzz" and deals with the *reproductive* aspect of the viral message.

Viral Marketing could be used as a tool for measuring diffusion. A viral video can be used as a pass along email to test and measure the diffusion of the link.

Consider the following IS procedure specified in order to comply with a specific ISP regarding the protection of workstations:

> *"...employees are required to lock their workstation when leaving their workplace temporarily. (the workstation can be locked by pressing the Ctrl+Alt+Delete keys together and then selecting 'Lock Workstation' or equivalent button)"*

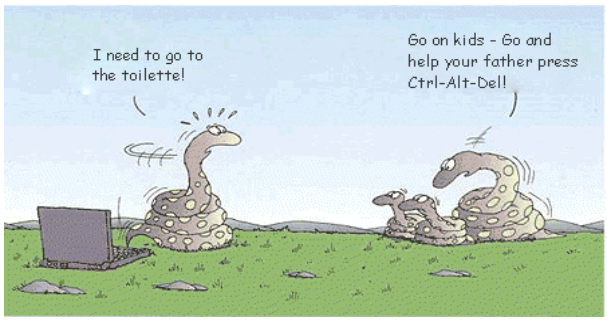
For this case, a viral message seems to be an option that the *change agent* (security administrator) could use in order to attempt a high rate of compliance towards the ISP. If the message is crafted in such a form that it satisfies the general characteristics mentioned above, the overall outcome is expected to be positive word-of-mouth. Figure 4.15 shows the main body of a proposed viral email message which includes the

three elements commented above: the *subject line* attempts to engage the interest of the individual; additionally, the recipient of the message would notice that it came from a *credible source* (the individual's *opinion leader* or a *friend*); involves a humorous element which is statistically a determinant factor that motivates an individual in forwarding emails; lastly, the message prompts the recipient to forward the message to *those who might need it*, a line that it is expected to cause a "buzz", that is, to stimulate the members of the informal communication network to talk about this issue. Since the message deals with a helpful tip, relatively easy to read, easy to understand and easy to implement, the effects of this message is expected to be positive word-of-mouth. It is worth noting that the overall character of the message is informal, as it shall appear to come from an *opinion leader initiative* not from the *change agent.* The idea of using informal communications to reinforce the core message of a security guideline is not new; scholars recognise the importance and the positive impact of encouraging informal contact, particularly in ISA initiatives [2, p. 545].

To: **Opinion leaders' followers**
Subject: **Why do it in 4 steps when you can do it in 2?**

Hi guys!

Have you noticed that when you lock down your computer, you typically do it in **four** time consuming steps ?

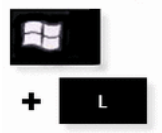



Yes, 4 steps:

1. **Ctrl**
2. **Alt** →
3. **Del**

**4. Lock Computer - button**


Actually, you could do exactly the same in just **two** steps: **Win+L**





I hope it helps!

Please forward this message to those you think it might be of some help.

**Figure 4.15** Main body of a proposed viral email message which includes the three elements commented above: engage the interest of the recipient, associated with a credible source, encourage forwarding the email.

## 4.10 Summary

In this chapter two communication models were discussed; Shannon and Weaver's *Linear Model of Communication* and Rogers and Kinkaid's *Convergence Model of Communication.* The latter offers a dynamic representation of the communication process which is presumably closer to reality as it includes some cognitive psychological process not considered in the former model. Nonetheless, the later model is not complete as it ignores additional cognitive elements, such as *affective responses*, *behaviour intentions* and the *attitude* itself towards a determined issue; these are elements that are involved at the moment of deciding to behave in a certain manner. Therefore, a combined approach is proposed by the author of this dissertation and referred to as *the Extended Convergence Model of Communication* (E-CMC).

The organisation's formal structure determines in part the behaviour of the employees; nonetheless, its inherent informal communication structure also exerts some influence in employees' behaviour. The information communicated through the informal communication structure travels faster along the organisation than through formal communication channels; therefore these informal communication structures are considered as an alternative for the diffusion of information. The informal communication structure can be modelled in terms of the Meta-Matrix of networks, resulting as the most relevant for the purpose of this dissertation the AxA and the AxK networks, which are used to identify informal communication roles such as *liaisons* and *bridges*, and *opinion leaders* respectively. The informal communication roles account for the 20% of employees within the organisation according to *Pareto's law.* Therefore, during a *social network analysis* the 20/80 proportion could be used as a threshold to recruit *liaisons, bridges* and *opinion leaders.* One recommendation to identify these informal communication roles is through an *unobtrusive method*, such as mining *social networks* from e-mail logs or e-mail archives. Lastly, in order to trigger the interpersonal network communications among employees, a viral marketing approach is proposed for spreading information and attempt to influence the attitudes and the ultimate employees' behaviour.

CHAPTER

# 5

# Information Security Awareness:

# An Innovation Approach

## Contents



## 5.1 Introduction

The purpose of this chapter is, first to comment on the elements of the DoI approach and how this theory could be used in the IS field, particularly for the implementation of an ISAP; therefore, the theory is analysed and approached from this perspective, leaving aside the elements that result irrelevant for the implementation of the ISAP. Then, second, to gather together the information covered in previous chapters to build the thesis proposed by this dissertation. For example, how the governance issue treated in Chapter 2 fits into the DoI theory, propose a combined social psychology approach in combination with the results of a SN analysis to achieve a behavioural change upon which the ISAP would be based.

The literature in the field of *innovation* is vast, nonetheless, according to Denning [103] and [104], the most influential studies are provided by Peter Drucker in his book "*Innovation and Entrepreneurship*" [105] and by Everett Rogers in his book "*Diffusion of Innovations"* [8]. The former provides a more theoretical approach where as the latter provides an empirical and more practical approach in the proposed framework [104]. The framework proposed by Rogers seems to be the most influential of these two studies; for instance [106] and [107] base their study in great part in Rogers' proposed framework. Moreover, Rogers' proposed framework has been widely used in the IT field [7, 108, 109]. For these reasons, what follows is a discussion of the *diffusion of innovations* theory, according to Rogers in [8]. In addition, a set of *generalizations* provided by Rogers in [8] are included as a roadmap for the proposal of the ISA approach. These *generalizations* summarise the findings and results of the empirical studies conducted in this field.

## 5.2 Elements in the Diffusion of Innovations

The DoI has its roots in the rural sociology practice of the 1940's which main purpose at the time was to address the problems in the rural sector [110, 111]. Rogers and Scott [110] refers to the study conducted by Bryce Ryan and Neal C. Gross in 1943 as the most influential study that determined in great part the methodology and the theoretical framework of the DoI as it is known today. The DoI theory has been applied in different areas and disciplines such as education, communication, marketing, sociology, public health [112], IT [108, 109] and many others. The *diffusion* studies in these areas or disciplines deal with the evaluation, adoption and implementation of innovations [109]. The diffusion of the internet for example, is a widely studied subject by *diffusion* scholars [110], [8] as many other innovations in the IT arena; however, the DoI theory seems to be ignored particularly in the IS discipline.

The term *diffusion* is used by Rogers [8, p. 5] to refer to a process that takes place over a period of time in which the social networks of a social system are involved in spreading a determined piece of information (or *innovation*) using determined communication channels. Hence, the main elements in the *diffusion* process are: the *innovation*, the *communication channels*, *time* and the *social system*.

The disadvantage of this method is that the approach is very likely to work as long as the newness of the idea remains, as this factor determines the individual's reaction towards the innovation [8, p. 12].

## 5.3 The Innovation

An Innovation, according to Rogers [8, p. 12], is in itself the *object* of the *diffusion process*, virtually anything that is perceived as new by an individual or group of individuals could be regarded as an innovation. For example, if an idea, a practice, a determined piece of technology, a service, etc is perceived as new then it could be regarded as an innovation. For instance, an ISA *initiative* could be regarded as an *innovation,* as it promotes a new form of practice in the daily activities or behaviour in general, where employees are enabled to make their decisions from an IS perspective, which is the ultimate goal of ISA. Nonetheless, for other scholars, *innovation*, more than a new "*thing*", is a practice in itself. Denning [103] for example, openly disagrees with the concept of *innovation* provided by Rogers in [8]. For Denning [103], an innovation deals with the process of adoption of the *object* that is perceived as new rather than an object being perceived as new. The author of this dissertation uses the concept of *innovation* provided by Rogers in [8], as it explains the underlying process that takes place when such *innovation* is *diffused* and how the behaviour of the adopting units is affected by the adoption of such *innovation*.

The *innovation* has several characteristics that determine the rate of its adoption by the intended adopters, that is, the following characteristics would determine the rate of adoption of the security behaviour and how the overall ISA *initiative* (the *innovation*) would be perceived by employees within the organisation:

- **Relative advantage.** Since the ISA is promoting a behavioural change, employees need to perceive as clear as possible why the behaviour proposed by the ISA initiative is better than the behaviour it supersedes. The advantage of the desired security behaviour could be expressed in economic terms and also considering convenience and/or satisfaction factors. "Generalization 6-1: *The relative advantage of an innovation, as perceived by the members of a social system, is positively related to its rate of adoption"* [8, p. 233]. The rate of adoption of the security behaviour would be determined in great part by the perception of its relative advantage [8].

- **Compatibility.** The ISA initiative shall be compatible with the organisational culture in order to achieve the adoption of the security behaviour that it promotes. Perhaps this is one of the factors that can help explain why employees find difficulties in adopting the required security behaviour. It was mentioned in Chapter 3 how the employees' schemata are sometimes in conflict with some ISP. Therefore, the adoption of the security behaviour (most of the times an incompatible innovation) requires first the adoption of another set of ethical principles, values and beliefs which may represent a slow process.

"Generalization 6-2: *The compatibility of an innovation, as perceived by members of a social system, is positively related to its rate of adoption*" [8, p. 249].

- **Complexity.** The change agent will attempt to achieve a behavioural change on the employee through the security messages and activities of the ISAC. The content of these messages and activities, whether they are training sessions, emails, leaflets, videos, security bulletins, etc. should be designed to be reasonable easy to understand and the advises easy to implement and use, that includes avoiding as much as possible the use of technical terms and unnecessary complex procedures. "Generalization 6-3: *The complexity of an innovation, as perceived by members of a social system, is negatively related to its rate of adoption"* [8, 257].

- **Trialability.** Frequently, in the marketing field, customers have the opportunity to try a product before they buy it. This would allow customers to obtain more information about the product prior to its adoption. In the ISA context, *trialability* would be present by providing employees with sufficient time to familiarise with the ISP and the required security behaviour before any enforcement policy takes place. "Generalization 6-4: *The trialability of an innovation, as perceived by members of a social system, is positively related to its rate of adoption*" [8, p. 258].

- **Observability.** Employees are more likely to adopt the security behaviour that is being promoted if the results of such behaviour are visible to others. As a result, the security behaviour becomes a motive of discussion for those who have not adopted and are seeking further information before they decide to adopt. In this regard, the example of the viral mail exposed in Chapter 4 seems to be a good candidate as it stimulates peer discussion among the members of a social network. "Generalization 6-5: *The observability of an innovation, as perceived by members of a social system, is positively related to its rate of adoption"* [8, p. 258].

Summing up, if the overall ISAP is designed in such a form that employees perceive it as having greater *relative advantage, compatibility, trialability, observability* and less *complexity,* the ultimate ISA goal (behavioural change towards IS issues) is more likely to be achieved [113].

## 5.4 Communication Channels

The *innovation* is just one of the main parts of the overall *diffusion* process. Part of the second main element has been covered in the first part of Chapter 3 when the *communication* process was first introduced and discussed. According to a definition provided by Rogers and Kinkaid in [56, p. 63], the *communication* process involves two or more entities in a continuous information exchange with the purpose of achieving a *mutual understanding* not of the *physical reality*, which may not be accessible for both entities, but of the reality perceived through different sets of information that moulds the individual's *schema*. The *communication channel* is the medium over which these messages are made available to the counterpart [8, p. 18].

Two particular types of communication channels have been introduced in the previous chapter, *localite channels* and *cosmopolite channels.* These are the types of channels intended to be used throughout the ISAP. It is important to distinguish between these two types of communication channels in order to determine which type is needed to spread a determined piece of information as fast as possible and which other is needed for persuasion. For instance, mass communication media such as radio or television are regarded as *cosmopolite communication channels* [8, p. 207]. The *cosmopolite communication channels* are more suitable for reaching massive audiences than for persuasion, whereas *localite channels* (interpersonal channels) are more suitable for persuasion than for reaching massive audiences [8, p. 207]. This means, that *cosmopolite communication channels* are better for conducting awareness campaigns, whereas *localite channels* are more suitable for launching behavioural change campaigns. For example, a *mass communication channel* would be used by the *change agent* to provide knowledge or awareness regarding the compliance requirements of the ISP within the organisation. Then, in order to promote a behavioural change, the *opinion leaders'* interpersonal channels (which includes face-to-face communication) would be used to deliver specific security guidelines and exert influence towards a positive attitude regarding IS issues. "Generalization 5-14: *Cosmopolite channels are relatively more important at the knowledge stage, and localite channels are relatively more important at the persuasion stage in the innovation-decision process*" [8, p. 207].

## 5.5 Time

Time is one of the elements that give this theory its strength [8, p. 20]. Time is involved in the *diffusion of innovations* in three different forms:

1. In the *innovation-decision process*.
2. In the *innovativeness* of the unit of adoption (an individual or a group of individuals).
3. In the innovation's rate of adoption.

### 5.5.1 Time in the innovation-decision process

The *innovation-decision process* (IDP) refers to the process in which the *attitude system* of the individual (or unit of adoption) becomes affected by the knowledge of the existence of an innovation. At different stages of the IDP, the individual aims to reduce uncertainty of the advantages and disadvantages of adopting an innovation by obtaining further information from their peers and from the individuals who have adopted the innovation already.

The IDP follows two different dynamics determined by the degree of structure of the social system; that is, for a low structured social system, the IDP involves the following stages: *knowledge of the innovation, persuasion, decision, implementation and confirmation* [8, p. 170] whereas for highly structured social systems such as organisations the IDP involves the following stages: *agenda setting, matching, redefining/restructuring, clarifying and routinizing* [8, p. 421]. Both types of IDP occurring in a time ordered sequence.

**Table 5.1** Innovation-decision processes and types.

| | **Individuals or unit of adoption (informal communication networks present low structure)** | **Structured social systems (formal communication networks)** | |
|---|---|---|---|
| **Innovation-decision process** | *knowledge of the innovation, persuasion, decision, implementation and confirmation* | *agenda setting, matching, redefining/restructuring, clarifying and routinizing* | |
| **Innovation-decision process types** | Optional innovation | Collective innovation decisions. | Authority innovation decisions. |

#### 5.5.1.1 Model of the IDP targeted to individuals (or unit of adoption)

"Generalization 5-12: *Stages exist in the innovation-decision process*" [8, p. 198].

- **Knowledge of the innovation.** When the *change agent* or security manager uses *mass communication channels* for example, employees are able to gain knowledge about the ISP and the security behaviour that the organisation is promoting [8]. In this stage, the *relative advantage* of the security behaviour could be communicated along with the new value system that would be needed to reduce conflict between the employees' schemata and the ISP; in other words, seek to enable compatibility between the ISP and the organisational culture. "Generalization 5-13: *Mass media channels are relatively more important at the knowledge stage, and interpersonal channels are relatively more important at the persuasion stage.*" [8, p. 205]. "Generalization 5.17: *The rate of awareness knowledge for an innovation is more rapid than its rate of adoption*" [8, p. 214].

- **Persuasion.** In this stage, is where employees form a favourable or unfavourable attitude towards the ISA initiative [8, p. 174]. As it was discussed in Chapter 3, the *attitude* of individuals could be influenced by affecting their schemata; that is, changing their beliefs, ideas and misconceptions, by supplying further information about the reality of the risks that the information of the organisation faces and the role they play in protecting it. The question now would be, who assures that the change agent possesses accurate information about the reality that is being promoted? The answer should involve a *mutual understanding,* not just with another individual who might be addressing the same problem, but a *mutual understanding* with an international recognised body of experts who reached consensus on how to solve common problems in the IS field; in other words, international standards of IS.

- **Decision.** The attitude formed about the ISA initiative is very likely to influence the ultimate decision taken by the employee that can result in the adoption or rejection of the promoted security behaviour. The latter, is an option that could in fact be taken at any stage of the IDP, not necessarily just in this stage; nonetheless, it is used here to illustrate the outcome of attempting to affect the individual's attitude system. This stage might become the cause of some discussion, as it could be argued that within an organisation and most of all, when treating with IS issues, employees shall not have the option to decide whether they will adopt or not the behaviour prescribed by the ISP. As it was mentioned before, an authoritarian position might not be the best for this case; as it could be motive for employee dissatisfaction, slow process of adoption, ineffective communications and negative attitudes against IS issues (more about this point later in this chapter) [8].

- **Implementation.** Gaining knowledge and forming an attitude about the ISP and the promoted security behaviour, and deciding whether to adopt it or not is all until this stage a mental process in the mind of employees. It is in this stage

where employees put into practice the adopted security behaviour. Eventually, the "newness" of the promoted behaviour disappears with its continuous use and become a part of the individuals' behaviour [8].

- **Confirmation.** Once the security behaviour has been adopted and implemented, the individual would seek to reinforce the decision already taken; if individuals perceive conflicting messages against the adopted behaviour then a state of *dissonance* may arise in the psychological reality of individuals, leading to reverse their decision to adopt the promoted security behaviour. The lack of reinforcement can also lead to *discontinuance* of the adopted security behaviour, either if it is by *replacement* or *disenchantment*. The former is a decision that the individual makes to reject the original security behaviour and adopt a "better" behaviour (*better* from the point of view of the employee) that supersedes it. The latter, is a decision that the employee makes to reject the adopted security behaviour after feeling disappointed, or after they perceive that the adopted security behaviour is not appropriate or do not represent any relative advantage. "Generalization 5-11: *Later adopters are more likely to discontinue innovations than are earlier adopters*" [8, p. 191].

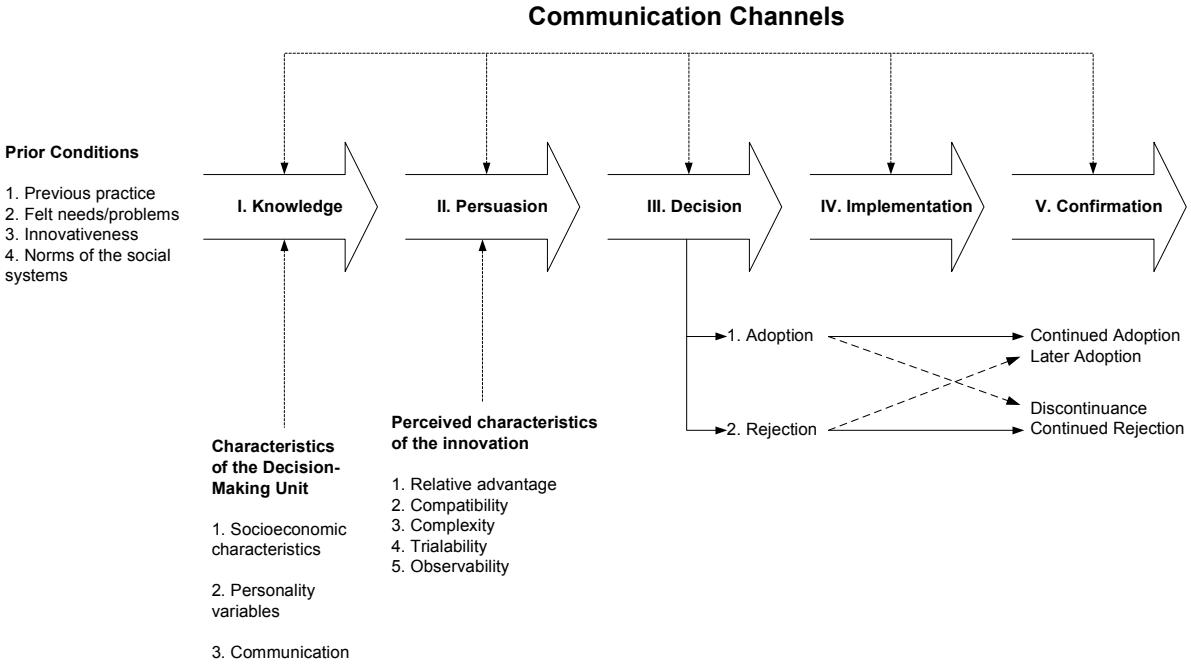



**Figure 5.1** Model of five stages in the Innovation-Decision Process [7].

### 5.5.1.2 Model of the IDP targeted to organizations (or unit of adoption)

The *innovation decision* process is different when the *diffusion of innovation* takes place within organisations. One main difference is that the main focus is implementation rather than adoption. The innovation process in organisations could

be seen as if it occurred in two phases, namely an *initiation* phase and an *implementation* phase. The former is involved with the compilation of information, conceptualisation and the plans surrounding the adoption of the innovation. The latter, is involved with all the activities that need to be carried out to put the innovation into use. The dotted line in Figure 5.1, denotes the decision to adopt and divides these two phases. For example, this is typically the process that takes place when an organisation decides to adopt IT solutions. There exists a close parallelism between the innovation process in organisations and the *risk management* process in IS, where risks are identified, analysed and then prioritised in order to address those that would represent a more negative impact against the business by selecting the appropriate security controls. This suggests that the risk management process in IS could be approached as an *innovation process in organisations*. "Generalization 10-1: *Lager organizations are more innovative*." [8, p. 409]. "Generalization 10-4: *A performance gap can trigger the innovation process.*" [8, p. 422].

- **Agenda setting.** The innovation process in an organisation begins with the identification of a problem and consequently the identification of the innovations that could help in solving that problem [8].

- **Matching.** In this stage a particular innovation is selected to address the identified problem and a deep analysis is performed in order to determine the extent to which the innovation will solve the problem that eventually results in a cost-benefit analysis [8]. The decision makers might act upon the result of these analyses, by accepting or rejecting the proposed innovation, denoted with the dashed line in Figure 5.2.

- **Redefining/restructuring.** Once the decision to adopt the innovation in the organisation is made, the innovation is *redefined* or *restructured* in such a form that fits the organisations' needs as close as possible. Notwithstanding, the organisation could also attempt to restructure itself in order to make possible the adoption of the selected innovation. This stage is particularly interesting for ISA as it will be commented below. "Generalization 10-5: *Both the innovation and the organization usually change in the innovation process in an organization.*" [8, p. 425].

- **Clarifying.** Is depicted as a stage where a clearer understanding of the adopted innovation is gradually reached by the members of the organisation as a result of its widespread use. The more the adopted innovation is used, the clearer the meaning becomes for the members of the organisation [8].

- **Routinizing.** Is a stage where the innovation is not perceived as such anymore, as it has come to form part of the regular activities carried out by the organisation [8].

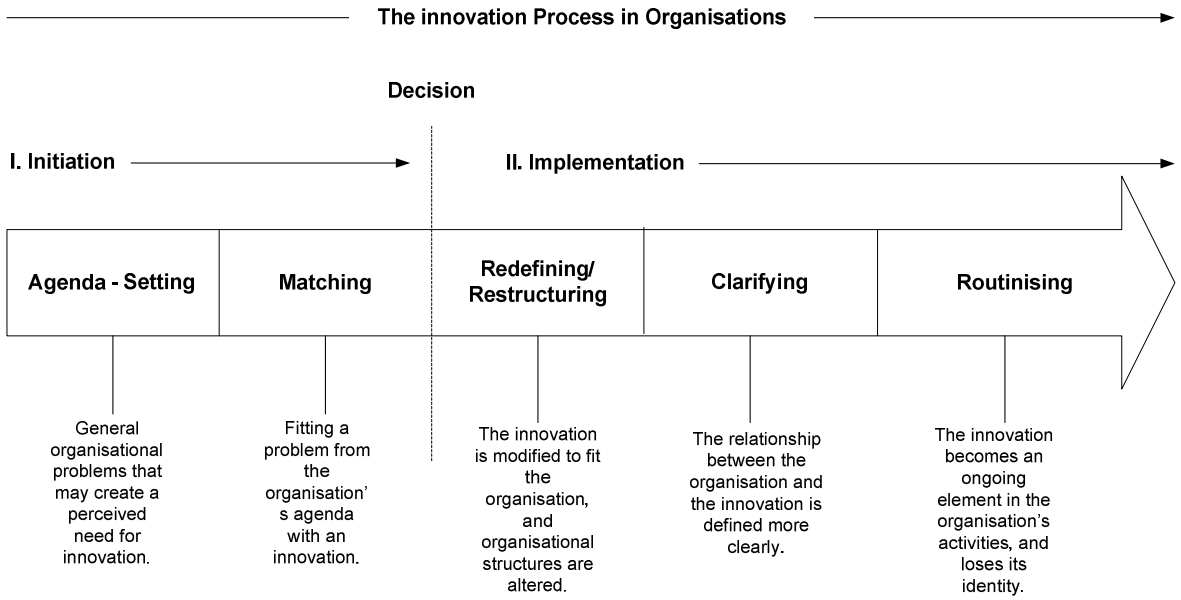



**Figure 5.2** A Model of five stages in the Innovation-Decision Process in Organisations [7].

### 5.5.1.3 Types of innovation-decisions

According to Rogers [8], there are three types of *innovation-decisions:*

a) *Optional innovation-decisions*. Refers to those decisions taken by the individual towards the adoption or rejection of an innovation regardless of the decisions taken by the rest of the members of the social system.
b) *Collective innovation-decisions*. Refers to those decisions achieved by consensus among the members of a social system towards the adoption or rejection of an innovation.
c) *Authority innovation-decisions.* Refers to those decisions towards the adoption or rejection of an innovation taken by a small group of individuals characterised by their power, technical expertise and high social status, members of a social system.

ISA is a special type of innovation, as it appeals to both types of *innovation-decision processes;* as an innovation adopted by the organisation and as an innovation targeted to individuals (Figure 5.3).


**Figure 5.3** ISA is a special type of innovation since it is treated as an innovation adopted by the organisation and as an innovation targeted to individuals.

In the former case, the organisation might *identify* the factual or potential for harm and loss, due to the risks that the business information faces, caused mainly by human errors (*agenda setting stage*). Once the problem is identified, ISA could be proposed as the innovation that could help in mitigating those risks (*matching stage*). In the *redefining/restructuring* stage, ISA would be *redefined* or *restructured* in such a form that fits the organisations' needs as close as possible. Similarly, ISA would require from the organisation to restructure itself in order to make possible the adoption of this innovation. As it was mentioned in Chapter 2, ISA shall be part of a formal IS framework, supported by all levels of management, which arguably, is only possible through the instantiation of the *IS governance* from the *corporate governance strategy*. The clarifying stage for ISA would be gradually reached in the measure that all levels of management become aware of the inherent risks associated with IT solutions and the business information to which employees have access. The *routinizing* stage would be reached once the IS governance strategy has been successfully instantiated and empowered by organisational authority to deliver and in determined cases enforce the ISP. Typically *collective* and *authority innovation-decisions* are involved in the process of adoption of innovations in organisations [8].

In the latter case, ISA would be treated as an innovation targeted to individuals, where individuals pass from knowledge of the ISAC, to form an attitude towards ISA initiatives, to decide whether to adopt or "*reject*" the promoted security behaviour, to start exercising the security advises delivered through the ISAC, and to the reinforcement of the decision of having adopted the security behaviour. In this case, *optional innovation-decisions* are involved in the process of adoption of innovations by individuals.

While some ISP shall be treated as *authority innovation-decisions,* where the executive management and board of directors exercise their faculty to decide whether to adopt or reject a proposed innovation, it shall not be the case for ISA. This is because of the ultimate objectives that are expected from the ISA initiatives, which are to achieve a long lasting (or permanent if possible) security behaviour on employees and nurture a security-minded culture that enables the members of the organisations to make security-minded decisions. If employees feel forced to comply with the requirements of the ISP rather than first prepare them to gradually adopt the required behaviour, then this authoritarian position is more likely to cause dissatisfaction (that leads to inefficiency as discussed in Chapter 3), resistance to change, and one of the most undesired consequences, a "least effort, sufficient to comply" attitude towards IS issues that would eventually result in severe security breaches.

The author of this dissertation proposes to treat ISA as if it was the case of an *optional innovation-decision*. For a fixed period of time, ISA would be treated as an *optional innovation-decision*, then after a reasonable amount of time, once the majority of employees have adopted or reached the *critical mass* (more about this topic below in this Chapter), shift the security initiative to an *authority innovation-decision* and communicate the new *decision* to all members of the organisation. In this form, employees are given the opportunity to gradually adopt the required security behaviour, provided the feeling that they are in *control* of making their decisions towards the adoption or rejection of the security behaviour, even if it is temporarily.

### 5.5.2 Time and the innovativeness of the unit of adoption

*Innovativeness* is a quality present in the unit of adoption (or individual) that refers to the extent that this unit adopts an innovation in an early stage more rapidly than the rest of the units [8, p. 22]. The members of a social system are classified by their *innovativeness* in five categories, *innovators, early adopters, early majority, late majority and laggards* [8, p. 22] (Figure 5.4). "Generalization 7-1: *Adopter distributions follow a bell-shaped curve over time and approach normality*" [8, p. 275].

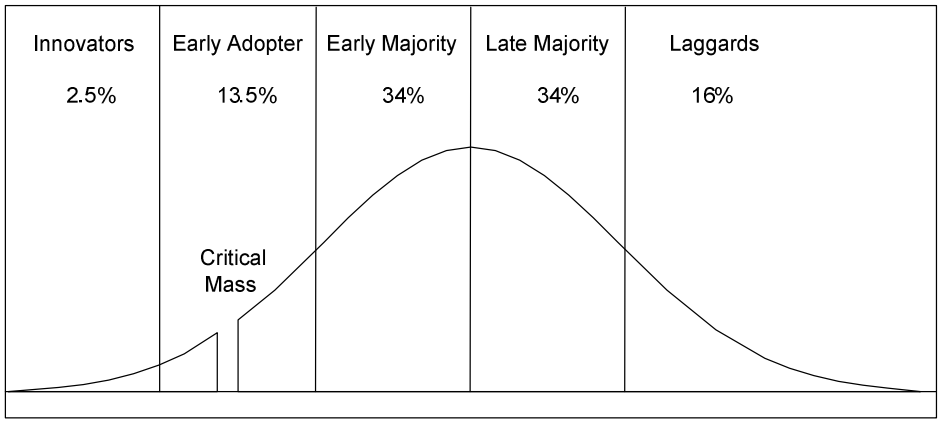



**Figure 5.4** Categories according to the innovativeness of the adopter [7].

These categories result from the amount of time required by the members of a social system to go through the IDP. The five categories proposed by Rogers in [8], represent abstractions that have been obtained from empirical studies. A description of these categories from the ISA perspective is provided next:

- **Innovators.** The adventurers; they are the most innovative members of the organisation as they represent the first 2.5% of the employees adopting the innovation [110]. *Innovators* are characterised by their interest in new ideas, their cosmopolite communication patterns, their relatively high socioeconomic status, their technical expertise and a relatively high tolerance to risk and uncertainty; these are characteristics that enable them to be the firsts in adopting an innovation. They are not *opinion leaders*; hence they do not exert influence in their peers towards the adoption of an innovation. Moreover, they may not be respected by some members of the social system, in part because of their relatively high degree of *heterophily* in respect to their fellow employees. Nonetheless, it is worth noting that *innovators* are a very important part of the *diffusion* process, acting as *gatekeepers*; hence it is through them that an innovation enters into the social system [8].

- **Early adopters.** The respected; they represent the next 13.5% of the employees adopting an innovation. The characteristics of the members in this category could be regarded as being opposite to those of the *innovators. Early adopters* are well respected members in the social system, they serve as models for other employees and it is in this category where the majority of *opinion leaders* are located; hence this category is typically the target of *change agents* to speed the *diffusion* process. In order to maintain their influential position, *early adopters* seek to provide objective evaluations about the innovation, which are then (if requested), communicated through informal communication networks. The

increasing adoption of an innovation by *early adopters* lead to reaching the *critical mass* (Figure 5.5), which might be one of the prime objectives pursued by *change agents* [8].

- **Early majority.** The deliberators; they represent the next 34% of the employees adopting an innovation, one of the two most numerous category of adopters. This category presents a low degree of opinion leadership and they usually adopt before the average member. As it can be appreciated in Figure 5.4, the position of the *early majority* in the *diffusion* process represent a link between those members who are very early in adopting an innovation and those who are late in adopting an innovation. In this category is where *liaisons* and *bridges* might be located, interconnecting the informal communication networks. They take their time to deliberate before they decide to adopt an innovation [8].

- **Late majority.** The sceptics; they represent the 34% of the employees adopting an innovation, the second most numerous categories of adopters. They typically adopt an innovation after the average member, if not after most of the members in a social system have adopted. The adoption is very likely to be the result of peer pressure in their informal communication network, due to the presence of a degree of resistance to change by the members of this category. As a consequence, members of the *late majority* receive the innovation with scepticism [8].

- **Laggards.** Die-hard; they represent the last 16% of employees adopting an innovation. In a *sociogram* most of them would be depicted as isolate nodes because of their *localite* communications channels. The resistance of *laggards* to adopt an innovation is nearly systematic, as they need to be sure that the new idea will not fail [8].

### 5.5.2.1 Early adopters' Generalizations

As early adopters are one of the categories that attract more the efforts of *change agents,* a vast amount of research has been done in this regard, resulting in several *Generalizations* related to *early adopters*. These *Generalizations* provide a close profile of the members in this category which result helpful to launch the ISA.

These categories are important for the purpose of this dissertation, as they represent different audience segments [114]. These segments are not just the intervals of adoption required by different members of social system to go through the IDP, but they also reveal the attitudes of the individuals towards the innovation [96]. Therefore, in order to achieve the desired objectives, an ISAC needs to be

something more than an indiscriminate marketing exercise of the required security behaviour targeted to all employees within an organisation; neither *innovators*, nor *early adopters*, nor the *early majority*, nor the *late majority,* nor *laggards* seems to *speak* the same *language* [96], in the sense that the perception of the same message is assimilated in different forms by members of each category, ranging from deep interest in the new idea to apathy and even active rejection. For this reason, each of these segments requires a different treatment during the ISAC [96]; they need to be approached according to their *innovativeness*.

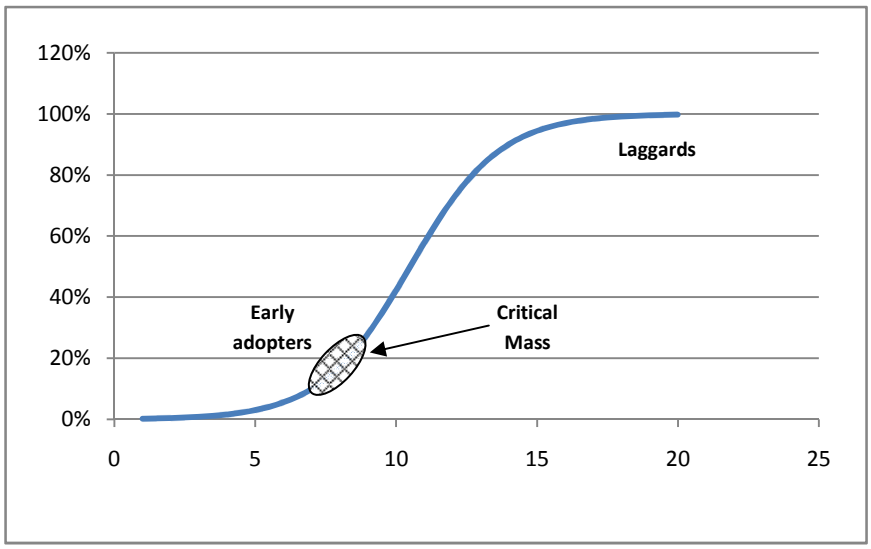



**Figure 5.5** The critical mass is reached once the majority of opinion leaders or members of the early adopters' category adopts the innovation, commonly reached between the 10% and 20% of adoption, following Pareto's law (image source in [7)].

**Critical Mass.** Gladwell [71] refers to this concept as "*the tipping point*". It is a concept that refers to a point during the *diffusion* process, where the rate of the adoption of the innovation "takes-off". The critical *mass* is more likely to happen when the majority of the *early adopters* or *opinion leaders* adopt the innovation; it is said that after this point, the rate of adoption becomes self-sustaining [8, p. 343]. It is worth noting that the *critical mass* is commonly reached between the 10% and 20% of adoption [8, p. 12], closely following *Pareto's law* (Figure 5.5). This means that by engaging 20% of the opinion leaders or members in the *early majority,* the rate of adoption would continue growing *virtually* without further efforts of the *change agent,* this is an attractive feature for both managers and change agents; managers would need to provide sufficient resources as to reach 20% of the opinion leaders while *change agents* can minimise the use of scarce resources to successfully reach a high rate of adoption of a given innovation.

### 5.5.3 Time and the rate of adoption

The *rate of adoption* concept requires the *time* factor in order to be able to specify the speed in which an innovation is adopted in a social system. Figure 5.5 depicts a cumulative representation of the adoption of an innovation over a time period of 20 weeks that results in an S-shaped curve. When the innovation is first launched, the *innovators,* approximately 2.5% of members in the social system are the first to adopt. Once the new idea is introduced to the social system by the *innovators,* the innovation reaches the *opinion leaders* or members of the *early adopter* category whose opinions are respected by other members in the social system. When the majority in this category adopt, the *critical mass* is reached, taking-off the rate of adoption almost in an exponential behaviour; that is, a great part of members in the social system decide to adopt within a relatively short period of time. As the number of adopters decrease, also does the rate of adoption until the *diffusion* process finishes. As it was mentioned earlier in this chapter, the rate of adoption of an innovation is directly affected by its perceived characteristics from members of the social system. It is worth noting that the *rate of adoption* of an innovation is measured within a social system; therefore, this distribution holds to study the *rate of adoption* of an innovation in a community, a social group or an organisation.

## 5.6 Social system

The term *social system* is defined by Rogers in [8, p. 23] as "*the set of interrelated units engaged in joint problem solving to accomplish a common goal*", for example the members of an organisation constitute a *social system* as they all have a common goal or mission (see Chapter IV for deeper discussion regarding this topic). "Generalization 8-13: *An individual is more likely to adopt an innovation if more of the other individuals in his or her personal network have adopted previously.*" [8, p. 359].

## 5.7 Marketing of the ISA initiative

Typically, prior (or sometimes along) to the launching of any product or service, a marketing campaign is also launched to create awareness in the target audience and prepare them for the adoption of the *product* [3] (p. 219); an initiative that could also be regarded as an initial conditioning campaign [1]. In this regard, McLean [1] suggest the *marketing mix* to treat ISA under a marketing perspective (Figure 5.6).

| | |
|---|---|
|  **Product** | The desired security behaviour and attitudes toward IS issues |
|  **Basic customer need** | Responsible, professional behaviour; protection against the consequences of others' actions and accidents; selfprotection against accusations of bad practice; conformance with accepted practice within the organisation. |
|  **Target market** | All employees (and temporary employees) of the organisation: agents and non-employee users of the organisation's IT; possibly shareholders, customers and the general public. |
|  **Price** | Time, attention, minor inconvenience. IT development and operations overheads. Balance between security and functionality. |
|  **Principal promotional tools** | Corporate newsletters and other promotional media: endorsement by opinion formers. |
|  **Delivery of the campaign** | Corporate communications channels. use of IT communication to reach IT. Mass / Cosmopolite communication channels. |

**Figure 5.6** The marketing mix for ISA [17].

### 5.7.1 The Marketing Mix for ISA, the Product.

The product would be the desired security behaviour and attitudes towards IS issues which in turn, as it is regarded as a *new practice,* represents an innovation.

**The *Basic Customer Need.*** The adoption of the product will be determined by its perceived characteristics and also by the customer's perception of needing to adopt the innovation in question. Therefore the product shall engage the interest of the customer and *create* the need to encourage its adoption. The innovation shall be relevant for the potential adopter; hence the need to reach a *common understanding* and a *common agreement* regarding the content of the security messages, between the *change agent* and *employees* prior to launching any campaign.

**Target Market.** The *target market* for ISA are all employees within the organisation. The security messages shall be relevant to the recipients and not all the recipients have the same IS concerns. For example, the IS concerns for the IT staff might be different from the IS concerns of the Human Resources department. This observation leads to use audience segmentation and design relevant security messages for each audience.

**Price.** The price for the promoted product is, instead of money, time, attention, a certain extent of inconvenience and an additional effort to embed into the daily activities IS principles. Opposite to what it would occur to other type of products, the *price* in this case could vary from one type of audience to another. In general, the *price* could be seen in terms of functionality. The more secure an environment, the less functional it turns and viceversa. The main point is that the security administrator should find a middle ground between security and functionality in order to offer a fair *price* that can be perceived as an attractive feature in the promoted product.

**Principal promotional tools.** One of the principal problems, when deliverin the ISAC, is failing to use specialised awareness materials. By specialised awareness materials the *ISF* refers to brochures, posters, reference cards, electronic documents, etc. According to the *Information Security Status Survey* [35], it is very common to deliver repetitive security messages using non-specialised awareness materials in approximately half of the awareness activities. Hence, the principal promotional tools should consider using the appropriate awareness material.

**Delivery of the campaign.** It refers to those tools that are going to be used to deliver the awareness of the product. In the case of ISA, mass communication media and cosmopolite channels are going to be used, as they enable a message to be spread along the organisation in a more efficient manner.

## 5.8 Information Security Awareness: an innovation approach

It shall be remarked that as little research has been done on applying the *diffusion of innovations* theory in the IS field, the proposed ISA approach must necessarily be to a certain extent hypothetical and suggestive. Further research needs to be done regarding the results of applying the proposed strategy and the extent to which the objectives are achieved through this approach.

If an IS framework is not officially installed within the organisation, the first ISA *initiative* would be to take the organisation through the IDP in organisations. Else, if an IS framework is already installed within the organisation, the following strategy could be implemented to achieve a behavioural change towards IS issues within the organisation.

The proposed strategy uses a *diffusion of innovations* approach; that is, the overall ISA *initiative* is treated as an *innovation* targeted to employees within an organisation, where the main goal is to achieve the adoption of the required security behaviour. In order to achieve such adoption, employees have to go through the IDP. This becomes one of the tasks of the *change agent* (security administrator responsible of the ISAP). As it was mentioned, the IDP comprises the following stages: *knowledge* of the innovation, *persuasion* to adopt the innovation by attempting to change their attitudes towards IS issues, *decision* to adopt or reject the innovation, *implementation* of the innovation when employees have decided to accept the innovation and *confirmation* of their decision. The *change agent* could influence each of these stages in different degrees. The first two stages are two active tasks, directly influenced by the *change agent*. The third stage is the consequence of the resulting evaluation of the preceding stages; nonetheless, according to the E-CMC, it is possible to have a positive attitude towards IS issues and also have the intention of adopting the security behaviour but ultimately deciding to reject the innovation. During the fourth stage, employees use the information and security procedures they were given in preceding stages to implement the innovation. Lastly, a commonly overlooked task in ISAP is the reinforcement of the adopted behaviour; although this might be an employee's internal mental process of confirming the adopted behaviour, the *change agent* can *facilitate* employees finding reasons for sticking to the adopted security behaviour.

In order to lead employees through the IDP, several campaigns need to be designed. The first campaign shall target the first stage of the IDP; hence, it needs to be a campaign designed to provide knowledge or awareness of the ISA *initiatives,* ISP, procedures, security guidelines and the required security behaviour. Henceforth, this campaign will be referred to as *information security knowledge campaign* (ISKC). The second campaign shall target the second stage of the IDP*;* hence, it needs to be a campaign designed to attempt persuasion towards the adoption of the required security behaviour. Henceforth, this campaign will be referred to as *information*

*security persuasion campaign* (ISPC). The third campaign shall target the fifth stage of the IDP; hence, it needs to be a campaign designed to provide supportive information to facilitate employees find reasons that support their decision of having adopted the security behaviour. Henceforth this campaign will be referred to as *information security confirmation campaign* (ISCC). Stage three is not targeted with a dedicated campaign as it is indirectly influenced by the preceding stages and stage IV does not need a dedicated campaign also, as the information regarding procedures and security guidelines could be delivered during the *awareness campaign* and the *persuasion campaign.*

The overall design of the proposed ISAP will consist of two broad phases. The first phase includes all tasks involved in the preparation of the *ISKC*. The second phase includes all tasks involved in the preparation of the *ISPC* and the *ISCC.* The *ISCC* is considered as part of the second phase because it could be regarded as a persuasion task.

The *ISKC* could be regarded as a *communication process* between the *change agent* and employees. This implies that employees have the opportunity to share their points of view, regarding the ISA *initiatives* promoted by the *change agent.* The *change agent* will then have to consider the opinions communicated by employees and adapt the content of the campaign's messages to reflect a *mutual understanding* that eventually would lead to *mutual agreement and collective action.* However, the extent to which the *change agent* can reach consensus and achieve *mutual understanding* and *mutual agreement* could be questioned, because of the potential high number of employees within the organisation and their dispersion over geographically distant regions. An alternative to this limitation is trying to reach consensus through *opinion leaders,* by applying Pareto's law; this would mean that through *mutual understanding* and *agreement* reached with *opinion leaders,* who represent 20%, at least 80% of employees would be involved in such consensus. Trying to seek *mutual understanding* and *mutual agreement* with 20% of the employees, result in a far more achievable task than trying to reach such consensus by communicating with the 100% of the employees within the organisation.

The *ISPC* could be regarded as a *communication process* between *opinion leaders* and their *followers,* and also between employee and employee. This implies that that the *opinion leader* is actively involved in the *diffusion* process, by providing further explanations to those followers seeking their support, in understanding the security messages until a *mutual understanding* and *agreement* is reached. In addition, further interpersonal network communications are triggered, when employees are asked to forward the security message to those who *might not* know about the security message. Nonetheless, it would be questionable the extent to which *opinion leaders* are engaged in the ISA *initiative* and the extent to which *employees* are expected to

talk about the promoted IS security issues. The first issue is expected to be overcome by prior *conditioning* or prior conversations, to engage the *opinion leaders* support; the latter issue, is addressed by using email content that have proved to engage employees' attention to pass along e-mail. In addition, this latter issue is reinforced by the communication efforts of bridges and liaisons.

The *ISCC* could be regarded as a *communication process* between the *change agent* and *adopters*, and between *opinion leaders* and *followers.* This campaign represents a form of persuasion, where the *change agent* and *opinion leaders* attempt to *persuade* employees and *followers,* respectively, to remain as adopters; hence the goal of the *communication process,* in the *ISCC,* is to reach a *mutual understanding* and *agreement*.

According to Rogers [8, p. 378], successful communication *campaigns* have considered the following steps:

1) Conducting a formative research.
2) Setting specific and reasonable campaign goals.
3) Using audience segmentation.
4) Designing *viral* mass media messages.

Nevertheless, there seems to be at least two steps missing. A fifth step, involving the *measurement of the effectiveness* of the ISAC, and a sixth step involving the *delivery of the security messages*. These six steps are going to be considered for the design of the three different campaigns proposed above. In addition, the generalizations mentioned during this chapter, along with generalizations mentioned in appendix A, are also going to be used to shape the design of the ISAP.

One limitation of the proposed approach, is that for every security topic or theme, three different campaigns would be needed, namely the ISKC, ISPC and ISCC; causing additional administration efforts. Nonetheless, the effectiveness of such strategy may be a compensating factor. Another apparent limitation of this approach is that as three different campaigns need to be conducted, someone could argue that more resources would be needed. This is not necessarily true; since the campaigns are managed from a 20/80 perspective (Pareto's law), fewer resources are supposed to be required in each delivery. Although this is a debatable point, the hypothesis is that this strategy would consume the same amount of resources provisioned for a traditional ISAP, nonetheless, with more effective results.

Steps involved in the *ISKC, ISPC* and *ISCC:*

1. Conduct a formative research.
2. Set SMART goals.
3. Use Audience segmentation.
4. Design *viral* mass media messages.
5. Set the *campaign's* effectiveness measurement approach.
6. Deliver the ISAC

What follows, is a suggested outline of each phase and the action plan of its associated campaigns.

### 5.8.1 Phase I - The ISKC

1. **Conduct a formative research.** The purpose in this first step, is to know the context and environment of the target audience, such as their informal communication structure, their informal communication roles and also try to assess the type of messages they are more receptive to, in order design the content of the security messages, which would be based on this information that are more likely to appeal employees' interests.

**Tasks involved in this stage:**

1.1 Mine social networks form email logs (server logs or email archives)

1.1.1 Perform a SNA over the email logs.

1.1.1.1 Compute Individual connectedness.

1.1.1.2 Compute Individual Integration.

1.1.1.3 Compute System Connectedness.

1.1.2 Mine AxA network from analysed data.

1.1.3 Identify informal communication roles.

1.1.3.1 Identify bridges.

1.1.3.2 Identify Liaisons.

1.1.3.3 Identify Gatekeepers.

1.2 Identify *Opinion leaders*

1.2.1 Use the nomination method to identify *opinion leaders.*

1.2.2 Use the *opinion leaders'* and *earlier adopters' generalizations* to confirm the identified *opinion leaders.*

1.2.3 Mine AxK network from the analysed data.

1.3 Identify audiences and the type of messages that would make sense for them.

1.4 Develop themes and topics.

1.5 Seek to reach a *mutual understanding* from employees identified as *bridges* and *liaisons,* regarding themes and topics of the security messages.

1.6 Consider the opinion of employees identified as *bridges* and *liaisons,* when designing the security content.

1.7 Seek to reach consensus (*mutual understanding*) through *opinion leaders,* regarding themes and topics of the security messages.

**2. Setting SMART goals.** SMART is the acronym for: *specific, measurable, action-required, realistic, time-delimited* [35, p. 34] and is commonly used to specify clear and well-defined objectives.

2.1 Formally define and document ISKC's objectives.

**3. Audience segmentation.** The audience is segmented in two different forms. According to their IS concerns and according to their informal communication networks.

3.1 Audience segmentation according to their informal communication networks:

3.1.1 Segment one formed by *bridges and liaisons* (20% of members in a social system).

3.1.2 Segment two formed by the rest of the members of the social system (80%).

3.2 Audience segmentation according to their IS concerns:

3.2.1 IT System Administrators.

3.2.2 Software developers.

3.2.3 Finance departments, etc.

**4. Design *viral* mass media messages and formal mass media messages.**

4.1 Design the type of messages for each identified audience.

4.2 Consider *opinion leaders'* opinions regarding the content of the security messages.

4.3 Design considerations:

4.3.1 Expose clearly in the message the *relative advantage* of the IS issue treated in the security message.

4.3.2 Expose clearly in the message the *value system* required to adopt the security behaviour.

4.4 Develop Viral Mass Media Messages

4.4.1 Design security message content using some form of humour.

4.4.2 At the end of the email ask the hypothetical recipient to forward the message to those who may not know about it.

4.5 Produce formal mass media messages and content for seminars and training sessions.

4.6 Seek to reach consensus (*mutual understanding*) through *opinion leaders* regarding the content of the security messages.

**5. Measure ISKC effectiveness**

5.1. Use a combination of internal protection and efficiency and effectiveness measurement approaches (see Chapter 2 for more information of the different approaches) to measure the ISKC effectiveness.

5.1.1. Get set the internal protection measurement approach.

5.1.2. Get set the efficiency and effectiveness measurement approach.

**6. Delivery of the content of the ISKC.**

6.1. Use the *communication channels' generalizations* (Appendix A).

6.2. Assess the effectiveness of the communication networks within the organisation.

6.3. Initiate the ISA effectiveness measurement approaches.

6.3.1. Initiate the internal protection approach.

6.3.2. Initiate the efficiency and effectiveness approach.

6.4. Set timescales for delivering the viral-content through bridges and liaisons (who represent the 20% of the employees).

6.5. Set timescales for delivering the formal security messages to each identified audience (summing up 100% of employees).

6.6. Use localite and interpersonal communication channels (face-to-face or direct communication) to deliver the security message through the informal communications structure:

6.6.1. Send customisable security messages to employees identified as bridges and liaisons (20%).

6.6.2. Initiate the ISKC by asking employees identified as bridges and liaisons to forward the viral-content security messages to members of their interpersonal communication network (20%)

6.6.3. Use cosmopolite and mass communication channels (email, intranet web site, internal magazine, etc.) to deliver the security messages 100% of employees:

6.6.3.1. Launch formal ISKC by delivering the security messages to the different identified audiences.

6.6.4. Based on the results of the effectiveness of the communication networks within the organisation repeat steps 6.6.2 and 6.6.3 as needed.

**NOTE:** *System connectedness* is an index particularly useful to assess the extent in which innovations are expected to be efficiently diffused within the organisation [59] (p. 144). The more connected the system, the more efficient the communication network. Hence timescales can be estimated considering this index. In addition, it is worth noting that efforts for identifying *opinion leaders* are made in this stage and not in the second phase as it would be expected, because the *change agent* seeks to achieve *consensus* through *opinion leaders* which is a task needed in phase I, in order to be able to design the content of the campaign's messages.

### 5.8.2 Phase II - The ISPC

1. **Conduct a formative research.** The purpose in the first step of phase II of the ISPC, is to know the context and environment of *opinion leaders*, such as their informal communication structure, their followers and also try to assess the type of messages that they are more receptive to, in order design the content of the security messages according to this information, which are more likely to appeal opinion leaders' and followers' interests.

   **Tasks involved in this stage:**

   1.1 Determine the informal communications structure of o*pinion leaders* and their *followers:*

   1.1.1 Mine AxK network from the analysed data.

   1.1.2 Identify *followers.*

   1.2 Identify *opinion leaders* for different audiences and the type of messages that would make sense for them.

   1.3 Seek to reach consensus (*mutual understanding*) through *opinion leaders* regarding the content of the security messages for the ISPC.

2. **Setting SMART goals.** SMART is the acronym for: *specific, measurable, action-required, realistic, time-delimited* [35, p. 34] and is commonly used to specify clear and well-defined objectives.

   2.1 Formally define and document ISPC's objectives.

3. **Audience segmentation.** The audience is segmented in two different forms. According to their informal communication networks and according to their IS concerns:

   3.1 Audience segmentation according to their informal communication roles:

   3.1.1 Segment one formed by *opinion leaders* (20% of members in a social system).

   3.1.2 Segment two formed by *followers* (80% of members in the social system).

3.2 *Opinion leaders* segmentation according to their IS concerns:

3.2.1 IT System Administrators.

3.2.2 Software developers.

3.2.3 Finance departments, etc.

**4. Design *viral* mass media messages.**

4.1 Design the type of messages for each identified audience.

4.2 Consider *opinion leaders'* opinions regarding the content of the security messages.

4.3 Design considerations:

4.3.1 Expose clearly in the message the *relative advantage* of the IS issue treated in the security message.

4.3.2 Expose clearly in the message the *value system* required to adopt the security behaviour.

4.3.3 Seek *compatibility* with current organisational culture when designing the security message.

4.3.4 Design the security message to be easy to understand, seeking to reduce *complexity*.

4.3.5 Provide sufficient information as to allow employees to *try* the security procedures and guidelines.

4.3.6 Prevent the impression of forcing the user to adopt the required security behaviour.

4.3.7 Seek to increase the strength and number of *driving forces* that support the adoption of the security behaviour.

4.3.8 Seek to reduce the strength and number of *resisting forces* against a favourable attitude towards the adoption of the security behaviour.

4.4 Develop Viral Mass Media Messages

4.4.1 Design security message content using some form of humour.

4.4.2 At the end of the email ask the hypothetical recipient to forward the message to those who may not know about it.

4.5 Seek to reach consensus (*mutual understanding*) through *opinion leaders* regarding the content of the security messages.

**5. Measure ISKC effectiveness**

5.1 Use a combination of *internal protection* and *efficiency and effectiveness* measurement approach (see Chapter II for more information of the different approaches) to measure the ISPC effectiveness.

5.1.1 Maintain the already started *internal protection* measurement approach.

5.1.2 Maintain the already started *efficiency* and *effectiveness* measurement approach.

**6. Delivery of the content of the ISKC.**

6.1 Refer to *communication channels' generalizations* (annexe).

6.2 Use localite and interpersonal communication channels (email, face-to-face communication, etc.) to deliver the security messages in a 20% mode:

6.2.1 Set timescales for delivering the viral-content through *opinion leaders* (20%)

6.2.2 Send customisable security messages to employees identified as *opinion leaders* (20%).

6.2.3 Initiate the ISPC by asking employees identified as *opinion leaders* to forward the *viral-content* security messages to members of their interpersonal communication network (20%).

6.2.4 Based on the *effectiveness* of the communication networks within the organisation repeat step 6.2.3 as needed.

### 5.8.3 Phase II - The ISCC

1. **Conduct a formative research.** The purpose in the first step of phase II of the ISCC, is to explore the extent to which employees are aware of the IS requirements and

assess the number of adopters in order to launch the *confirmation campaign* which essentially will aim to provide reinforcing information to support the employees' decisions regarding their decision to adopt the innovation.

1.4 Seek to determine the number of adopters from the results of the campaign's effectiveness measurement approaches.

1.5 Determine the informal communications structure of o*pinion leaders* and their *followers:*

1.5.1 Use the mined AxK network from the ISKC.

1.5.2 Identify *followers.*

1.6 Identify *opinion leaders* for different audiences and the type of messages that would make sense for them.

1.7 Seek to reach consensus (*mutual understanding*) through *opinion leaders* regarding the content of the security messages for the ISPC.

**2. Setting SMART goals.** SMART is the acronym for: *specific, measurable, action-required, realistic, time-delimited* [35, p. 34] and is commonly used to specify clear and well-defined objectives*.*

2.2 Formally define and document ISPC's objectives.

**3. Audience segmentation.** The audience is segmented in two different forms. According to their informal communication networks and according to their IS concerns:

3.3 Audience segmentation according to their informal communication roles:

3.3.1 Segment one formed by *opinion leaders* (20% of members in a social system).

3.3.2 Segment two formed by *followers* (80% of members in the social system).

3.4 *Opinion leaders* segmentation according to their IS concerns:

3.4.1 IT System Administrators.

3.4.2 Software developers.

3.4.3 Finance departments, etc.

**4. Design *viral* mass media messages.**

4.6 Design the type of messages for each identified audience.

4.7 Consider *opinion leaders'* opinions regarding the content of the security messages.

4.8 Design considerations:

4.8.1 Expose clearly in the message the *relative advantage* of being adopters of the promoted innovation.

4.8.2 Expose clearly in the message how the adopted *value system* required for the adoption of the security behaviour is compatible with their value system.

4.8.3 Expose clearly in the message how they comply with the organisation's ISP by being adopters of the promoted security behaviour. Avoid using negative reinforcements.

4.8.4 Seek to increase the strength and number of *driving forces* that support the adoption of the security behaviour.

4.8.5 Seek to reduce the strength and number of *resisting forces* against a favourable attitude towards the adoption of the security behaviour.

4.9 Develop Viral Mass Media Messages

4.9.1 Design security message content using some form of humour.

4.9.2 At the end of the email ask the hypothetical recipient to forward the message to those who may not know about it.

4.10 Seek to reach consensus (mutual understanding) through opinion leaders regarding the content of the security messages.

**5. Measure ISKC effectiveness**

5.2 Use a combination of *internal protection* and *efficiency and effectiveness* measurement approach (see Chapter II for more information of the different approaches) to measure the ISPC effectiveness.

5.1.3 Maintain the already started *internal protection* measurement approach.

5.1.4 Maintain the already started *efficiency* and *effectiveness* measurement approach.

**6. Delivery of the content of the ISKC.**

6.3 Refer to *communication channels' generalizations* (annexe).

6.4 Use localite and interpersonal communication channels (email, face-to-face communication, etc.) to deliver the security messages in a 20% mode:

6.2.5 Set timescales for delivering the viral-content through *opinion leaders* (20%)

6.2.6 Send customisable security messages to employees identified as *opinion leaders* (20%).

6.2.7 Initiate the ISPC by asking employees identified as *opinion leaders* to forward the *viral-content* security messages to members of their interpersonal communication network (20%).

6.2.8 Based on the *effectiveness* of the communication networks within the organisation repeat step 6.2.7 as needed.

The three campaigns proposed in this dissertation, could be matched to the phases discussed in Chapter 3, section 3.5 "conditioning principles in marketing". For instance, the ISKC would represent the initial conditioning campaign (section 3.5.1, Chapter 3), as it provides knowledge or awareness about the innovation, targeting all potential adopters. The ISPC would represent the behavioural change campaign (3.5.2, Chapter 3), as it attempts to influence employees' attitude towards a favourable perception of IS issues. Finally, the ISCC would represent the *point of delivery campaign* (section 3.5.3, Chapter 3) and the *branding campaign* (section 3.5.4, Chapter 3), as it attempts, among other things, to provide reinforcing messages to remain as adopters of the security behaviour. In Table 5.2, the relationship between the proposed campaigns and the marketing conditioning campaigns is showed and their appearance in the corresponding IDP's stage.

In another set of ideas, it is important to make a further annotation regarding the types of communication channels mentioned in section 4.6 of Chapter 4, which are needed to deliver in a more accurate form the security messages. According to Rogers [8, p. 207]:

> *"Cosmopolite communication channels are those linking an individual with sources outside the social system under study. Interpersonal channels may be either local or cosmopolite, while mass media channels are almost entirely cosmopolite"*

This means that there are at least three different communication channels: *interpersonal-cosmopolite*, *interpersonal-localite* and *mass-cosmopolite* communication channels (see Table 5.2). In the context of an organisation, these types of channels would define the extent in which a determined channel is used by determined employees.

**Table 5.2** Types of communication channels according to [8].

| **Cosmopolite communication channels:** Link an individual with sources outside the social system. | |
|---|---|
| **Interpersonal communication channels** | |
| Cosmopolite | Localite |
| **Mass media communication channels** | |
| Cosmopolite | |

For example, consider the e-mail service, to which all employees within the organisation have the same level of access to this potentially mass media communication channel. It is worth noting that its use may vary from one employee to another; while the average employee would use it most of the time as an *interpersonal-localite* communication channel, *bridges* and *liaisons* would use it as an *interpersonal-cosmopolite* communication channel, and change agents would use it as a *mass-cosmopolite* communication channel.

The use of the email service by *opinion leaders* is interesting, as they are required to use it as an *interpersonal-localite* communication channel to exert their influence over their peers; nonetheless, they may also use it as an interpersonal-*cosmopolite* communication channel, through which they acquire new ideas and maintain a certain level of cosmopoliteness.

Table 5.2, summarises the proposed strategy that lead employees throughout the IDP and the main components of the campaigns outlined above:

**Table 5.3** Summary of the strategy to lead employees through the innovation-decision process.

| | Innovation-Decision Process | | | | |
|---|---|---|---|---|---|
| | **Knowledge** | **Persuasion** | **Decision** | **Implementation** | **Confirmation** |
| **Proposed Campaigns** | ISKC | ISPC | Indirectly by ISKC and ISPC | | ISCC |
| **Marketing Conditioning Principles** | *Phase I*. Initial Conditioning Campaign | *Phase II.* Behavioural Change Campaign | | | *Phase III.* Point of Delivery Campaign and *Phase IV.* Branding Campaign |
| **Communication channels** | Interpersonal-localite and mass-cosmopolite communication channels | Interpersonal-localite communication channels | | | Mass-cosmopolite and Interpersonal/localite communication channels |
| **Informal communication roles** | Bridges, Liaisons | Opinion Leaders | | | Opinion Leaders |
| **Participants in the E-CMC** | Change Agent-Opinion leader (representing employees) and employees-employees | Opinion Leaders-Followers and Employees-Employees | | | Change Agent-Adopters, Opinion Leaders-Followers and Employees-Employees |
| **E-CMC goals** | Mutual Understanding Knowledge/Awareness and | Mutual Understanding and Mutual Agreement | Induced Collective Action | | Mutual Understanding and Mutual Agreement |
| **Segments** | 2 segments, bridges/liaisons and IS concerns. | 2 segments, Opinion leaders and IS concerns. | | | 1 segment (100% of members) |
| **Delivery method** | 20/80 | 20/80 | | | 20/80 |
| **Perceived characteristics** | Relative advantage | Compatibility Complexity Trialability Observability | | | Relative advantage Compatibility Complexity Trialability Observability |

The columns are indexed by each phase of the IDP that takes place when the innovation is targeted to individuals: *knowledge, persuasion, decision, implementation* and *confirmation.* Then, each campaign is associated with the corresponding stage of the IDP; the *knowledge* stage is associated with the ISKC (which represent the *initial conditioning campaign*), the *persuasion* stage is associated with the ISPC (which represent the *behavioural change campaign*) and the *confirmation* stage is associated with the ISCC (which represent the *point of delivery campaign and branding campaign*). Similarly, each type of communication channel is associated with its corresponding campaign at the corresponding stage.

For the ISKC, which takes place in the first stage of the IDP, mass-cosmopolite and interpersonal-communication channels are used, to spread as fast as possible the security message and attempt an initial conditioning towards the acceptance of the security message, through the participation of the *informal communication roles* involved in this stage; namely *bridges* and *liaisons.* When the campaign is launched, the communication process takes place, where the main goal is first to gain a mutual

understanding between the change agent and employees (*opinion leaders* are regarded as followers' representatives) and among employees, and then gain knowledge of the innovation being "*marketed*". For the campaign of this stage, 2 type of segments are identified, one is comprised by those employees identified as bridges and/or liaisons and the second is a group composed of different segments according to their IS concerns. The delivery method is referred to as the 20/80 campaign delivery mode, which represents an alternative method that copes with the acceptance of a changing environment and finally the characteristics under which the security messages shall be designed. The following stages, of the IDP, could be interpreted in the same manner as the first stage was interpreted.

It shall be noted that the decision and implementation stages are not directly influenced with a particular campaign. They are indirectly influenced with the preceding campaigns, to provide employees with the opportunity to cope with the required security behavioural change in a self pace manner and avoid a "compulsory impression" which would significantly affect the employees' attitude towards IS issues.

## 5.9 Summary

An *innovation* refers to any *thing* that is perceived as new by potential adopters; hence, the *diffusion of innovation* refers to the process of making the *innovation* available to all potential adopters within a social system, through pre-established social networks, over a determined period of time. From this definition the main elements of the *diffusion of innovations* theory can be distinguished, those are: the *innovation* which is the object that the change agent seeks to be adopted*;* the *communication channels* which are the mediums over which knowledge or awareness of the innovation is communicated; *time* which segments the audience in terms of the time that they take to adopt an innovation and the *social system* which involves the pre-established social networks and how they are interconnected among each other with the purpose of achieving a common goal*.*

The perceived characteristics of an innovation, such as the *relative advantage, compatibility, complexity, trialability* and *observability,* determine its rate of adoption. Therefore, designing the security messages under these characteristics, could considerably improve the adoption of the desired security behaviour.

The *Diffusion of Innovations* theory, conveys the different components and techniques covered in previous chapters and combine them altogether into an integrative framework to achieve a positive attitude and behavioural change regarding IS issues, which represent the ultimate goals of an ISA initiative. Moreover, by designing the

overall ISAP under the *diffusion of innovations* theory, could aid to overcome ISA's most common problems discussed in Chapter 2.

The author of this dissertation proposes to conduct three different IS campaigns, which would be necessary to achieve and maintain the desired security behavioural change on employees, namely the ISKC, the ISPC and the ISCC. In addition, since the audience is segmented according to the audience's IS concerns, the content of the security messages are designed accordingly and also considering the opinions resulting from the continuous communication between the change agent and those employees that are playing an informal communication role within the organisation, which would ensure an appealing and relevant content for the intended recipients.

Finally, a 20/80 campaign delivery mode is proposed. This delivery mode involves sending in advanced an "informal" security message to those employees identified as bridges, liaisons and opinion leaders and then launching the formal IS campaign, targeting all employees, to reinforce the message. This campaign delivery mode represents an alternative method that copes with the acceptance of IS issues in a changing environment.

# Conclusions

CHAPTER

6

Contents



## 6.1 General Conclusions

*Information Security* is regarded in great part as a problem about people; hence, the need for a more holistic approach in order to understand human behaviour in the *Information Security* field, which requires a multidisciplinary approach. Recent worldwide events are considering this approach and they have conveyed multidisciplinary teamwork, composed by computer security researchers, psychologists, behavioural economists, sociologists and philosophers among others, to address and understand the human side of security. This dissertation represents one of these efforts in approaching *Information Security* from different perspectives. A holistic approach would enable security practitioners to understand the human side of security and as a result be more effective on reaching the pursued security objectives. However, this approach may pose additional challenges, not just in the research field by conveying and reaching consensus among multiple disciplines, but at the organisational level.

According to the results of several international surveys, ISA initiatives have failed to meet their objectives due to informal IS management frameworks; unclear reasons for implementing ISA; a lack of formal and documented objectives; a lack of top management support; failing to use specialised awareness materials; measuring knowledge of employees rather than measuring the effectiveness of the ISAC and a lack of sufficient resources to maintain an ISAP, among the most common causes.

The present dissertation project proposes an ISA framework based on Innovation theory to address these problems, contributing in this form to the active participation and behavioural change of an individual towards the acceptance and compliance of the ISP within an organisation.

The proposed approach addresses ISA from the perspectives of: *management* (chapter 2), *psychology* (chapter 3) and *social networking* (chapter 4), aiming to give a balanced view of a solution to these issues.

The first topic discussed in Chapter 2 of this dissertation, is the management perspective. It was argued, in that chapter, that ISA initiatives are more likely to thrive if they are supported by the top management; that is, in order to achieve the goals pursued by the ISAP, the programme itself needs to be supported by the highest authority within the organisation and all other levels of management, otherwise the overall programme could hardly be maintained and as a consequence fail to achieve its objectives. A proposed solution in this regard, was to instantiate IS as a governance strategy, which required from the organisation, as a first step, to recognise the value of information and then proceed to derive the IS governance from the enterprise governance strategy; thus, any ISA initiative would be supported by a formal IS framework and all levels of management, enabling in this form the ISAP, not just to be launched as an isolated exercise to raise awareness in IS issues, but as an active process embedded in the information security management framework. As a result, the proposed solution would help to address three of the most common ISA's problems: being conducted under an informal IS management framework, the lack of top management support and the lack of sufficient resources to maintain an ISAP.

In order to launch an ISAP and expect a certain extent of success, first, it needs to be supported by a formal IS management framework and then pursue its ultimate objectives. The latter issue was the main topic discussed in Chapter 3, along with the psychological techniques that would enable security practitioners to achieve a positive attitude towards IS issues and build the framework to further achieve the desired behavioural change. The reason for aiming to change the attitude in advance, is to attempt a permanent behavioural change and nurture a security-minded culture; hence, all employees' decisions would be made under an IS perspective. Chapter 3 gathers the main techniques used by social psychology (later discussed in chapter 4), which are mentioned and briefly described to gain a deeper insight on the building blocks of social psychology that essentially applies these techniques to the social context in order to understand individual and group behaviour. Two of the most common ISA's problems are unclear reasons for implementing ISA and consequently a lack of formal and documented objectives. Nonetheless, by designing the overall ISAP to achieve a positive attitude towards IS and achieve the security behaviour described on the ISP, these two problems would be effectively addressed and minimized.

Social psychology applies the fundamental psychological techniques discussed in Chapter 3 to the social context of individuals, as it recognises that a given individual's behaviour is in part the result of the influence received by members of the same social network. Therefore, Chapter 4 analysed the role that social networks play in achieving a behavioural change. Since social networks involve a communication process among the members of a social system, two of the most common models of communication were discussed. Furthermore, a combined model of communication was proposed by the author of this dissertation, with the purpose to gain a deeper insight to understand the individual's complex decision making process that leads individuals to behave in a determined manner. In addition, it was discussed that for every formal communication structure, there is an informal communication structure, with its own informal communication roles. The extent to which these two communication structures differ, serves as an indicator to determine how accurate and appropriate the current organisation's formal communication structure is. The informal communication roles; *bridges, liaisons* and *cosmopolites* play a determinant role in the effectiveness in which the information flows within an organisation. Moreover, there is evidence of the existence of another informal communication role commonly referred to as *opinion leaders.* These individuals are characterised by a degree of cosmopoliteness and their power to exert a certain level of influence on their peers. Therefore, identifying *bridges*, *liaisons* and *opinion leaders* is one of the first objectives of *change agents* before launching an innovation, as they can be employed to initiate an epidemic behaviour for spreading a determined piece of information wide along the organisation, which would also result in saving some of the *change agents'* scarce resources.

By employing the *opinion leader's* influence through the use of viral marketing techniques and stimulating face-to-face communications, the persuasion rate towards a positive attitude regarding IS issues could be effectively improved and as a consequence result in the desired behavioural change necessary to comply with the organisational ISP. In addition, a combined approach for measuring the effectiveness of the ISA initiative needs to be used in order to be able to address one of the ISA's most common problems: measuring knowledge of employees rather than measuring the effectiveness of the ISAC.

The perceived characteristics of an innovation, provided by the *diffusion of innovations* theory, represent an alternative to address one of the ISA's most common problems, which is, failing to use specialised awareness materials. This problem is addressed by designing the types and content of the security messages, considering these characteristics that must be perceived by potential adopters. The degree in which these characteristics are perceived, determine in great part the rate of adoption of the innovation.

*Diffusion of Innovations* theory provides one alternative to convey the different components and techniques covered in previous chapters and combine them altogether into an integrative framework, to achieve the ultimate goals of ISA and overcome its most common problems, by treating the overall ISA initiative as an innovation being marketed within the organisation. The author of this dissertation proposes to conduct three different IS campaigns, which would be necessary to achieve and maintain the desired security behavioural change on employees, namely the ISKC, the ISPC and the ISCC. In addition, the content of the security messages are designed according to each identified audience and to opinions resulting from the continuous communication between the *change agent* and those employees that are playing an informal communication role within the organisation, which would ensure an appealing and relevant content for the intended recipients. Finally, the proposed mode of delivery of each campaign, involves sending in advanced an "informal" security message to those employees identified as *bridges*, *liaisons* and *opinion leaders* to initiate a *word-of-mouth,* regarding a determined IS topic, which would serve as an initial conditioning phase. Then the formal information security campaign would be launched targeting all employees. In this dissertation, this is referred to as the *20/80 campaign delivery mode*, which represents an alternative method that copes with the acceptance of a changing environment.

## 6.2 Main objectives of the dissertation project

The main objectives pursued by this dissertation were covered in the following form:

1. **Base the ISA on the DoI theory**. Covered in Chapter 5 by treating the overall ISAP as an innovation and outlining the three different campaigns.
2. **Apply marketing principles to the ISA framework.** Covered in part in Chapter 3, Chapter 4 and Chapter 5, by considering a conditioning marketing campaign, viral marketing techniques and the marketing mix for ISA respectively.
3. **Address common problems which result of the poor delivery of an ISA program**. The most common problems of ISA and how they were covered are mentioned at the beginning of this chapter.
4. **Identify and exploit SN as an alternative channel to deliver the security message.** Covered in Chapter 4 and Chapter 5, by considering those employees playing an informal communication role within the organisation, to help spread a piece of information and exert influence towards the acceptance of IS issues.
5. **Apply viral marketing techniques to the delivery phase of the ISA program to reinforce and maximize the impact of the security message.** Covered in Chapter 4 and Chapter 5, by proposing to use email as one of the communication channels and during the IS campaigns respectively.

6. **Provide an alternative method to deliver an ISA program under the perspective of the 80/20 principle.** Covered in chapter 4 and Chapter 5, by identifying those employees playing any of those three informal communication roles and designing the IS campaigns, considering these roles as alternative communication channels, respectively.
7. **Provide an alternative method that copes with the acceptance of a changing environment.** Covered in Chapter 4 and Chapter 5, by launching the IS campaigns considering Pareto's law, commonly referred to as the 80/20 principle.

The scope of this thesis is to propose an alternative method to conduct an ISAP, based on the DoI theory. The implementation of an ISA with an Innovation approach is beyond the scope of this thesis and form part of the research agenda for further investigation.

## 6.3 Research Agenda

1. Implement the proposed approach in this dissertation project in an operating organisational environment and validate the extent in which the hypothesised improvements are present, and compare the results against traditional ISA initiatives.

2. One of the components of this dissertation is employing pre-established social networks to initiate an epidemic behaviour in respect to a determined piece of information. In the literature, it is also referred to as *social contagion*. For this purpose several techniques are currently being researched and they may represent an alternative method for achieving a behavioural change on individuals. It has been argued that *social contagion* could also be achieved through the appropriate use of *memes* (pronounced as /mi:m/, similar to gene), a term coined in 1979 by Richard Dawkings in his book "The Selfish Gene", who opened with this term, a new field of research. Hence, the use of *memes,* for spreading a determined idea, could be used to ensure a certain level of a positive attitude towards IS issues.

3. Social networks represent a fertile ground to do further research in how they could be employed in the IS field and particularly when launching ISA initiatives.

4. The proposed communication model resulted from combining the *attitude system,* presented in Chapter 3 of this dissertation and the *Convergence Model of Communication* presented in Chapter 4 of this dissertation, shall be validated with further research when aiming to reach a *common understanding* and *common*

*agreement* that would lead to *collective action* when initiating the process of communication.

5. Conduct further investigation to assess the extent in which the data retrieved from the SNA serves to automatically identify *opinion leaders.*

6. One hypothesis, derived from the discussion of social networks, performed in Chapter 4, leads to speculate about the informal communication patterns unveiled by the SNA. Presumably, the resultant informal communication patterns and the informal communication roles would determine the spread rate of a virus attack. Hence, a proposed counter measure that would need to be validated is that by protecting first the computers held by those employees playing an informal communication role, it would diminish the rate of infection in approximately 80%, according to Pareto's law.

# References

[1] McLean, K., "Information Security Awareness - Selling the Cause," *IFIP/Sec '92: Proceedings of the IFIP TC11, Eigth International Conference on Information Security,* North-Holland Publishing Co, Amsterdam, The Netherlands, The Netherlands, 1992, pp. 179-193.

[2] Purser, S.A., "Improving the ROI of the security management process," *Computers & Security,* Vol. 23, No. 7, 2004, pp. 542-546.

[3] Purser, S., "A Practical Guide to Managing Information Security (Artech House Technology Management Library)," Artech House, Inc, Norwood, MA, USA, 2004,

[4] Stanley, A.K., "The Status of IT Security in Leading European Organisations," *IFIP/Sec '92: Proceedings of the IFIP TC11, Eigth International Conference on Information Security,* North-Holland Publishing Co, Amsterdam, The Netherlands, The Netherlands, 1992, pp. 61-72.

[5] Siponen, M., "Five dimensions of information security awareness," *SIGCAS Comput.Soc.,* Vol. 31, No. 2, 2001, pp. 24-29.

[6] Price Water House Coopers, "2008 Information Security Breaches Survey," Department for Business, Enterprise & Regulatory Reform, Technical Report, United Kingdom, 2008.

[7] Gurbaxani, V., "Diffusion in computing networks: the case of BITNET," *Communications of the ACM,* Vol. 33, No. 12, 1990, pp. 65-75.

[8] Rogers, E., "Diffusion of innovations," New York, 1995,

[9] Galliers, R., and Leidner, D.E., "Strategic Information Management: Challenges and Strategies in Managing Information Systems," Butterworth-Heinemann, Newton, MA, USA, 2002,

[10] Dhillon, G., Tejay, G., and Hong, W., "Identifying Governance Dimensions to Evaluate Information Systems Security in Organizations," *HICSS '07: Proceedings of the 40th Annual Hawaii International Conference on System Sciences,* IEEE Computer Society, Washington, DC, USA, 2007, pp. 157b.

[11] Stanton, J.M., Marshall, P., and and K. Stam, "Behavioral Information Security: Defining the Criterion Space." 2003,

[12] Saltzer, J.H., and Schroeder, M.D., "The protection of information in computer systems," *Proceedings of the IEEE,* Vol. 63, 1975, pp. 1278-1308.

[13] Hansche, S., "Designing a Security Awareness Program: Part I." *Information Systems Security,* Vol. 9, No. 6, 2001, pp. 14.

[14] Leach, J., "Improving user security behaviour," *Computers & Security,* Vol. 22, No. 8, 2003, pp. 685-692.

[15] Nellis, R., "SANS Institute - Creating an IT Security Awareness Program for Senior Management," 2007,

[16] Wagner, G.C., "Information Security's Biggest Enemy," 2006,

[17] Schneier, B., "Beyond Fear: Thinking Sensibly about Security in an Uncertain World," Springer-Verlag New York, Inc, Secaucus, NJ, USA, 2003,

[18] Posthumus, S., and von Solms, R., "A framework for the governance of information security," *Computers & Security,* Vol. 23, No. 8, 2004, pp. 638-646.

[19] von Solms, R., and von Solms, S.H.(., "Information security governance: Due care," *Computers & Security,* Vol. 25, No. 7, 2006, pp. 494-497.

[20] Williams, P., "Information Security Governance," *Information Security Technical Report,* Vol. 6, No. 3, 2001, pp. 60-70.

[21] Klempt, P., Schmidpeter, H., Sowa, S., "Business Oriented Information Security Management - A Layered Approach," *OTM Conferences (2),* 2007, pp. 1835-1852.

[22] von Solms, B., "Corporate Governance and Information Security," *Computers & Security,* Vol. 20, No. 3, 2001, pp. 215-218.

[23] Mossel, E., and Roch, S., "On the submodularity of influence in social networks," *STOC '07: Proceedings of the thirty-ninth annual ACM symposium on Theory of computing,* ACM, New York, NY, USA, 2007, pp. 128-134.

[24] Stolfo, S.J., Hershkop, S., Hu, C., "Behavior-based modeling and its application to Email analysis," *ACM Trans.Inter.Tech.,* Vol. 6, No. 2, 2006, pp. 187-221.

[25] EvenDar, E., and Shapira, A., "A Note on Maximizing the Spread of Influence in Social Networks," *WINE,* 2007, pp. 281-286 ee = {http://d.do.org/10.1007/978-3-540-77105-0_27.

[26] Zhou, D., Manavoglu, E., Li, J., "Probabilistic models for discovering e-communities," *WWW '06: Proceedings of the 15th international conference on World Wide Web,* ACM, New York, NY, USA, 2006, pp. 173-182.

[27] IT Governance Institute, "Information Security Governance: Guidance for Board of Directors and Executive Management," IT Governance Institute, United States of America, 2006.

[28] Deloitte, "2007 Global Security Survey," Deloitte Touche Tohmatsu, United Kingdom, 2008.

[29] Computer Security Institute, "CSI Survey 2007: The 12th Annual Computer Crime and Security Survey," Computer Security Institute, 12th Annual Computer Crime and Security Survey, United States of America, 2008.

[30] Allen, J., "Governing for Enterprise Security," 2007,

[31] Anonymous "CERT's Podcast Series: Security for Business Leaders," Vol. 2008, No. 10/06/2008,

[32] ENISA - European Network and Information Security Agency, "A User's Guide: How to Raise Information Security Awareness," 2007,

[33] Kruger, H.A., and Kearney, W.D., "A prototype for assessing information security awareness," *Computers & Security,* Vol. 25, No. 4, 2006, pp. 289-296.

[34] Anonymous "Oxford English Dictionary Welcome," Vol. 2008, No. 10/06/2008,

[35] Information Security Forum, "Effective Security Awareness: Technical Report," Information Security Forum, United Kingdom, 2002.

[36] PentaSafe Security Technologies, "2002 Security Awareness Index Report: The State of Security Awareness among Organizations Worldwide," PentaSafe Security Technologies, 2002.

[37] Parker, B.D., "Motivating the Workforce to Support Security," 2007,

[38] PriceWaterHouseCoopers, "ENISA - Information security awareness initiatives: Current practice and the measurement of success," PwC, 2007.

[39] Information Security Forum, "The Standard of Good Practice for Information Security," Information Security Forum, United Kingdom, 2007.

[40] Computer Security Institute / Federal Bureau of Investigation, "2006 CSI/FBI Computer Crime and Security Survey," Computer Security Institute, 11th Annual Computer Crime and Security Survey, United States of America, 2007.

[41] Kabay, M.E., "Using Social Psychology to Implement Security Policies," *Computer Security Handbook,* edited by John Wiley & Sons, 2002, pp. 35.

[42] von Solms, B., and Thomson, M.E., "Information security awareness: educating your users effectively," *Information Management & Computer Security,* Vol. 6, No. 4, 1998, pp. 167.

[43] Zimbardo, P.L., Michael, "The psychology of attitude change and social influence," Boston, Mass., 1991,

[44] Puhakainen, P., "A design theory for information security awareness," 2006,

[45] Skinner, B.F. ed., "The Behaviour of Organisms: An Experimental Analysis," Prentice-Hall, 1938,

[46] Sherrington, C., "The integrative action of the nervous system / by Charles S. Sherrington," New Haven, 1911, pp. 1 .

[47] Peter, J.P., and Nord, W.R., "A Clarification and Extension of Operant Conditioning Principles in Marketing," *Journal of Marketing,* Vol. 46, No. 3, 1982, pp. 102-107.

[48] Peel, D., "The significance of behavioural learning theory to the development of effective coaching practice," Vol. 3, No. 1, 2007, pp. 18.

[49] Lindesmith, A.R., and Strauss, A.L., "Comparative Psychology and Social Psychology," *The American Journal of Sociology,* Vol. 58, No. 3, 1952, pp. 272-279.

[50] Schneier, B., "Hall Of Fame - Bruce Schneier - Reconceptualizing Security," Vol. 2008, No. 29/06/2008, 2008,

[51] Skinner, B.F., "Science and human behaviour," Macmillan, New York, 1953, pp. 1 .

[52] Hewstone, Miles Stroebe,Wolfgang Stephenson, "Introduction to social psychology :" Oxford :, 1996,

[53] Zimbardo, P., G., Ebbesen, E., B., and Maslach, C. eds., "Influencing attitudes and changing behaviour - an introduction to method, theory and applications of social control and personal power," Addison-Wesley, 1969,

[54] Pahnila, S., Siponen, M., and Mahmood, A., "Employees' Behavior towards IS Security Policy Compliance," *HICSS '07: Proceedings of the 40th Annual Hawaii International Conference on System Sciences,* IEEE Computer Society, Washington, DC, USA, 2007, pp. 156b.

[55] Stuart, E.W., Shimp, T.A., and Engle, R.W., "Classical Conditioning of Consumer Attitudes: Four Experiments in an Advertising Context," *The Journal of Consumer Research,* Vol. 14, No. 3, 1987, pp. 334-349.

[56] Rogers, E.M., and Kincaid, D.L., "Communication networks: Toward a new paradigm for research," 1981,

[57] Shannon, C.E., "A Mathematical Theory of Communication," *Bell System Technical Journal,* No. 27, 1948, pp. 379-423.

[58] Faris, E., "The Beginnings of Social Psychology," *The American Journal of Sociology,* Vol. 50, No. 6, 1945, pp. 422-428.

[59] Rogers, E.M., and Agarwala-Rogers, R., "Communication in Organisations," Free Press, New York, 1976,

[60] Krebs, V., "Managing Core Competencies of the Corporation," Vol. 2008, 1996,

[61] Blundel, R., and Blundel, R., "Effective organisational communication : perspectives, principles and practices," Financial Times Prentice Hall, Harlow, England; New York, 2004,

[62] Anonymous "Employment and Labour Market Analysis - Employment in Europe," Vol. 2008, No. 11/07/2008,

[63] Carley, K., Lee, J., and Krackhardt, D., "Destabilizing networks," *Connections,* No. 24, 2002, pp. 79-92.

[64] Carley, K., "Information Security: The Human Perspective," *Connections,* 2000, pp. 1-5.

[65] Cai, D., Shao, Z., He, X., "Mining hidden community in heterogeneous social networks," *LinkKDD '05: Proceedings of the 3rd international workshop on Link discovery,* ACM, New York, NY, USA, 2005, pp. 58-65.

[66] Kempe, D., Kleinberg, J., and Tardos, E., "Maximizing the spread of influence through a social network," 2003,

[67] Wu, F., Huberman, B.A., Adamic, L.A., "Information Flow in Social Groups," 2003,

[68] Domingos, P., and Richardson, M., "Mining the network value of customers," *KDD '01: Proceedings of the seventh ACM SIGKDD international conference on Knowledge discovery and data mining,* ACM, New York, NY, USA, 2001, pp. 57-66.

[69] Kempe, D., Kleinberg, J.M., and Tardos, {., "Influential Nodes in a Diffusion Model for Social Networks," *ICALP,* 2005, pp. 1127-1138.

[70] Bird, C., Gourley, A., Devanbu, P.T., "Mining email social networks," *MSR,* 2006, pp. 137-143.

[71] Gladwell, M., "The Tipping Point: How Little Things Can Make a Big Difference," Back Bay Books, 2002,

[72] Škerlavaj, M., and Dimovski, V., "Social Network Approach to Organizational Learning," Vol. 2008, No. 01/05,

[73] Valente, T.W., and Davis, R.L., "Accelerating the Diffusion of Innovations Using Opinion Leaders," *Annals of the American Academy of Political and Social Science,* Vol. 566, No. The Social Diffusion of Ideas and Things, 1999, pp. 55-67.

[74] Feick, L.F., and Price, L.L., "The Market Maven: A Diffuser of Marketplace Information," *Journal of Marketing,* Vol. 51, No. 1, 1987, pp. 83-97.

[75] Cosmas, S.C., and Sheth, J.N., "Identification of Opinion Leaders across Cultures: An Assessment for Use in the Diffusion of Innovations and Ideas," *Journal of International Business Studies,* Vol. 11, No. 1, 1980, pp. 66-73.

[76] Godes, D., Mayzlin, D., Chen, Y., "The Firm's Management of Social Interactions," *Marketing Letters,* Vol. 16, No. 3, 2005, pp. 415-428.

[77] Persky, J., "Retrospectives: Pareto's Law," *The Journal of Economic Perspectives,* Vol. 6, No. 2, 1992, pp. 181-192.

[78] Koch, R., "The 80/20 Principle: The Secret of Achieving More With Less," Nicholas Brealey Publishing, 2007,

[79] Kvam, K., Lie, R., and Bakkelund, D., "Legacy system exorcism by Pareto's principle," *OOPSLA '05: Companion to the 20th annual ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications,* ACM, New York, NY, USA, 2005, pp. 250-256.

[80] Scott, J., "Social network analysis :" London :, 1991,

[81] Tichy, N.M., Tushman, M.L., and Fombrun, C., "Social Network Analysis for Organizations," *The Academy of Management Review,* Vol. 4, No. 4, 1979, pp. 507-519.

[82] Tyler, J.R., Wilkinson, D.M., and Huberman, B.A., "Email as Spectroscopy: Automated Discovery of Community Structure within Organizations," 2003,

[83] Silk, A.J., "Response Set and the Measurement of Self-Designated Opinion Leadership," *The Public Opinion Quarterly,* Vol. 35, No. 3, 1971, pp. 383-397.

[84] Schwartz, M.F., and Wood, D.C.M., "Discovering shared interests using graph analysis," *Communications of the ACM,* Vol. 36, No. 8, 1993, pp. 78-89.

[85] Gloor, P.A., Laubacher, R., Dynes, S.B.C., "Visualization of Communication Patterns in Collaborative Innovation Networks - Analysis of Some W3C Working Groups," *CIKM '03: Proceedings of the twelfth international conference on Information and knowledge management,* ACM, New York, NY, USA, 2003, pp. 56-60.

[86] Culotta, A., Bekkerman, R., and McCallum, A., "Extracting social networks and contact information from email and the web," *In CEAS-1,* 2004,

[87] Carvalho, V.R., Wu, W., and Cohen, W.W., "Discovering Leadership Roles in Email Workgroups," *CEAS 2007,* Mountain View, CA, 2007 bib2html_dl_pdf = http://www.cs.cmu.edu/~vitor/publications/papers/carvalho07ceas.pdf,

[88] Adamic, L., and Adar, E., "How to search a social network," *Social Networks,* Vol. 27, No. 3, 2005, pp. 187-203.

[89] Choudhury, T., and Pentland, A., "Characterizing social networks using the sociometer," *In Proceedings of the North American Association of Computational Social and Organizational Science (NAACSOS,* 2004,

[90] Phelps, J.E., Lewis, R., Mobilio, L., "Viral Marketing or Electronic Word-of-Mouth Advertising: Examining Consumer Responses and Motivations to Pass Along Email," *Journal of Advertising Research,* Vol. 44, No. 04, 2005, pp. 333-348.

[91] Modzelewski, F.M., "Finding a Cure for Viral Marketing Ills," 13th September 2000,

[92] Subramani, M.R., and Rajagopalan, B., "Knowledge-sharing and influence in online social networks via viral marketing," *Communications of the ACM,* Vol. 46, No. 12, 2003, pp. 300-307.

[93] Jurvetson, S., and Draper, T., "Viral Marketing," November 1998,

[94] Leskovec, J., Adamic, L.A., and Huberman, B.A., "The Dynamics of Viral Marketing," 2005,

[95] Richardson, M., and Domingos, P., "Mining knowledge-sharing sites for viral marketing," *KDD '02: Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining,* ACM, New York, NY, USA, 2002, pp. 61-70.

[96] Cyrot, J.L., Urdl, C., and Alves, I.G., "Networks Work: Viral Marketing as a Tool for Launching Innovations," 2003,

[97] Patel, N., "Internet based viral marketing for global competition: The road ahead," *Conference on Global Competition and Competitiveness of Indian Corporate,* Indian Institute of Management Kozhikode, 2007,

[98] Dobele, A., Toleman, D., and Beverland, M., "Controlled infection! Spreading the brand message through viral marketing," *Business Horizons,* Vol. 48, No. 2, 2005, pp. 143-149.

[99] Ludwig, M.A., "The Little Black Book of Computer Viruses," Vol. Volume One: The Basic Technology, American Eagle Publications, Inc., 1996,

[100] Helm, S., "Viral Marketing - Establishing Customer Relationships by 'Word-of-mouse'," *Electronic Markets,* Vol. 10, No. 3, 2000, pp. 158.

[101] Bharathi, S., Kempe, D., and Salek, M., "Competitive Influence Maximization in Social Networks," 2007, pp. 306-311.

[102] Anonymous "cost effective viral marketing and viral seeding," Vol. 2008, No. 20/07/2008,

[103] Denning, , "The social life of innovation," *Communications of the ACM,* Vol. 47, No. 4, 2004, pp. 15.

[104] Denning, , "Innovation as language action," *Communications of the ACM,* Vol. 49, No. 5, 2006, pp. 47.

[105] Drucker, P., "Innovation and entrepreneurship : Practice and Principles," Oxford : Great Britain, 1994,

[106] Brown, L., "Innovation diffusion :" London :, 1981,

[107] Sundbo, J., "The theory of innovation :" Cheltenham :, 1998,

[108] Prescott, M.B., "Diffusion of innovation theory: borrowings, extensions, and modifications from IT researchers," *SIGMIS Database,* Vol. 26, No. 2-3, 1995, pp. 16-19.

[109] Prescott, M.B., and Conger, S.A., "Information technology innovations: a classification by IT locus of impact and research approach," *SIGMIS Database,* Vol. 26, No. 2-3, 1995, pp. 20-41.

[110] Rogers, E.M., and Scott, K.L., "Diffusion of Innovations Model and Outreach from the National Network of Libraries of Medicine to Native American Communities," Vol. 2008, No. 06/07/2008, 2006,

[111] Strang, D., and Soule, S.A., "Diffusion in Organizations and Social Movements: From Hybrid Corn to Poison Pills," *Annual Review of Sociology,* Vol. 24, 1998, pp. 265-290.

[112] Anonymous "Diffusion of Innovations - NCOA," Vol. 2008, No. 06/07/2008,

[113] Fuller, M.A., Hardin, A.M., and Scott, C.L., "Diffusion of virtual innovation," *SIGMIS Database,* Vol. 38, No. 4, 2007, pp. 40-44.

[114] Valente, T.W., "Social network thresholds in the diffusion of innovations," *Social Networks,* Vol. 18, No. 1, 1996, pp. 69-89.

# Appendix A - Summary of Generalizations

## A.I Innovation's Perceived Characteristics

"Generalization 6-1: *The relative advantage of an innovation, as perceived by the members of a social system, its positively related to its rate of adoption"* [8] (p. 233).

"Generalization 6-2: *The compatibility of an innovation, as perceived by members of a social system, is positively related to its rate of adoption "* [8] (p. 249).

"Generalization 6-3: *The complexity of an innovation, as perceived by members of a social system, is negatively related to its rate of adoption"* [8] (p. 257).

"Generalization 6-4: The trialability of an innovation, as perceived by members of a social system, is positively related to its rate of adoption" [8] (p. 258).

"Generalization 6-5: The observability of an innovation, as perceived by members of a social system, is positively related to its rate of adoption" [8] (p. 258).

## A.II Communication Channels

"Generalization 5-14: *Cosmopolite channels are relatively more important at the knowledge stage, and localite channels are relatively more important at the persuasion stage in the innovation-decision process*" [8] (p. 207).

"Generalization 5-13: *Mass media channels are relatively more important at the knowledge stage, and interpersonal channels are relatively more important at the persuasion stage.*" [8] (p. 205).

## A.III Time

"Generalization 5.17: *The rate of awareness knowledge for an innovation is more rapid than its rate of adoption*" [8] (p. 214).

## A.IV Innovation in Organisations

"Generalization 10-1: *Lager organizations are more innovative.*" [8] (p. 409).

"Generalization 10-3: *The presence of an innovation champion contributes to the success of an innovation in an organization.*" [8] (p. 414).

"Generalization 10-4: *A performance gap can trigger the innovation process.*" [8] (p. 422).

"Generalization 10-5: *Both the innovation and the organization usually change in the innovation process in an organization.*" [8] (p. 425).

## A.V Distribution of Adopter's Categories

"Generalization 7-1: *Adopter distributions follow a bell-shaped curve over time and approach normality*" [8] (p. 275).

## A.VI Earlier Adopters versus Later Adopters

"Generalization 5-15: *Mass media channels are relatively more important than interpersonal channels for earlier adopters than for later adopters*" [8] (p. 211).

"Generalization 5-16: *Cosmopolite channels are relatively more important than localite channels for earlier adopters than for later adopters*" [8] (p. 213).

"Generalization 5-11: *Later adopters are more likely to discontinue innovations than are earlier adopters*" [8] (p. 191).

"Generalization 5-18: *Earlier adopters have a shorter innovation-decision period than do later adopters*" [8] (p. 249).

"Generalization 7-2: *Earlier adopters are no different from later adopters in age*" [8] (p. 288).

"Generalization 7-3: *Earlier adopters have more years of formal education than do later adopters.*" [8] (p. 288).

"Generalization 7-4: *Earlier adopters are more likely to be literate than are later adopters*" [8] (p. 288).

"Generalization 7-8: *Earlier adopters have greater empathy than do later adopters.*" [8] (p. 289).

"Generalization 7-9: *Earlier adopters may be less dogmatic than are laters adopters*" [8] (p. 249).

"Generalization 7-10: *Earlier adopters have a greater ability to deal with abstractions than do later adopters*" [8] (p. 289).

"Generalization 7-11: *Earlier adopters have greater rationality than do later adopters.*" [8] (p. 249).

"Generalization 7-12: *Earlier adopters have more intelligence than do later adopters.*" [8] (p. 289).

"Generalization 7-13: *Earlier adopters have a more favourable attitude toward change than do later adopters*" [8] (p. 290).

"Generalization 7-14: *Earlier adopters are better able to cope with uncertainty and risk than are later adopters.*" [8] (p. 290).

"Generalization 7-15: *Earlier adopters have a more favourable attitude toward science than do later adopters.*" [8] (p. 290).

"Generalization 7-16: *Earlier adopters are less fatalistic than are later adopters.*" [8] (p. 290).

"Generalization 7-17: *Earlier adopters have higher aspirations (for formal education, higher status, occupations, and so on) than do later adopters.*" [8] (p. 290).

"Generalization 7-18: *Earlier adopters have more social participation than do later adopters*" [8] (p. 290).

"Generalization 7-19: *Earlier adopters are more highly interconnected through interpersonal networks in their social system than are later adopters.*" [8] (p. 290).

"Generalization 7-20: *Earlier adopters are more cosmopolite than are later adopters.*" [8] (p. 290).

"Generalization 7-21: *Earlier adopters have more contact with change agents than do later adopters.*" [8] (p. 291).

"Generalization 7-22: *Earlier adopters have greater exposure to mass media communication channels than do later adopters.*" [8] (p. 291).

"Generalization 7-23: *Earlier adopters have greater exposure to interpersonal communication channels than do later adopters.*" [8] (p. 249).

"Generalization 7-24: *Earlier adopters seek information about innovations more actively than do later adopters.*" [8] (p. 291).

"Generalization 7-25: *Earlier adopters have greater knowledge of innovations than do later adopters.*" [8] (p. 291).

"Generalization 7-26: *Earlier adopters have a higher degree of opinion leadership than do later adopters*" [8] (p. 291).

## A.VII Opinion leaders

"Generalization 8-3: *Opinion leaders have greater exposure to mass media than their followers.*" [8] (p. 316).

"Generalization 8-4: *Opinion leaders are more cosmopolite than their followers.*" [8] (p. 317).

"Generalization 8-5: *Opinion leaders have greater contact with change agents than their followers.*" [8] (p. 317).

"Generalization 8-6: *Opinion leaders have greater social participation than their followers.*" [8] (p. 317).

"Generalization 8-7: *Opinion leaders have higher socioeconomic status than their followers.*" [8] (p. 318).

"Generalization 8-8: *Opinion leaders are more innovative than their followers.*" [8] (p. 318).

"Generalization 8-9: *When a social system's norms favour change, opinion leaders are more innovative, but when the system's norms do not favour change, opinion leaders are not especially innovative.*" [8] (p. 318).

## A.VIII Social System

"Generalization 8-1: *Interpersonal diffusion networks are mostly homophilous*" [8] (p. 307).

"Generalization 8-2: *When interpersonal diffusion networks are heterophilous, followers seek opinion leaders of higher socioeconomic status, with more formal education, with a greater degree of mass media exposure, who are more cosmopolite, have greater contact with change agents, and are more innovative.*" [8] (p. 308).

"Generalization 8-12: *Individuals tend to be linked to others who are close to them in physical distance and who are relatively homophilous in social characteristics.*" [8] (p. 341).

"Generalization 8-13: *An individual is more likely to adopt an innovation if more of the other individuals in his or her personal network have adopted previously.*" [8] (p. 359).

# Appendix B – Identifying Opinion Leaders

One of the key roles of senior managers and service improvement project leaders is to identify and work with local opinion leaders to accelerate the spread of innovation and good practice throughout local, regional and national systems.

The concept of the opinion leader in the role of spreading good practice is that this person is usually among the first to know about new ideas and that their peers look to them for guidance about whether the innovations should be adopted or not. They have an important role influencing the behavior of others in the system.

It is worth noting Rogers' innovativeness-needs paradox; namely, the person who most needs the innovation is often the last person to adopt its use. Early adopters often implement new practices even though they are not in the greatest need for the change. Using opinion leaders and early adopters to implement new practices may reflect a 'line of least resistance' approach to change and may not make sufficient impact on overall improvement objectives.

Rogers suggests the target 'audience' involved in adopting a new practice can be segmented into groups according to the time they take to change their behavior; from innovator, early adopter, and early majority through to late majority and laggard. It is essential to note that these terms are descriptors for a specific innovation and are not 'personality' types.

Individuals can be both innovators and laggards, depending on the innovation or good practice. Thus, to identify early adopters and opinion leaders the specific area of practice needs to be taken into account. It is important not to make the assumption that because the person was an opinion leader for one innovation that they might also an opinion leader be for another, entirely different innovation.

**Characteristics of Opinion Leaders**

- Higher social status
- More years of formal education
- Greater literacy
- Higher aspirations and ambition
- Tend to belong to larger groups
- Demonstrate empathy, rationality
- Exposed to and uses variety of media
- Greater knowledge of innovation

(Reference: Rogers, E (1995) The Diffusion of Innovations (4th Ed), The Free Press, USA)

## Ways to identify opinion leaders

**(1) Ask Questions**

Project leaders can continually ask questions to discover opinion leaders. Some useful questions are:

• *"Who would you turn to for advice on this topic?"*

• *"You are always learning new ways of doing things. What was the last time you can remember doing something different? Where / from whom did you get the idea?"*

• *"Before you implement something new, is there a specific person with whom you check it out?"*

**(2) Do an Analysis**

One method of identifying opinion leaders is to ask the questions above, and specifically relate it to the goals of the intended change, and then map the results on a matrix. Put the initials of each person both at the top and along the side of the matrix. Then mark in each square who most frequently listens to the opinion of whom.

When you total up the results the key opinion leaders will be those with the higher scores I.e. the most people would refer to them for advice and their opinion on a subject.

**What can go wrong?**

I thought someone who had lots of local connections and contacts would be an opinion leader but this doesn't seem to have worked out that way? Individuals who have dense personal networks, lots of tightly woven and inter-related contacts often don't have the contact with external people that would help them spread the word of an innovation or hear about new ideas. Look for individuals who have good local networks, but also lots of external contacts and interests.

*We did an analysis of opinion leaders but the people in the group disagree with the results.*
This is very personal information and some people may not like to have it shared. So check before you do the analysis. Your assessment may highlight someone as an opinion leader that no-one would have expected. Alternatively it might indicate that someone who thought they were an opinion leader aren't really seen by their colleagues as one. All of this would need careful facilitation. It's important to think through what you intend to do with the information before you start an analysis.

*Just using the term 'opinion leader' seems to cause resistance.*
This term is value laden and turns some people off in a negative way. It is sometimes useful to use the term "key influencer" or "role model".

*There isn't an opinion leader in the group in which I work.*
There will be one somewhere. Look outside the immediate group. To whom are the members of the groups talking?

# Appendix C - Glossary of Terms

**Adopter categories** refer to the classifications of the members of a social system on the basis of their innovativeness.

**Adoption** is a decision to make full use of an innovation as the best course of action available.

**Average clique connectedness** is the degree to which the average member of a clique is linked individual in his/her clique.

**Average system connectedness** is the degree to which the average member of a system is linked to other individuals in the system.

**Awareness-knowledge** refers to the information that an innovation exists.

**Bridge** is an individual who links two or more cliques in a system from his/her position as a member of one of the cliques.

**Champion** is a charismatic individual who throws his or her weight behind an innovation, thus overcoming indifference or resistance that the new idea may provoke in an organization.

**Change agent** is an individual who influences clients' innovation-decisions in a direction deemed desirable by a change agency.

**Clique connectedness** is the degree to which the cliques in a system are linked to each other.

**Clique integration** is the degree to which the cliques linked to a focal clique are linked to each other.

**Clique** is a subsystem whose elements interact with each other relatively more frequently than with other members of the communication system.

**Clique openness** is the degree to which the members of a clique are linked to other external to the clique.

**Collective innovation-decision** is the choice to adopt or reject an innovation that is made by consensus of the members of a system.

**Communication campaign** is a campaign to generate specific effects, on the part of a relatively large number of individuals, within a specified period of time, and through organized set o communication activities.

**Communication** is a process in which participants create and share information with one another in order to reach a mutual understanding.

**Communication network analysis** is a method of research for identifying the communication structure in a system, in which relational data about communication flows are analyzed by using some type of interpersonal relationship as the unit of analysis.

**Communication network** consists of interconnected individuals who are linked by patterned flows of information.

**Communication structure** is the arrangement of the differentiated elements that can be recognized in the patterned communication flows in a system.

**Compatibility** is the degree to which an innovation is perceived as being consistent with the existing values, past experiences, and needs of potential adopters.

**Complexity** is the degree to which an innovation is perceived as difficult to understand and use.

**Confirmation** occurs when an individual seeks reinforcement of an innovation-decision that has already been made but mat reverse this decision if exposed to conflicting messages about the innovation.

**Connectedness** is the degree to which a focal unit is linked to other units.

**Convergence** is the tendency for two or more individuals to move toward one point of for one individual to move toward another, or for two individuals to come together and unite in a common interest or focus.

**Cosmopoliteness** is the degree to which an individual is oriented outside of a social system.

**Critical mass** is the point at which enough individuals in a system have adopted an innovation such that the innovation's further rate of adoption becomes self-sustaining.

**Decision** occurs when an individual engages in activities that lead to a choice to adopt or reject an innovation.

**Diffusion** is the process in which an innovation is communicated through certain channels over time among the members of a social system.

**Divergence** is the tendency for two or more individuals to move away or apart.

**Diversity** is the degree to which the units linked to a focal unit are heterogeneous in some variable.

**Dyad** is composed of two individuals connected by a communication link.

**Heterophily** is the degree to which pairs of individuals who interact are different in certain attributes.

**Homophily** is the degree to which two or more individual who interact are similar in certain attributes.

**Individual connectedness** is the degree to which a focal individual is linked to other individuals in a system.

**Individual diversity** is the degree to which the members of an individual's personal communication network are heterogeneous in some variable.

**Individual integration** is the degree to which the members of an individual's personal communication network are linked to each other.

**Information** a difference in matter-energy that affects uncertainty in a situation where a choice among various alternatives exists.

**Innovation** is an idea, practice, or object that is perceived as new by an individual or other unit of adoption.

**Innovation-decision process** refer to the process through which an individual (or other decision-making unit) passes from first knowledge of an innovation to forming an attitude toward the innovations, to a decision to adopt or reject, to implementation and use of the new idea, and to confirmation of this decision.

**Innovativeness** is the degree to which an individual or other unit of adoption is relatively earlier in adopting new ideas than the other members of a system.

**Interlocking personal network** is one in which an individual interacts with a set of dyadic partners who interact whit each other.

**Knowledge** occurs when an individual learns of the innovation's existence and gains some understanding of how it functions.

**Liaison** is an individual who links two or more cliques in a system, but who is not a member of any clique.

**Observability** is the degree to which the results of an innovation are visible to others.

**Openness** is the degree to which a unit exchanges information with its environment.

**Opinion leadership** is the degree to which an individual is able to influence other individual's attitudes or overt behaviour informally in a desired way with relative frequency.

**Optional innovation-decision** refers to the choices to adopt or reject an innovation that is made by an individual independent of the decision y other members of the system.

**Personal communication network** is those interconnected individuals who are linked by patterned communication flows to a focal individual.

**Persuasion** takes place when an individual forms a favourable or unfavourable attitude toward an innovation.

**Rate of adoption** refer to the relative speed with which an innovation is adopted by members o a social system.

**Rejection** is the decision of not to adopt an innovation.

**Relative advantage** is the degree to which an innovation is perceived as better than the idea it supersedes.

**Social system** is a set of interrelated units involved in joint problem solving to accomplish a common goal.

**Sociogram** is a graphic means for displaying the patterns of communication or social choice in a system.

**Sociometry** is a means of obtaining quantitative data about communication patterns among the individuals in a system, by asking each respondent to whom he/she is linked.

**Structure** is the arrangement of the components and subsystems within a system.

**System effects** are the influences of the structure and/or composition of a system on the behaviour of the members of the system.

**System** is a set of interrelates parts coordinated to accomplish a set of goals.

**System openness** is the degree to which the members of a system are linked to others external to the system.

**Targeting** refer the process of customizing the design and delivery of a communication program on the basis of the characteristics of an intended audience segment.

**Trialability** is the degree to which an innovation may be experimented with on a limited basis.

**Uncertainty** is the degree to which a number of alternatives are perceived with respect to the occurrence of an event and the relative probabilities of these alternatives.

**Unobtrusive method** is a measure that directly removes the observer form the events being studied.