Chapter VII
Social Aspects of Information Security: An International Perspective

Paul Drake
Centre for Systems Studies Business School, University of Hull, UK

Steve Clarke
Centre for Systems Studies Business School, University of Hull, UK

ABSTRACT

This chapter looks at information security as a primarily technological domain, and asks what could be added to our understanding if both technology and human activity were seen to be of equal importance. The aim is therefore, to ground the domain both theoretically and practically from a technological and social standpoint. The solution to this dilemma is seen to be located in social theory, various aspects of which deal with both human and technical issues, but do so from the perspective of those involved in the system of concern. The chapter concludes by offering a model for evaluating information security from a social theoretical perspective, and guidelines for implementing the findings.

INTRODUCTION

Within this chapter, we first look at the dominant approach to information security (ISec), establishing it as a domain in which technological factors predominate, and insufficient consideration is given to human issues. Building on this foundation, a picture is presented of the complexity of ISec, from which it is argued that the practice *ought* to pay more attention to the ways in which differing perceptions might give rise to a different ISec practice.

The tensions in ISec are presented as occurring between theory and practice on the one hand, and social and technological on the other. From this position, the question posed becomes: "How can we build an ISec practice which is grounded theoretically, and which addresses both technological and social issues?"

The source of a solution to this dilemma may be found in social theory. Various aspects of social theory deal with both human and technical issues, but do so from the perspective of those involved in the system of concern. Our approach, therefore, has been to build models to evaluate and implement ISec, both based explicitly on theories of social action.

BACKGROUND TO INFORMATION SECURITY

From a Technological to a Human-Centred Perspective

Currently, the practice of information security (ISec) aims primarily to protect information and to ensure it is available to those authorised to access it. This approach is emphasized by the well established definition of information security to be found in the U.S. Department of Defense "Orange Book" (DOD, 1985):

In general, secure systems will control, through use of specific security features, access to information such that only properly authorised individuals, or processes operating on their behalf, will have access to read, write, create, or delete information.

Within the United Kingdom, a similar perspective on ISec can be seen in UK government publications, for example the Communications-Electronics Security Group[1] (CESG 1994), The British Standard for Information Security Management (ISO 2000; BSI 2003), and in the documentation and practice within a large number of organisations who have adopted information security practices. In all of these cases, the primary concern is to protect the *confidentiality* and *integrity* of *information,* and to restrict its *availability*: the so called "CIA" of ISec.

So, this is ISec practice—but where has this practice come from? A brief look at the development history of the British Standard, outlined, gives an indication of this in the UK.

The sources of the Standard (BS7799) are traceable to the 1990s, when a group of security professionals formed a committee under the auspices of the British Standards Institute, and with the support of the UK government's Department of Trade and Industry, to document current "best information security practice" based on the current experience, knowledge, and practice of those contributing. The product of this effort was the Code of Practice for Information Security Management (BSI, 1993). The committee continued to work towards maintaining and improving the code of practice, and today it has developed into the British Standards for Information Security (ISO, 2000; BSI, 2002). The same committee continues to maintain and revise this Standard. During the various iterations, Part 1 of the Standard has been accepted by the International Organization for Standardization, commonly known as ISO, as an international standard, ISO-17799.

Part 1 of the Standard (ISO, 2000) is a code of practice which contains around 130 controls to be considered and implemented. Part 2 (BSI, 2003) contains the same number of controls but *specifies* their use and is therefore auditable. Both parts of the Standard provide guidance for the development and implementation of a risk-based management system that allows the continued assessment and management of risks. This is delivered through an information security management system (ISMS) that incorporates a cycle which, in essence, compiles a list of the 130 controls and determines whether the absence or inadequate implementation of these controls is likely to harm the organisation and if so, by how much. Proper management of risks and correct implementation of applicable controls can attract certification to the Standard and the right to use the