IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB9016

Chapter XIV

On the Role of Human Mortality in Information System Security: From the Problems of Descriptivism to Non-Descriptive Foundations

Mikko T. Siponen
University of Oulu, Finland

ABSTRACT

The question of whether ethical theories appealing to human morality can serve as a means of protection against information system security breaches has been recognized by several authors. The existing views concerning the role of ethics in information systems security can be divided into two categories. These are (1) expressions about the use of human morality and (2) arguments claiming that the use of ethics is useless or, at best, extremely

restricted. However, the former views are general statements lacking concrete guidance and the latter viewpoint is based on cultural relativism, and can be thus classified as descriptivism. This paper claims that the use of ethical theories and human morality is useful for security, particularly given that Hare's Overriding thesis has validity — though it has its limitations, too. This paper further argues that descriptivism (including the doctrine of cultural relativism) leads to several problems, contradictions and causes detrimental effects to our well-being (and security). Therefore, an alternative approach to using ethics in minimizing security breaches that is based on non-descriptive theories is proposed. The use of non-descriptivism will be demonstrated using Rawls' concept of the "veil of ignorance." The limitations of non-descriptivism, and appealing to human morality in a general sense, will also be discussed. Finally, suggestions for future research directions are outlined.

INTRODUCTION

The relevance of security solutions and procedures depends on the motivation of the users to comply with the security solutions/procedures provided. Many studies indicate that users fail to comply with information security policies and guidelines (e.g., Goodhue & Straub, 1989; Parker, 1998; Perry, 1985). It is widely argued (e.g., Loch & Carr, 1991; Anderson, 1993; Parker, 1998; Vardi & Wiener, 1996; Neumann, 1999) that a remarkable portion of security breaches are carried out by organizations' own employees. Several proposals have been made to tackle this human problem; the solutions range from (1) increasing the users' motivation (e.g., McLean, 1992; Perry, 1985; Siponen, 2000a; Thomson & von Solms, 1998), (2) using ethics (e.g. , Kowalski, 1990; Leiwo & Heikkuri, 1998a, 1998b), (3) organizational/professional codes of ethics (e.g., Harrington, 1996; Straub & Widom, 1984; Parker, 1998), to (4) using different deterrents (e.g., Straub, 1990). With respect to the second issue — Can human morality function as a means of ensuring information security? The existing works can be divided into two categories. The first category covers expressions concerning the use of human morality including Kowalski (1990), Baskerville (1995), Siponen (2000) and Dhillon & Backhouse (2000):

- "*Security administrators are realizing that ethics can function as the common language for all different groups within the computer community*" (Kowalski, 1990).
- "*Proper user conduct can effectively prevent [security] violations*" (Baskerville, 1995, p. 246).