Ethics in the Security of Organizational Information Systems

Sushma Mishra
Virginia Commonwealth University, USA

Amita Goyal Chin
Virginia Commonwealth University, USA

INTRODUCTION

Organizational security initiatives by corporations have been voted number one for IT project priorities for the year 2006. The increasing concern for the security of information systems is further intensified with the plethora of governmental regulations emphasizing security, both of information systems and of soft data. The Health Insurance Portability and Accountability Act (HIPPA), the Sarbanes Oxley (SOX) Act, and the U.S. Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (U.S. PATRIOT) Act make it mandatory to ensure the security of electronic records and the integrity of data. Security of informational assets is a huge responsibility for organizations that are IT intensive. A strong IT infrastructure in organizations brings convenient and fast access to data across the globe. With such access comes an added burden in the form of protection and safeguarding of crucial data. Since soft data is more vulnerable to malicious attacks from outsiders than physical hard copies of data, which may be securely locked in an office, it calls for organized and efficient information assurance practices in the form of detection and prevention of breaches in networks, data usage procedures, and data storage procedures. Various sophisticated technical solutions to these problems such as firewalls, access control models, and cryptography technology are available. However, these technical efforts to ensure the integrity of information are not sufficient to achieve a secure information system in an organization. The organizational as well as behavioral issues of security endeavors need to be explicitly planned for by management. After all, it is the human aspect of security that is the weakest link in an integrated security approach to information systems.

BACKGROUND

An information system is a system that emerges from the interaction of information technology and an organization (Lee, 2004). Thus an information system incorporates not just the information technology component, but also the human aspects of implementing and monitoring the technology. The organizational context in which IT has been implemented, the culture prevalent in the organization, the norms, the rules, and the practices are as equally important as the technical sufficiency of the security framework in an organization. The security solutions are implemented by the employees. The human link has been found to be the weakest in the security solution (Bottom, 2000; Gonzalez & Sawicka, 2002; Vroom, Cheryl, & Von Solms, 2004). Research has shown that the threat to security from the insiders of an organization (i.e., the employees) exceeds that from outsiders (i.e., hackers) (Schultz, 2002). There are various reasons suggested for this in the research literature: lack of internal controls and lack of normative pressure (Dhillon, 2001), ignorance or disregard for security policies (Bottom, 2000), and no consideration being given to human factors in the system development methodology (Hitchings, 1995). For comprehensive security management, information systems security should be ensured at three levels—formal, informal, and technical (Dhillon, 2007). The informal level is the common practices, norms, and culture of the organization. To ensure security at this level, the professional ethics of the organization and the personal ethics of the employees are of paramount importance. It is this element of the behavioral aspect of security that we will emphasize in this article.

MAIN FOCUS OF THE ARTICLE

Ethics is the study of morality, representing the basic societal values and the code of conduct and actions that guide the behavior of individuals or groups. Ethics shapes the individual belief system that guides an individual and tells him or her whether an action is good or bad. Ethics are a function of many factors such as cultural, geographical, economical, and philosophical motivations. Since the subjectivity part is inherent in the concept of ethics, there are no universal agreements about the definition or domain of ethics. Research in ethics combines inputs from many disciplines such as sociology, economics, psychology, anthropology, and history. Ethics help us in making moral judgments and influence our decisions in issues regarding "what is good" and "what is bad." In our context, ethics helps us decide how to make judgments regarding security and protection of informational assets. Individuals are influenced by the environment and behave accordingly, but one's deep-seated values do not change easily.

While some researchers (e.g., Freeman & Peace, 2004) have begun exploring the concept of ethics in information systems, we are largely still in a nascent stage of development. Thus there is no clear map of the "IT ethics domain that identifies major land masses, compass directions, levels of analysis, or recommended pathways" (Laudon, 1995, p. 33) to be followed. Based on the existing ethics literature, Laudon (1995) divided the moral space covered by ethical concepts into the following dimensions:

- **Phenomenology vs. Positivism:** This particular dimension provides guidance in an ethical dilemma—that is, it seeks to answer the question "What should I do?" For phenomenologists, the good is given in a situation; it is derived from the logic and the language of the situation. For positivists, the real world has to be observed and the ethical principles have to be derived from the situation.
- **Rules vs. Consequences:** Rules-based ethicists, or people belonging to the deontological school of thought, believe that there are certain rights and certain wrongs, and that actions that are correct and are right should be taken. Such actions are universal in nature and do not depend on specific context. They tend to follow certain rules in all situations. According to ethicists, who believe in consequential ethics, right or wrong is based on the context of the decision and on the consequences of the action taken. They believe that the end justifies the means—that is, if the results are good, then the actions leading to that result are also good.
- **Individuals vs. Collectivities (micro vs. macro levels):** The locus of moral authority is another criterion on which ethicists differ in opinion. While they agree that how an individual makes a decision is the subject of ethics research, they differ on who has the authority to make the decisions. Some argue that individuals decide for themselves what is right and what is wrong. Others argue that moral authority must be located in larger collectivities, for example the organization or the society. Even government could have a large authority to shape such decisions. There are problems with both lines of thinking. The individuals set their own rules and their own standards of morality, and do not consider the context of society to which they belong, whereas believers in collectivities introduce a moral relativism concept that defines all its decisions based on the democratic principle of majority. They believe in following the mob.

In order to understand the process of assessing the importance of ethics in information systems research (Mason, 1986), especially in the security domain, we must first consider the following major issues:

- **Privacy:** The personal information about individuals must be protected and their privacy respected
- **Accuracy:** Someone should be accountable to ensure that information is accurate
- **Property:** Information ownership should be clear. The question of how to decide who can access what information needs to be answered
- **Accessibility:** It must be clear what kind of information an organization is allowed to obtain and under what conditions

In an assessment of the values of managers regarding information systems security, Dhillon and Torkzadeh (2006) found that developing and sustaining an ethical environment is one of the basic objectives of creating a secure information system in an organization. An