Chapter 4
International Ethical Attitudes and Behaviors: Implications for Organizational Information Security Policy

Dave Yates
University of Maryland, USA

Albert L. Harris
Appalachian State University, USA

ABSTRACT

Organizational information security policy must incorporate organizational, societal, and individual level factors. For organizations that operate across national borders, cultural differences in these factors, particularly the ethical attitudes and behaviors of individuals, will impact the effectiveness of these policies. This research looks at the differences in attitudes and behaviors that exist among five different countries and the implications of similarities and differences in these attitudes for organizations formulating information security policies. Building on existing ethical frameworks, we developed a set of ethics scenarios concerning data access, data manipulation, software use, programming abuse, and hardware use. Using survey results from 599 students in five countries, results show that cultural factors are indicative of the differences we expected, but that the similarities and differences among cultures that should be taken into account are complex. We conclude with implications for how organizational policy makers should account for these effects with some specific examples based on our results.

INTRODUCTION

Increasing numbers of organizations are operating multi-nationally, if not globally. Some of these organizations employ workers in locations across the globe; others serve global markets. In either case, these organizations face unique challenges implementing information policy – their stated goals and procedures for managing and securing internal and external information and the systems for storing, transferring, and processing that information. While information security policy deals with every aspect of protecting information, one of the most vulnerable areas of information security is the unethical decisions made by agents of an

DOI: 10.4018/978-1-61692-245-0.ch004

organization who were trusted to act otherwise, such as employees and sometimes customers. In information security, this is known as the insider threat. Sometimes information security challenges stem from conflicting technological standards, but more often are due to a lack of awareness of different ethical and social norms from one location to another (Lu, Rose, & Blodgett, 1999; Volkema, 2004). For multi-national companies, cultural differences could be a relevant factor when considering insider threats and information security policy.

The importance of both cultural differences and ethical attitudes for information security was recently recognized by world organizations as being highly influential for maintaining information security. Recently, the United Nations Education, Science, and Cultural Organization (UNESCO) has taken as a priority the discussion of what it calls "info-ethics" and the challenges of understanding ethical technology use in different regions of the world, such as Africa, Latin America, and Europe (http://www.unesco.org/webworld). A prominent example is the copying of software outside of licensing agreements, which in some cultures is not seen as unethical, but in others is deemed unethical and illegal. Another example shows that married couples and members of collectivist communities such as Australian aboriginal groups routinely share confidential passwords and personal identification numbers (PINs), despite bank warnings that such information must be kept private (Singh, Cabraal, Demosthenous, Astbrink, & Furlong, 2007). A third example is the Maori people of New Zealand. The Maori have the concept of kaitiakitanga—guardianship and care of data about Maori. Kaitiakitanga introduces the concept of tiaki. Tiaki means to look after and guard, wherein, the emphasis is placed on collective ownership in order to serve purposes of improvement and benefit for all first and foremost. For the Maori, rights of data ownership and intellectual property are subsets, not supersets, of the broader ethic of collective ownership (Kamira, 2007). Cultural differences do not just span countries. Take, for example, the conflicting records management practices in the United States with so-called "sunshine laws". Florida and Ohio (Sitton, 2006) mandate open access to records that contain personally identifying information, compared to states such as Texas and Iowa that more tightly control government records disclosure.

Laws come from ethics, not the other way around. Cultural norms and laws of a country co-evolve; they influence each other, and both are intimately reflective of the relevant ethics. It is our belief however, that while organizations must take local laws into account when formulating and implementing information security policies, they do not always take into account local cultural differences. This is problematic. Understanding laws is only part of the picture; understanding cultural differences is a critical piece of the puzzle. Because the internet operates as one, large and globally interconnected system, the information security practices in one country have implications worldwide. When cultural norms conflict, or are misunderstood, it is difficult to guarantee that information security policies generated in the context of a given cultural norm (such as in the United States) will be effective elsewhere.

Organizations crossing boundaries must not only be sensitive to local laws, but must institute policies that will allow them to successfully interface with local populations. Often laws alone cannot help organizations shape these policies and identify differences, but a better understanding of the needs and expectations of users (internal, such as employees, and external, such as customers) might provide needed insight (Mitrakas, 2006; Sitton, 2006). The significance of this research then is based on the premise that organizations will be able to better formulate information security policies given enhanced understanding of differences in cultural norms specific to information security.

In most organizations - commercial, private, or public - information security policy is a necessity.