IT Security Culture Transition Process

Leanne Ngo
Deakin University, Australia

INTRODUCTION

The information superhighway is here and stretching further than the eye can see. Our working environment is becoming ever more hectic and demanding, computers and information technology are more pervasive, and limitations are perishing. The once solo dimension of information and technology is now multifaceted and convoluted in disposition (Ngo & Zhou, 2005). As a result, organizations need to be more vigilant than ever in actively responding to new information and technology security challenges and to ensure survivability in this new age.

Over the years many information technology (IT) security approaches—technical, managerial, and inst itutionalization—have surfaced. Also safeguards and countermeasures have been developed, practiced, and learned within organizations. Despite all these attempts to reduce and/or eradicate IT security threats and vulnerabilities, the issue still continues to be problematic for organizations. Solutions are needed that will reach the core of the problem—safeguarding and controlling *humans*—the human aspect of IT security.

Humans are a pervasive element in our businesses and critical infrastructures, the element which interacts with systems, services, information, and information technology. Furthermore, humans are responsible for the design, development, operation, administration, and maintenance of our information systems and resources. Therefore the ultimate success of any effort to secure information resources depends largely on the behavior and attitudes of the humans involved. While technological solutions can solve some information security problems, even the finest technology cannot succeed without the cooperation of humans. IT security is not just a technical problem that can be solved with technical solutions, but also a human problem that requires human solutions.

This article reviews the current literature on the human aspect of IT security within an organizational context. Human-related IT security concerns are summarized, and current human-related IT security solutions are examined and discussed. In this article, we consider IT security culture as a plausible solution to improving IT security-related behavior and attitudes of humans. We present our IT security culture transition model that is currently being trialed in three organizations to assist with increasing IT security awareness and hence improve the IT security culture of the individuals (managers and employees) and overall organization. Further, we discuss the potential individual psychological experiences of managers and employees during the transitional change towards IT security culture change.

BACKGROUND

Human-related IT security problems relate to how people associate themselves and interact with security. Here, human-related IT security problems are presented as well as current human-related solutions regarding the controlling and management of the human-side to IT security.

Human-Related IT Security Problems

Human factors impeding IT security within an organizational context with examples include:

1. **How humans perceive risk people:** People do not know to analyze risk properly and therefore this leads to improper actions.
2. **Ability to make security decisions:** Organizations cannot expect general employees to be IT security experts on top of their daily work.
3. **Human memory limitations:** This is a result of our inability to remember numerous and complex passwords.
4. **Trust:** We must have faith and confidence in the security of our computers.
5. **Usability:** This includes individuals trading off between security and practicality.

6. **Social engineering:** This means being manipulated to do things we would not normally do.

These human factors stem from the norms of natural human tendencies. Natural human tendencies suggest that humans are emotional, manipulative, and fallible. For example, humans want to get their job done and want to be helpful. People are helpful and therefore as a consequence are easily deceived, as exemplified by the success of social engineering attacks (Mitnick & Simon, 2002). Furthermore, humans are irrational and unpredictable. Unlike computers that can be programmed to process instructions in some logical order, humans on the other hand are irrational and complex and do unpredictable things. Barrett (2003) states for all the cleverness that organizations put into formulating creative, innovative, and secure efforts, they all can be breached if the users are reckless, therefore insinuating that recklessness and carelessness are common natural human tendencies. Natural human tendencies put an organization at risk of many security-related threats.

A better understanding of these predispositions will provide organizations and the greater community with a better chance of protecting and securing the human aspect of information security.

Current Human-Related IT Security Solutions

Current human-related IT solutions encompass understanding the human aspects and enforcing compliant behaviors and attitudes towards IT security. These current solutions include:

- **Behavioral Auditing for Compliance:** Current auditing (security) methods do not cover effectively the behavior of the employees. Vroom and von-Solms (2004) proposes the concept of behavior auditing for compliance as a way of understanding, identifying, and resolving IT security-related human behavior concerns. However, auditing human behavior is very difficult to attain reliable and valid results due to humans being unpredictable by nature.
- **IT Security Policy:** IT security policy has the potential to enforce compliant security behavior and attitudes of employees (Wood, 2004). IT security policies are a set of rules that outline how information and technology is to be protected to achieve the organization's security goals. This allows humans to understand what is expected from them and be accountable for their actions. Simply telling people to behave in a certain way can be one option, but managers should not expect human to always act as prescribed. Also, reiterated by Dekker (2003), procedures do not rule human behavior and suggest that procedures should be seen as resources for action instead of an expectation about human behavior.
- **Security Training and Education Programs:** A good security training program helps improve a user's decision-making skills by providing them with the necessary knowledge about security threats and the consequences of their actions (Leach, 2003). With the growing numbers of mobile employees, enterprises are at greater risks due to their employees with inadequate understanding of current security threats and risks to their computers. This simply illustrates the need for better security education on current security threats and best practices for humans.
- **Ethical Standards of Behavior:** Eloff and Eloff (2003) and Jones (2004) researched ethical standards of behavior related to security and asserted that in order to change a user's behavior, there needs to be some form of guidelines on which to base such behavior. The authors maintained that following such established guides like the IEEE professional code can promote good behavior and influence others to do so.
- **Leveraging off technology to reduce human error:** IT systems have become increasingly complex. Consequently, human errors resulting from operating these systems has increased. Experts have highlighted how IT has now gone beyond legitimate users' control to use information systems honestly and appropriately without causing a security breach. Legitimate users such as employees are more likely to put a priority on getting their work tasks completed rather than 'think' about security (Besnard & Arief, 2004). These authors suggest better software design with security built-in, that is, invisible to the user.

Any approach to human information security should aim to achieve transparent security—that is, built-in security either in technology or defused into the daily lives of humans, whereby security is not seen as an