Chapter XXV
Behavioral Information Security

Isabelle J. Fagnot
Syracuse University, USA

ABSTRACT

The effectiveness of information security can be substantially limited by inappropriate and destructive human behaviors within an organization. As recent critical security incidents have shown, successful insider intrusions induce a fear of repeated disruptive behaviors within organizations, and can be more costly and damaging than outsider threats. Today, employees compose the majority of end-users. The wide variety of information that they handle in a multitude of work and non-work settings brings new challenges to organizations and drives technological and managerial change. Several areas of studies such as behavioral information security, information security governance and social engineering to name a few, have emerged in an attempt to understand the phenomena and suggest countermeasures and responses. This paper starts by defining behavioral information security and provides examples of security behaviors that have an impact on the overall security of an organization. Threats' mitigations are then depicted followed by future trends.

INTRODUCTION

Behavioral information security refers to the study of the human aspect of information security. This aspect of information security has been taken into account only recently. Beforehand, information security referred principally to its mechanical elements–the security status of an organization was only characterized by the quality and accountability of the technical aspect of its information systems. Accordingly, one critical security attribute that organizations tend to neglect is the consequence of human behaviors on the organization's overall information security and assurance. This omission becomes disturbingwhen an organization needs to collect an increasing amount of customers, clients, patients, and coworkers' sensitive information to operate. The organization is then responsible to insure the sensitive information's security and privacy.

In today's information society, information technology (IT) end user communities mostly consist of employees. This fact increases the amount of human mistakes within organizations. Yet employees' behaviors are still being misguidedly neglected by managers and security analysts. The human factor of information security plays an important role in corporate security

status. Today, a vigilant organization should pay close attention to both aspects of security: highly secure technical information systems and well-developed information security policies. If employees have not received proper security training and are unaware of the safeguarding policies and procedures–and if corporate governance is not reinforced–then the security of the information flowing into the organization will be jeopardized (David, 2002). Assuring up-to-date security awareness of employees is essential for optimizing security against threats to an organization. The media coverage of several recent vital security incidents, that caused in some cases the organization at stake to close down, has brought more attention to insider threats (Keeney, Kowalski, Cappelli, Moore, Shimeall, and Rogers, 2005). The cost of such encounters for the victim organizations has been tremendous. Consequently, a new area of corporate governance emerged: information security governance (Conner, Noonan, & Holleyman, 2003) which stresses the fact that security policies and procedures in organizations must be well articulated, adhered to by employees, and regularly reinforced by management.

The purpose of this chapter is twofold: To define behavioral information security illustrated by specific employees' behaviors that might enhance or hinder information security and to examine what countermeasures could help heighten the security status within organizations and mitigate the threat.

BACKGROUND

Information security, particularly its human aspect, is a fairly recent phenomenon of general research interest, and it has been intensifying as information technologies keep developing and corporations routinely depend upon it for their success. The capability of information security, however, is faced with a growing preponderance of vulnerabilities, becoming a source of apprehension in organizations as attacks—whether coming from the outside or the inside—gain in sophistication, incidence, and cause financial loss.

On the one hand, computers' technical security has expanded with computers' growth. On the other hand, it is only for the past decade—coinciding with the exponential growth of the Internet, thus more information circulating and more human beings involved in its flow—that more attention has been devoted to the human factor and to behavioral information security. As more cases of hacking, outside intrusions, data loss, insider threats, time loss, costs, and so forth occur and are made public, research is being undertaken to uncover, explain, and find solutions to counter such harmful behaviors.

At present insider threats are receiving better consideration (Keeney et al., 2005) due to recent acknowledgments that attacks on organizations are more successful when perpetrated from the inside rather than from the outside (Schultz, 2002). The fact that some insider attacks were successful has made organizations more aware of possible recurrences in the same vein. Insider threats may not only be extremely monetarily costly, but also harm an organizations reputation (Ernst & Young, 2002). Consequently, the effectiveness of information security can be substantially limited by inappropriate and destructive human behaviors within the organization. Behavioral information security, then, begins to develop coherent concepts, theory, and research germane to how humans behave in organizations and how that behavior affects information security.

MAIN THRUST OF THE CHAPTER

Behavioral Information Security: Significant Behaviors

Recognizing the human factor of information security, a team of researchers at Syracuse University School of Information Studies conducted, for over three years, a seminal project on the politics, motivation, and ethics of information security in organizations.[1] This research study exemplifies the topic of behavioral information security: excerpts of the analysis are presented in this section corroborating with the literature on information security.