ELSEVIER

Applied Ergonomics 38 (2007) 143–154

APPLIED ERGONOMICS

www.elsevier.com/locate/apergo

Human errors and violations in computer and information security: The viewpoint of network administrators and security specialists

Sara Kraemer, Pascale Carayon*

*Department of Industrial and Systems Engineering, Center for Quality and Productivity Improvement, University of Wisconsin-Madison,
610 Walnut Street 575 WARF, Madison, WI 53726, USA*

Received 8 May 2005; accepted 17 March 2006

Abstract

This paper describes human errors and violations of end users and network administration in computer and information security. This information is summarized in a conceptual framework for examining the human and organizational factors contributing to computer and information security. This framework includes human error taxonomies to describe the work conditions that contribute adversely to computer and information security, i.e. to security vulnerabilities and breaches. The issue of human error and violation in computer and information security was explored through a series of 16 interviews with network administrators and security specialists. The interviews were audio taped, transcribed, and analyzed by coding specific themes in a node structure. The result is an expanded framework that classifies types of human error and identifies specific human and organizational factors that contribute to computer and information security. Network administrators tended to view errors created by end users as more intentional than unintentional, while errors created by network administrators as more unintentional than intentional. Organizational factors, such as communication, security culture, policy, and organizational structure, were the most frequently cited factors associated with computer and information security.

Keywords: Human error; Violation; Computer security; Work system; Macroergonomic; Qualitative research

1. Introduction

The National Research Council Computer Science and Telecommunications Board (2002) has distinguished between accidental and deliberate causes of poor computer and information security (CIS): "*Accidental causes* are natural (e.g., a lightening surge that destroys a power supply in a network that causes part of the network to fail) or human but non-deliberate (e.g., an accidental programming error that causes a computer to crash under certain circumstances, or the unintended cutting of a communications cable during excavation). Accidental causes figure prominently in many aspects of trustworthiness beside security, such as safety or reliability. Deliberate causes are the result of conscious human choice." (National Research Council Computer Science and Telecommunications Board, 2002, pp. 3–4). In the CIS literature, deliberate causes are referred as 'attacks'. Attackers, those who seek to cause damage deliberately, may be able to exploit an error accidentally introduced into the system. In this paper, we will refer to accidental causes, as described in the National Research Council Computer Science and Telecommunications Board (2002), as *human error*. Deliberate causes will refer to the concept of violations: deliberate actions that deviate from processes. The concept of violations is two-fold: (1) violations of malicious intent (e.g., insider threats, hackers, terrorists) and (2) violations of a non-malicious nature, the deliberate actions that deviate from CIS processes that may or may not result in decreased CIS performance. In this context, human errors and violations do not assign blame to the individual. Rather, it is important to examine the different elements of

*Corresponding author. Tel.: 1 608 263 2520; fax: 1 608 263 1425.
E-mail addresses: skraemer@cqpi.engr.wisc.edu (S. Kraemer), carayon@engr.wisc.edu (P. Carayon).

0003-6870/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.apergo.2006.03.010

the system that can lead to human errors and violations, such as faulty equipment, poor management practices or unclear procedures (Reason, 1997).

Previous studies demonstrate the ever-present risks in computer and information system security, and the importance of the accidental and deliberate causes, or threats, that exist within these security systems. Causes of deliberate attacks have been described as resulting from poor management or operational practices, rather than human error (Computer Science and Telecommunications Board-National Research Council, 2002). However, this is not necessarily true. For example, in the fall of 2000, Western Union was victim to an attack that was attributed to human error rather than a design flaw. A hacker electronically entered one of Western Union's computer servers without permission and stole about 15,700 customer credit card numbers. The incident occurred after the system was taken down for regular maintenance, and a file containing the credit card information had inadvertently been left unprotected when the system was returned to operation (Stokes, 2000). In addition, Whitman's (2003) study found that the IS directors, managers, and supervisors ranked technical software failures or errors and acts of human error failure (for a combined total of 2231 responses) higher than deliberate software attacks (2178 responses). Whitman's (2003) findings support recognition of human error and failure as a significant area for consideration in the field of CIS. In addition, examining accidental causes may allow an organization to identify weaknesses in its systems or processes that may be deliberately exploited.

The field of human factors has developed models and concepts for understanding and characterizing varying types and levels of human error, which have been used successfully in various industries to analyze causes of accidents (Reason, 1997). These taxonomies not only explore the cognitive mechanisms involved in human error (Rasmussen et al., 1994), but also emphasize the role of organizational and management factors in the creation of error-prone conditions (Reason, 1997). We propose that taxonomies and models of human error can be used to identify and characterize vulnerabilities of computer and information systems.

This paper examines the "accidental" causes (i.e. human errors) and "deliberate" causes (i.e. violations) in CIS. We examine how models of human error and macroergonomics can be used to understand accidental causes errors. We also argue that knowledge generated from the understanding of accidental causes can help build better defense mechanisms against deliberate attacks. Using data collected from interviews with network administrators and computer security specialists, we identify the human and organizational elements contributing to CIS. This study encompasses two objectives:

(1) Identify human errors, violations, and associated mechanisms that contribute to vulnerabilities and breaches in CIS systems.
(2) Characterize the human and organizational elements associated with human errors and violations in CIS systems.

2. Conceptual framework

We have developed a 'macroergonomic' conceptual framework to identify and describe the work system elements contributing to human errors that may cause CIS vulnerabilities (Carayon and Kraemer, 2002). Our conceptual framework provides a basis for understanding the various linkages of human and organizational factors to human error contributing to security (see Fig. 1). It is a synthesis of various frameworks describing work systems elements (e.g. the macroergonomic framework) and human error (e.g. human error taxonomies).

According to the macroergonomic work system model developed by Smith and Carayon (Carayon and Smith, 2000; Smith and Carayon-Sainfort, 1989), a work system may be conceptualized as having five elements: the individual, task, tools and technologies, environment and the organization. The interplay of these elements may create conditions that contribute to human error and violations. These errors may result in security vulnerabilities and sometimes result in security breaches, if the vulnerability is exploited. We used the work system model as a guide to define specific categories of elements that may contribute to human errors and violations.

The middle section of the framework describes the various dimensions of human errors and violations. Within various cognitive processing stages, different types and levels of human error may occur. Perhaps the most widely known and accepted human error taxonomy is the skill-rule-knowledge (SRK) framework of Rasmussen (1982). This framework postulates that errors may be divided into categories based upon an individual's level of performance. The errors are distinguished by both psychological and situational variables that together define an 'activity space' on to which the three performance levels are mapped. The three performance levels are: (1) skill-based level errors, which are made with routine, highly practiced tasks in a predominantly automatic capacity with occasional conscious checks on progress. It is thought that in this activity space people perform very well most of the time; (2) rule-based performance level occurs when a change is needed to modify the automatic behavior found at the skill-based level. At this point the person may apply a memorized or documented rule, with periodic checks to monitor the progress and outcome of the actions; and (3) knowledge-based performance is an activity space met only after repeated failure and without a pre-existing solution. Errors have been categorized as either mistakes or slips and lapses (Reason, 1990; Norman, 1983). Using Rasmussen's (1982) SRK model of human performance, mistakes can be further categorized into rule-based mistakes and