Protecting Organizational Information Resources

MICHAEL D. WYBO
DETMAR W. STRAUB, JR.
University of Minnesota

This paper presents an overview of the empirical evidence concerning the nature of computer abuse against organizations and viable control mechanisms. A model of perpetrator motivation is presented and General Deterrence Theory is proposed as an appropriate theoretical basis for the design and implementation of computer abuse countermeasures. In this theoretical context, specific actions that computer security specialists, information systems managers, and EDP auditors can take to reduce the likelihood of computer abuse in their organizations are proposed.

The use of computer-based technologies in the processing and storage of organizational information resources is standard practice in the 1980s. Many of today’s business procedures and services are possible only because of the computer’s ability to process large numbers of individual transactions quickly and accurately. However, as with any other technological extension of man, computer systems are subject to abuse, and their failure to perform in the manner intended can endanger the very enterprises they were designed to serve and protect. The computer in its roles as an information processor, deliverer, and repository has become a vehicle and/or target for abuse. The potential threat to organizations from intentional misuse of computer systems and organizational data is real. Furthermore, management and law enforcement have been slow in responding to fundamental changes being wrought by the computer, and this sluggish response may be adding to the uncertainty surrounding the computer abuse issue.

Defining Computer Abuse

The terms “computer fraud,” “computer crime,” and “computer abuse” are often used interchangeably to mean the intentional misuse of computer system assets such as hardware,
data, programs, and computer service (Parker, 1976, 1981; Straub, 1986b).

Fraud denotes deception, the “intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right” (Webster, 1967). This first definition describes what is thought of as computer crimes, that is acts that can involve criminal or civil sanctions. These acts range from a clerk’s addition of a small amount of overtime pay to his own paycheck every week to sophisticated embezzlement schemes involving large sums of money. A second definition of fraud—an “act of deceiving or misrepresenting” (Webster, 1967)—is more generic and intimates activities that simply violate organizational policies or mores; for example, an employee’s use of the organization’s computer system during off hours to run his own information service bureau.

Neither of the terms, computer fraud nor computer crime, connotes acts of sabotage. Sabotage may not necessarily involve deception and may not necessarily be illegal. Organizations nevertheless may find it desirable to punish the offense in order to deter future violations. In order to reduce confusion and include as many possible facets of the phenomena under discussion, the term computer abuse is used to refer to all of the above mentioned types of misuse of information resources.

The term computer abuse as used here refers to the deliberate misuse of information resources. Although it is conceivable that system users may unintentionally perpetrate incidents of computer abuse, such unintentional incidents may be avoided through adequate informational and training programs. Intentional abuses have the potential for much more serious consequences and for being more difficult to detect and deter.

Lastly, the term computer abuse is used to refer to the misuse of organizational information resources by individuals. Computer abuse may be conceived in terms of (a) organizational or individual perpetrators. From a social and legal perspective, the Organization/Organization, Organization/Individual, and Individual/Individual perpetrator/victim combinations of abuse require social regulation outside the organizational environment. Responses to abuse by individuals against organizations, however, occur largely within the organization (Straub & Nance, 1989) and, in all likelihood, will continue to be handled internally in spite of newly enacted federal and state laws directed specifically at computer abuses. Internal handling predominates because abuses are embarrassing and perceived as a sign of lax security (Straub, 1986b). These Individual/Organization abuses therefore hold the greatest promise for improving management of the risk. The bulk of the research into computer abuse to date, moreover, has been in this domain.

The operational definition of computer abuse used in the remainder of this discussion is based on distinctions suggested by Kling (1980) and elaborated by Straub and Nance (1989):

Computer abuse is unauthorized, deliberate, and internally recognizable misuse of assets of the local organizational information system by individuals, including violations against:

1. hardware (and other physical assets associated with computers such as theft or damage to terminals, CPUs, disk drives, and printers)
2. programs (such as theft or modification of programs)
3. data (such as embezzlement or modification of data)
4. computer service (such as unauthorized use of service or purposeful interruption of service).
Related Content

A Conceptual Framework to Improve Project Team Learning in Major Projects
Hani Gharibeh (2015). International Journal of Information Technology Project Management (pp. 61-76).
www.igi-global.com/article/a-conceptual-framework-to-improve-project-team-learning-in-major-projects/123966?camid=4v1a

Determinant of Information Quality and Use of Executive Information Systems (EIS) in UK
www.igi-global.com/chapter/determinant-information-quality-use-executive/10096?camid=4v1a

www.igi-global.com/article/human-resource-decision-support-systems/50911?camid=4v1a

A Framework for Extending Potency and Reducing Competitive Risk in the IT Strategic Systems Portfolio
James D. White, Theresa A. Steinbach, Linda V. Knight and Alan T. Burns (2003). Business Strategies for Information Technology Management (pp. 96-114).
www.igi-global.com/chapter/framework-extending-potency-reducing-competitive/6106?camid=4v1a