

MISQ Archivist

Beyond Deterrence: An Expanded View of Employee Computer Abuse

Robert Willison and Merrill Warkentin

Abstract

Recent academic investigations of computer security policy violations have largely focused on non-malicious noncompliance due to poor training, low employee motivation, weak affective commitment, or individual oversight. Established theoretical foundations applied to this domain have related to protection motivation, deterrence, planned behavior, self-efficacy, individual adoption factors, organizational commitment, and other individual cognitive factors. But another class of violation demands greater research emphasis: the intentional commission of computer security policy violation, or insider computer abuse. Whether motivated by greed, disgruntlement, or other psychological processes, this act has the greatest potential for loss and damage to the employer. We argue the focus must include not only the act and its immediate antecedents of intention (to commit computer abuse) and deterrence (of the crime), but also phenomena which temporally precede these areas. More specifically, we assert the need to consider the thought processes of the potential offender and how these are influenced by the organizational context, prior to deterrence. We believe the interplay between thought processes and this context may significantly impact the efficacy of IS security controls, specifically deterrence safeguards. Through this focus, we extend the Straub and Welke (1998) security action cycle framework and propose three areas worthy of empirical investigation—techniques of neutralization (rationalization), expressive/instrumental criminal motivations, and disgruntlement as a result of perceptions of organizational injustice—and propose questions for future research in these areas.

Keywords: Computer abuse, employee computer crime, information systems security, deterrence, neutralization, motivation, disgruntlement, organizational justice, instrumental crimes, expressive crimes