Available online at www.sciencedirect.com
ScienceDirect

Information and Organization 16 (2006) 304–324

INFORMATION AND ORGANIZATION

www.elsevier.com/locate/infoandorg

Understanding the perpetration of employee computer crime in the organisational context

Robert Willison *

Copenhagen Business School, Howitzvej 60, DK-2000 Frederiksberg, Denmark

Received 6 February 2006; received in revised form 25 February 2006; accepted 29 August 2006

Abstract

While hackers and viruses fuel the IS security concerns for organisations, the problems posed by employee computer crime should not be underestimated. Indeed, a number of IS security researchers have turned their attention to the 'insider' threat. Of this group, several focus on the offender, either in terms of a series of attributes required for perpetration, or with reference to forms of safeguards aimed at negating such behaviour. These studies are complemented by those texts which examine the organisational context in which rogue employees commit computer crime. Currently, however, there has been a lack of insight into the relationship between the offender and the context, during the commission process. To address this deficiency, two criminological theories are advanced. This paper illustrates how the theories, entitled the Rational Choice Perspective and Situational Crime Prevention, can be applied to the IS domain, thereby offering a theoretical basis by which to analyse the offender/context relationship during perpetration. By so doing, practitioners may use these insights to inform and enhance the selection of safeguards in a bid to improve prevention programmes. Furthermore, the importation of the Rational Choice Perspective and Situational Crime Prevention into the IS field opens up potentially new areas for future research.

© 2006 Elsevier Ltd. All rights reserved.

Keywords: IS security; Criminology; Employee computer crime; Perpetration

* Tel.: +45 3815 2388; fax: +45 3815 2401.
E-mail address: rw.inf@cbs.dk.

1471-7727/$ - see front matter © 2006 Elsevier Ltd. All rights reserved.
doi:10.1016/j.infoandorg.2006.08.001

1. Introduction

While hackers and viruses fuel the security concerns of organisations, the threat of employee computer crime should not be overlooked. This message is echoed by numerous security surveys which point to the magnitude of the 'insider' problem (CSI/FBI, 2004; DTI/PWC, 2004; Ernst & Young, 2004). The 2004 CSI/FBI Computer Crime and Security Survey (CSI/FBI, 2004) revealed that approximately 50% of security breaches occurred within the organisation. From another perspective, respondents to the UK DTI/PWC (2004) survey were asked about the source of their worst security incident. For small size (1–49 employees) organisations, 32% stated the source was internal. However, this figure rose to 46% and 48%, respectively, for medium (50–249 employees) and large (250 + employees) companies.

Against this backdrop, a number of researchers have turned their attention to the security problems posed by employee computer crime (Harrington, 1996; Kesar & Rogerson, 1998; Straub, 1990). Of this group, several focus on the offender, either in terms of a series of attributes required for perpetration, or with reference to forms of safeguards aimed at negating such behaviour. These studies are complemented by those texts which examine the organisational context in which rogue employees commit computer crime. Currently, however, there has been a lack of insight into the relationship between the offender and the context during the perpetration of computer crime. To address this oversight, this paper focuses on the stages an offender must go through in order for a crime to be committed, i.e. the procedural stages. Two criminological theories, entitled the Rational Choice Perspective (Clarke & Cornish, 1985, 2000; Cornish & Clarke, 1986) and Situational Crime Prevention (Clarke, 1997), are advanced to support analysis of the stages comprising employee computer crime. Rather than focussing on 'why' and 'how' people become criminals, these theories focus on the perpetration of crime. It is argued that the Rational Choice Perspective and Situational Crime Prevention may complement existing security strategies by potentially offering a theoretical basis by which to identify offender behaviour in all of the procedural stages, and the associated criminal choices which underpin their actions. In so doing, practitioners may use these insights to inform and enhance the selection of safeguards to prevent the successful perpetration of employee computer crime. Furthermore, through the application of the two theories in the IS field potentially new areas for future research are suggested.

The proceeding section of the paper reviews the related literature. This is followed by a discussion which centres on the difference between those criminological theories which focus on the criminal act as opposed to theories of criminality. The discussion serves as an introduction to a description of the two bodies of theory advanced in this paper, namely the Rational Choice Perspective and Situational Crime Prevention. The penultimate section discusses how these approaches can be used to address the procedural stages of computer crime, followed by the conclusion and suggestions for future research.

2. Employees and computer crime

Of the related IS security literature which examines the insider threat, a number of these studies focus on the offender, either in terms of a series of attributes required for perpetration, or with reference to forms of safeguards aimed at negating such behaviour. These texts are complemented by those studies which examine the organisational

Download English Version:

https://daneshyari.com/en/article/555045

Download Persian Version:

https://daneshyari.com/article/555045

Daneshyari.com