Understanding the offender/environment dynamic for computer crimes

Robert Willison (Department of Informatics, Copenhagen Business School, Copenhagen, Denmark)

Information Technology & People
ISSN: 0959-3845
Publication date: 1 April 2006

Abstract

Purpose
While a number of IS security researchers consider the threat posed by employees who perpetrate computer crime, there is currently a lack of insight into how the offender interacts with the criminal context both prior to and during commission. A greater understanding of this relationship may complement existing security practices by possibly highlighting new areas for safeguard implementation. To help facilitate a greater understanding of the offender/environment dynamic, this paper, therefore, aims to assess the feasibility of applying three criminological theories to the IS security context. Rather than focusing on why people become criminals, these theories entitled routine activity theory, environmental criminology and the rational choice perspective, focus on the criminal act.

Design/methodology/approach
Drawing on an account of the Barings Bank collapse, events highlighted in the case study are used to assess whether concepts central to the theories are supported by the data.

Findings
Analysis indicates support for the concepts central to environmental criminology and the rational choice perspective. While case study evidence supports two of the concepts advanced by routine activity theory, as a whole the theory is found wanting, as the "guardianship" and "handled offender" concepts appear to lack the necessary sophistication to theoretically accommodate and explain supervisory and control failings cited in the case study.

Research limitations/implications
While future research could encompass continued application of the theories to further assess their suitability for the IS domain, consideration could also be given to the application of the preventive tools and methods which have been developed in tandem with the three criminological approaches. Another stream of future research may involve the application of the theories in conjunction with existing security practices.

Practical implications
Greater knowledge of the offender/context dynamic may feasibly enhance existing security practices by possibly highlighting new areas for safeguard implementation.

Originality/value
From an IS security perspective, there is currently a lack of insight into the offender/context dynamic. The paper presents a group of criminological theories, which have previously not been considered for application in the IS context. The theories may feasibly throw light on the behaviour of offenders in the criminal context, both prior to and during commission.

Keywords
Data security, Computer crime, Criminology, Criminals, Behaviour

Citation
https://doi.org/10.1108/09593840610673810

Download as .RIS

Publisher: Emerald Group Publishing Limited
Copyright © 2006, Emerald Group Publishing Limited

To read the full version of this content please select one of the options below

You may be able to access this content by logging in via Shibboleth, Open Athens or with your Emerald Account.

To rent this content from Deepdyve, please click the button.

If you think you should have access to this content, click the button to contact our support team.
Alternatively referred to as cyber crime, e-crime, electronic crime, or hi-tech crime. Computer crime is an act performed by a knowledgeable computer user, sometimes referred to as a hacker that illegally browses or steals a company's or individual's private information. In some cases, this person or group of individuals may be malicious and destroy or otherwise corrupt the computer or data files. Examples of computer crimes. Below is a listing of the different types of computer crimes today. Clicking on any of the links below gives further information about each crime.

- Computer crimes may go undetected, as when someone breaks into a computer, copies files, and then leaves without detection by the system or its operators.
- Computer crimes may not be reported to police or prosecutors.
- The Uniform Crime Report system does not include classifications for computer crimes and no other national system exists for collecting statistics about the problem.
- Arrests are not a reliable source for computer crimes because the charges may be placed under an unrelated statute, especially when the computer has advanced a crime, as in embezzlements.

The information available on computer crime is limited. For example, the speed and ability to communicate with people is fostered by the Internet, a worldwide network that is used to send communiqués and provide access to the world-wide web. On the state level, the one thing upon which there is much unanimity is that theft of information or money in electronic form is much the same as theft in any other form. State laws on computer crime, therefore, focus on theft of information or money through the use of a computer or an on-line computer service. Virtually every state requires that one have the requisite mental state before they may be convicted of a computer crime. Computer crimes encompass unauthorized or illegal activities perpetrated via computer as well as the theft of computers and other technological hardware. As firms of all sizes, industrial orientation, and geographic location increasingly rely on computers to operate, concerns about computer crime have also risen, in part because the practice appears to be thriving despite the concerted efforts of both the law enforcement and business communities to stop it. But computer experts and business consultants alike note that both international corporations and modest family-owned businesses can do a