Decision Support Systems 50 (2011) 702–714

Contents lists available at ScienceDirect

Decision Support Systems

journal homepage: www.elsevier.com/locate/dss

Detecting complex account fraud in the enterprise: The role of technical and non-technical controls

Sigi Goode *, David Lacey

School of Accounting and Business Information Systems, College of Business and Economics, The Australian National University, Acton 0200, Australia

ARTICLE INFO

Available online 19 August 2010

Keywords:
Fraud
Controls
Security
Time exposure
Loss

ABSTRACT

Complex fraud, involving heightened offender knowledge of organizational processes, can be especially damaging to the firm. Much research has focused on technical, quantitative detection methods. This paper uses multidimensional scaling of empirical fraud event data from a large telecommunications firm to illustrate how technical and socio-technical fraud controls are used to detect fraud at varying levels of time exposure and dollar loss. The evidence suggests that technical controls only detect one third of fraud cases with zero time exposure and loss. More complex fraud is detected with a range of technical and socio-technical controls from inside and outside the firm. Interviews with twelve fraud managers and investigators are used to confirm the findings.

1. Introduction

Corporate and financial fraud, the obtaining of money, goods and services through illicit or deceptive means, is a serious ongoing problem for the modern enterprise [4,37]. Holtfreter [34] cites figures of up to US$600 billion in employee-related frauds. Newer threats to the financial sector, involving techniques of social engineering to gather account details and remote network-based attacks [13], are increasingly the purview of organized criminal networks [69]. The popular literature, in particular, provides coverage to a range of these types of fraud, including intellectual property theft, financial mismanagement, identity and ownership fraud. A number of authors argue that general fraud levels are increasing [35,74].

Scholarly research in the area of fraud is difficult. Studies of financial fraud are hampered by problems of access to offender, organization and offence data. Firms can also be reluctant to admit that they have a security or fraud problem within their operations. Managers may not wish to open their firm to enquiry or analysis from outside groups, including academic researchers, lest it affect their reputation in the market. It is rare for external researchers to be granted access to original, unsanitized data. In addition, empirical analysis of fraud incidents is made harder because the data itself can be poorly organized or incomplete [22]. Further, many authors hold that this control environment is the purview of the audit function [16,51], comprising a significant political and regulatory mandate [26]. Indeed, formal normative control frameworks exist for the purposes of effective audit conduct [12].

Amid the problem of increasing fraud levels on one hand, and the difficulty associated with researching fraud on the other, important gaps exist in research understanding of fraud identification and fraud detection. Much prior work has focused on theoretical approaches for developing technical detection systems (such as [4,7,20,30,37,49]) and operational methods for fraud prevention and awareness (such as [66]). However, as Caplan [8, p.103] notes, "fraud risk factors cannot easily be combined into effective predictive models". We know little of the system controls actually used in firms to detect and handle fraud [21], and the social approaches that complement these technical means [3]. In the words of D'Arcy and Hovav [17, p.117], the "disproportionate focus on technical security countermeasures may partially explain why IS misuse remains a significant problem". The research corpus needs input on the types of controls that comprise the firm's security posture and how these controls interact with each other with respect to different threat types.

A second gap in understanding exists with respect to the response of controls to new fraud species. Much prior work has also focused on individual fraud types, such as identity theft [29], intellectual property fraud [31] or insurance fraud [14]. However, given the modern firm's level of popularity and interconnection, it may not be feasible to focus on just one kind of fraud at the expense of all others that could befall the firm. Also, in order to obtain the greatest business case value, managers will likely need to be able to justify control funding based on detection success rates: employing networks of controls is hence a cost-effective approach to detect and prosecute fraud. Non-technical (or socio-technical) controls may also assist in this context. In the words of Dhillon and Backhouse [21, p.126], "computer security is not, per se, a technical problem. It is a social and organizational problem because the technical systems have to be operated and used by people". To further complicate matters, analysis of real world data is

* Corresponding author.
E-mail address: sigi.goode@anu.edu.au (S. Goode).

0167-9236/$ – see front matter © 2010 Elsevier B.V. All rights reserved.
doi:10.1016/j.dss.2010.08.018

made more difficult by the number of organizational and individual actors that interact with the firm with respect to fraud commission, detection and prevention. Neither the firm nor the offenders operate in isolation: they share information and techniques, altering their behavior and strategy accordingly. An analysis method is hence needed that can effectively simplify our view of these control mechanisms.

This paper presents a case study of a large telecommunications carrier in the Asia Pacific region. The paper reveals the types of controls used to detect account-related fraud. This detection is compared against the degree of loss (equivalent dollars lost) and time exposure (the length of time for which the offender has been able to execute damage in the firm).

The aim of this paper is to illustrate and explore how technical and non-technical controls relate to each other in order to detect and investigate fraud. The goal of this paper is not to develop a new method for detecting fraud, but rather to highlight the use of non-technical controls as part of the control mix. In doing so, we aim to answer calls from authors such as [22,39,60] for further work into non-technical organizational security controls. The paper contributes in two ways. First, analysis by way of empirical data is rare in the published research literature. This paper provides insight into both the theatre of real world threats and the methods used to detect fraud in an actual firm. Second, this paper provides some of the first published evidence of the use of different control combinations to detect and ameliorate different fraud types and their complexities. This work hence illustrates the effectiveness of quantitative detection response with respect to fraud complexity.

This discussion leads to the study's research questions:

What is the relationship between technical and non-technical controls in preventing and detecting fraud losses?
How does this relationship change in the context of time exposure and the prevention and detection of losses?

The rest of this paper is structured as follows. The next section provides a brief overview of prior theory on control and detection management. The paper then details the research method, including the multidimensional scaling (MDS) technique for data analysis. This is followed by an overview of the fraud environment at play with respect to the case firm. In order to lend context to the analysis, the paper first presents an overview of the types of fraud seen in the case firm. The paper then presents the analysis of the controls in use, dividing the analysis into quantitative controls used to detect fraud at its inception, and the collections of controls used to detect more complex fraud with positive time exposure levels. Finally, conclusions are offered.

2. Theory on controls

The modern enterprise is a complex interaction of individuals and groups. Heightened internetworking between firms has also contributed to this complexity, as firms join together for the benefits of partnership and cooperation. These firms operate within a complex environment, comprising real and perceived threats from both within and outside the firm. The concept of organizational control has received considerable coverage in the business literature [27,50]. Managerial control systems play various important roles in the firm [33]. They act as a platform for audits, they support the validation and benchmarking of organizational units and business areas, and they assist in aligning managerial performance and remuneration in the context of agency effects. Ultimately, these managerial control systems are integral to effective organizational governance. Understandably, firms may be keen to reveal, discuss and even advertise their managerial control methods in order to encourage investor and shareholder confidence. Recent highly publicized problems of financial mismanagement and corporate collapses have resulted in heightened scrutiny and expectations of internal systems and services of these firms. In the same way that managerial control preserves the financial operations of the firm, so security controls preserve the mechanics and effectiveness of the firm's information systems.

However, firms are more reluctant to reveal their security models to outside scrutiny, and empirical literature coverage of security controls has been more sparse. To varying levels, the firm must open its operations to these groups, accepting and distributing information, products and services as needed. Firms commonly employ controls to manage and maintain the integrity of these operations [54]. Such controls aid in detecting and preventing fraud [8]. The primary purpose of such functions in the firm is to keep the organization's financial and non-financial systems running to specification [32,59]. In this respect, controls rely on the information present in the firm, provided by the firm's systems, actors and other functions.

Categorizing the roles played by different controls has been an important aspect of prior work. In the context of security and fraud control, a significant amount of prior theoretical work in IS has focused on the dual principles of deterrence and prevention, to varying degrees [71]. The value of this dual perspective lies in stopping illegitimate activity from affecting the system in the first instance. Not all such deterrence is effective, and another body of work has sought to examine fraud once it has entered the system [62]. Krishnan et al. [42] discuss the role of controls in preventing and detecting data error. Bagchi and Udo [2] discuss detection and prevention techniques for online threats.

Other significant work has classified security controls according to functional and threat categories. In part, this work has arisen out of a need to identify effective control structures in the face of investment returns, demand for business value and rising incidences of threats. For example, Straub [61] surveyed a group of firms to ascertain their approaches to deterrence and prevention, in addition to motivational and environmental factors. Loch et al. [47] surveyed 131 managers to determine their understanding of threats to the enterprise. Holtfreter [34] surveyed 663 organizational victims of internal fraud in the United States. Respondents were asked to report on the type and number of control mechanisms organizations used to detect and prevent fraud.

Recent work has highlighted the ability of the firm to adapt to the complexity of the threat environment. Operational and transactional data can be unclean and poorly kept [1]. Different investigators have different specialties (e.g. analysts, field specialists, technical specialists, etc.) with correspondingly different abilities and priorities for data-entry and management. Similarly, offenders are aware that, first, the data they provide could be used to track and curtail their behavior and, second, that well organized and more complete data is likely to make the investigative process easier. Offenders can muddy the analytical waters by altering spellings, dates and other personal information in order to confound these investigative processes. Point of sale staff, sometimes involving off-shore call centers, can also be a weak point, open to social engineering. Finally, individual fraud cases may not be wholly self-contained, and may actually be part of a larger fraud program, perpetrated by multiple identities [46]. Analysis methods that depend on clean and pure data are unlikely to be effective. In these circumstances, non-technical approaches are likely to be more useful. To this end, Dhillon and Backhouse [21, p.128] argued, "While technical controls are vital, especially with regard to who accesses computer systems and to what they are allowed to do once admitted, sophisticated future users of information systems will have to address the organizational problems at a time when the form the organization takes is being revolutionized".

Accordingly, recent research has worked to explore the role played by social countermeasures, by differentiating between technical and non-technical controls. Technical controls may be largely automated, quantitatively weighing historical data against incoming cases and