IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP5137

This paper appears in *Managing Modern Organizations Through Information Technology*, Proceedings of the 2005 Information Resources Management Association International Conference, edited by Mehdi Khosrow-Pour.

A Model of Controlling Occupational Fraud in Virtual Organizations

Paul J. Komiak and Sherrie Xiao Komiak

Faculty of Business Administration, Memorial University of Newfoundland, St. John's NF A1B 3X5, Canada, {pkomiak, skomiak@mun.ca}

With organizations becoming more complex, dynamic, and global, and due to the availability of new telecommunications and computing technologies, especially the Internet, forming virtual organizations is becoming common as a modern organizational strategy. A virtual organization (VO) is primarily characterized as being a network of independent, geographically dispersed organizations with a partial mission overlap (Larsen and McInerney 2002). The VOs' benefits have been well researched, including efficiency and cost savings, enhanced customer focus and market penetration, reduced competition, and knowledge sharing (Burgers, Hill et al. 1993), and there is a stream of literature enumerating the benefits and providing criteria and guidance for virtual organizations (Markus and Agres 2003).

Yet despite their growing prevalence, the change in organizational form and context of work enabled by virtual organizations suggests hidden threats to the organization and may leave such organizations susceptible to economic loss. The introduction and maintenance of the VO is far from unproblematic. The same factors that yield the benefits exacerbate the motivations, opportunities, and rationalizations – the three-factor model - of occupational fraud (Albrecht, Wernz et al. 1995).

More than a media fanfare and public curiosity, occupational fraud, e.g., asset misappropriations, corruption, and fraudulent financial reporting, is a widespread problem that affects practically every organization, regardless of size, location, or industry. The Association of Certified Fraud Examiners estimated that six percent of revenues would be lost in 2004 because of occupational fraud. Applied to the U.S. Gross Domestic Product, this translates to losses of approximately $600 billion. Thus, it is important to study occupational fraud in organizations. So far, little research has been done on the subject of occupational fraud as organizations shift to virtual-based forms. It is clear that there is a need to understand better the causal processes in the context of VOs and to facilitate the prevention, detection and correction of occupational fraud. This paper aims at developing a framework to understand the risk occupational fraud in virtual organizations.

THEORETICAL BACKGROUND

The Symbiotic Association of Occupational Fraud and the VO

We believe the risk of occupational fraud is greater in the VO because, as the literature suggests, with the redefinition of the role of the individual in the organization (Conner 2003), the need for increasing coordination and information through open communication systems and free association of individuals and groups within and outside the organization (Daboub 2002), the use of subcontracting and reliance on information technology (Fitzpatrick and Burke 2003), and the globalization and internationalization of virtual relationships (Helms, Ettkin et al. 2000), transactions in a virtual organizational context have taken on added dimensions – complexity, informality, reliance on trust, and general, rather than specific, monitoring. These four characteristics present separate opportunities for occupational fraud, and become more potent factors when combined as they are in the virtual organization.

Although trust appears to be an enabling condition for virtual organizations, trust alone does not ensure a successful VO (Gallivan 2001). Too much or too little trust, too much or too little control, and the existence of non-subscribers – those prone to dishonest behavior – may put the VO at risk. Anecdotal and applied research evidence suggest that the proclivity towards employee dishonesty is widespread; experimental research (Morris, Marshall et al. 2002), empirical research (McKendall, DeMarr et al. 2002), and survey research (Brief, Dukerisch et al. 1996) confirm these views. Thus, studying the risk of occupational fraud in the VO is important, because the results from these studies require an explanation beyond what organizational and trust theories provide.

Occupational fraud is defined as the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of employer's resources/assets (ACFE 2004). An example of the risk of occupational fraud is competitive intelligence. Without necessarily meaning to, organizations can invite fraud as a means of obtaining goals. Success or failure often depends upon an organization's ability to build, maintain or eradicate competitive advantages. Conversely, its competitors will make every effort to gather and analyze the information in attempts to overcome the competitive advantage. Some of the methods that organizations use to gather business intelligence are entirely legal – government filings, competitive data bases, print media (Fitzpatrick and Burke 2000) – while others are "creative" and many, illegal – bribery, conflict of interest, extortion. According to the American Society for Industrial Security, occurrences of economic espionage in American business have grown by more than 260 percent since 1985 ; the financial consequences may amount to $250 billion annually (Shaneley and Crabb 1998).

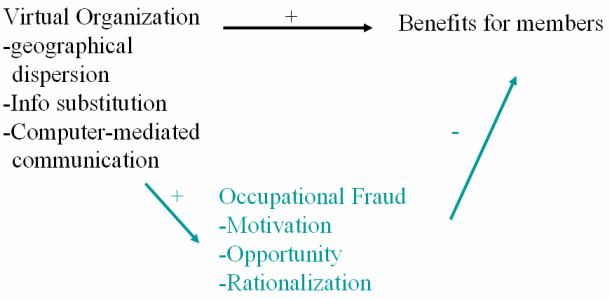
As another example, the changing nature of the organization and the extensive use of information and telecommunications technology (Warren and Hutchinson 2000) have created new threats and risk factors. An organization usually will use the same technology, accounting procedures, and other techniques across its various departments, but that homogeneity will rarely exist when two complex organizations transact business (CICA 1996). The creation of information infrastructures that allow the rapid exchange of ideas and information, and unfettered access in virtual teams, have displaced traditional audit trails, (Kerwin, Stepanek et al. 2000). That creates problems for each organization that wants to monitor a transaction. In particular, it is not clear that managerial accounting and control systems and audit techniques are able to support the new ways of working envisaged. A recent estimate shows the loss to information security threats, excluding external threats, e.g. viruses, at $250 billion (Hopwood, Sinason et al. 2000).

In this article, we argue that the symbiotic association of occupational fraud and the VO may be explained by identifying the factors and processes that enable the VO yet exacerbate the conditions for occupational fraud. We develop a model of trust and control in the virtual organization to explain why the conditions that are conducive to the creation and maintenance of a VO are the same conditions that increase the vulnerability of an organization to occupational fraud (Figure 1).

Major Theories of Occupational Fraud

Early studies (Cressey 1973; Hollinger and Clark 1983; Sutherland 1983; Albrecht, Wernz et al. 1995) focused primarily on developing a model

Figure 1. A Model of Occupational Fraud in VO



of the occupational offender. Cressey's study (1973) articulated the three factor model for fraud: 1) a perceived unsharable financial need – such as personal failures, business reversals, physical isolation, or status gaining – 2) a perceived opportunity - when information about a member's deeds may be unknown to others or when misbehaviors are not easily detected - and 3) rationalization. Similarly, Albrecht, Wernz et al. (1995) suggest that three factors are involved in occupational fraud: personal, situational, and some way to rationalize the act.

In the context of traditional organizations, Cressey (1973) and Hollinger, and Clark (1983) propose that employee fraud is mainly a result of workplace conditions: employee theft is significantly related to job dissatisfaction. Additional research on occupational fraud suggests that the level of employee dissatisfaction relates to dysfunctional behavior. These studies disclose several pertinent relationships between the perpetrators and the frauds they committed: lack of segregation of responsibilities, placing undeserved trust in key employees, imposing unrealistic goals, and operating on a crisis basis were all pressures or weaknesses associated with fraud.

Sutherland (1983) believes that learning of criminal behavior occurs with other people in a process of communication. A learning process involving two specific areas: the techniques to commit the crime, and the attitudes, drives, rationalizations, and motives of the criminal mind. Recently, Conner (Conner 2003) explores the existence of this relationship between referent selection and the changing nature of organizations; this relationship potentially undermines how members of VOs form judgments and make decisions, and how performance measures and incentives affect motivation and performance.

Hollinger and Clark (1983) also suggest that every employee can be tempted to steal from his employer - motivations and opportunities seem to be interactive: the greater the economic need, the less weakness in internal controls is needed to accomplish the fraud; the greater the weakness in controls, the less motivational need (Bologna and Lindquist 1995). The theory assumes that people are greedy and dishonest by nature. Ample anecdotal and empirical evidence also indicates that this human factor is the weakest link in occupational fraud (Hecht and Murphy 2000).

Because the virtual work environment may expose the organization to an increased risk of occupational fraud, the need exists for a model of how trust and control can reduce the risk of occupational fraud.

TOWARD A MODEL OF CONTROLLING OCCUPATIONAL FRAUD IN THE VIRTUAL ORGANIZATION

Built upon prior theories of occupational fraud, our model (Figure 1) examines the risk of occupational fraud in virtual organizations. Our model suggests that the same features of VOs that enable the benefits also exacerbate the conditions for occupational fraud; this, in turn, decreases the benefits of VOs. Our model suggests that control and trust can affect the risk of occupational fraud because a member in a VO can trust another member, if membership is valuable financially, socially, and emotionally and any violation, e.g., fraud, will risk the membership.

Increasingly Common Virtual Work Relationships

VOs are different from traditional organizations. Prior research examines various characteristics of VOs (e.g. Bultje and Wijk 1998; Larsen and McInerney 2002), including geographical dispersion, a network of independent organizations, semi-stable relationships, etc. As shown in Figure 1, we believe that VOs are fundamentally different from traditional organizations in terms of geographical dispersion, information substitution and computer-mediated communication.

- Geographical dispersion: Whereas partnerships in traditional organizations rely on co-locating staff, VOs avoid this by using information technology (Larsen and McInerney 2002). Virtual teams require their members to rely heavily on the use of information technology to overcome limitations of time and/or location.
- Information substitution: In VOs, the flow of information at least partially substitutes for the flow of physical business processes in traditional organizations. Information gathering/sharing enables the gathering and tracking the customers' personal and members' organizational information. Information technology provides powerful new capabilities such as surveillance, monitoring, and data warehousing and mining.
- Computer-mediated communication: In VOs, computer-mediated communications replace interpersonal interactions in traditional organizations, raising issues of computer efficacy and the absence of interpersonal connections. IT transforms relationships between people, depersonalizing human contact and replacing it with nearly instant, paperless communication.

VOs have benefits over traditional organizations. Virtual organizations have been credited with requiring less capital, having less overhead expense, being able to utilize technology from various sources, being more entrepreneurial, and being able to act more quickly (Markus and Agres 2003). Our model expects that the VO's features (i.e. geographical dispersion, information substitution and computer-mediated communication) are positively associated with the VOs' benefits.

Proposition 1: In VOs, geographical dispersion, information substitution and computer-mediated communication will increase the benefits of VOs.

Risk of Occupational Fraud Caused by Virtual Organizations

Based on Cressey (1973)'s classical model of occupational fraud, our model also suggests that occupational fraud in VOs consists of motivation, opportunity, and rationalization. Our model expects that the VOs' features (i.e. geographical dispersion, information substitution and computer-mediated communication) will increase the risk of occupational fraud because these features result in the fragmentation of control and of responsibility. These features can lead to a reduced ability of people to control systems and to the placing of unquestioning, blind trust in technology. The opportunities for accidental misuse or intentional abuse become greater.

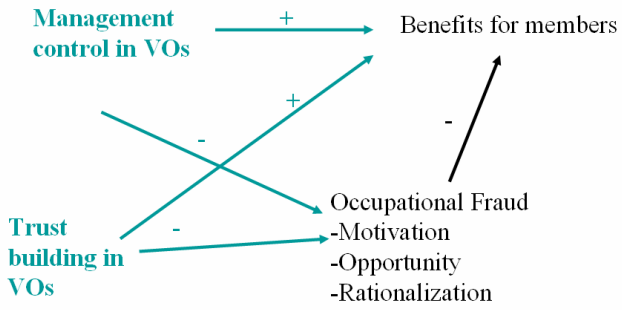
Proposition 2: In VOs, geographical dispersion, information substitution and computer-mediated communication will increase occupational fraud.

Proposition 3: In VOs, occupational fraud will decrease the benefits of VOs.

Controlling Occupational Fraud in Virtual Organizations

Our model (Figure 2) suggests that controls can be employed to reduce the risk of occupational fraud. In examining control in the workplace, we build upon the considerable body of knowledge generated about the theories of crime causation. Based upon our review of the literature, we propose a preliminary framework that suggests control in the workplace consists of both formal and informal social controls. Formal controls

Figure 2. A Model of Fraud Control in VO



can be described as external pressures that are applied through both positive and negative sanctions, i.e., the Theory of Differential Reinforcement (Akers 1977). Informal controls consist of the internalization by the employee of the group norms of the organization, i.e., the Social Control Theory (Hirschi 1969). Several researchers have concluded that informal controls provide the best deterrent. Hollinger and Clark (1983) pointed out that companies with a strong policy against absenteeism have less of a problem with it. As a result, they expect policies governing employee fraud to have the same impact. Formal organizational controls provide both good and bad news. A traditional business organization is full of checkpoints and control systems that are evidence of a lack of trust (Hacker and Mason 2003). However, organizations need to rethink the manner in which these principles are implemented in the virtual organization as there are negative effects of checkpoints and control systems on employees in the virtual environment (Knights, Noble et al. 2001). Overly stringent monitoring can defeat the flexibility and sense of personal control that the virtual organization is supposed to foster. If the result is damaged company loyalty and morale, that can have undesirable consequences such as economic loss and the potential for unethical behavior (Furnell and Dowland 2000).

Researchers have also examined the perception of control, not necessarily the reality of employees being caught if they committed a fraud. Hollinger and Clark (1949, 1983) conclude that informal social controls provide the best deterrent. More recently, and perhaps more importantly, is the conclusion that fraud and work place deviance are in large part a reflection of how management at all levels of the organization is perceived by the employee (Beasley, Carcello et al. 1999). This supports the notion that the greatest deterrent is the idea that an employee will be caught, not the threat of punishment by his employer. Creating an ethical climate may be the answer to workplace deviance and clearly worth further attention.

Proposition 4a: In VOs, formal controls will decrease occupational fraud.

Proposition 4b: In VOs, informal controls will decrease occupational fraud.

Control (e.g. electronic monitoring), however, can be counterproductive, because one of the advantages of VOs that employees really value is the flexibility they have in their workplace (Larsen and McInerney 2002). Therefore, if we are to enjoy the benefits of the VO, we will have to rediscover how to run organizations based more on trust than on control (Handy 1995).

It is not easy but it is possible to build trust within VOs. The difficulty arises because members in a VO may be brought together for temporary projects only, they may never meet face-to-face, and they may not have ever worked together before. However, it is still possible for members in a VO to develop high level of initial trust due to institution-based trust and the disposition to trust (McKnight, Cummings et al. 1998).

Our model expects that trust building in VOs will decrease occupational fraud. First, compared to a distrusted person, a trusted person has less motivation to commit fraud, and he is less likely to explore the opportunities for occupational fraud. Second, a member of a VO usually makes a rational choice on whether to behave in a trustworthy manner or not based on his conscious calculation on the advantages and disadvantages of trustworthy behaviors. Usually a member joins a VO to achieve certain goals, thus the VO membership should be valuable for the member. When membership of VOs is valuable financially, socially, and emotionally and when occupational fraud will risk the membership, the VO member will have reduced motivation to commit occupational fraud.

Proposition 5: In VOs, building trust will decrease occupational fraud.

RESEARCH IMPLICATIONS AND CONCLUSIONS

Our primary conclusion in this article is that VO's can lead to an unintended high risk of occupational fraud, which will decrease the benefits brought by the VO. The conditions that are conducive to the creation and maintenance of a VO are the same conditions that increase the vulnerability of an organization to occupational fraud.

Our distinction between the benefits and risks of the VO raises important issues that merit further conceptual and empirical work. That virtual organizations vary on dimensions of temporal and geographic distribution, lifecycle and member roles, creates organizational and leadership challenges. An important contribution can be made from research addressing the distinguishing characteristics for different forms of virtual organizations and the types of fraud they are susceptible to. Obviously, there is a need for research that investigates organizations across the typology of virtual organizations and frauds. This has the most relevance to elaborating the understanding whether control or trust building will reduce the different types of occupational fraud.

Significant empirical work is needed in order to obtain evidence regarding the propositions we make in this article. First, reliable and valid instruments reflecting the constructs should be developed and then used to test the various subsets of the model. Second, the models interactive effects should be tested. In the next phase, we plan to empirically test the models by utilizing surveys or experiments.

REFERENCES

(Due to the word limit, the reference list is abridged. The complete reference list is available upon request)

Akers (1977). Deviant behavior: a social learning approach. Belmont, Wadsworth Publishing Company**:** 425.

Albrecht, W. S., G. Wernz, et al. (1995). *Fraud bringing light to the dark side of business.* Burr Ridge IL, Irwin.

Beasley, M. S., J. V. Carcello, et al. (1999). "COSO's new fraud study: What does it mean for CPA's." *Journal of Accountancy* 187(5): 12-13.

Bologna, G. J. and R. J. Lindquist (1995). *Fraud auditing and forensic accounting.* New York, John Wiley & Sons.

Brief, A. P., J. M. Dukerisch, et al. (1996). "What's wrong with the Treadway Commission Report?..." *Journal of Business Ethics 15*(2): 183-198.

Bultje, R. and J. V. Wijk (1998). "Typology of virtual organisations, based on definitions, characteristics and typology." *Virtual-Organization.net Newsletter 2*(3): 7–21.

Burgers, W., C. W. Hill, et al. (1993). "A theory of global strategic alliances..." *Strategic Management Journal 14*(6): 419.

CICA (1996). *Audit implications of EDI: An audit technique study.* Toronto, CICA.

Conner, D. S. (2003). "Social comparison in virtual work environments…" *Journal of Occupational and Organizational Psychology 76*: 133.

Cressey, D. R. (1973). Other People's Money: A Study in the Social *Psychology of Embezzlement.* Montclair, Patterson Smith.

Daboub, A. J. (2002). "Strategic alliances, network organizations, and ethical responsibility." *S.A.M. Advanced Management Journal 67*(4): 40.

Examiners, A. o. C. F. (2004). Report to the nation on occupational fraud and abuse. Austin TX, ACFE.

Fitzpatrick, W. M. and D. R. Burke (2000). "Form, functions, and financial performance realities for the virtual organization." *S.A.M. Advanced Management Journal 65*(3): 13.

Fitzpatrick, W. M. and D. R. Burke (2003). "Competitive intelligence, corporate security and the virtual organization." *Advances in Competitiveness Research 11*(1): 20.

Furnell, S. M. and P. S. Dowland (2000). "A conceptual architecture for real-time intrusion monitoring." *Information Management and Computer Security 8*(2): 65-75.

Gallivan, M. J. (2001). "Striking a balance between trust and control in a virtual organization: a content analysis of open source software case studies." *Information Systems Journal 11*: 277-304.

Hacker, K. L. and S. M. Mason (2003). "Ethical gaps in studies of the digital divide." *Ethics and Information Technology 5*(2): 99.

Handy, C. (1995). "Trust and the virtual organization." *Harvard Business Review 73*: 40–50.

Hecht, K. and C. Murphy (2000). Current computer security threats to american business: A high level review. *DIA/FBI/NSA Joint Commission on Technology Protection.* Santa Clara.

Helms, M. M., L. P. Ettkin, et al. (2000). "Shielding your company against information compromise." *Information Management and Computer Security 8*(3): 117-130.

Hirschi (1969). *Causes of Delinquency*. Berkeley, University of California Press.

Hollinger, R. C. and J. P. Clark (1983). *Theft by employees.* Lexington MA, Lexington Books.

Hopwood, W. S., D. Sinason, et al. (2000). "Security in a web-based environment." *Managerial Finance 26*(11): 42.

Kerwin, K., M. Stepanek, et al. (2000). "At Ford, e-commerce is job 1." *Business Week*: 74-78.

Knights, D., F. Noble, et al. (2001). "Chasing shadows: Control, virtuality and the production of trust." *Organization Studies 22*(2): 311.

Larsen, K. R. T. and C. R. McInerney (2002). "Preparing to work in the virtual organization." *Information & Management 39*(6): 445-456.

Markus, M. L. and B. M. C. E. Agres (2003). "What makes a virtual organization work?" *MIT Sloan Management Review 42*(1): 13.

McKendall, M., B. DeMarr, et al. (2002). "Ethical compliance programs and corporate illegality: Testing the assumptions of the corporate sentencing guidelines." *Journal of Business Ethics 37*(4): 367-383.

McKnight, D. H., L. L. Cummings, et al. (1998). "Initial Trust Formation in New Organizational Relationships." *Academy of Management Review 23*(3): 473-490.

Morris, S. A., T. E. Marshall, et al. (2002). "Impact of user satisfaction and trust on virtual team members." *Information Resources Management Journal 15*(2): 22.

Shaneley, A. and C. Crabb (1998). "Corporate espionage no longer a hidden threat." *Chemical Engineering 105*(13): 82.

Sutherland, E. H. (1983). *White Collar Crime: The uncut version.* New Haven CT, Yale University Press.

Warren, M. and W. Hutchinson (2000). "Cyber attacks against supply chain management systems." *International Journal of Physical Distribution and Logistics Management 30*(7/8): 710-716.