Social Embeddedness and Sharing Security Information: Bridging the Cost Benefit Gap

Sigi Goode
School of Accounting and Business Information Systems, College of Business and Economics, The Australian National University, sigi.goode@anu.edu.au

David Lacey
School of Accounting and Business Information Systems, College of Business and Economics, The Australian National University

Follow this and additional works at: http://aisel.aisnet.org/acis2009

Recommended Citation
http://aisel.aisnet.org/acis2009/39

This material is brought to you by the Australasian (ACIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ACIS 2009 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.
Social Embeddedness and Sharing Security Information: Bridging the Cost Benefit Gap

Sigi Goode
David Lacey

School of Accounting and Business Information Systems
College of Business and Economics
The Australian National University
Email: sigi.goode@anu.edu.au

Abstract
Firms may collaborate in order to mitigate security risks. However, prior economic arguments about the benefits and costs of sharing security information appear inconsistent. This paper uses social embeddedness to explain how restricted approaches to information sharing support inter-firm trust, problem-solving and collaboration while unrestricted sharing approaches can obstruct relationship-building. This social embeddedness perspective is supported using a case study of a large Asia-Pacific telecommunications provider. The results demonstrate the benefits of sharing security information with competitors. Empirically, investigations involving both internal and shared information have lower exposure and loss rates than cases where only internal controls are used. The study raises implications for both theory and practice.

Keywords: Embeddedness, Sharing, Fraud, Control, Social, Competition, Telecommunications

INTRODUCTION
Security continues to be a problem for the modern firm, with recent estimates of US$25 billion in costs of security breaches and other threats (Gal-Or and Ghose 2005). Firms may collaborate to mitigate these threats. However, prior rational economic arguments with respect to information sharing seem inconsistent. For instance, on one hand some governments have created formal sharing hubs, notably to mitigate terrorist threats, whereby member firms benefit from periodic vulnerability updates. Examples include Information Sharing and Analysis Centers (ISACS) (Sveen et al. 2007), Computer Emergency Response Teams (CERT) (Gal-Or and Ghose 2005). Yet, on the other hand, some argue that firms should keep security measures, processes and intrusions secret, especially from likely competitors (Gordon and Loeb 2001, Sheng et al. 2005). The risks of disclosure include adverse market reactions both to the original firm (Hausken 2007) and to other firms in the same industry (Cavusoglu et al. 2004), and a loss of confidence from both customers and governments (Gal-Or and Ghose 2005). Even if firms did share information, Gordon et al. (2003) argue that market free riders will exhaust any benefit from sharing.

This paper disentangles this debate by framing prior discourse in terms of social embeddedness. The paper theorises that when a firm can control the groups with whom it shares security information, it can build trust between its interorganisational partners and this leads to the net benefits that have been theorised in the literature. However, when the firm cannot restrict the recipients of its security information, it loses familiarity with trading partners, no trust develops, and this leads to the theorised (and demonstrated) net costs of information sharing. To provide empirical support for these benefits, the paper uses a case study of a large telecommunications firms in the Asia-Pacific region, using access to two years’ worth of both customer fraud data and the relevant case investigation files. Analysis of this archival data was supplemented by semi-structured interviews with the firm’s security and fraud manager and investigators over the life of the project. This paper contributes to knowledge by providing some of the first empirical evidence of the benefits of sharing security information. The paper hence informs ongoing debate about the relative benefits of sharing or concealing security information (such as Hu et al. 2007). The paper also informs on the social dimension of security controls, answering calls from Im and Baskerville (2005) and Dhillon and Backhouse (2001).

This paper is structured as follows. The next section reviews the sharing literature to develop a theoretical foundation for enquiry. This is followed by a discussion of the study’s case research method and approach. The paper then evidence of each of the three structural antecedents of social embeddedness. This is followed by implications for both theory and practice.
SECURITY INFORMATION SHARING AND SOCIAL EMBEDDEDNESS

Firms may collaborate in order to address significant, organised and adaptive threats. Restricted sharing arrangements allow firms to choose how they share information. Unrestricted sharing requires firms to disclose security incidents to investors and market regulators. While there may be economic benefits to sharing, security information is delicate, so trading in it is also dangerous. Because the threat environment can be nimble, security information can also be unpredictable. In an attempt to unravel this problem, we first conducted a literature search for all papers that critically examined security information sharing, as shown in Table 1. Papers were coded by the authors, and two other senior staff verified the coding.

Table 1. Prior Literature in Security Information Sharing, Disclosure and Announcement

<table>
<thead>
<tr>
<th>Type of Sharing</th>
<th>Citation</th>
<th>Context</th>
<th>Method</th>
<th>Costs</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted sharing (inter-firm sharing and notification)</td>
<td>Schoechter and Smith (2003)</td>
<td>Attack prevention in Computer Networks</td>
<td>Economic models</td>
<td>• Increased vulnerability</td>
<td>• Shapers improve security reputation</td>
</tr>
<tr>
<td></td>
<td>Gordon et al. (2003)</td>
<td>Computer security</td>
<td>Economic models</td>
<td>• Free riders don't contribute</td>
<td>• Increases knowledge of shapers</td>
</tr>
<tr>
<td></td>
<td>Slagell and Yurek (2005)</td>
<td>Network intrusion</td>
<td>Framework design</td>
<td>• Privacy concerns</td>
<td>• Reduced spending for each firm</td>
</tr>
<tr>
<td></td>
<td>Slagell et al. (2005)</td>
<td>Network intrusion</td>
<td>Software design</td>
<td>• May also inform attackers</td>
<td>• Increase in total welfare</td>
</tr>
<tr>
<td></td>
<td>Hausken (2007)</td>
<td>Cyber attacks</td>
<td>Game theory</td>
<td>• Attackers are better informed</td>
<td>• Knowledge of attack vectors</td>
</tr>
<tr>
<td></td>
<td>Boeyen (2007)</td>
<td>Financial fraud</td>
<td>Framework design</td>
<td>• Free riders</td>
<td>• Better training and learning</td>
</tr>
<tr>
<td></td>
<td>Burststein (2007)</td>
<td>Network intrusion</td>
<td>Theoretical</td>
<td>• Cost of data preparation</td>
<td>• Vulnerability identification</td>
</tr>
<tr>
<td>Unrestricted sharing (disclosures and announcements)</td>
<td>Cavusoglu et al. (2008)</td>
<td>IT Security investment</td>
<td>Game theory</td>
<td>• Insight into hacker behaviour</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hsin et al. (2005)</td>
<td>Collaborative Network Defense</td>
<td>Software design</td>
<td>• Privacy concerns</td>
<td>• Improved detection understanding</td>
</tr>
<tr>
<td></td>
<td>Zhao et al. (2008)</td>
<td>Internet security</td>
<td>Game theory</td>
<td>• Communications overhead</td>
<td>• Promotes security standards</td>
</tr>
<tr>
<td></td>
<td>Gal-Or and Ghose (2005)</td>
<td>Information security breaches</td>
<td>Game theory</td>
<td>• Increased product demand</td>
<td>• Useful for discovering coordinated attacks</td>
</tr>
<tr>
<td></td>
<td>Li and Rao (2007)</td>
<td>Software vulnerability</td>
<td>Empirical archival (1,570 incidents)</td>
<td>• Possibility of social loss</td>
<td>• Improved bug fixing</td>
</tr>
<tr>
<td></td>
<td>Freeman (2007)</td>
<td>Software vulnerability</td>
<td>Case study</td>
<td>• Adverse publicity</td>
<td>• Cost sharing between firms</td>
</tr>
<tr>
<td></td>
<td>Arora et al. (2006)</td>
<td>Software vulnerability</td>
<td>Empirical archival (2,952 incidents)</td>
<td>• Increased vulnerability</td>
<td>• Improved product quality</td>
</tr>
<tr>
<td></td>
<td>Arora and Telang (2005)</td>
<td>Software vulnerability</td>
<td>Economic model and case study</td>
<td>• Increased attacks</td>
<td>• Improved product quality</td>
</tr>
<tr>
<td></td>
<td>Arora et al. (2008)</td>
<td>Software vulnerability</td>
<td>Economic models</td>
<td>• Signals system vulnerability to attacker</td>
<td>• Increased awareness</td>
</tr>
<tr>
<td></td>
<td>Johnson (2008)</td>
<td>P2P File Sharing</td>
<td>Empirical archival (30 banks)</td>
<td>• Availability of confidential information</td>
<td>• Increases vulnerability awareness</td>
</tr>
<tr>
<td></td>
<td>Ghose and Rajan (2006)</td>
<td>Information security investment</td>
<td>Economic models</td>
<td>• Compliance costs</td>
<td>• Improves software quality</td>
</tr>
<tr>
<td></td>
<td>Campbell et al. (2003)</td>
<td>Information security breaches</td>
<td>Event study (43 incidents)</td>
<td>• Loss of market value</td>
<td>• Greater accountability</td>
</tr>
<tr>
<td></td>
<td>Telang and Wattal (2007)</td>
<td>Software vulnerability and Market Reaction</td>
<td>Event study (147 incidents)</td>
<td>• Loss of market value</td>
<td>• Control vulnerability identification</td>
</tr>
</tbody>
</table>

The table makes clear the competing views regarding the relative merits and drawbacks of externalising security information. Studies in Table 1 are sorted according to the type of sharing studied. By grouping prior work according to their implied interpretation of sharing, it can be seen that prior debate about the costs and benefits of sharing may have been due to varied interpretations of externalising security information itself. On one hand, restricted approaches to externalising security information, such as external and internal sharing, seem to suggest
a majority of benefits. On the other hand, studies of unrestricted approaches, such as disclosure and market announcements, seem to suggest a balance of costs. In other words, prior studies have held that restricted sharing should yield benefits, while unrestricted forms of sharing, such as disclosure, are costly.

We propose that purely economic perspectives do not fully explain these circumstances. For example, transaction cost approaches emphasize bargaining behaviour between buyers and sellers, such that self-interest compels opportunistic trading (Ghoshal and Moran 1996). Yet, in the short term, buyers and sellers cannot be sure of the value or relevance of security information before they have seen it. Game theoretic approaches have seen frequent application to these information sharing arrangements. However, the theoretical position that game players will defect against other information suppliers is inconsistent with the theoretical benefits to restricted sharing seen in Table 1. If actors do defect because of costs in the current period, they are unable to build the inter-organisational relationships that could give them insight into future costs and benefits. Without maintaining close relationships with other firms, organisations also can not know the value of their own security information in isolation.

In contrast, social embeddedness offers a possible explanation for why restricted sharing yields greater benefit than unrestricted sharing. Under this perspective, inter-organisational behaviour is underpinned by social interaction and relationships (Uzzi 1997). Instead of calculating returns to transactions based on punctuated self-interest and short term economic rents, firms prefer long term cooperation based on interpersonal ties (Dore 1983, Romo and Schwartz 1995). This relationship building provides a number of benefits to the firm. Over time, firms engage in repeated problem solving activities, build trust, and encourage greater collaboration (Chatfield and Yetton 2000). These “value constellations” (Lee 2001) deliver benefits to trading, the supply chain and operational efficiency (Schopler 1987, Van de Ven 2005, D’Aubeterre et al. 2008). Alternatively, when firms are unable to interact and develop ties, embeddedness will be low. Stable collaboration eludes participants because they do not develop social relations outside conventional economic trades (Granovetter 1985, Rai et al. 2009).

Social embeddedness comprises three main components, each with a set of structural antecedents (Uzzi 1996). First, the capacity to reciprocate actions and support for voluntary relationship contributions leads to trust. Second, face to face interaction and greater use of tacit understanding lead to fine-grained information. Third, collaboration and persistence, as opposed to market exiting behaviour, lead to joint problem solving. Amid these three components, trust acts as the primary overarching structure (Uzzi 1997).

Applying social embeddedness to sharing security information, we posit that restricted sharing should yield benefits because the market participants are able to build trust, transact in fine-grained information, and solve problems together by virtue of closer social relationships. This perspective appears consistent with early empirical evidence from Loch et al. (1992) indicating that respondents perceived little threat from competitors and external networks. However, unrestricted forms of sharing, such as disclosure, are costly because the firm loses control over who receives their security information, and the shared experiences that ordinarily promote collaboration and trust do not form. However, while there is empirical support for the costs of unrestricted sharing, there has been no prior empirical validation of the benefits of restricted sharing. With social embeddedness as a foundation, we use a case study to address this gap.

**RESEARCH METHOD**

Research into fraud is particularly difficult, due to problems of researcher access and trust, problems of identifying subjects and incidents, and the veracity of data itself (Kotulic and Clark 2004). Sensitive to these concerns, our overall research approach was one of careful relationship-building with the participating firm. The case study firm is a foreign owned Australian telecommunications carrier, employing more than 3,000 people. The firm offers a range of hardware products and telecommunications services, sold both by the firm, and through a network of agent dealers spread across the region. These include conventional voice services, such as reverse-charges and international trunk dialling, landline, long-distance and mobile voice communications, as well as data services such as broadband and dialup internet access.

Methodologically, we aimed for both quantitative and qualitative analysis approaches, after Benbasat et al. (1987). In order to best make sense of the phenomena under investigation, we used a number of data sources to build an understanding of the case (Salkind 2003). Unique among these is that the case firm has, where possible, granted us access to their full customer fraud data over a two year period, including case notes made by the investigators themselves. This data provided rich insight into the firm’s investigation processes and controls.

The first stage of the analysis involved data inspection. Textual post-coding was used to investigate and classify the case notes, using coding processes described by Ryan and Bernard (2000). Where confusion or disagreement arose, the opinions of two other researchers were sought. This stage revealed the complex nature of the various fraud types and investigative processes at hand. To make sense of these relationships and principle findings, we
conducted a series of semi-structured interviews with fraud managers during and after the collection of the fraud data, using Yin (2003). These interviews, in concert with documentation, were used to inform and gain insight into the processes in use in the firm (Seidman 1991).

As is the case with many modern firms, this firm takes a structured approach to new customer procedures, using a range of standard general and application controls to verify identity and intention at the account creation stage. These controls include written policies, physical and electronic access devices, user logging, semantic and syntactic data checks, application credit histories and objective identification checks. Importantly, the data analysed in this paper constitutes cases of actual fraud, and not simple bill delinquency. These fraud cases have hence been able to overcome or bypass these static general controls.

**TRUST**

The first component of embeddedness, trust, relates to the belief that exchange partners do not act in self-interest at another partner’s expense (Uzzi 1997). Our analysis first illustrates the importance placed on interpersonal and inter-organisational relationships in the security function. First, with regard to extracting value from control networks, the interviewees couched their operations in terms of providing high profile, identifiable business value to the firm and, interestingly, to external groups. The ability to deliver clear benefit was critical in order to effectively convince senior management to fund ongoing and expanded activities. One senior investigator noted,

“Time is a critical factor in our work, in terms of time to detect and time to confirm the suspicion of fraud, and subsequent action to suspend the account”

In this context, maintaining an unworkable institutional control was not viable and could contribute adversely to the fraud unit’s reputation and value effectiveness. In their own judgment of what controls most effectively responded to the criminality confronting the organisation, the interviewees were unified in their belief in the value of a networked and combined approach. When prompted on this aspect, the manager stated,

“As our performance measures indicate, we are much more superior in both preventing and detecting fraud against the company where we have access to information from within and outside the company”.

This finding is a key departure from prior literature, in that within the case study firm, and among some other firms the telecommunications industry, fraud control is not solely an internalised process. A networked approach to mixed control deployment was integral to disrupting criminal behaviour, with a senior investigator stating,

“Criminals could be stopped overnight if both government and private victim organisations talked about what they are seeing. The crooks rely on the blindness of victim organisations as a winning strategy in their endeavours”

The interviewees were also prompted to comment on the balance between competition and collaboration. The case study organisation depends on competitors, banks, credit reference authorities and other external sources of information for both prevention and detection control purposes. In particular, competitors could provide a rich source of information on potential and actual fraud cases. Expanding on this finding, the manager stated,

“The scary thing is that to do this [fraud response] job effectively, we actually rely upon the good work of our competitors in the industry. Likewise, these same competitors rely on us”

As an example of the important role played by competitors, the senior investigator provided the example of call selling operations, stating,

“With call selling, where an organised crime group obtains ten, twenty, or more mobiles and some landlines, then on-sells these to their criminal network or let’s say their community of interest to disrupt law enforcement, they tend to operate a pretty complex network of phones involving many carriers. These operations hit the industry hard, often with great speed and little warning. We have controls in place that detect part of the picture, for example high billing or hot destination flags, but to get enough of the picture, we need other industry members”.

While competitors could benefit from sharing fraud and security information, non-shareers could be effectively penalised. The manager revealed that, “it becomes known throughout the industry quite quickly who’s playing ball and who’s not. It can work the other way, you know”. This comment highlights the potential costs of not sharing fraud information between firms, and it suggests that non-sharing firms may become victims of fraud before they have a chance to develop appropriate controls and counter-measures.

The interviewees saw rich, informal systems partly as a panacea for, and a reaction to, the significant time taken for the firm to develop appropriate formalised security controls. While formalized controls could be effective, the criminal element could quickly develop new methods to overcome them. As a partial response to this sluggishness, security champions inside the firm had created informal interpersonal networks, sometimes based
on personal contacts at other institutions. The manager noted, “I just run the show, my staff do all the work”. In this context, the interviews also informed the possibility that different investigative approaches among industry members was a strength, and not a weakness. Varying institutional controls coupled with ‘home-grown’ security controls could make systematic fraud harder. For example, the manager noted, “Although to some extent we rely upon each other for information on suspected fraud, we don’t know too much about how each telco actually structures and undertakes their fraud function. That part of what we do I guess is still entrenched within the ‘competitiveness’ of industry”.

This suggested that widespread adoption of ‘industry best practice’ could, in some cases, actually work against identifying fraudulent activity because each firm conducts their analyses in the same way, with the same data.

**FINE-GRAINED INFORMATION**

The second component of embeddedness, fine grained information, relates to the use and exchange of tacit and proprietary information with related firms. This second stage of the analysis illustrates the extraction and employment of fine-grained information to mitigate fraud threats, exploring the relation between the fraud types faced by the firm, and the controls used to detect this fraud. Figure 1 gives an overview of the types of fraud seen in the case firm. Howard’s (1997) taxonomy is used, describing the tools (the point of origin), access (the facilitating or enabling functions involved) and results of fraud (the ensuing fraud types and their degree of technical sophistication).

**Figure 1: Fraud Tools, Access and Results**

First, the tools or initiating points of fraud in the case data comprised identity fraud, identity theft, no direct interface, and the perpetrator’s actual identity. Consistent with Brenner (2004), identity theft was defined as the theft of a real person’s identity, living or dead, such as their name, date of birth, or a combination of both that would lead to the association of the fraud with an innocent third party. Identity fraud was defined as the use of a fictitious identity that could not be attributed to an innocent third party (whether this third party existed or not). The case data also featured instances where no direct interface occurred, whereby the system was compromised without the perpetrator having direct contact with the firm. Examples of this included stolen handsets and mobile broadband dongles, possibly in order to obtain credit card details from merchants and banks as a pre-cursor to credit card fraud. Finally, in some cases, the perpetrator did not conceal their identity when committing the fraud.

Accesses were the points of direct engagement that enabled or facilitated the fraud with respect to the firm. The first was Subscription, where the perpetrator committed the fraud by direct application to the firm. Channels can include website applications, mail, retail outlets and dealers (where the dealer is not suspected of intentionally facilitating the fraudulent application). The second was the Dealer, where resellers and agents intentionally facilitate or originate fraudulently acquired products and services. The third access was Internal fraud, where an employee of the case study firm facilitated or originated the fraud. The fourth access was Infrastructure, whereby a perpetrator had obtained direct physical access to communications or data services without having to interact with the carrier’s application or customer account environment.
Results ranged from relatively straightforward thefts of phone handsets to sophisticated crimes such as call selling. Here, a perpetrator with a fraudulent identity applies for a mobile phone, who then uses this phone to sell international communications services to others without charge (particularly to ‘hot destination’ countries that are likely to be monitored by law enforcement). Although the precursor fraud may be subscriber or dealer fraud through the use of identity fraud, the on-use of these services relies techniques to conceal normal call patterns. For example, in some of the high-toll frauds detected by the firm, the call selling group would route their international calls via pre-defined satellites that disguise normal caller patterns. Perpetrators may also exploit billing cycles, reducing the effectiveness of account payment controls. In addition to these frauds against the carrier’s systems, each of these frauds could also be part of a larger fraud on a different organisation. For example, a customer may aim to establish a credible history with the carrier so as to build another identity (perhaps with which to acquire a credit card at another firm). In this regard, the firm can be at once a victim, an accessory and an instrument to fraud.

The next stage of the analysis explored the organisational response use of information and understanding to the fraud environment. The first coding pass revealed 35 primary controls. This list was subsequently distilled down to 17 controls. Table 2 shows the full list of controls and their observed attributes.

Table 2. Fraud Controls Used in the Case Firm

<table>
<thead>
<tr>
<th>Internal Controls</th>
<th>Preventive (P) Detecte (D)</th>
<th>Institutional (I)</th>
<th>Automatic (A) Diskretionary (D)</th>
<th>Initial (I) Subsequent (S)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dealer Audit</td>
<td>B I D B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Associated Accounts</td>
<td>B I A B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fraud Database Check</td>
<td>B I A B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Hot Destination Flag</td>
<td>D I A B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High Tolling Flag</td>
<td>D I A B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bill Return to Sender</td>
<td>D I A B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Point of Application Referral</td>
<td>P I A B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Billing Department Referral</td>
<td>D I A B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Uncontactable</td>
<td>B N D B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Contacted – Suspicious</td>
<td>B N D B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>External Controls</td>
<td>Preventive (P) Detecte (D)</td>
<td>Institutional (I)</td>
<td>Automatic (A) Diskretionary (D)</td>
<td>Initial (I) Subsequent (S)</td>
</tr>
<tr>
<td>Credit Report</td>
<td>B I A B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Customer Detection of Identity Theft</td>
<td>D N D B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carrier Alert</td>
<td>B N D B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Banking Alert</td>
<td>B N D B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Law Enforcement Enquiry</td>
<td>B N D B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employer Check</td>
<td>B N D B</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other (e.g. “Tip Off”)</td>
<td>B N D B</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The textual coding process proved very useful in the initial analysis. It allowed the researchers to review not only the function of the controls, but also the information contexts in which the controls were used. First, controls were either internal to the firm, or external to its operations. A significant number of fraud cases were identified or solved using notice and information from external groups, such as banks, law enforcement or, interestingly, other telecommunications firms. Second, for each case, there was a single originating system control that began the investigation process. For some types of fraud, one or more subsequent controls were then used in the evidence-gathering process. For complicated fraud, such as identity theft, these subsequent controls were instrumental in building the chain of evidence eventually leading to remedy. Third, in addition to the formal control methods used to detect and investigate fraud, a number of informal controls were used. For example, in one case an investigator had built a relationship with another staff member, who periodically notified that investigator of suspicious accounts, customers or dealers. Close working relationships between investigators allowed them to share ‘hunches’ that formal technical controls could not otherwise pick up (such as identifying particular customer accents, mis-spellings of surnames or familiar residential addresses). Fourth, not all controls were invoked for each case. Many cases apprehended with zero loss and exposure were identified using automatic screening controls shortly after the account creation stage. However, other controls were invoked on a more discretionary basis. An example of this is the dealer audit control, which could be instigated if a particular dealer had triggered another control (such as a high spending alert or a billing alert).
JOINT PROBLEM SOLVING

The third component of embeddedness, joint problem solving, describes the firm’s ability to coordinate problem-solving activities with other external actors. We first illustrate how the controls discussed in the previous section are used together to effect a fraud control outcome. We then present empirical evidence of how external information sharing is beneficial to the firm. The controls presented in the previous section were frequently used in concert to produce an effective system defence. Figure 2 shows examples of the combinations of controls that can be used in the investigation process.

![Table](http://example.com/table.png)

Analysis was then conducted to determine whether there was any financial advantage of collaborating with external groups in the investigation process. Of the 3247 cases, 2880 cases exhibited positive financial losses. A Two Way Analysis of Variance (ANOVA) was conducted on the cases involving these positive losses. Positive Exposure was used as a covariate. Table 3 shows the descriptive statistics for the controls and fraud types featured in the data set. Table 4 shows the results of the ANOVA tests. The testing revealed several interesting phenomena with regard to Control Type, which exhibited a main significant effect with an F statistic of 14.742. Regardless of Fraud Type, mean losses were lowest when both internal and external controls were used.

![Table](http://example.com/table.png)

![Table](http://example.com/table.png)
With regard to Fraud Type, Identity Fraud is by far the most common with 2348 cases exhibiting positive losses. The least common Fraud Type was Identity Theft, but also one of the most complex to execute. The mean values show that seven cases of Identity theft were detected by internal controls alone, but 20 were detected solely by external parties, before the firm’s own internal systems. The most effective control method for identifying Identity Theft was the use of both internal and external controls in the investigation process. This evidence suggests that firms in the sharing network are better off than the otherwise similar firms who operate alone.

The value of external sharing networks is also evident in detecting Identity Theft cases solely by external controls. Mean losses were highest for Identity Theft discovered by external controls (2328.1). That the firm’s internal controls had not identified these cases suggests that perhaps the offenders had developed systematic ways of evading apprehension via intimate knowledge of the case firm and its internal systems. External controls may have been able to identify these offenders because these external controls were functionally different to those of the case firm. Predictably, external controls were not frequently used to identify Dealer Fraud: as most dealers are contractually bound to a single telecommunications network provider, it is unlikely that an external entity would be able to reliably observe the internal mechanics of a dealer. Such problems would be best detected by internal dealer audits (of the 410 cases of dealer fraud, 309 were identified by dealer audits).

CONCLUSIONS

Prior literature has conceptualised alternative information sharing postures. This study has contributed to this discourse through advancing theory on the nature and behaviour of operational security controls in a highly competitive and rapidly evolving industry. Using a social embeddedness foundation, this research presented an inter-organisational perspective where practice actually relies on the removal of competitive barriers for successful information system control and security performance. Whereas some prior work has argued that human actors are the least secure point in a system (Perry 1985, Vroom and von Solms 2004, Im and Baskerville 2005), this study indirectly finds that human actors can also be of tremendous advantage in the detection process, particularly when given the benefit of effective information sharing networks. Human actors can provide tacit insight into a fraudulent case, using intuition, memory and ‘gut feeling’ to determine a case’s veracity.

The study may be open to a number of limitations. First, some of the testing in this study was based on observed or detected criminal activity. Such detection may not be perfect and the cases brought to light may exhibit unseen bias. Second, the actual frequency of fraud types may vary from those seen in this paper, as well executed fraud may evade detection. These limitations are likely to affect many empirical fraud studies of this nature.

This study is some of the first work to empirically reveal the benefits of using external and internal controls in the system control ecology. A number of avenues for future work arise. The analysis demonstrated that performance outcomes were enhanced where combinations of controls were employed. Further work on the effect of criminal complexity on control combinations, reliance and performance is required. In particular, future work could examine the extent to which control selection is influenced by collaborative performance level targets and competitive practice. This study also saw evidence of a move away from purely technical solutions to security problems. Echoing the advice of Siponen (2005), more research work into socio-technical and social approaches for identifying risky behaviour would be valuable.

REFERENCES


Salkind, N. J., (2003), Exploring Research, Prentice Hall, New Jersey, USA

Seidman, I., (1991), Interviewing as Qualitative Research, Teachers College Press, New York, USA


Yin, R. K., (2003), Case Study Research Design Methods, SAGE Publications, Los Angeles, USA

COPYRIGHT

[Sigi Goode / David Lacey] © 2009. The authors assign to ACIS and educational and non-profit institutions a non-exclusive licence to use this document for personal use and in courses of instruction provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive licence to ACIS to publish this document in full in the Conference Papers and Proceedings. Those documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors.