Summer 10-6-2011

EXPLORING INFORMATION SECURITY CONTROLS USING INFORMATION FRAUD EPISODES: CASE STUDY EVIDENCE FROM A LARGE TELECOMMUNICATIONS FIRM

Sigi Goode

David Lacey

EXPLORING INFORMATION SECURITY CONTROLS USING INFORMATION FRAUD EPISODES: CASE STUDY EVIDENCE FROM A LARGE TELECOMMUNICATIONS FIRM

Goode, Sigi, The Australian National University, Canberra 0200, Australia, sigi.goode@anu.edu.au

Lacey, David, The Australian National University, Canberra 0200, Australia, david.lacey@anu.edu.au

Abstract

Fraud and security continue to be problems for firms. Fraud information is typically incomplete and deliberately obfuscated. These qualities make fraud events harder to detect using conventional security controls. This study uses a knowledge management framework to explore how different types of controls are used to detect and investigate information fraud.

The analysis is based on the customer fraud database of a large Asia-Pacific telecommunications provider. Semi-structured interviews were also conducted with the firm's fraud unit. The study finds that IS controls, with high task programmability and outcome measurement, are used to detect the majority of fraud cases. However, more complex fraud cases use clan controls for detection. The paper also provides insight into the way in which combinations of controls are used to investigate cases. The study raises implications for both theory and practice.

Keywords: *Information Fraud, Control, Information Sharing, Telecommunications*

1 Introduction

Information fraud is a significant threat to the modern firm and its information systems (Im and Baskerville 2005). Contemporary threats in the digital economy include data theft, extortion and employee and customer fraud. Kallinikos (2005:188) argued that, "electronic 'identity' theft and fraud...are conspicuous unintended consequences brought about by the global interlocking of IT-based systems and artefacts". Estimates of US$25 billion in costs of security breaches (Gal-Or and Ghose 2005) have been offered. For these reasons, information fraud and security remain key topics on the IS research agenda (Ransbotham and Mitra 2009).

One gap in understanding lies in the relationship between fraud controls and fraud information types, and understanding how IS controls are used to detect fraud events. Firms are reluctant to reveal their security models to outside scrutiny, and empirical literature coverage of security controls has been more sparse. Firms tend to under report instances of fraud, for a variety of reasons. Estimating the frequency and cost of incidents is difficult, as firms can be reluctant to disclose breaches out of embarrassment, concerns about market confidence or ignorance. Even if managers can overcome such problems, determining an appropriate level of funding for security prevention can be difficult (Cavusoglu et al. 2004, Bodin et al. 2005). Finally, managers may feel that academic study is too intrusive or untrustworthy to warrant cooperation (Kotulic and Clark 2004). These problems mean that gaining access to relevant incident and response data, if it even exists, is difficult. In addition, most prior work has examined the use of IS controls for the purposes of detecting system malfeasance (such as server intrusions). However, information systems are not used in isolation: rather they are woven into the organisation's operating fabric. We require a better understanding of how these IS controls are used in a business environment to detect information fraud.

Fraud information differs from much other information that is present in the firm in that it may be deliberately incomplete, misleading and uncertain. This paper conceptualises fraud events as knowledge items, with varying levels of codifiability, completeness and diversity. The paper investigates how combinations of controls comprising both IS and organisational controls are used to detect fraud in a business setting. This paper reports on case study research involving a large telecommunications company 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 confirmatory semi-structured interviews with the firm's security and fraud unit. From this case study, we present a series of fraud episodes and illustrate how different controls were used to effect a detection outcome. The study's research question is:

How are IS controls used in the information fraud detection process?

This paper is structured as follows. The next section develops the paper's theoretical frame. This is followed by a discussion of the study's research method and approach. The paper then details the case firm, followed by an analysis of the investigative controls used in the investigation, and the incidences and types of fraud. Semi-structured interviews are then used to review the findings. This is followed by implications for both theory and practice. Finally, conclusions are made.

2 Background

Information fraud describes deception involving falsifying or fabricating information about individuals, identities or transactions, often for direct or indirect commercial gain. It may be executed by individuals (such as customers or employees) or groups (such as firms and organised crime groups). Organisations are inevitable targets of information fraud threats (Zyglidopoulos et al. 2009) because of the heightened internetworking and greater reliance on data collection and processing that characterises modern commerce.

However, fraud is difficult and problematic, for a number of reasons. Fraud is likely to be well-concealed and deliberately obfuscated. The falsification associated with fraud means it can also be difficult to distinguish genuine individuals and transactions from false or fraudulent artefacts. Managers can also be reluctant to admit that information security can affect their firm (Straub and Welke 1998) and they may have difficulty identifying at-risk information and organisational assets (Whitman 2003). Further, the greater the duration of the fraud, the more financial, operational and reputational damage can be done to the firm.

Because these security threats can undermine the functioning of the firm, controls may be used to prevent, extinguish or ameliorate this fraud (Boss et al. 2009). The concept of organisational control has received considerable coverage in the business literature. In the same way that managerial control preserves the financial operations of the firm, so information security controls preserve the mechanics and effectiveness of the firm's information management practices.

From an information security perspective, controls have typically been divided into technical, IS controls and non-technical, humanistic controls (Dhillon and Backhouse 2000). Technical controls are likely to be automated, triggered by or evaluating incoming cases using detection algorithms based on classification, probability and extraordinary behaviour. These IS controls need not rely on significant human intervention or judgement. Non-technical controls, on the other hand, typically involve investigative processes and are often invoked by human investigators. In order to understand how these control systems handle fraud information, we need first to understand the types of fraud information seen in the firm.

3 Information Fraud Events as Organisational Knowledge

Organisational knowledge describes the "provision of organisational histories, knowledge, competencies and skills" (Randall et al. 2001:113). It reflects the various 'understandings' (Feldman and Rafaeli 2002) about the firm, its processes and contents. Managing this knowledge has been seen as integral to organisational strategy and performance because past experiences and understanding may be used to solve current and future problems.

Organisational knowledge has various forms and prior research has worked to describe this knowledge in various ways. One relevant framework is presented in Turner and Makhija (2006). These authors review prior literature and develop three qualities to describe knowledge types, being codifiability, completeness and diversity. Codifiable knowledge is typically well understood and easily articulated. Such knowledge is typically explicit and may be easily broken down into component parts for simpler sharing. Uncodifiable knowledge is less easily related to others: while it may be highly relevant to the organisation, its component parts are less easy to identify and capture. Hence, codifiable knowledge may be easier to distill into direct or unambiguous rules and policies. Uncodifiable knowledge is likely to be harder to solidify in this way.

Completeness reflects the degree of fullness of the knowledge, and whether the knowledge is sufficient and adequate for use. Complete knowledge is not lacking key components and is hence easier to adapt to its intended purpose. Incomplete knowledge, on the other hand, may be missing important aspects. Sufficiently complete information hence supports decision-making, while incomplete information may require the decision-maker to acquire more information in order to make up for the lack of evidence and meaning.

Diversity describes the number and range of concepts that comprise the knowledge. Knowledge with greater diversity may arise from numerous sources and have multiple inter-related meanings and conceptualisations. These meanings may in turn have multiple indicators arising from their various constituent areas of application and origin. Knowledge with low diversity is characterised by fewer competing concepts and meanings: its existing 'understandings' may be shared and agreed upon by the knowledge holders such that the meaning of these parameters is more uniform.

The movement and use of this knowledge is influenced by the organisational controls in place in the firm. These controls guide the processes and routines in use in the firm (Lange 2008, Gopal and Gosain 2010). Typically, these controls are used to preserve the administrative and financial operations of the firm, by governing how information is used and reported. In turn, these controls align the operation of the firm with the organisation's goals and policies. Prior research in the management literature has yielded three categories of controls in use in the firm (Eisenhardt 1985). These are outcome controls, process controls and clan controls. Outcome controls relate to outputs desired by the firm. Process controls describe and guide the processes used in the firm. Clan controls describe informal social processes used among organisational actors. Table 1 describes these three control types in terms of the knowledge descriptors discussed above, yielding the study's research framework.

		Knowledge Descriptors		
Control Type	Control Description	Codifiability	Completeness	Diversity
Outcome	Defines outcomes. Useful where process is hard to prescribe, but desired outcome is known.	High	High	Low
Process	Guides processes. May delineate processes into clearly specified steps and tasks.	High	High	Low
Clan	Used where process is not well known or understood, and outcomes are not easily measureable or are ambiguous.	Low	Variable	High

Table 1. Control Types and Knowledge Descriptors

Because they deal with knowledge that is highly codifiable and complete, outcome and process controls are likely to be more easy to automate than clan controls (which rely more on social interaction and tradition). Accordingly, technical information systems are more likely to support outcome and process controls because of their structured analytical and programmable nature (Ouchi 1979, Eisenhardt 1985). On the other hand, clan controls might not lend themselves well to automation because they incorporate less structured interaction based on custom and opinion.

4 Research Method

Eliciting participation and response sensitive for topics is challenging and can be difficult. Research into fraud is particularly difficult, due to problems of researcher access, trust, identifying incidents, and the veracity of data itself. Accordingly, our overall research approach was one of careful relationship-building with the participating firm, a major telecommunications firm in the Asia Pacific Region. A case study method was appropriate to the research because of the revelatory nature of the participating firm (Yin 2003), whereby access to the research phenomena has hitherto been difficult to acquire. The case study gave us closer proximity to the phenomena at hand and allowed us to examine the interplay between the controls and information items.

Data Source	Purpose
Fraudulent customer and investigation database	Quantitative analysis of fraud and control use
Interviews with fraud managers and investigators	Confirmatory and additional insight into investigation
PowerPoint presentations	Overview of controls in context of business processes
New dealer sign-up forms	Understanding new dealer creation agreements
New customer sign-up documentation	Understanding identification process for new customers

Table 2. Sources of Data

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). The case firm granted us access to their full customer fraud data over a two year period. Table 2 lists the main data sources used in the study. Unique among these is that the case firm has, where possible, granted us access to their customer fraud data over a two year period.

Analysis of the fraud data set proceeded along two fronts. The first stage of the analysis involved a quantitative inspection of the data. For each fraud incident, the data set also contained the case investigation notes made by the fraud investigators themselves. These notes provided rich insight into the firm's investigation processes, and the controls used to detect and subsequently prove fraud cases.

The case files and investigation notes were analyzed using textual post-coding methods (Krippendorff 1980, Weber 1990). The coding was conducted by the authors, with involvement from two fraud investigators at the case firm. A third senior academic checked the coding once it was complete. Each case's investigation notes were open coded, to identify important control concepts. The initial list of controls was then further refined in order to identify links and patterns. Where confusion or disagreement arose, the opinions of two senior researchers were sought. An example of this coding follows, using a small case excerpt. As in Ryan and Bernard (2000), relevant text is underlined and the descriptive factor follows in square brackets.

> *Massive debt on Mob Iraq & Turkey* **[Hot_Destination]** *$2500.00 no rebill yet.* ***[High_Toll_Report]*** *Sent to Cancellations to terminate. Suspect this account is tied to the Box Hill file.*

To make sense of these control relationships, we conducted a series of semi-structured interviews with four fraud investigators at the case firm, and investigators at eight other large financial and telecommunications firms, and a law enforcement unit. We held multiple interviews with each participant, numbering approximately three with each interviewee. These interviews were used to inform and gain insight into the processes in use in the firm (Seidman 1991), in concert with documentation from within the firm. Most interviews were held at the investigators' place of work.

5 The Case Firm

Since 2000 there has been significant growth in demand for telecommunications provision, in particular Internet and mobile services. Worldwide, telecommunications service revenue is more than $US1.7 trillion dollars per year, and growing (ITU 2008). The Asia-Pacific region alone has been one of the world's largest markets, with connection rates of more than three new users every second (ITU 2008). Consequently, the industry is one of significant competition.

The case study organisation is a foreign-owned Australian telecommunications carrier, employing more than 3,000 people. The firm offers a range of hardware products and telecommunications services. These include conventional voice services, such as landline, long-distance and mobile voice communications, as well as data services such as both broadband and dialup internet access. These services are in addition to conventional telecommunications services such as reverse-charges and international trunk dialling. These products and services are sold both by the firm, and through a network of agent dealers spread across the region.

The organisation 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 third party identification checks.

The next section discusses the types of fraud observed. The paper then presents the firm's control methods and structures.

5.1 Types of Fraud

Howard's (1997) process-based threat taxonomy has received considerable use in prior IS literature, and provides a useful basis for exploring fraud in the firm. Howard's (1997) taxonomy was used to frame the tools (the point of origin), access (the facilitating or enabling functions involved) and results of fraud (the ensuing fraud types). Figure 1 depicts the types of fraud seen at the firm.

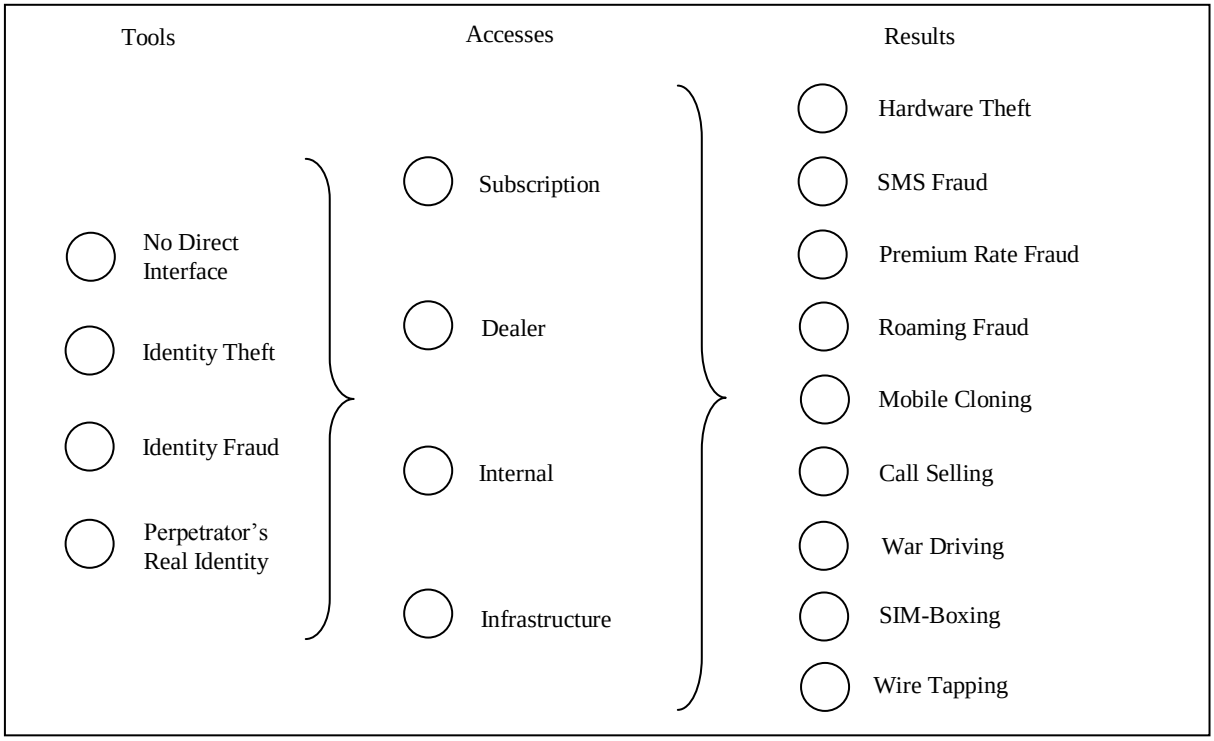

Figure 1: Fraud Tools, Access and Results

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 case study organisation. 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 made no attempt to conceal their real identity when committing the fraud.

Accesses were the points of direct engagement that enabled or facilitated the fraud. 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 of these threats were varied, and highlighted the significant complexity of this 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 destinations', countries that are likely to be monitored by law enforcement groups). Although the precursor fraud may be subscriber or dealer fraud through the use of fictitious or stolen identities, the on-use of these services relies upon a technique that conceals normal call patterns through international communications networks. For example, in some of the high-toll frauds detected by the case study, the call selling group would route their international calls via pre-defined satellites that disguise normal caller patterns. This technique relies on knowledge of communication systems to further distance the real perpetrators of the fraud from their activities. Perpetrators may also exploit billing cycles, thereby 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 a victim, an accessory and an instrument to fraud.

5.2 Types of Security Controls

The next stage of the analysis explored the organisational response to this fraud environment. The first coding pass revealed 35 primary controls. This list was subsequently distilled down to 18 controls. Exploration of the case firm's operational controls revealed that 11 controls used for investigation are deployed for both preventive and detective purposes. With the exception of the *Customer Detection* control, the remaining controls are used for both preventive and detective purposes. Table 3 lists the IS controls and their observed attributes, in the context of the study's research framework. Table 4 lists the non-technical controls.

Control Name	Control Type	Description
Fraud Database Check	Outcome	Matching applicant attributes against fraud database upon initial detection (i.e. not at point of application)
Formal Telco Alert	Outcome	Formal notification from telecommunications retail or network partner
Dealer High Spend	Outcome	Internally generated report based on accounts with high spend/owed amounts were clustered against a dealer
Associated Accounts	Process	This case relates to another investigation that is already in the firm's fraud database
Hot Destination Flag	Process	Monitoring of customer calling activity against international dial codes (e.g. Iran, Syria, Iraq, Sri Lanka, and Pakistan)
High Toll Report	Process	Call usage and account balance alert, generated automatically across the firm's service range and portfolio
Billing Department Referral	Process	Automated referral from billing of suspected fraud based on charge back/rejection of upfront handset
Credit Agency Report	Process	National credit agency credit report at the point of application identifies suspected or proven history of fraud

Table 3. IS-Based Fraud Information Controls Used in the Case Firm

Control Name	Control Type	Description
Customer Uncontactable	Outcome	An investigator in the firm's fraud unit has attempted to contact the suspect, but was unable to make contact
Dealer Audit	Outcome	An ordered investigation into a dealer's affairs and documentation
Bill Return to Sender	Process	Bill has been returned to sender. These may also arrive internally from a 'collections' team to the fraud department
Employer Check	Process	Applicant does not work where stated in application or employer does not exist
Point of Application Referral	Process	Internal email message from frontline applications unit, containing information about suspect applications
Investigator Suspicious	Clan	An investigator within the firm's fraud unit contacted the suspect, but their behaviour was evasive, inconsistent or otherwise suspicious
Customer Detection	Clan	Suspected identity theft victims questioning bill received from the firm, claiming they had not acquired the service. May also involve verification of customer identity (e.g. fax photo and compare against application)
Telco Alert	Clan	Other telecommunications carriers informally share information on suspect persons, groups or organizations
Banking Alert	Clan	Informal group of firms, mostly banks, who distribute information about known or suspected fraudulent customers, behaviours and schemes
Law Enforcement Enquiry	Clan	Police enquiries give an indicator to the firm of persons and groups of interest
Other (e.g. "Tip Off")	Clan	Notification from Telecommunications Industry Ombudsman, or a 'tip off' from an external source

Table 4. Non-technical Fraud Information Controls Used in the Case Firm

5.3 Security Control Structures in Information Fraud Episodes

The data revealed both the function of and the contexts in which the controls were used, and various other dimensional attributes. For each case, there was a single originating control that instigated the investigation process. Most often, this originating control was an IS-based control. For some types of fraud, one or more subsequent controls were then used in the evidence-gathering process. These subsequent controls were instrumental in building the chain of evidence for complicated fraud, such as identity theft, where the fraud information could exhibit significant diversity and incompleteness.

Not all controls were invoked in each case. Many events apprehended without loss were identified using technical IS controls shortly after the account creation stage. However, other controls were invoked on a more discretionary basis. For example, a significant number of fraud cases were identified or solved using information gleaned from other organisations, such as banks, law enforcement and other telecommunications firms. In addition to process and outcome controls, a number of clan controls were used: there were instances where an investigator had built a relationship with another staff member, who periodically notified the investigator of suspicious accounts, customers or dealers. Close working relationships allowed investigators to share 'hunches' that formalised process and outcome controls could not otherwise pick up (such as identifying particular customer accents, mis-spellings of surnames or familiar residential addresses).

Figure 2 shows examples of the combinations of controls that can be used in the investigation process. For example, in one case of dealer fraud, a dealer audit control was enough to detect culpability and complete the investigation. The second case of dealer fraud, however, was only detected because an associated account had seen irregular activity: subsequent investigation revealed a systematic program of forged customer details on the part of the dealer. In the next case, an internal billing referral control

identified the case, followed by another billing referral. In this incident, the fraud was only uncovered once the investigator became suspicious of the customer (a clan control). In the first case of identity theft, the customer had made calls to a 'hot destination' (a process control, but not usually sufficient to identify fraud). A subsequent internal billing referral control identified an unpaid account, but it was only when a relative of the customer notified the firm that the case was fully identified. In this case, the original customer had been dead for three years, and the perpetrator had used their details post-mortem for call-selling purposes. The final case shows an incident where the same control can appear more than once in the evidence chain. Here, a clan control signalled the possible identity theft when another telecommunications provider notified the firm. A suspicious investigator flagged the account, followed by more information from another telecommunications provider.

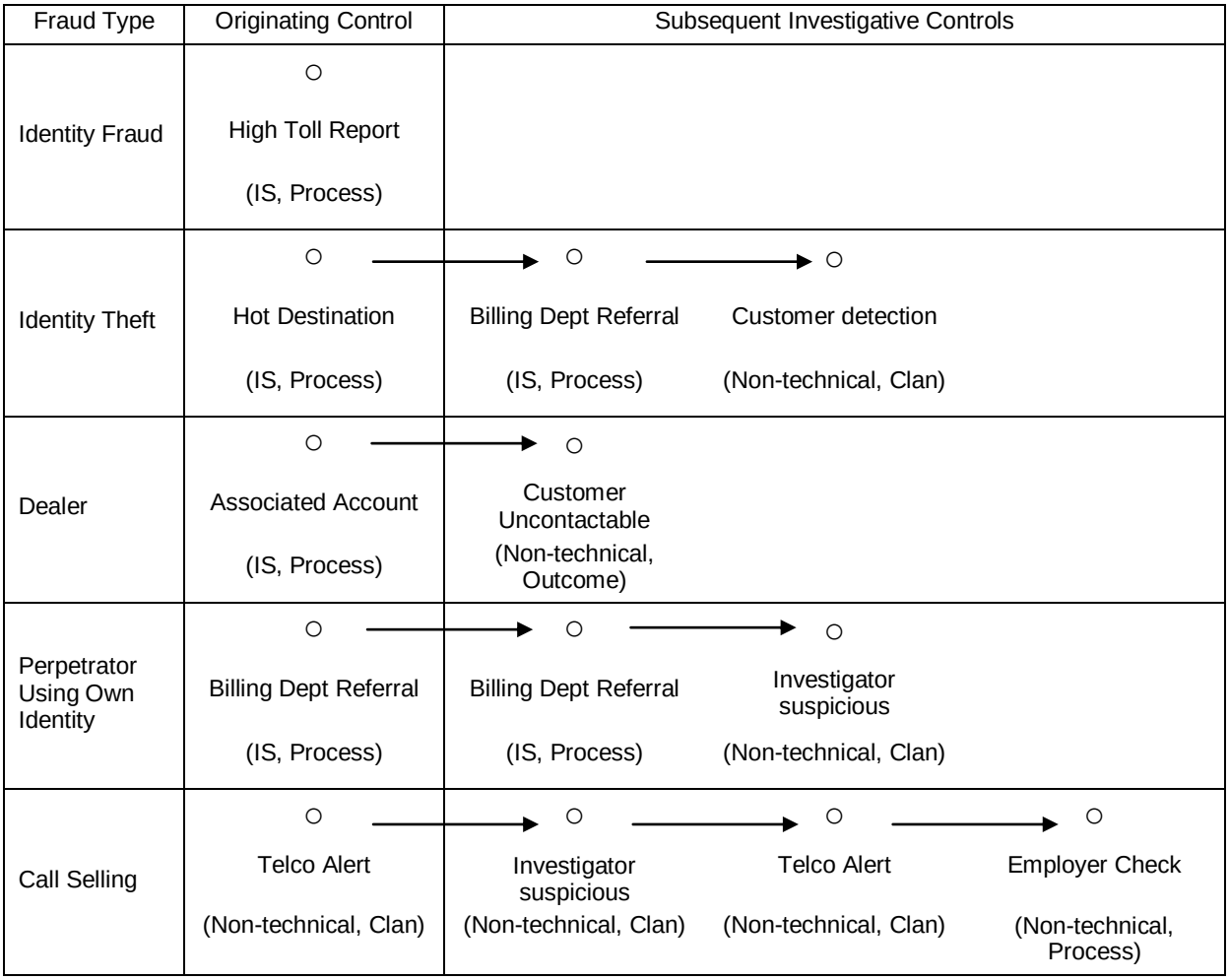

Figure 2. Fraud Types and Chains of Confirmation

6 Discussion and Conclusions

Security controls are integral to maintaining IS performance. This study has contributed to this discourse through advancing understanding of the nature and behaviour of operational security controls in an empirical setting. The analysis of the case study firm's investigation processes revealed several new attributes of information system controls with respect to control use. The study found that

IS-based controls were either outcome or process controls. These control types were typically suited to codifiable, complete knowledge that exhibited low diversity. The majority of cases were initially detected using IS-based controls. Clan controls were often used later in the investigative process to gather additional information about these fraud events. These controls typically involved knowledge with less structured processes and outcomes, depending more upon individual interpretation.

The study may be open to a number of limitations. First, some of the testing conducted in this study was based on observed or detected criminal activity. Such detection may not be perfect and, as a result, the cases brought to light may exhibit some unseen bias. Second, the actual frequency of these fraud types may also vary from those seen in this paper, as systematic and efficient fraudulent behaviour remains undetected. Cases of well executed fraud may be able to evade the control systems in place. These limitations are likely to affect many empirical studies into fraud of this nature. Third, it is necessary to view these results as being grounded in the context of a large telecommunications company operating within a highly competitive and often unpredictable environment.

Evidence in this paper has highlighted the variety of control types used in the investigative process. Much prior work has focused on formalised process and output controls for managing fraud knowledge, with less focus on clan controls. If investigators find clan controls useful in fraud detection, then perhaps they contain value that has not been identified or captured in prior literature. These informal social controls could be used as an effective bridge between more technical IS-based controls. We need theory that goes beyond the focus on formal controls for preventing fraud entering the system, because this limits our understanding to reactive postures. By examining informal clan control structures, we can better understand how to alleviate fraud types the firm has not yet seen.

The paper also delivered evidence that the investigation of some fraud actually depends on input from other firms, including competitors. Importantly, however, the finding highlights the fact that the firm does not operate in isolation, and viewing it under this lens will likely yield an incomplete picture.

The study raises a number of implications for practice. First, while valuing security controls continues to be a problem, practitioners could consider allocating costs to combinations of controls rather than single controls. Evidence in this paper shows that a collection of controls is often used to identify fraud, implying that operational costs should ideally be factored over a range of controls. Smaller firms are less able to absorb the costs of information fraud, with fewer resources for detection. Offenders may be drawn to such firms because of the limited security controls in place. Practitioners should consider the particular benefits that these small firms could bring to information-sharing networks in light of their alternative capacity for information gathering.

There was evidence that other organisations might identify threats before the case firm, possibly because they use different controls. Whereas opportunistic offenders may lack the planning and execution skills to perpetrate fraud with significant loss or exposure, more organised groups may have the resources to evaluate and adapt to new controls. In this capacity, having a wider array of controls and control combinations could itself be an effective deterrent because the additional learning burden raises barriers to fraud commission. Practitioners should carefully evaluate whether ‘best practice’ guidelines are effectively making their data gathering methods more similar to their competitors.

Whereas some prior work has argued that human actors are the least secure point in a system (Perry 1985, Vroom and von Solms 2004), this paper indirectly finds evidence that human actors can also be of tremendous advantage in the detection process, particularly when given the benefit of effective information sharing networks (Hu et al. 2007). Human actors may be able to provide tacit insight into a fraudulent case, using intuition, memory recall and ‘gut feeling’ to determine a case’s veracity. Interview participants also argued that these clan controls, particularly externally-focused controls, were important to the investigative process. These informal controls appear to be an effective way of improving the confirmation process.

A number of avenues for future work arise. The findings in relation to organizationally independent and dependent operational controls have relevance to future work on control system design. Here, the

study observed controls originating from within and outside the firm. Similarly, because firms have limited resources and different infringements affect different levels of the firm at different times, not all controls are likely to be triggered or employed at once. Additional work on the underlying processes for conducting systems-level control solutions in response to or in anticipation of an event could make a significant contribution. In particular, future work could examine the extent to which control selection is influenced by performance level targets and competitive practice.

This study also saw evidence of a move away from purely technical solutions to security problems towards more sociotechnical approaches (Herath and Rao 2009). Echoing the advice of Siponen (2005), more research work into socio-technical and social controls for identifying risky behaviour would be valuable. For example, discretionary dealer audits were effective in identifying dealer fraud in this case. On one hand, audits are costly to administer and may be reputationally damaging for smaller legitimate dealers. Yet, on the other hand, as with individual offenders, fraudulent dealers may exhibit behavioural differences to legitimate dealers. Greater understanding of this ongoing relationship, from a behavioural perspective, might improve the apprehension of such dealers, while reducing the need for audit processes and other technical controls.

A final avenue concerns control valuation for information systems security. Prior thinking has held that firms should identify threats to information assets, and then accordingly fund the controls that meet those threats. Evidence in this paper has suggested that more than one control is likely to be used in identifying and prosecuting the threat case. From this perspective, funding a single control is unlikely to be as effective as funding the suite of controls that address the most likely threats observed. It may even be that the firm can spend less in total, but gain greater overall information system security effectiveness by funding controls that work in concert to detect information fraud.

References

Bodin, L., Gordon, L. A., Loeb, M. P., (2005) "Evaluating Information Security Investments Using the Analytic Hierarchy Process", Communications of the ACM, 48:2, 78-83

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A., Boss, R. W. (2009) "If someone is watching, I'll do what I'm asked: Mandatoriness, Control, and Information Security", European Journal of Information Systems, 18:2, 151-164

Brenner, S. W., (2004) "U.S. Cybercrime Law: Defining Offenses", Information Systems Frontiers, 6:2, 115-132

Cavusoglu, H., Mishra, B. K., Raghunathan, S., (2004) "A Model for Evaluating IT Security Investments", Communications of the ACM, 47:7, 87-92

Cavusoglu, H., Mishra, B., Raghunathan, S., (2005) "The Value of Intrusion Detection Systems in Information Technology Security Architecture," Information Systems Research, 16:1, 28-46

Cavusoglu, H., Raghunathan, S., Yue, W., (2008) "Decision Theoretic and Game Theoretic Approaches to IT Security Investment", Journal of Management Information Systems, 25:2, 281-304

Dhillon, G., Backhouse, J. (2000) "Information System Security Management in the New Millennium," Communications of the ACM, 43:7, 125-128

Eisenhardt, K. M. (1985) "Control: Organizational and Economic Approaches", Management Science, 31:2, 134-149

Feldman, M. S., Rafaeli, A., (2002) "Organizational Routines as Sources of Connections and Understandings", Journal of Management Studies, 39: 309-332

Gal-Or, E., Ghose, A., (2005) "The Economic Incentives for Sharing Security Information", Information Systems Research, 16:2, 186-208

Gopal, A., Gosain, S., (2010) "The Role of Organizational Controls and Boundary Spanning in Software Development Outsourcing: Implications for Project Performance", Information Systems Research, 21:4, 960-982

Herath, T., Rao, H. R. (2009) "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations", European Journal of Information Systems, 18:2, 106-125
Howard, J. D., (1997) "An Analysis of Security Incidents on the Internet, 1989-1995", Ph.D. Dissertation, Department of Engineering and Public Policy, Carnegie Mellon University
Hu, Q., Hart, P., Cooke, D., (2007) "The Role of External and Internal Influences on Information Systems Security - a Neo-Institutional Perspective", Journal of Strategic Information Systems, 16:2, 153-172
Im, G., Baskerville R. L., (2005) "A Longitudinal Study of Information System Threat Categories: the Enduring Problem of Human Error", Database for Advances in Information Systems, 36:4, 68-79
ITU (2008) Yearbook of Statistics Telecommunication Services 1997-2006, International Telecommunication Union, Geneva
Kahn, C. M., Roberds, W., (2008) "Credit and Identity Theft", Journal of Monetary Economics, 55, 251-264
Kallinikos, J., (2005) "The Order of Technology: Complexity and Control in a Connected World", Information and Organization, 15, 185-202
Kotulic, A. G., Clark, J. G., (2004) "Why There Aren't More Information Security Research Studies", Information & Management, 41:5, 597-607
Krippendorff, K., (1980) Content Analysis: an Introduction to its Methodology, Beverly Hills, CA: Sage Publications
Lange, D., (2008) "A Multidimensional Conceptualization of Organizational Corruption Control", Academy of Management Review, 33:3, 710-729
Ouchi, W. G. (1979) "A Conceptual Framework for the Design of Organizational Control Mechanisms", Management Science, 25:9, 833-848
Perry, W., (1985) Management Strategies for Computer Security, Butterworth Publishers, Boston
Png, I. P. L., Wang, Q., (2009) "Information Security: Facilitating User Precautions Vis-À-Vis Enforcement against Attackers", Journal of Management Information Systems, 26, 97-121
Randall, D., Hughes, J., O'Brien, J., Rouncefield, M., (2001) "'Memories are Made of This': Explicating Organisational Knowledge and Memory", European Journal of Information Systems, 10:2, 113-121
Ransbotham, S., Mitra, S., (2009) "Choice and Chance: A Conceptual Model of Paths to Information Security Compromise", Information Systems Research, 20, 121-139
Ryan, G. W., Bernard, H. R., (2000) "Data Management and Analysis Methods" in Denzin, N. K., Lincoln, Y. S., Handbook of Qualitative Research, 2nd Ed., Sage Publications, UK
Salkind, N. J. (2003) Exploring Research, Prentice Hall, New Jersey, USA
Seidman, I., (1991) Interviewing as Qualitative Research, Teachers College Press, New York, USA
Sieber, U., (1986) The International Handbook on Computer Crime: Computer-Related Economic Crime and the Infringements of Privacy, Chichester: Wiley Publishers
Siponen, M. T., (2005) "Analysis of Modern IS Security Development Approaches: Towards the Next Generation of Social and Adaptable ISS Methods", Information and Organization, 15:4, 339-375
Siponen, M. T., Iivari, J., (2006) "Six Design Theories for IS Security Policies and Guidelines", Journal of the Association for Information Systems, 7:7, 445-472
Straub, D. W., Welke, R. J., (1998) "Coping with Systems Risk: Security Planning Models for Management Decision Making", MIS Quarterly, 22:4, 441-469
Turner, K. L., Makhija, M. V., (2006) "The Role of Organizational Controls in Managing Knowledge", Academy of Management Review, 31:1, 197-217
Vroom, C., von Solms, R., (2004) "Towards Information Security Behavioural Compliance", Computers & Security, 23:3, 191-198
Weber, R. P., (1990) Basic Content Analysis, 2nd Ed., Newbury Park, CA: Sage Publications
Whitman, M. E., (2003) "Enemy at the Gate: Threats to Information Security", Communications of the ACM, 46:8, 91-95
Yin, R. K., (2003) Case Study Research Design Methods, SAGE Publications, Los Angeles, USA
Zyglidopoulos, C. S., Fleming, P., Rothenberg, S., (2009) "Rationalization, Overcompensation and the Escalation of Corruption in Organizations", Journal of Business Ethics, 84:1, 65-73