2007

Participants Involved In Identity Fraud

Rodger Jamieson
University of NSW, r.jamieson@unsw.edu.au

Greg Stephens
University of NSW, g.stephens@unsw.edu.au

Donald Winchester
University of NSW, d.winchester@unsw.edu.au

121. Participants Involved In Identity Fraud

Rodger Jamieson*
University of NSW,
r.jamieson@unsw.edu.au

Greg Stephens
University of NSW,
g.stephens@unsw.edu.au

Donald Winchester
University of NSW,
d.winchester@unsw.edu.au

Abstract

This paper sets out a model of the participants involved in identity fraud. This model will be verified through discussions with industry experts from key Australian organisations involved in and impacted by identity fraud.

Keywords: Community and Culture, Organisational Learning, Information Systems (IS), Knowledge Sharing and Sense-Making, Identity and Identity Fraud

* We acknowledge and thank the Australian Transaction Reports and Analysis Centre (AUSTRAC) Steering Committee, the Australian Research Council (ARC), and industry linkage partners for monetary and in-kind contributions to this research-in-progress.

Introduction

This paper starts to address the critical issue of how to combat the relentless attacks of identity fraud and related crime perpetrators, and to mitigate targeted organisations' losses, in the context of a landscape that is large and diverse. Together, all of the participants (excluding the perpetrators) are actors in the community of 'identity' guardians through the security and privacy of our public, and confidential or 'sensitive' information. Where 'identity' in our context is one's own proof of identity (POI) documentation and personal identifying information (PII) - a password for bank account access, for example.

Information Systems (IS), with the advances in technology, play a significant and growing role in the collection, storage, sharing and analysis of identity information. The management, sense-making (Cecez-Kecmanovic 2004; Cecez-Kecmanovic and Jerram 2002) and organisational learning (Janson et al. 2007) of this growing knowledge base from these identity repositories is critical to mitigate identity crimes. Industry and government are now taking this phenomenon seriously. Anonominity granted to perpetrators by identity fraud and the Internet, means jurisdictional borders are not a restriction.

The POI detail includes biometric, attributed, and biographical characteristics. Biometric characteristics, such as finger prints, retina, voice and facial patterns, are mostly fixed and stable over time. Attributed characteristics include our names and biographical characteristics, of which education and employment information are examples. Attributed and biographical data change and are accumulated over ones life. Where and how perpetrators acquire illegitimately issued and fraudulently obtained POI or PII is paramount for identity fraud prevention strategies. Without mitigating the perpetrators attacks the integrity of the whole Australian Identification System (AIS) is at risk.

We are motivated by these facts to provide an inter-organisational categorising framework of the identity fraud participants' in Australia. The conceptual model will show interactions between categories of participants. Those interviewed in this study face a well-recognised dilemma between 'customer service' and the obligation to 'know-your-customer'; versus identity fraud prevention, detection and deterrence processes to maintain customer trust and their own business reputation and integrity.

Recent identity fraud related surveys from the United States (ID Analytics 2007) and United Kingdom (CyberSource 2007) show the diverse nature of the identity fraud phenomenon within communities. These surveys have drawn the public and associated political attention away from perpetrators and towards the victims of identity crime. These surveys are similar to earlier surveys in that they inform the community through diverse media alerts about needed safeguards to protect the public from the threat of (identity) crimes (Rosenbaum 1988). The cost of identity fraud in Australia was estimated to be AU$1.1 billion in 2002 (Cuganesan and Lacey 2003). The fear of identity crime is limiting the further adoption in e-commerce/IT/IS (hereafter IS) via the Internet or other channels.

The next section discusses the research methodology that will be used and is followed by a brief literature review. Our classification of identity fraud participants is presented and discussed with implications and limitations. Conclusions and research agenda are then presented.

Methodology

The aim of this research-in-progress is to determine the main categories of identity fraud participants (in Australia) and how they interact with one another to deter, detect, and prevent perpetrators. We hypothesise that target organisations within a sector and across sectors that cooperate, coordinate, communicate and learn through networking, knowledge sharing and sense-making have a better chance to mitigate identity crimes.

Table 1: Proposed Interview Organisations

Organisational Code	Participant Organisation
1	Bank 1
2	Bank 2
3	Bank 3
4	Licensing Authority 1
5	Licensing Authority 2
6	Telecommunications 1
7	Government Agency 1
8	Government Agency 2
9	Government Agency 3
10	Government Agency 4
11	Government Agency 5
12	U.S. Criminologist

The research design identifies, from the literature, some existing identity crime participants (Cuganesan and Lacey 2003; Tan 2002; Wang et al. 2006). Semi-structured interviews will be undertaken. First, a pilot interview will be conducted to evaluate the proposed questions for their utterances, coverage and to determine interview duration. The interviews will be recorded, transcribed and analysed using NVIVO 7 2006. The organisations from which interviewees will be drawn are presented in table 1.

At the top level, our interview protocol will follow several main themes including: what is identity fraud in your organisation; managing identity fraud; identity fraud reporting; and identity fraud issues and research. As this paper is research–in-progress we do not discuss in detail our model's components.

Literature Review

"Social control has been defined as the use of rewards or punishment to ensure the members of a group, such as, a family, organisation, neighbourhood, or society, will obey the group's rules or norms" (Greenberg et al. 1985 in Rosenbaum 1988, p.5). "Whereas formal social control is derived from written rules and laws and is enforced by police and the courts, informal social control is based on custom or social norms and is enforced by the citizenry through behaviours such as surveillance, verbal reprimands, rejection, warnings, and other pressures to encourage conformity" (Rosenbaum 1988, p.5). An earlier implemented example of seeking the public's help to deter, prevent and detect crimes was 'neighbourhood watch'.

More recently, the United States (US) and her allies have called upon their people to fight the 'war on terrorism' and to report anything suspicious. Similarly in IS, computer users may band together and alert the public about the latest virus attack (Saydjari 2006). Recent research (Chua et al. 2003, p.5) suggested that an "action to combat internet fraud, involves mechanisms associated not only with markets (price mechanisms) but also with hierarchies (authority) and communities (social relationships)". Contemporaneous research on communities (see Chua et al. 2003, pp.8-9 and references therein) "has examined their ability to complement the mechanisms of hierarchical governance by means of informal, communities of practice, and social capital. Research in these streams has demonstrated that shared interests within communities can mitigate self-interested and opportunistic behavior". For example, from private sector organisations or monopolistic behavior in general.

Since the 1960's, microprocessors have facilitated the growth in IS (Clarke 2006). To mitigate this phenomenon organisations have had to adapt through sense-making (Cecez-Kecmanovic and Jerram 2002), knowledge sharing (Cecez-Kecmanovic 2004) and learning (Janson et al. 2007) internally and across organisations from a multi-organisational or community perspective. In Australia, inter-organisationally this is being facilitated by industry associations, peak bodies, and government committees made up of inter-agency participants.

A Model Categorising Identity Fraud Participants

The participants involved in identity fraud are numerous and involve more people and organisations than just the perpetrator(s). Figure 1 shows our categories of the main participants and their interactions. The model was derived from the literature and from our previous research into identity fraud (Jamieson et al 2007b; Jamieson et al 2007a)

Government Agencies

Government agencies in figure 1 interact with all other categorised players including the private sector through targeted organisations' interaction. They are diverse and include: regulators; legislators; welfare (POI issuers and users); and research. Regulatory Bodies' (Federal, State, and Local) regulations, rules and codes of conduct are required to prevent anarchy.

Private Sector

The dominant non-government (industry) POI users are those organisations targeted by identity fraud perpetrators, such as financial institutions (banks), utility organisations, and retailers.

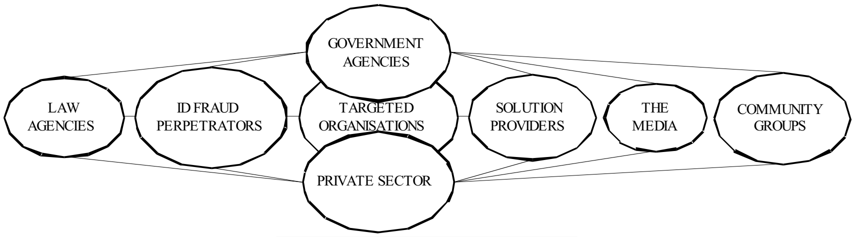

Figure 1. Participants in Identity Fraud

Law Agencies

Law enforcement, courts, and corrections systems are the focus of this section. For law enforcement, one of the difficulties in combating identity fraud and related crimes arises from a unique feature of the crime pertaining to the legal jurisdiction responsible for adjudication of a crime. Where the legislation making such acts a crime is passed in a particular location and that location has no jurisdiction over another location(s).

Identity Fraud Perpetrators

We classify identity fraud perpetrators into four distinct categories – organised crime, sophisticated perpetrators, opportunistic perpetrators, and agents (refer Jamieson et al. 2007b).

Targeted Organisations

Perpetrators target both public and private organisations. Perpetrators target these organisations to obtain POI/PII and then using this illegally obtained information by-pass security to score an economic benefit – committing identity fraud acts. Target organisations to-date have predominantly been financial institutions – especially banks, utility organisations, retailers and government welfare agencies but include all sectors of economic activity (see Cuganesan and Lacey 2003).

Solution Providers and Other Experts

Solution providers include: technology organisations; researchers; industry associations; manufacturers; and standard setters of POI documents. In an IS context, solution providers are playing an increasing part in the identity fraud player landscape. Due to the pervasive increase of the Internet and e-commerce as an attack channel and the innovations in IS related methods of attack (refer Jamieson et al. 2007b).

The Media

Media organisations may be owned by government or private organisations. They include: television; radio; newspapers; and magazines. Often organisations, associations, peak bodies, and community groups, both publicly or privately operated have their own media sections and personnel who from time to time release information directly to members and the public in real time via their websites or via the media.

Community Groups

Community based groups, set up to mitigate identity crimes are backed by government or the private sector as outlined above, e.g., Australian High Tech Crime Center and Australia Bankers Association. Other collectives are privacy groups (e.g., Australian Privacy Foundation) who provide a balance in the debate for consumer protection for privacy and security of their identity information and rights from government and industry.

Implications and Limitations

We expect there will be major positive implications for organisations that collaborate within and across sectors, industry and government. With organisation's that collaborate placing themselves in a better position to deter, detect and prevent identity fraud perpetrator events than organisations that chose not to collaborate. A limitation of this study is that we will not interview perpetrators or participants from community groups, the media, or solution providers. As this is research in progress we will endeavour to seek comment about these sectors from our industry experts. Also the communities within different states and jurisdictions will differ across countries. However, we start the process within an Australian context.

Conclusion and Research Agenda

Our approach seeks to conceptualise the sense-making model of knowledge management in organisations (Cecez-Kecmanovic 2004; Cecez-Kecmanovic and Jerram 2002) and organisational learning (Janson et al. 2007) to an inter-organisational context grounded from industry and government participant interviews. Feedback from industry experts should show that public and private sectors need to collaborate to combat identity fraud perpetrators, and to put in place better identity fraud defenses.

References

Cecez-Kecmanovic, D., "A sensemaking model of knowledge in organizations: a way of understanding knowledge management and the role of information technologies". Knowledge Management Research & Practice (2:3), 2004, pp. 155-168.

Cecez-Kecmanovic, D., and Jerram, C., "A Sensemaking Model of Knowledge Management in Organisations," ECIS (June), 2002, pp. 894-904.

Chua, C., Wareham, J., and Robey, D., Anti-Fraud Mechanisms in Internet Auctions: The Role of Markets, Hierarchies and Communities of Practice," Unpublished Working Paper, Georgia State University, 2003, pp. 1-53.

Clarke, R., "Key Aspects of the History of the Information Systems Discipline in Australia," Australasian Journal of Information Systems (14:1), 2006, pp. 123-140.

Cuganesan, S., and Lacey, D., "Identity Fraud in Australia: An evaluation of its nature, cost and extent". Standards Australia International Ltd. Sydney, 2003.

CyberSource., :Third Annual UK Online Fraud Report: Online Payment Fraud Trends and Merchants' Response," CyberSource Corporation (2007 Edition), 2007, pp. 1-20.

ID Analytics., "US Identity Fraud Rates by Geography February 2007," ID Analytics, Inc. 2007, pp. 1-12.

Jamieson, R., Winchester, D., and Smith, S., "Development of a Conceptual Framework for Managing Identity Fraud," Proceedings of the Hawaii International Conference on System Sciences (HICSS) 40, 2007a, pp. 1-10.

Jamieson, R., Stephens, G., Winchester, D., "An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts," PACIS 11th Annual Conference, New Zealand, July, 2007b, pp. 1-14.

Janson, M., Cecez-Kecmanovic, D., Zupancic, J., "Prospering in a Transition Economy Through Information Technology-Supported Organizational Learning," Info Systems Journal 2007 (17), pp. 3-36.

Rosenbaum, D., "Community Crime Prevention: A Review and Synthesis of the Literature," Justice Quarterly (5:3), 1988, pp.1-74.

Rosenbaum, D., “The Theory and Research Behind Neighborhood Watch: Is It a Sound Fear and Crime Reduction Strategy?” Crime and Delinquency 1987, (33:1), pp. 103-134.

Saydjari, O., “Privacy-Enabled Global Threat Monitoring,” IEEE Security & Privacy 2006, pp. 60-63.

Tan, H., “E-Fraud: Current Trends and International Developments,” Journal of Financial Crime (9:4), 2002, pp. 347-354.

Wang, W., Yuan, Y., Archer, N., “Identity Theft: A Contextual Framework for Combating Identity Theft,” IEEE Security and Privacy (March/April), 2006, pp. 30-38.