2009

Information Security in an Identity Management Lifecycle: Mitigating Identity Crimes

Rodger Jamieson
University of New South Wales, r.jamieson@unsw.edu.au

Lesley Pek Wee Land
The University of New South Wales, l.land@unsw.edu.au

Stephen Smith
The University of New South Wales, Stephen.Smith@commerce.nsw.gov.au

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

Donald Winchester
The University of New South Wales, d.winchester@unsw.edu.au

Information Security in an Identity Management Lifecycle: Mitigating Identity Crimes

Rodger Jamieson
The University of New South Wales
r.jamieson@unsw.edu.au

Lesley Land
The University of New South Wales
l.land@unsw.edu.au

Stephen Smith
The University of New South Wales
Stephen.Smith@commerce.nsw.gov.au

Greg Stephens
The University of New South Wales
g.stephens@unsw.edu.au

Donald Winchester
The University of New South Wales
d.winchester@unsw.edu.au

ABSTRACT

Identity management is a wide area that deals with identifying individuals or entities in a system (such as a nation, community, network, or organization) and controlling access to resources or use and flow of transactions (e.g., financial) within systems by associating user rights and restrictions with the established identity (identifiers). A qualitative interpretive methodology was adopted with industry and government organizational experts interviewed. In addition, secondary data were collected and analyzed. We used a lifecycle frame to interpret themes and issues from interview transcripts and other collated secondary data. The paper's contribution is to make sense of 'identity' in offline and/or online channels and to extend a 3-stage identity management lifecycle framework (IDSP, 2008) to four which includes: initial 'enrolment', 'transacting' 'database', and 'purging'.

Keywords

Information systems (IS), identity management, identity attributes lifecycle, identity crimes (fraud/theft/deception).

INTRODUCTION

Robust information systems (IS) security strategies are required to minimize the risks of identity crime in identity management systems of government and private organizations. Public and private organizations must make sure they do not expose their own or others' identity (or personal identifying information (PII), e.g., account passwords) details. Information systems security (ISS) in an offline or online context may require different security protocols to prevent external or internal identity crime perpetrator breaches or intrusions. The 'circularity effect' of identity document enrolment, the ability whereby one piece of identity or PII can be used to reconstruct an individual's 'identity set' of proof of identity (POI) documents in a nations identity system (federated) often allows identity crime perpetrators to gather enough details, once a starting point for POI/PII is accessed (The Identity Theft Prevention and Identity Management Standards Panel, IDSP, 2008; Jamieson, Land, Stephens and Winchester, 2008). Similarly, in the private sector with interactions between the public or private sector, appropriate ISS policies need to be adhered to. These policies may be directed by legislation, *de facto* or *de jure* standards, guidelines, protocols, directives or rules (Australian Government, 2008; Clauß and Köhntopp, 2001; IDSP, 2008). In Australia, "identity theft (a subset of identity fraud and identity crime) is generally considered to refer to the theft and use of personal identifying information of an actual person, as opposed to the use of a fictitious identity. This can include the theft and use of identifying personal information of persons either living or dead" (the Model Criminal Law Officers' Committee, MCLOC, 2008, p. 18). Identity deception is the use of a fictitious, false, or assumed (or other synonyms) identity acts (i.e., intentional misuse of POI or PII other than by theft for some (financial or economic) gain, or to avoid a cost).

According to Javelin Strategy & Research Inc., identity fraud costs United States (US) businesses and consumers an estimated US$50 billion in 2008 (Kim, 2009). In the US in 2008, there were a total of 656 data breaches and 35,691,255 records exposed (Identity Theft Resource Center (ITRC), 2009a). Dissecting these statistics between electronic and paper, it was found that electronic classification had the majority of total breaches (82.3%) and exposed data records (98.4%) (ITRC,

2009c). This result is contrary to the findings in a recent identity theft survey that suggested most identity fraud events were due to traditional methods and not online, where only 11 percent occurred - 11 percent was also recorded for data breaches (Kim, 2009). The mixed findings suggest further research is required in identity management techniques to help mitigate identity and related crimes (money laundering, terrorism, trafficking – drugs, etc.). Table 1 shows the percentages of data breaches and records exposed, by category, with records in the Banking/ Credit/ Financial category being most exposed. "In an unprecedented case, three out of four German households have had bank account data compromised and it's for sale on the black market" (Fragala, 2008, p.2). "The theft of personal information by hackers (for example) is so prevalent - and efficient - that stolen credit card details now sell for as little as eight cents (US) a card, a report by one of the world's biggest computer security companies says" (Fossi, 2009; Walters, 2009, p. 1).

Category	Data Breaches (%)*	Records Breached (%)
Banking/Credit/Financial	11.9	52.5
Business	36.6	16.5
Educational	20.0	2.3
Government/Military	16.8	8.3
Medical/Healthcare	14.8	20.5

Table 1. Summary by Category of 2008 Data Breach Statistics in the US

Source: Identity Theft Resource Centre (ITRC), 2009b. * May not be 100% due to rounding.

Available statistics from other countries for identity crime and data breach events point out the economic severity of these acts and their impact on entities across time and space (Canadian Internet Policy and Public Interest Clinic (CIPPIC), 2007; Choo, Smith and McCusker, 2007; Fossi, 2009; Jamieson et al., 2008; KPMG Forensic, 2009; McAfee, 2009; Meulen, 2006; Organisation for Economic Co-operation and Development (OECD), 2008; Sproule and Archer, 2008a, 2008b; United Kingdom Home Office, 2006; Urbas and Choo, 2008). Comparing these identity crime statistics across nations over time has proved to be problematic often due to definitional issues (Jamieson, Land, Sarre, Steel, Stephens and Winchester, 2008). However, it is clear that there is a significant (and arguably growing on a global basis,) financial and economic cost to organizations, individuals or customers from identity and related crimes (acts or events where they are not legislated against). The main objective of this study is therefore to investigate a framework whose components would help to combat these costs. A better understanding of the identity (POI and PII) lifecycle may improve the management of identities (Bosworth, Jaweed and Wright, 2005). We propose a broad research question initially to draw out issues related to our main objective. Our research question is:

What are the critical components of an identity management life cycle needed to combat identity and related crimes?

The next section reviews the identity management literature. The following sections discuss the methodology and frame, results, and implication and limitations. The final section concludes and suggests future avenues of research in identity management.

LITERATURE REVIEW

Identity management may not have a definitive meaning, but technology-based identity management, "in its broadest sense, refers to the administration and design of identity attributes, credentials, and privileges" (Cavoukian, 2007, p.5). Three types of identity management include: centralized (a firms' username and password or a country's identity card); user-centric (individual control e.g., student identity card for concessions); and federated - a mix of centralized and user-centric (Cavoukian, 2007; Jøsang and Pope, 2005). The ability to federate identity across organizations while maintaining clear trust, liability, and cost responsibilities, is a major challenge for organizations as they continue to chase efficiency in cross-organizational business and customer-relationship processes (Buell and Sandhu, 2003).

A recent study comprised of three working groups compiled "an inventory of existing standards lifecycle, guidelines, best practices and compliance systems related to identity theft prevention and identity management … (and) also included applicable laws, regulations, proposed legislation. … (they *sic*) identified and prioritized various identity fraud-related problems" (IDSP, 2008, p.3). IDSP (2008) identified some general gaps based on their research into three identity standard lifecycle approaches (*viz.*, issuance of identity credentials; the exchange of identity data; and the maintenance of identity

information). These gaps included; the issuance verification process needs to be fortified; authentication weaknesses e.g., in the approach to shared secrets and social security numbers have been hijacked by identity thieves, who then use them to commit fraud, and relying only on what a person knows (single factor authentication) makes the identity crime perpetrator's job easier; and organizational mismanagement of personal data (IDSP, 2008). Lifecycle models have been used elsewhere to explain concepts of identity management. Bosworth et al. (2005) argue their meanings and associated defined lifecycles (birth, in-life, and death) for entities, identity, identifiers and credentials. Reports by governments for implementing smart cards have investigated introducing a lifecycle framework consisting of four parts (e.g., acquisition of custom cards, card personalization and activation, change of functionality, and card revocation) (Australia Government, 2008).

To date, most innovations by organizations for ISS in the management of information that relies on identity have been able to be broken, abused or circumvented by identity crime perpetrators. However, a new quantum encryption technique may finally be a reality. It is reported to be uncrackable by changing the cryptography field infinitely (Mullins, 2008). "Quantum cryptography relies for its security on the fact that it is impossible to measure a quantum object without changing it" (Mullins, 2008, p. 24). In Australia (and other countries) "there is an interdependence of (Commonwealth) government agencies' identity processes, with agencies being highly reliant on the integrity of each other's documents for establishing individuals' identities" (Hawker, 2001, p.3). This identification system is often called a federated system as opposed to a nations' centric-system where there is an identity card – a unique identity identifier (document or card or smartcard). Clarke (2008) discusses misunderstandings and myths in identity management. Reports from an industry perspective often discuss identity management in global terms of requirements or convergence for instance (OneName Corporation, 2001; Rutkowski, 2007).

METHODOLOGY

An interpretive qualitative research design was adopted including: the use of an industry-based pilot interview; and cross-sectional participant interviews based on 12 in-depth interviews, desk research and content analysis of secondary data (Klein and Myers, 1999). In addition, we use secondary data 'key word' database searches for terms such as, identity management, identity management life cycle, identity, identity fraud, identity theft, and identity deception to build a better picture of the literature. Recordings were transcribed and transcripts coded using 'key word themes' in NVivo 2 (QSR International, 2005) qualitative analysis software. Interviewees were provided with transcripts so that they could retract any sensitive information or correct or add details from databases or other secondary data sources not available at interview time. Interview duration varied from 45 minutes for two teleconferences where interviewees were provided the questionnaire instrument by email in advance to approximately 90 minutes for face-to-face interviews. Interviews were conducted (or supervised) by senior experienced academics, industry personnel, and an honors student. Ethical approval was sought and granted by the university ethics committee. A pilot interview was undertaken to test the survey instrument's open-ended questions (which are not included here due to space constraints). The four main themes of the survey instrument were: What is Identity Fraud in Your Organisation; Managing Identity Fraud; Identity Fraud Reporting; and Identity Fraud Issues and Research. The organizations selected were large financial institutions, a large telecommunication organization, and government agencies that issue or use proof of identity documentation or other personal identifying information and are most targeted by identity crime or related crime (money laundering, terrorism, trafficking – people, weapons, drugs, illicit material) perpetrators. The interviewee experts' backgrounds included: law enforcement, legal, accounting, computer forensics, information technology, fraud, information systems security, and auditing. Table A1 in the Appendix shows the interview participants code, category, and roles or job titles from their business cards. However, the general objectives of all employees of the interviewed organizations are to stop fraud of which identity crime (identity fraud, identity theft, and identity deception) is a growing part.

The research design for this paper sought to model a 'lifecycle' approach to identity and its management in the private and public sector and their various interrelationships between the sectors (Bosworth et al., 2005). Several main themes and issues were observed from analyzing the interview transcripts with respect to the identity lifecycle within organizations in an identity crime context – enrolment, transacting, database, and finally purging (Australian Government, 2008; Bosworth et al., 2005; Clarke, 2008; IDSP, 2008). These themes are important because in practice, payments for example are "not generally compromised during transfer but are compromised when received, stored, or archived" (Glaser, 2008, p.3). Each theme and related issues from participant quotes impact an organization's perspective on identity management and how it anticipates future perpetrator innovations (Australian Government, 2008). Enrolment sought to identify and assess issues relating to the issuance of identity documents or PII (Clarke, 2008; IDSP, 2008). Transacting sought issues to verify and authenticate transactions where an identity needed to be verified and authenticated. This was made more difficult when deals were across jurisdictions with respect to linking identities of an entity and trust between parties including any third parties (IDSP, 2008). Database addressed issues relating to the ongoing maintenance and management of identity information. Purge related to issues for the removal of POI or PII from an organization's databases or database repositories (IDSP, 2008).

DISCUSSION OF RESULTS

> "The average individual (entity) is not aware of how easy it is for their identification (identity identifiers) to be compromised – through for instance a mailing list, or when filling out a warranty form, or by sending off a resume for a job" (Interview Participant 1). "I really don't want to put my social security number (SSN) or my mother's maiden name on a paper application" (Interview Participant 12, see Appendix, Table A1). "They have all been lost, stolen or compromised in some way" (Interview Participant 1).

The above interviewee quotes illustrate some of the issues regarding identity details falling into the wrong hands. Tables 2, 3, 4 and 5 shows more examples of interviewee quotes and related issues selected from transcript narratives that were analyzed using NVivo qualitative software (QRS International, 2005). In the following sub-sections four components developed from themes in the collected data, important to identity management systems lifecycle, are discussed. They are critical to both online and offline IS environments.

Enrolment

Enrolment is the critical first step in the identity lifecycle for an entity (individual, organization, also could be a machine) where the enrolling organization must attain accurate entity details for the identity captured. The captured detail may also act as an identifier template for repeat verification or authentication by the issuer organization e.g., a financial institution, retailer or government agency (Bosworth et al., 2005; IDSP, 2008). A problem often espoused by individual organizations who issue documentation used in a federated identity system as part of their 'normal' business is that the documentation, for example a driver's license, is used as POI. Its purpose is for the proof of being able to drive a certain type of vehicle in a particular place (or at a certain time) not as POI (IDSP, 2008).

Issue	Quote	Participant
Customer identification and authentication in the enrolment stage of the IDM lifecycle	"Somewhere in the relationship lifecycle you've done an authentication of their identity - at the start. And once you move from there to the customer number and the three digit personal identifying number (PIN), and that then forms the basis for authenticating who they are."	2.1
	"Issues of different jurisdictions and different laws (need to be considered)."	3.1
Enrolment integrity of customer identity (POI) details	"You can't avoid that first initial step of proving, or stating this is me. Stating your identity and proving that that's who you are. Or the term now people use is evidence of identity, rather than proof."	4.3
Inability to link aliases or pseudonyms to one real (legal) identity	"Actors, entertainers and authors have always used aliases or pseudonyms. The problem is when they actually don't go through a formal process of changing their name. The problem is where the two names can't be automatically linked."	11
Determining identity theft or deception	"The big area where there are issues for us, in terms of account opening identification, is of course fake (identity deception) or stolen documents (identity theft)."	10

Table 2. Enrolment component of identity management life cycle - issues, interviewee quotes and participant code

Transacting

The transacting element of the lifecycle is listed second however it is dynamic in nature and interfaces with the database element of an entity's identity frequently (or seldomly) any time between enrolment and being purged. During this stage of the lifecycle, an entity's identity is most vulnerable and insecure because the entity relies on counterparty trust of a *bone fide* organization and not a perpetrator mimicking an organization to capture the identifiers of the identity. The mimicking by

perpetrators may happen with methods such as social engineering, phishing or scams for instance. A review of the Financial Action Task Force's 40 (FATF-40) recommendations and the Financial Transactions Reports Act 1988 (and later FATF-40 + 9 recommendations and the Anti-Money Laundering and Counter-Terrorism Financing Act 2006, which was fully implemented by December 2008) for money laundering and crime financing, shows it is not just about identification for financial institutions (and from 2006 bullion and gambling sectors) at a transaction level. It is also about how to establish the 'know-your-customer' requirement and updating that information (Jensen, 2008). When we are talking about verification of identity on a day-to-day basis through remote anonymous channels, secure identity management systems and controls need to be in place to identify people (entities). Advances in data mining and other techniques can permit analysis of transactions in real-time and in stored data.

Issue	Quote	Participant
Managing and monitoring the identity(ies) in a transaction lifecycle	"That lifecycle includes things like opening an account, doing maintenance on that account, credit and card type applications, and a collection process."	1
Personal verification of a customer's POI and or PII	"The accuracy of the documents is in question. It's this idea that I ask enough wallet and non-wallet questions to give myself some comfort that the person who I'm dealing with is who they say they are."	2.1
Background POI/PII verification	"Well we do the initial identity checking, we have a system called Integrated Fraud Detection System, and that is monitoring usage according to age of account and various other parameters."	6.2
Third party POI/PII verification	"The main way we're considering identity fraud is in programme delivery context, as in a third party (Participant 8) are delivering our payments for us, so as you can imagine if identity fraud was out of control, you could have significant exposure in terms of incorrect outlays."	9.2

Table 3. Transacting component of identity management life cycle - issues, interviewee quotes and participant code

Database

Issue	Quote	Participant
Importance of risks involved when inputting data, controls and reviews of data	"The most obvious problem that comes to mind is again the initial verification process because if you've got unclean data on your database, then they are going to be used and there is low integrity of identifying data".	5
	"We decide what data is required, to validate and authenticate the veracity of the information. We specifically look for instances of incorrectness and false representation."	8.3
	"Our staff certify original documents, type it into our system, and basically they're then qualified. We have issues around the integrity of the data as well, but we maintain and host the processes to collect that. We have lists of the identity documents and maintain new documents and issues surrounding verification for people as well."	8.5
Use of database queries to combat identity crime perpetrators	"We've got extensive information in what's called our data warehouse … we share some of that information with other government departments as well. And if there is an issue, then we can interrogate those databases and look at instances of fraud that we can then investigate and look at how we can address the issue. And where it's a systemic issue, then what we need to do in order to minimize that risk."	7

Table 4. Database component of identity management life cycle - issues, interviewee quotes and participant code

Integrity of changes to identity details was seen as important not just because the changes were legal requirements under the privacy laws for example, but also for customer relationships and establishing and maintaining trust between parties (entity and organizations). Trust was important between organizations as well, especially due to the nature of identity information 'silos' when identity (POI or PII) data is purchased or shared (Clarke, 2008). "Data compromises can expose consumers to the threat of identity theft or related fraud, damage the reputation of the entity that experienced the breach, and carry financial costs for everyone involved. While "perfect security" does not exist, all entities that collect and maintain sensitive consumer information must take reasonable and appropriate steps to protect it" (US Government, 2007, p.5).

Purge

The purge of an entity's identity from a data set or database would seem necessary and logical after an individual's death or if the person decided to stop doing business with an organization (e.g., change banks). In practice the experts noted that this seldom occurred. An entity's identity (identifiers) often remained in an organization for many years, often indefinitely, after its immediate expiry or use and is often maintained due to legal reasons (e.g., for tax purposes).

Issue	Quote	Participant
Need to manage and purge obsolete identity data (details)	"Why go to the extent of adding a completely new customer when there are millions of customers already there and many of them are no longer current, like have left the country or died or whatever?"	8.5
Need to identify and purge incorrect identity data	"We electronically archive records (identity), but we are able to go back further. One of the reasons why we do keep them indefinitely is because a lot of the other organizations, especially the enforcement agencies, tend to rely on us for information, so we, in fact, actually have paper records that go back to the 1980s, because the police require this information."	4.2

Table 5. Purge component of identity management life cycle - issues, interviewee quotes and participant code

Another side of this argument is that, for example legislation in the US, the Computer Fraud and Abuse Act (1996) is used to prosecute perpetrators who "threaten to delete data, crash computers, or knock computers off of the Internet using a denial of service attack" (US Government, 2007, pp. 66-67).

IMPLICATIONS AND LIMITATIONS

Practical implementation of an efficient identity management system requires knowledge of the lifecycle of an 'identity' to combat identity and related crimes, fraud, thefts or deceptions. A limitation of this research could be that our experts' perspectives were from an Australian or US context. Further research could interview experts based in other countries. We endeavored to mitigate this potential bias with as wide as possible secondary data search.

CONCLUSION

Making sense of an entity's 'identity' in offline and/or online environment is critical for a secure identity management system. Tables 2, 3, 4, and 5 illustrate a selection of quotes and related issues from transcripts of experts in public and private organizations that are confronted with identity crime perpetrators on a daily basis; they seek to disrupt business operations and take entities' identities. Critical to the successful adoption and uptake of identity management systems is the understanding of its lifecycle components (enrolment, transacting, database and purge) for an entity's identity (identification). Participant experts were conscious of how legislation impacted their business operations when managing the identity of customers (entities). Laws covering data protection, privacy, finance and money laundering were all stated to add extra costs to their businesses. The offsetting benefits were less clear, yet portrayed as necessary for an organization's, industry's or government's trust and reputation in the eyes of their customers and the public. Privacy and data protection legislation were suspected to help the perpetrators more than organizations and hinder organizations sharing information stored in 'data silos' that could be used to verify a genuine customer and identify perpetrators (or suspected). The sharing of information across sectors including government and private organizations was thought an important component of a successful identity management policy in identifying an entity (Otjacques et al., 2007).

Future research should more fully investigate the 'issues' (Tables 2-5) identified and more innovations from science that may secure 'identity' transacting of entities (e.g., cryptography) to prevent intrusion or abuse for government and private organizations.

ACKNOWLEDGEMENTS

The authors wish to acknowledge the assistance and cooperation of participants from the organisations sponsoring this Identity Fraud Linkage Research Project and to AUSTRAC Consortium and the Australian Research Council for their research grant.

REFERENCES

1. Australian Government. (2008) National smartcard framework, *Department of Finance and Deregulation*, December, 1-50.
2. Backhouse, J. (Ed.) (2005) Structured account of approaches on interoperability, *Future of Identity in the Information Society (Fidis)*, July, 1-77.
3. Bosworth, K., Lee, M. G. G., Jaweed, S., and Wright, T. (2005) Entities, identities, identifiers and credentials: What does it all mean, *BT Technology Journal*, 23, 4, October, 25-36.
4. Buell, D. A., and Sandhu, R. (2003) Identity management, *IEEE Internet Computing*, November/December, 26-28.
5. Cavoukian, A. (2007) 7 Laws of identity: The case for privacy-embedded laws of identity in the digital age, 1-24. (accessed February 6 2008, http://www.identityblog.com/wpcontent/resources/7_laws_whitepaper.pdf).
6. Choo, K-K. R., Smith, R., and McCusker, R. (2007) Future directions in technology-enabled crime, 2007-2009, *Australasian Institute of Criminology*, 78, 1-166.
7. CIPPIC. (2007) Identity theft: Introduction and background, *Canadian Internet Policy and Public Interest Clinic (CIPPIC),* 1, March, Ottawa, 1-27.
8. Clarke, R. (2008) (Id)Entities (mis)management the mythologies underlying the business failures, Working paper, Xamax Consultancy Pty Ltd, April, 1-19.
9. Clauß, S., and Köhntopp, M. (2001) Identity management and its support of multilateral security, *Computer Networks*, 37, 205-219.
10. Economist, The. (2006) Complying with the rules for identity management. *IdenTrust*, 1-28.
11. Fragala, T. (2008) 75% of German households have identities stolen, Truston, December, 1-3.
12. Glaser, D. (2008) Reducing the cost and pain of PCI compliance, *CyberSource*, December, 1-11.
13. Hawker, D. (2001) Certainty of identity: A fundamental of security, *Seminar on eSecurity and eCrime*, 19-20 July, Sydney, Australia, 1-4.
14. IDSP. (2008) Final report volume I: Findings and recommendations, ANSI-BBB, Identity Theft Prevention and Identity Management Standards Panel (IDSP), January, 1-139.
15. ITRC. (2009a) ITRC breach report 2008 final, Identity Theft Resource Center (ITRC), January, 1-201.
16. ITRC. (2009b) ITRC breach stats report 2008 final, Identity Theft Resource Center (ITRC), January, 1-22.
17. ITRC. (2009c) ITRC breach stats - paper vs electronic summary 2008 final, Identity Theft Resource Center (ITRC), January, 1.
18. Jamieson, R., Land, L., Stephens, G., and Winchester, D. (2008) Identity crime: The need for an appropriate government strategy, *Forum on Public Policy Online,* Spring, 1-32.
19. Jamieson, R., Land, L., Sarre, R., Steel, A., Stephens, G., and Winchester, D. (2008) Identity crime definitions, *Proceedings of the ACIS*, December, 2008, Christchurch, New Zealand, 442-451.
20. Jensen, N. (2008) Creating an environment in Australia hostile to money laundering and terrorism financing: A changing role for AUSTRAC [online], *Macquarie Journal of Business Law*, 5, 93-111.
21. Jøsang, A., and Pope, S. (2005) User centric identity management, *Proceedings of AusCERT*, Gold Coast, Australia, May, 1-13.
22. Kim, R. (2009) 2009 identity fraud survey report: Consumer version, Javelin Strategy & Research, February, 1-22.

23. Klein, H., and Myers, M. (1999) A Set of Principles for Conducting and Evaluating Interpretive Field Studies, *MIS Quarterly,* 23(1), 67-93.
24. KPMG Forensic. (2009) Fraud survey 2008: 2008 survey of fraud in Australia and New Zealand, KPMG International, 1-46.
25. McAfee. (2009) Unsecured economies: Protecting vital information, McAfee, Inc., 1-34.
26. Meulen, N. van der. (2006) The challenge of countering identity theft: Recent developments in the United States, the United Kingdom, and the European Union, *Report commissioned by the National Infrastructure Cyber Crime program (NICC), International Victimology Institute Tilburg (INTERVICT),* September, 1-36.
27. Model Criminal Law Officers' Committee (MCLOC). (2008) Final report identity crime, *Commonwealth of Australia*, March, 1-46.
28. Mullens, J. (2008) 'Quackers' attack quantum coding's halo of invincibility, *New Scientist*, October, 24-25.
29. OneName Corporation. (2001) Requirements for a global identity management service, *W3C Workshop on Web Services*, 11-12 April, San Jose, CA USA, 1-3.
30. Organisation for Economic Co-operation and Development (OECD). (2008) Scoping paper on online identity theft: Ministerial background report, *Organisation for Economic Co-operation and Development*, DSTI/CP(2007)3/Final, 1-69.
31. Otjacques, B., Hitzelberger, P., and Feltz, F. (2007) Interoperability of e-government information systems: Issues of identification and data sharing, *Journal of Management Information Systems*, Spring, 23, 4, 29-51.
32. QSR International. (2005) NVivo, QSR International Pty, Ltd, 2, Melbourne, Australia, www.qsrinternational.com.
33. Rutkowski, T. (2007) An emerging global convergence on identity management, ITU Regional Seminar on "Identity Management and e-Signatures", Damascus-Syria, 29-31 October, 1-15.
34. Sproule, S., and Archer, N. (2008a) Measuring identity theft in Canada: 2006 consumer survey, *McMaster eBusiness Research Centre (MeRC) DeGroote School of Business, MeRC Working Paper*, 21, January, 1-102.
35. Sproule, S., and Archer, N. (2008b) Measuring identity theft in Canada: 2008 consumer survey, *McMaster eBusiness Research Centre (MeRC) DeGroote School of Business, MeRC Working Paper*, 23, July, 1-70.
36. Fossi, M. (Ed.) (2009) Symantec Global Internet Security Threat Report Trends for 2008, Symantec, XIV, April, 1-110. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf
37. United Kingdom Home Office. (2006) Updated estimate of the cost of identity fraud to the UK economy. (http://www.identity-theft.org.uk/ID%20fraud%20table.pdf, accessed 18 December, 2006).
38. Urbas, G and Choo, K. R. (2008) Resource materials on technology-enabled crime, technical and background, *Australasian Institute of Criminology*, 28, 1-96.
39. US Government. (2007) Combating identity theft: A strategic plan, President's identity theft task force, April, 1-120.
40. Walters, C. (2009) Hackers' discount - stolen card details for 8 cents, *Sydney Morning Herald Online*, April 15, 1-2. http://www.smh.com.au/articles/2009/04/14/1239474875517.html

APPENDIX

Participant Code	Participant Category	Participant Role
1	Bank	1. Head of Fraud
2	Bank	1. Chief Manager Operational Control 2.Fraud Management
3	Bank	1. Manager Research and Intelligence 2. Intelligence Officer 3. Business Services 4. General Manager Strategy and Security Risk
4	State License Authority	1. Control Management 2. Manager of Financial and Operational Audit 3. Investigations – External Fraud
5	State License Authority	1. Manager
6	Telecommunications	1. Fraud Risk 2. Investigative Analyst
7	Government Agency	1. Compliance, Integrity and Documentation Examination
8	Government Agency	Five Managers – with legal, accounting, IT and fraud experience
9	Government Agency	Director Internal Audit and three other managers
10	Government Agency	1. Deputy Director
11	Government Agency	1. Senior manager
12	U.S. Criminologist	1. Academic – Professor

Table A1. Interview Participant Code, Category and Role Key