Identity Crime: The Need for an Appropriate Government Strategy

Rodger Jamieson, Lesley Land, Greg Stephens and Donald Winchester

Rodger Jamieson, Professor, Information Systems, Technology and Management, University of NSW, Australia
Lesley Land, Lecturer, Information Systems, Technology and Management, University of NSW, Australia
Greg Stephens, Senior Lecturer, Information Systems, Technology and Management, University of NSW, Australia
Donald Winchester, School of Banking and Finance, University of NSW, Australia

Abstract

Identity Crime is a serious problem in today's society costing individuals, organisations and governments millions of dollars in prevention, control, detection and prosecution. This paper aims to provide an introduction to the problem of identity crime in cyberspace together with a discussion of Government strategies for managing this problem. Critical components of a Government strategy to manage identity crime include: legislation, public vigilance and awareness programs, information protection, identity management, law enforcement and justice systems, education and training, reporting procedures, collaboration and alliances, and victim support.

The enactment of legislation, as a strategic policy instrument to mitigate identity fraud and related crime (money laundering, terrorism, trafficking), is a critical aspect of current and future strategies of governments (both nationally and internationally). With appropriate legislation, organisations may act with increased certainty of policy and laws to aid prosecution, recovery and remediation, both civil and criminal.

This paper draws from our research into identity fraud with a number of Australian government and private organisations, and particularly investigates strategies and policies for supporting the enactment of legislation to manage identity fraud and related crimes in cyberspace. Our framework for management of identity fraud in organisations involves a number of phases, stages, and steps. The policy, recovery, and remediation stages especially benefit from appropriate government legislation of identity fraud, identity, data protection, data matching, information sharing, cyber crime, and privacy. The paper briefly discusses inter-jurisdictional issues and collaboration to deter perpetrators, which are gaining prominence for those drafting new or amending current law in these areas. The paper concludes with suggestions for Government strategy in this area.

1. Introduction

This paper investigates essential components for a robust strategy to combat identity crime in cyberspace for governments. The term 'cyberspace' was coined by William Gibson in his 1984 novel "Neuromancer". Our scope defines cyberspace as the Internet; an online or digital world including more recent inter-connective innovations like mobile devices such as phones and personal digital assistants. Cyberspace is a channel enabler and facilitator of identity crime. It is liked by perpetrators due to the anonymity of the transaction process. The scope of ID fraud is not just limited to cyberspace; it includes offline creation of identities. Identity crime is a serious problem in the world today costing individuals, organisations and governments millions of dollars in losses, and expenditure on prevention, control, detection,

and prosecution. Set out below is a summary of a number of studies that have attempted to determine identity crime costs (amounts in billions in stated currency).

- United States of America (US): "According to the Federal Trade Commission, identity theft cost American consumers US$5 billion and businesses US$48 billion last year, in 2005" (Ilett 2006) versus surveyed losses in the United States of America of US$56.6 billion in 2005 and falling to US$51 billion in 2006" and "$45 billion in 2007" measured by Javelin Strategy & Research (2006, 4; 2007, 5; 2008, 2);
- United Kingdom (UK): "The reported annual cost of identity fraud has reached £1.72 billion" up from £1.3 billion in 2004 (UK Home Office 2006);
- Canada: "Annual cost was Canadian $2.5 billion to Canadian consumers and businesses, and the total annual cost to the Canadian economy was estimated at Canadian $5 billion" (Brown and Kourakos 2003);
- Australia: The cost of identity fraud in Australia was estimated to be "Australian $1.1 billion a year with an estimation error of Australian $130 million in 2001-2002" (Cuganesan and Lacey 2003); and the
- Global cost of identity crime in all its forms: "US$221 billion by the end of 2003 (Aberdeen Advisory Group, May 2003) and estimate as high as US$2 trillion by December 2005?" (The Fraud Advisory Panel 2003).

With organisations being targeted by identity fraud perpetrators and incurring huge losses we also argue for implementation of an identity crime enterprise model.

'Identity' has three main attributes - biometric (physiological and behavioural characteristics), attributed, and biographical. In transacting with other entities in cyberspace we often use personal identifying information, such as, passwords, key tokens or personal identification numbers (PINs). Personal identifying information (PII) permits the authenticity

or identifiability of an individual being verified. Verification is based on a prior exchange of details (identity) and questions plus their answers (unique to the individual) between parties. Identity attributes and personal identifying information within the scope of this paper are both critical information (documentation or data) enablers and facilitators of identity crimes.

Identity crime, "refers to offences in which a perpetrator uses a false identity in order to facilitate the commission of a crime" (Australasian Centre for Policing Research 2006). Identity fraud, "refers to the gaining of money, goods, services or other benefits through the use of a false identity" (Australasian Centre for Policing Research 2006). Identity fraud events are preceded by identity theft and identity deception acts, where another's 'identity' is used and the perpetrator seeks anonymity to commit a crime. Identity theft is generally defined "as the misappropriation of the identity (such as the name, date of birth, current address or previous addresses) of another person, without their knowledge or consent. These identity attributes (proof of identity) are then used to obtain goods and services in that person's name" (Credit Industry Fraud Avoidance System (CIFAS) 2007). We define identity deception (sometimes referred to as false identity, fabricated identity, identity manipulation, assumed identity, identity takeover and synthetic identity fraud) as "all other methods a perpetrator uses to obtain an 'identity' that is not their own. Identity deception encompasses the use of a false, lent or borrowed, not necessarily real, identity". Similar to identity theft, identity deception includes the use of personal identifying information as an instrument to commit other crimes (i.e., identity fraud and/or related crimes) (Jamieson, Stephens & Winchester 2007; Lockhart, Jamieson, Winchester & Sarre 2007).

The dangers of online identity crimes are now well-known. More organisations are attempting to provide solutions to these problems. However, perpetrators continue to innovate. For example, recent developments in quantum mechanics allow hackers to break

into even the most secure financial institutions (Barnett 2008). Others continue with online scams defrauding the gullible.

Little or no government strategies and a lack of organisational policies for cyberspace identity security, enables and facilitates potential increases in identity crime and related crime (money laundering, terrorism, trafficking – people, drugs, weapons etc.) costs placed on the individual and society as a whole. This paper aims to fill these observed gaps. We provide an introduction to the problem of identity crime acts in cyberspace together with a discussion of components in a government strategy for managing this problem. The next section describes the background and related literature. The third section explains our methodology. The fourth section discusses essential components for a government identity crime strategy. The fifth section briefly discusses inter-jurisdictional issues. The sixth section looks at implications and limitations. The final section concludes and provides suggestions for governments.

2. Background and Related Literature

> *"There is a heavy price to pay for mistaking components of strategy for strategy itself, or misreading the strategic effect of components. It is more important than ever to remember that strategy operates at a systemic level and that the intellectual framework for strategic thinking flows from a holistic perspective that is more art than analysis"* (Singer 2008, 96).

This study is preliminary in nature for a number of reasons. The current literature is sparse in the specific areas of identity crime, related crimes (money laundering, terrorism, trafficking e.g., people, drugs, weapons etc.) via the cyberspace channel, and its mitigation especially where inter-jurisdictional cases are concerned. Notable exceptions include Phair (2007), Smith and Urbas (2001) and Lininger and Vines (2005) in a phishing context. Jamieson, Stephens & Winchester (2007) investigate identity fraud categorising three main attacks channels used by insiders, organised crime, sophisticated and opportunistic

perpetrator groups; traditional, mechanical/digital devices, and cyberspace. Wang, Yuan, & Archer (2006) introduce an identity theft framework to identify stakeholders and the interactive relationships that play multiple roles in combating identity theft. Within the cyberspace channel examples of methods used by perpetrators include: phishing; pharming; key logging; hacking; viruses; vishing and many others (for more details, see, Phair 2007; Lininger and Vines 2005).

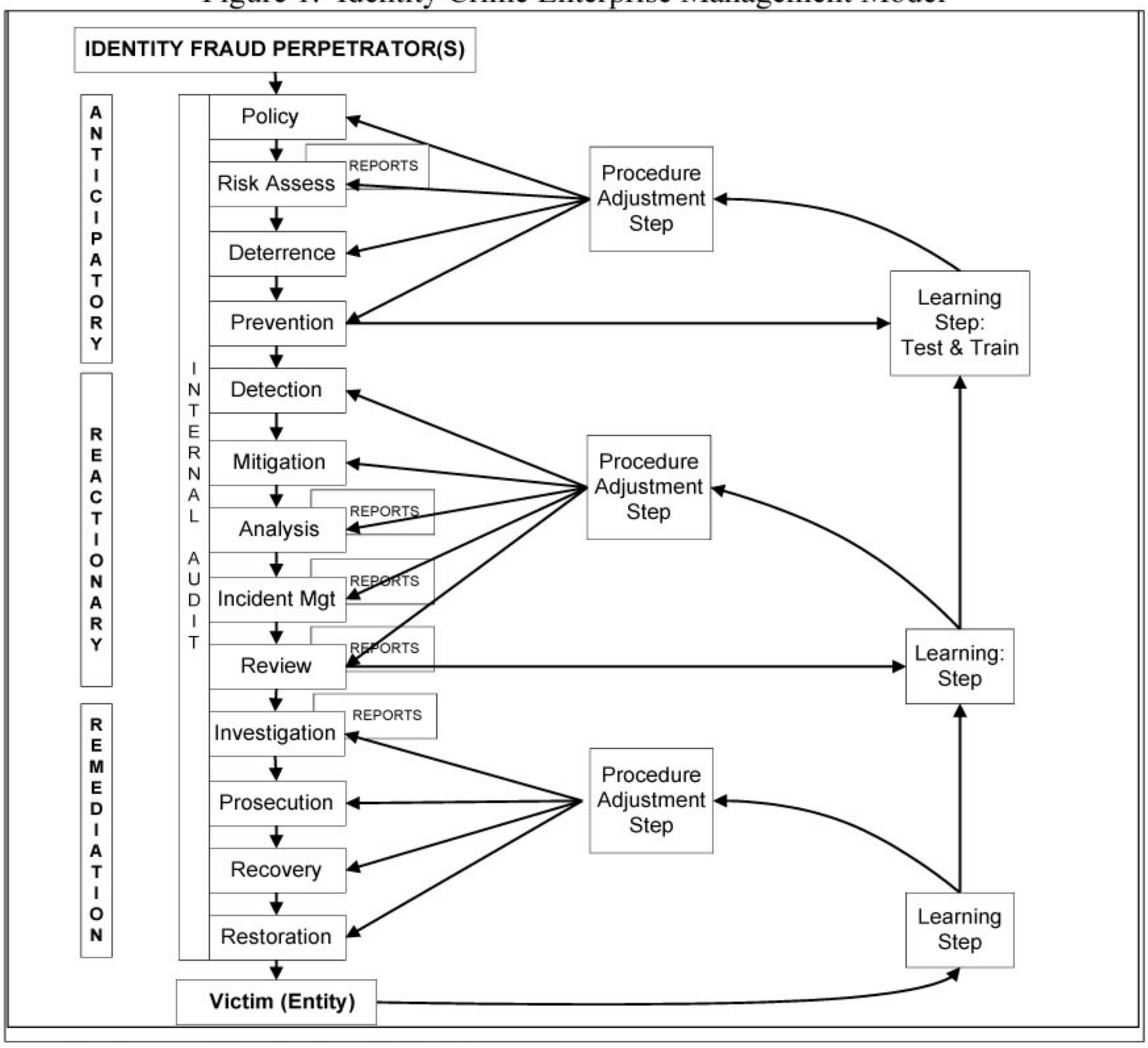
The related literature has investigated cyberspace in terms of trust in online transactions (Kleist 2007; Skogsrud, Benatallah, & Casati 2003), security (Phair 2007), data breaches (Schwartz and Janger 2007; Phair 2007), fraud (Smith and Urbas 2001, McLaughlin 2003), organised crime (McCusker 2006; Phair 2007), digital forensics (Kanellis Kiountouzis, Kolokotronis, & Martakos 2006) and criminal inter-jurisdictional issues (Lim 2007; Hayashi 2007; Spang-Hanssen 2004; Sofaer and Goodman 2001). Stimulating the need for research and solutions are surveys that show trends or the current state of these issues in the areas of identity crime (ID Analytics 2007; Synovate 2007; Baum 2006, 2007; Javelin Strategy & Research 2007, 2008; UK Home Office 2006; Privacy Rights Clearinghouse 2005; Aberdeen Advisory Group 2003), fraud (CyberSource 2007), cybercrime (Wall 2003), data breaches (Bagchi and Udo 2003; Gordon and Loeb 2002; Hinde 2002), and security (e.g., Deloite 2005) from targeted countries like the US, UK, Canada, and Australia. The findings illustrate the need for implementing a government strategy and sound organisational policy to mitigate identity crimes in cyberspace.

Prior research found that organisations and government agencies that are proactive and implement an identity fraud framework (refer Figure 1) and are driven by good policy have several advantages over those who do not (Jamieson, Winchester, Smith 2007). First, organisations are showing their preparedness to combat the insider's (e.g., employee, ex employee etc.) 'attack channel' . Insiders are the highest category of perpetrators of losses

for identity fraud (second is organised crime). By implanting a zero tolerance policy for insider identity crime acts, the organisation also severs the insider-organised crime link. Second, the direction from executive management to measure, manage and mitigate the problem can be a significant cultural shift delivering positive organisational outcomes. Third, the implementation of the management models' (Figure 1) phases (anticipatory, reactionary, remediation), stages (policy, risk assessment, deterrence, prevention, detection, mitigation, analysis, incident management, review, investigation, prosecution, recovery, restoration, and audit), and steps (reporting, procedural adjustment, learning) by enterprises, is granted more certainty by transparent government identity crime management strategy components, such as, legislation (refer Figure 2). Finally, application of the identity crime enterprise management model works in offline and cyberspace situations. Both situations are dynamic, and impact on each other as perpetrators' methods are innovating between attack categories at increasing speeds. The organisational model in Figure 1 accounts for this dynamism with procedural adjustment, learning and reporting steps and stages.

To be effective, a government strategy must be holistic and include the owners and operators of business, private organisations or government agencies. These entities are the first line of defence against perpetrator attack and have a responsibility to take reasonable measures to ensure that their systems are secure both from the outside and inside. They are also in the best position to detect attacks and take the first critical steps to respond by reporting intrusions. At the most basic level, law enforcement needs victims to report to them when their systems are breached and where their identity details are (or may have been) taken. Identity fraud victims, however, are often even more reluctant to call law enforcement than other business victims. Reasons for businesses non disclosure include: loss of reputation, large financial losses, and extended court proceedings (refer, Jamieson, Stephens, & Winchester 2007, for more details).

Figure 1. Identity Crime Enterprise Management Model



Source: Jamieson, Winchester, & Smith 2007.

3. Methodology

This study, investigates strategies and policies for supporting the enactment of legislation to manage identity fraud and related crimes in cyberspace. Our framework for the management of identity fraud in organisations (see Figure 1) draws from our research into identity fraud with a number of Australian government and private organisations.

We interviewed 11 organisations (27 experts from different backgrounds, and roles e.g., fraud, finance, accounting, audit, legal, ex law enforcement) and a United States

criminologist to gain intelligence and to learn from his experience on the identity (theft) fraud phenomenon. Interviews were semi-structured and most were face-to-face with an approximate duration of 90 minutes. Two out-of-state interviews were conducted by teleconference.

Organisations were selected because they issued and/or used identity documents and/or were primary targets of perpetrators (e.g., banks, retailers, government welfare, and Road Transport Authorities for driver licenses). Insights from interviewing the United States criminologist were extremely valuable as at that time only the United States had enacted identity crime (theft) legislation. Interviewee transcripts were recorded, transcribed, and coded using qualitative analysis software (NVivo 2 2002). Participant interview dialogue enhanced our formulation of identity crime definitions (refer Lockhart et al., 2007) and in turn, the scope for development of ideas and themes to consolidate components in the framework of a government strategy to manage identity crime. This framework is presented as a concept map (Figure 2). Our framework is based on what governments should be doing in this area derived from the interviews and literature. We then look at what governments are actually doing in practice. For example, in Australia the New South Wales state government is using security standard *AS/NZS17799:2005* (this standard has since been superseded by 27001 and 27002) for the 'information protection' strategy component in Figure 2.

4. Components for Government Identity Crime Strategy

Figure 2. Strategy Components for Government to Manage Identity Crime

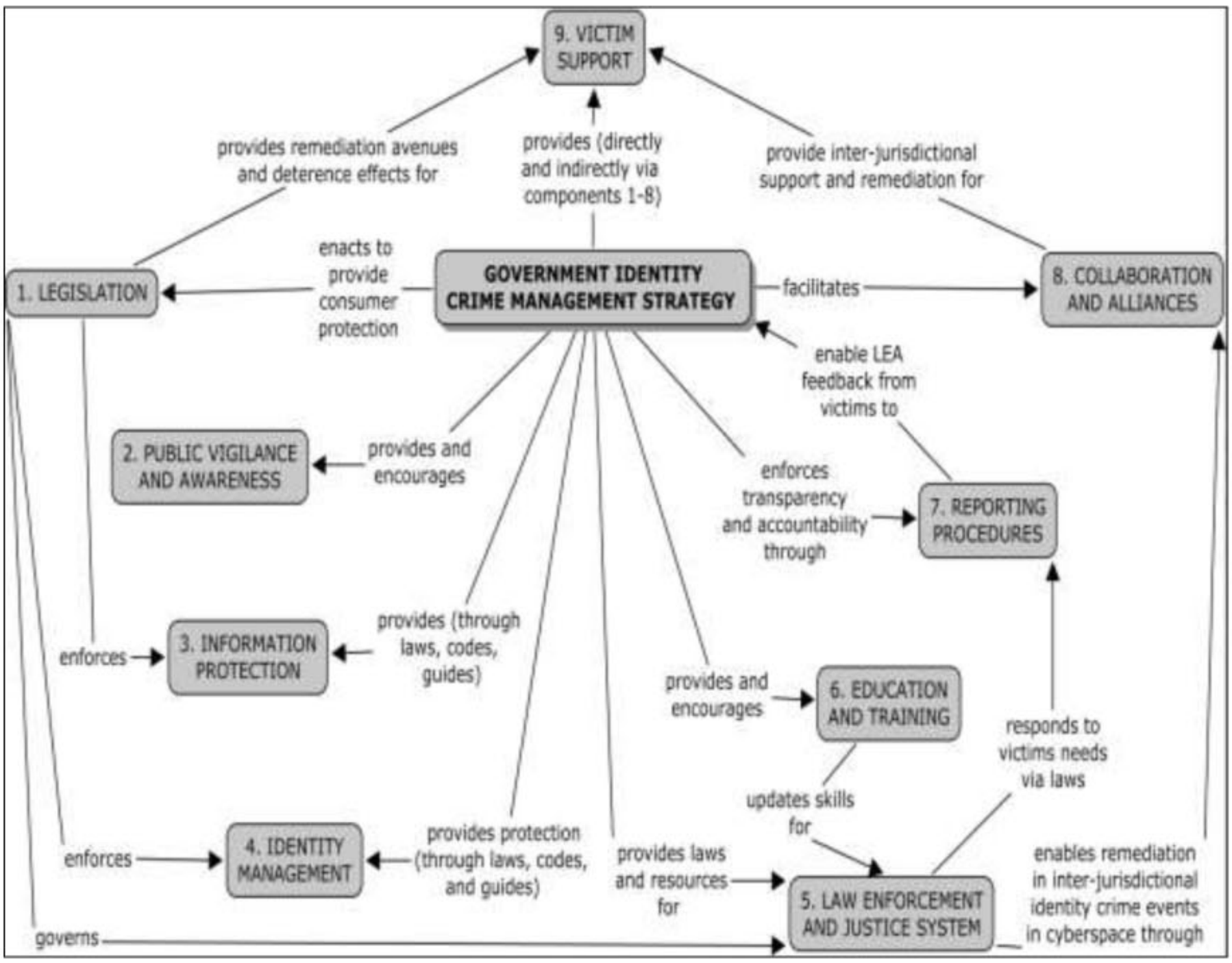


Figure 2, shows the components for a government strategy to manage identity crime presented as a concept map.

4.1 Legislation

In this subsection we investigate for Australia, Canada, UK, and the US any legislation enacted that is specific to identity crime, and related issues; false identification, privacy and the use of personal data, and credit law. Legislation in respect to these areas is relevant to controlling identity crimes in cyberspace (Paul 2006).

The US is the leader in enacting identity crime laws nationally and within most states. Starting with the Federal Identity Theft and Assumption Deterrence Act of 1998 (18 USC 1028) which makes identity theft a crime with maximum penalties of up to 15 years imprisonment and a maximum fine of US$250,000. Later, the Credit and Debit Card Receipt Clarification Act of 2007, the Fair and Accurate Credit Transactions Act of 2003 (FACTA) – both amendments to US federal law, the Fair Credit Reporting Act (FCRA), and the Identity Theft Penalty Enhancement Act of 2004 were enacted to strengthen systems and procedures as the identity crime phenomenon and related crimes evolved. Australia, Canada, and the UK currently do not have specific national identity crime laws. Australia and Canada have bills before their parliaments for general discussion, consideration and approval prior to enactment. In Australia, the state of South Australia has specific identity crime legislation. The state of Queensland also enacted specific identity crime legislation in 2007. The South Australian Criminal Law Consolidation (Identity Theft) Amendment Act 2004 includes specific offences related to identity theft. These are:

- Assuming a false identity or falsely pretending to have particular qualifications to be entitled to act in a particular capacity and intending to commit or help commit a serious criminal offence;
- Making use of another's personal identification information intending to commit or help commit a serious criminal offence;
- Possessing or producing material that would enable someone to assume a false identity or exercise a false right of ownership intending to use it or allow another to use it for a criminal purpose;
- Possessing equipment for making material that would enable someone to assume a false identity or exercise a false right of ownership intending to use it to commit one of these offences; and

- With the offences attracting a maximum jail term of up to 12 years.

Other relevant legislation include: false identification laws; laws governing privacy and the use of personal data; and banking and finance laws (see Paul 2006, for US examples) as well as laws increasing penalties for terrorism, money laundering and trafficking (drugs, human, weapons etc.). Australia, Canada, UK, and the US all have many laws covering these broad themes. These laws have been developed over many years and often introduced before identity acts or events became significant and numerous enough to require specific legislation for prevention, detection, deterrence, control, remediation, and stronger prosecution requirements.

4.2 Public Vigilance and Awareness

In Australia the Australian Federal Police (similarly, the FBI in the US, Metropolitan Police in UK, the Mounted Police in Canada) and other government agencies have initiated consumer education programs which have made consumers more aware of the danger of leaving personal information vulnerable or unprotected.

Individuals and entities are urged to use credit monitoring and take other measures such as being alert for fraudulent activity (fraud alerts) on credit cards and if lost or suspected stolen, contact the issuer immediately and place a stop on the card (credit freeze). Well known credit monitoring agencies include: Veda Advantage; Dun and Bradstreet; Equifax; Experian; and TransUnion. Credit monitoring allows consumers to learn if someone is seeking to borrow money or get a new credit card in their name as well as other changes made to their credit report. Many banks, insurance firms and other organisations have also launched insurance policies to protect customers against identity crime. Consumers may also dispute credit card transactions if the products/services they purchase are not delivered.

Identity crime (e.g., theft) insurance typically pays for the costs of restoring ruined credit, including lost wages and telecommunications bills.

4.3 Information Protection

In Australia, Canada, the UK, or the US, no comprehensive national law yet exists that generally requires notification of breaches of security involving personal information (in the US the Gramm-Leach-Bliley Act (the "GLBA") requires notification of data breaches, but the GLBA only applies to financial institutions). At the state level, California passed the first data breach notification statute in 2003, currently over 30 states (Florida, Montana, New York, and North Dakota among them) and one local jurisdiction have enacted similar laws (though many of these laws contain significant differences). The California law (2002) requires owners, licensors, or simply custodians of personal information to notify data subjects whose information was or is reasonably believed to have been acquired in an unauthorised manner (Kronish 2007, pp. 1-3). Rubel (2005) outlines Security Breach Bills and passed Legislation in the 49 other State Legislatures plus New York City.

In the United States, the Privacy Rights Clearinghouse presents on their website (http://www.privacyrights.org/ar/ChronDataBreaches.htm) a chronology of data breaches that is intermittently updated. As of January 28, 2008 there were an estimated total of 217,586,014 *known* individuals' identities breached. On January 26, 2005 the Federal Trade Commission (FTC) announced they had reached a settlement with ChoicePoint for their data security breach in April of 2005. The total civil penalties and customer redress was stated as US$15 million dollars (US $10 million in civil penalties and US $5 million for consumer redress). The financial penalties are only part of the settlement; ChoicePoint has also been ordered to implement new procedures to ensure that it provides consumer reports only to legitimate businesses for lawful purposes, to establish and maintain a comprehensive

information security program and to obtain audits by an independent third-party security professional every other year until 2026 (Henry 2006, pp. 1-2). On January 27, 2008, ChoicePoint agreed to pay US $10 million to settle a class action lawsuit (Privacy Rights Clearinghouse 2008). Government and organisations need appropriate levels of computer security especially for mobile computer and related devices according to the data stored or accessible on the equipment including encryption and secure passwords (e.g., alpha-numeric).

4.4 Identity management

Identity management does not have a clearly defined 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). Cavoukian (2007) gives examples of three types of identity management, centralised (a firms' username and password or a states identity card), user-centric (individual control e.g., student identity card for concessions), and federated - a mix of centralised and user-centric.

One definition of identity management is "managing various partial identities (usually denoted by pseudonyms) of the individual, i.e. administration and design of identity attributes as well as choice of the partial identity and pseudonym to be (re-) used in a specific context or role" (Pfitzmann and Hansen 2006, see p.25). Traditionally, identity management has been concerned with managing an organisation's employees to ensure that their authentication and authorisation information is consistent and up-to-date within the organisation's information systems. This traditional arena continues to pose many challenges for security architects and designers, especially given the large base of legacy systems. However, the true value of identity management comes into play with business partners and consumers. The ability to federate identity across organisations while maintaining clear trust, liability, and cost responsibilities is a major challenge for organisations as they continue to chase efficiency and

cost savings in cross-organisational business and customer-relationship processes (Buell and Sandhu 2003).

Appropriate security policies are needed to reduce the vulnerability in identity management systems in the public and private sectors. Government and organisations must make sure they do not expose their own or others' identity (or personal identifying information) details – for example refer to the loss of 11,000 Military ID cards by UK defence forces reported in King (2008). The 'circularity effect' of identity document enrolment, the ability where one piece of identity or personal identifying information can be used to reconstruct an individual's 'identity set' of proof of identity documents often allows identity crime perpetrators to gather enough details once a starting point for proof of identity/personal identifying information is accessed.

An example of a digital identity-management system is multiple and dependable digital identity (MDDI) whose aim is to safeguard data, including identity information (see Damiani 2003). Some of the better known federated identity management solutions include: Liberty Alliance (www.project liberty.org); Microsoft Passport (www.passport.com); web services, WS-Federation (A specification, by IBM and Microsoft); and Security Assertion Markup Language, SAML (refer Organisation for the Advancement of Structured Information Standards (OASIS)). These are an attempt to develop an open, interoperable standard for digital identity management and to manage Web based identification and authentication (Buell and Sandhu 2003; Durante 2003; Wang, Yuan & Archer 2006). In the United States the following legislation governs identity management: Sarbanes-Oxley Act, Patriot Act (2001), and the Electronic Signatures in Global and National Commerce Act (2000). Similarly, in Australia "under the Privacy Amendment (Private Sector) Act (2000), website operators that collect personal information online must take reasonable steps to ensure that Internet users know who is collecting their information and how it is to be used,

stored and disclosed" (The Economist Intelligence Unit 2006, p.19). In the European Union several directives regulate identity management: money laundering (2005/60/EC), value added tax invoicing rules (2001/115/EC), community framework for electronic signatures (1999/93/EC), data protection (1995/46/EC), among others.

4.5 Law Enforcement and Justice System

The purpose of this strategy component is to focus on identity crime and the main aim is to prevent and reduce the incidence of all stages of identity crime from deterrence, detection, prevention, and control to remediation and recovery, and to assist victims of identity crime. This strategy component is enabled, facilitated and strengthened by a robust legislative strategy component. Law enforcement includes the police, research, and infrastructure, such as databases and communications (secure) networks to liaise with local, national and international counterparts. The justice system involves the courts (criminal and civil) that preside over perpetrator cases and deliver judgments. Judgments may be monetary and/or custodial in nature.

The level of perpetrator sophistication, innovation and criminal networking capability creates significant challenges for law enforcement. Initiatives in the areas of research and identity crime data collection are critical for law enforcement to (1) keep up-to-date with perpetrator methods of attack, to monitor and to police targeted regions; and (2) to assist targeted organisations monitor critical targeted products/services, as well as other important areas such as organised crime and high-tech crime innovations. The importance of this component in the overall strategy to mitigate identity crime is to continually elevate law enforcement agencies to the cutting edge in technology and skills to maintain their competitive advantage in prevention, detection, deterrence, and control over perpetrators. For example, the Australian government set up the Australian Crime Commission (ACC) on 1

January 2003. The ACC aims to reduce the incidence and impact of serious and organised criminal activity. Similarly, the Australian High Tech Crime Centre (AHTCC) was set up on 2 July 2003. The role of the AHTCC (AHTCC Online 2008) is to:

- provide a national coordinated approach to combat serious, complex and multi-jurisdictional technology enabled crimes, especially those beyond the capability of single jurisdictions;
- assist in improving the capacity of all jurisdictions to deal with technology enabled crime; and
- support efforts to protect the National Information Infrastructure (NII).

An integral part of the AHTCC is the Joint Banking Finance Sector Investigation Team (JBFSIT) combating internet banking fraud. In addition, the Australian Identity Fraud Protection Register (AIPR), commenced in 2004, following on from the Identity Fraud Register Pilot which began in February 2002. This national data collection allows law enforcement agencies to detect and stop the use of fraudulent identities (AUSTRAC 2007, p.21).

Legislation that provides for increased punishment will not stop all identity crime perpetrators cyberspace attacks, especially those from the criminal organisation category. However, proper resourcing of law enforcement and the justice system will prevent, deter, detect, and control through target hardening. Specific groups are needed to focus on identity crime in the cyberspace channel where specialist technical skills are required in forensics and evidence gathering to support due process in the justice system (refer Brungs and Jamieson, 2005). To prosecute identity crime perpetrators successfully law enforcement agencies require as many details of the perpetrator attack as possible be gathered from victims, whether they be individuals or entities. Evidence a victim needs to keep includes any

documentation that provides an audit trail of what happened. Important documentation may include: bank statements; credit card receipts; cancelled cheques; voice mail or text messages, faxes; emails, photos, computer forensic evidence and other related information that may seem trivial at the time. This may also include output from software monitoring systems within victim organisations. The law enforcement and justice system component is linked to the next component education and training.

4.6 Education and Training

Education (see Wang et al., 2006) and training (see also Commission of the European Communities 2007) can help prevent and detect identity crimes. As identity crime is a serious and increasingly prevalent activity, businesses and consumers need to take preventative measures to minimise the chance of becoming a victim.

In an exploratory study to assess consumer preparedness, Milne (2003) measured the self-reported behaviour of 61 college students with an average age of 21 (65% were male) and 59 non-students with an average age 36 years (49% male) against thirteen identity theft preventative activities that were suggested by the Federal Trade Commission (US). Milne (2003, p.338) found that "consumer education appeared to be adequate for several identify theft preventative behaviours, but not for others". For example, students in over 66% of cases were practicing theft prevention for PINs and passwords, social security cards, and were not carrying more credit cards than needed in their wallet or purse. They also did not dispose of credit card receipts in public waste containers and checked billing statements or destroyed unwanted credit card offerings. However, few students practised theft prevention when ordering new cheques, choosing to receive them from the bank via surface mail, had ordered a copy of their credit card report within the last year, or had not determined marketer's use of their personal identifying information. Non-students were also careful (>67% who answered)

with PINs and passwords in wallets and purses, not leaving mail in mailboxes for more than two days, shredded unwanted credit card offerings, and with social security card numbers when asked for by merchants. Practices that few non-students followed (<45% practice) included: carrying their social security card in their wallet or purse, having banks mail out their new cheques, and not ordering a copy of their credit card report within the last year. Based on his exploratory study, Milne (2003) recommended a continued increase in consumer education, especially as identity theft gets more sophisticated and moves to cyberspace. A future research area suggested was to "examine business responsibility in minimising identity theft" (Milne 2003, p.401).

It is an established fact that technological developments produce a need for continuous training with respect to identity crime in cyberspace and cyber crime issues, for example, law enforcement and judicial authorities. The European Union Commission in close cooperation with Member States and other competent organisations, such as, Europol, Eurojust, the European Police College (CEPOL) and the European Judicial Training Network (EJNT), work to achieve a European Union level coordination and interlinking of all relevant training programmes (Council of Europe 2007). Similarly, "the U.S. Department of Justice's Office of Overseas Prosecutorial Development, Assistance and Training (OPDAT) are specifically tasked with providing assistance to strengthen criminal justice institutions in other nations and enhancing the administration of justice abroad. Often working in tandem with OPDAT is its sister unit within the Department of Justice, the International Criminal Investigative Training Assistance Program (ICITAP), which provides assistance to police forces in developing countries throughout the world. The International Criminal Investigative Training Assistance Program's assistance is designed to strengthen police investigative capacities and imbue respect for human rights and the rule of law in emerging police forces" (Swartz 2001, p.10).

4.7 Reporting Procedures

In the United States, the Identity Theft and Assumption Deterrence Act of (1998), directs the Federal Trade Commission to establish procedures for educating the public, receives complaints, and coordinates enforcement efforts with various investigatory agencies. Well designed transparent reporting procedures need to be put in place at government agencies and organisations to exploit weak controls on the obtaining of proof of identity and personal identifying information details.

Several organisations have been set up by government and private organisations that allow consumers to file complaints. For example, eConsumer permits consumers to file a cross-border complaint that will be quickly accessible to multiple government enforcement agencies. Econsumer is a joint project of consumer protection agencies from 21 nations. The information contained in a complaint allows the appropriate government agencies to detect current fraudulent activity (schemes or scams etc.) and help decide what action to take. Reporting a complaint assists in helping prevent other consumers from being victimised in a similar manner. On April 24, 2001, responding to the challenges of multinational Internet fraud, and working to enhance consumer protection and consumer confidence in e-commerce, thirteen countries unveiled econsumer.gov, a joint effort to gather and share cross-border e-commerce complaints. The project has two components: a multilingual public Web site, and a government, password-protected Web site. The public site provides general information about consumer protection in all countries that belong to the International Consumer Protection Enforcement Network (ICPEN), contact information for consumer protection authorities in those countries (as of May 2008 there were 35 countries including the European Union and OECD), and an online complaint form. Using the existing Consumer Sentinel network (a database of consumer complaint data and other investigative information operated

by the United States Federal Trade Commission), the incoming complaints are shared through the government Web site with participating consumer protection law enforcers (e.consumer online 2008). Another similar organisation is the Reporting Economic Crime On-line (RECOL) administered by the Royal Canadian Mounted Police in Canada.

Credit reports, security freezes and fraud alerts, are free in some countries and relatively inexpensive in others. In the United States, the Fair and Accurate Credit Transactions Act (FACTA) which was passed in 2003, is a federal law which allows consumers to request and obtain a free credit report once every twelve months from each of the three nationwide consumer credit reporting companies (Equifax, Experian and TransUnion). Similarly, in the United Kingdom you have the right to request a Statutory Credit Report from any of the three credit reference agencies (Callcredit, Experian and Equifax) who, under the Data Protection Act (1998), are permitted by law to charge you (currently £2) for each request you make. Details that you will also be asked for include: your name, date of birth, full current, and previous address(es). Canadian residents are able to get free credit reports by mail from credit bureaus (Northern Credit Bureaus, TransUnion and Equifax). In Australia residents are able to get free credit reports (within 10 working days) from either Veda Advantage or Dun and Bradstreet. Additionally, as an example, Veda Advantage offer a credit alert package (currently A$30 annually) that notifies you whenever someone applies for credit in your name. Economic losses can become expensive, if a security intrusion turns into identity fraud.

4.8 Collaboration and Alliance

Most legislation for cybercrime and certainly for identity crime is nationally based – country, state, etc. This is a problem for remedial actions when identity crime acts occur in cyberspace (see section 5 for inter-jurisdictional issues). Collaboration and alliances between

nations to legislate across several countries in relation to what is considered illegal and occurs in one country, initiated from and proceeds used in another via cyberspace is at an embryonic stage (Lim 2007). Within a nation there is the need for groups to be responsible for coordinating and participating in the negotiation of bilateral and multilateral treaties on international crimes, such as, identity crime. Cooperation between nations matters, such as extradition, mutual assistance and international transfer of perpetrators through agreements or treaties is also required. Future collaboration between nations is needed to legislate for identity crimes facilitated in cyberspace. Currently most actions for remedy are by mutual agreement or convention between countries rather than all encompassing legislation across countries; (e.g., Council of Europe Cybercrime Convention of 2001 – a signed agreement by over 43 countries but ratified by only six countries in July 2004).

Cyberspace related law, directives, treaties, conventions, agreements, and codes across countries are critical to resolve identity crime related acts occurring in cross border situations. Regions or groups of countries leading the cybercrime fight include: the Council of Europe (COE) Convention on Cybercrime, group of eight (G8, countries), the Organisation of American States, Asia Pacific Economic Cooperation (APEC), United Nations (UN), European Union (EU), the Commonwealth States, Organisation for Economic Cooperation and Development (OECD), Association of Southeast Asian Nations (ASEAN) Group of States, all seeking to reach the goal of a global legal framework against cybercrime. There are also many other groups, bodies, committees, and forums with a global focus. An example is, the Information Systems Audit and Control Association, which is a global body dedicated to the security of information technology systems.

The Council of Europe Convention on cybercrime of 2001 (see Dunn, Krishna-Hensel, and Mauer 2007, for more information), entered into force on July 1, 2004 and is a significant achievement in the fight against cybercrime. By ratifying or acceding to the

Council of Europe Convention of Cybercrime, or implementing the principles, countries agree to ensure that their domestic laws criminalise conducts that are described in the substantive criminal law section and to establish the procedural tools necessary to investigate and prosecute such crimes. This is the harmonising of national legal approaches on cybercrime. As of January 2008, the total numbers of signatures not followed by ratifications is 21 countries. A total of 22 countries have ratified/acceded including: Albania, Armenia, Bulgaria, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Hungary, Iceland, Latvia, Lithuania, Macedonia, Netherlands, Norway, Romania, Slovenia, Slovakia, Ukraine, and the United States. As can be noted from the list of COE countries and the regional or groups of countries, there are many countries in more than one group which facilitates knowledge development through information sharing in combating identity crime through cyberspace crime agreements, treaties, codes and directives.

4.9 Victim Support

The last component in our government strategy list is by no measure the least significant. In fact, all eight other components' activity is aimed at helping the victims – entities or individuals - of identity crimes to protect them or facilitate a remedy process. Consumers, who believe they have been a victim of deceptive practices on the Internet, can register their complaint at www.econsumer.gov, International Consumer Protection Enforcement Network's global online complaint mechanism. Seventeen member countries have access to this mechanism for the purposes of monitoring online conduct, and taking enforcement actions where possible (e.g., see http://www.econsumer.gov/english/contentfiles/pdfs/econsumer_sta ts.pdf). Also the Organisation for Economic Cooperation and Development governments have agreed on guidelines outlining a framework for international cooperation to protect consumers against

the growing problem of cross-border fraud, particularly on the Internet. Inter-jurisdictional issues reinforce the importance of the last two government identity crime strategy components facing governments in the future as noted by Lim (2007).

5. Inter-jurisdictional issues

The International Criminal Police Organisation, INTERPOL (also Europol, the European Union's criminal intelligence agency of 27 countries), is an organisation that facilitates transnational law enforcement cooperation[1]. The international policing agency provides all of its member countries with instant, direct access to a wide range of criminal information through a variety of databases. This enables the global law enforcement community to connect seemingly unrelated pieces of data, thereby facilitating investigations and enhancing international police cooperation. These databases, accessible through the International Criminal Police Organisation's I-24/7 global police communications system, have the following features: compliance with international standards; legally founded; technologically advanced; accessible through I-24/7's virtual private network; embedded security features; and flexibility to permit user customisation. To date however, the International Criminal Police Organisation has not added any type of cybercrime, including identity crimes, to its annual crime statistics. But two databases are important in this area. First, the stolen and lost travel documents database contains information on more than 15

---

[1] International Criminal Police Organisation (INTERPOL) is an intergovernmental organisation that facilitates cooperation between the criminal police forces of more than 180 countries. The international policing agency aims to promote the widest-possible mutual assistance between criminal police forces and to establish and develop institutions likely to contribute to the prevention and suppression of international crime. International Criminal Police Organisation agents do not make arrests.

million travel documents reported lost or stolen by 125 countries. Second, the stolen administrative documents database contains information on 185,000 official documents which serve to identify objects, for example, vehicle registration documents and clearance certificates for import or export. Identity crime committed in cyberspace is clearly, however, an international problem. The International Criminal Police Organisation, collects, stores, analyses and shares information on cybercrime with its 186 member countries through its I-24/7 global police communications system. Other aspects of International Criminal Police Organisation's cybercrime programme are designed to:

- facilitate operational cooperation among member countries through a list of contact officers available around the clock for cybercrime investigation;
- increase the exchange of information among member countries on cybercrime modus operandi through regional working parties and training workshops;
- assist member countries in the event of cyber attacks or cybercrime investigations through investigative and database services; and
- develop strategic partnerships with other international organisations and private-sector bodies (INTERPOL Online 2008).

The International Court of Justice (previously the Permanent Court of International Justice) in The Hague, Netherland, acts as a world court. The Court has a dual jurisdiction, it decides, in accordance with international law, disputes of a legal nature that are submitted to it by States (jurisdiction in contentious cases); and it gives advisory opinions on legal questions at the request of the organisations of the United Nations or specialised agencies authorised to make such a request (advisory jurisdiction). The International Court of Justice was established by the Charter of the United Nations, which provides that all Member States

of the United Nations are automatically parties to the Court's Statute. The composition and functioning of the Court are organised by this Statute, and by the Rules of the Court which are drawn up by the Court itself.

The Convention on Cybercrime of the Council of Europe is the only binding international instrument on the issue of cybercrime. It serves as a guideline for any country developing comprehensive national legislation against cybercrime and as a framework for international cooperation between State parties to this treaty (Commission of the European Communities 2007).

> "The Council of Europe Convention (2001) is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography and violations of network security. It also contains a series of powers and procedures such as the search of computer networks and interception. Its main objective, set out in the preamble, is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international cooperation" (Commission of the European Communities 2004).

The Convention, which was adopted and entered into force in 2004, contains common definitions of different types of cybercrime and lays the foundation for a functioning judicial cooperation between contracting states (Commission of the European Communities 2007). The lack of global legislation (i.e., only conventions or treaties exist) for identity crime facilitated in cyberspace (i.e., cross-border cyber crime legislation) adds to the complexity of the situation (Lim 2007; Commission of the European Communities 2007).

Collaboration between governments and associated alliances among law enforcement agencies is proving an effective method to detect, prevent, deter, and control perpetrators. The Council of Europe Cybercrime Convention 2001 "addresses an important problem: the difficulties law enforcement has in pursing criminals across national borders, something that is common in Internet crime" (Lemos 2001, p. 2).

In November 2001, the members of the Council of Europe signed an extraordinarily broad new treaty to increase cooperation among law enforcement officials of different nations. Officially, this Cybercrime Convention was drafted by the 43-member Council of Europe, with the U.S., Canada, Japan and other countries participating as observers. In reality, American law enforcement officials have been among the primary drivers behind the treaty. The Cybercrime Convention does three major things:

- It includes a list of crimes that each member country must have on its books. The treaty requires criminalisation of offenses such as hacking, the production, sale or distribution of hacking tools, and child pornography, and an expansion of criminal liability for intellectual property violations (Articles 2-11).
- It requires each participating nation to grant new powers of search and seizure to its law enforcement authorities, including the power to force an Internet service provider to preserve a citizen's internet usage records or other data, and the power to monitor a citizen's online activities in real time (Articles 16-22).
- It requires law enforcement in every participating country to assist police from other participating countries by cooperating with 'mutual assistance requests' from police in other participating nations 'to the widest extent possible' (Articles 23-35). [http://www.treatywatch.org/about.html]

Better communication between law enforcement bodies in multi-jurisdictional scenarios, will facilitate more cross-border collaboration and alliances, in the form of task forces or working groups. Otherwise identity crime and related crimes in cyberspace will thrive in countries or states where government rule of law is poorly established, for example, Russia and China. "Russia is one of the least cooperative countries, when it comes to fighting

cybercrime originating within its borders" (O'Connell 2007, p.1). "China has surpassed Russia as the biggest producer of malware" (Brenner 2007, p.2). For instance, "in October 2006, the National Bank of Australia took active measures against Rock Phish (a group of phishers), both directly and via a national anti-phishing group to which the bank's security director belonged. A Russian Internet service provider, Russia Business Network, retaliated by crashing the bank's home-page for three days" (Economist.com 2007, p.2). But Russia Business Network, does not violate Russian law, the illegal activities are all carried out by groups that buy hosting services from them.

The current laws and treaties do not specifically cover identity fraud or other identity crimes such as identity theft or identity deception. Only the US has identity theft laws at the national level. This means other laws need to be used to prosecute identity crime and related crimes such as laws under the broad themes of false identification; privacy and the use of personal data; and credit laws, among others. Further legislation needs to be passed by governments at the national level to alleviate inter-jurisdictional law enforcement and justice system impasses for identity crime in the cyber channel. National identity crime laws will facilitate conventions, treaties, and directives across borders to prevent, detect, deter, and control these events.

6. Implications and Limitations

This research informs theory by presenting an identity crime strategy for government with nine critical components that requires further research and validation. In practice, this strategy model will enable identity crime planners to effectively manage identity crime attacks. Benefits include having a proactive government strategy of action for each major component that anticipates, reacts to, and remedies identity crime acts. This provides a government with a ready set of components to implement immediately. Limitations of this

study are that in most cases we identified only national laws applicable to our main theme - identity crime in cyberspace. For brevity we leave for further study the state, territory, provincial, or local laws. We could also capture cornerstone cases which highlight situations where laws could be developed to prevent or prosecute future occurrences.

7. Conclusion and Suggestions

Implications of the legislation component of government strategy to manage identity crime are far reaching. In terms of mitigating the scale of the estimated economic impact, cost and resources for implementation of a proposed strategy the public vigilance and awareness component is the least expensive and potentially most reinforcing. However, it places all the emphasis of a potential identity crime event on the unknown targeted victim.

Identity crime has a lot of dimensions and should be dealt with by governments from a holistic perspective. The framework we put forward in the context of cyberspace is applicable to other channel categories such as traditional or manual identity creation or the use of mechanical or digital devices such as skimmers. Identity crime is a growing global phenomenon even though some survey reports show identity theft in the United States to be declining. The supposed United States decline in the cost of identity theft may be because of target hardening due to more resources now focused on detection, prevention, deterrence, and control measures. In addition, the lag effects of the introduction of United States federal and state legislation is having on current and potential perpetrators.

The identity crime phenomenon is a multi-jurisdictional issue, requiring a collaborative approach that takes into account cross-border; international, national, and local requirements. Many developed countries have initiated research to assess the current nature and extent of identity crime within their boundaries or undertake regular surveys to show trends over time. However, the methodologies across regions or countries differ and there is a

need for more reliable figures and statistics about identity crime. To date, definitional issues are given as reason for inconsistencies across time and location. This raises the need for the 'reporting procedure' component of a strategy to be, appropriate, consistent, transparent, and in agreement across jurisdictions. Collaboration and alliances should facilitate and enable information sharing within the bounds of privacy regimes of parties, whether bilateral or multilaterally.

Education and training for victims on identity crime attacks, reasons for being targets, prevention, detection, deterrence, and control areas, is important. Similarly, law enforcement agency personnel need to have their skills updated for identity crime acts within cyberspace. Within the justice system there is the ongoing need for education and training in digital and computer forensics and evidence gathering to bring crime investigations and prosecutions against perpetrators to satisfactory closure. This will positively act as further deterrence for the community in general.

Public vigilance and awareness programs in the community about the risk of being a target victim of identity crime will prevent and detect some criminal activity. These programs will also have some deterrence effects for perpetrators, knowing that individually and collectively they are being monitored.

Legislation impacts many of the other strategy components in our framework as a deterrent to identity crime. A delay with the introduction of specific identity crime legislation by many developed nations is frustrating those nations or states and cross-border collaboration for law enforcement and justice. Reasons put forward to law enforcement and justice systems, by governments has to date been that identity crimes are covered by provisions in other already enacted law criminalising the act or event accordingly. This negates any urgency in writing legislation for identity crime as a standalone criminal code. Yet governments have enacted legislation expeditiously when warranted e.g., terrorism

legislation. Issues of an inter-jurisdictional nature require a major effort to work on solutions. Conventions, directives and treaties at least are a step in the right direction. Legislation enacted to criminalise cross border acts and events for identity crime in cyberspace relies on government collaboration and alliances.

Suggestions for governments first of all, are to consider, then develop and implement a national strategy and components as outlined in this paper, while working within the current inter-jurisdictional agreements. The next important step is to enact identity crime legislation at the national level. The agreement for identity crime in cyberspace in the future will hopefully be enacted in legislation – this should be the target of countries in regional groupings. This will permit identity crime perpetrators to be prosecuted within and across borders where identity crime legislation is enacted and where cross-nation agreements or laws permit.

8. References

AUSTRAC "The Extent of Money Laundering in and through Australia in 2004" (2007): 1-125. http://www.aic.gov.au/crc/reports/200304-33.pdf

Australasian Centre for Policing Research (ACPR) 2006, Standardisation of definitions of identity crime terms: A step towards consistency, Commonwealth of Australia (145.3), March, pp. 1-22.

Bagchi, K., and Udo, G. "An Analysis of the Growth of Computer and Internet Security Breaches," *Communications of AIS* 12 (2003): 684-700.

Barnett, Stephen., Identity fraud to be debated http://news.scotsman.com/ education/ Identity-fraud-to-be-debated.3617954.jp 2008.

Baum, K., "Identity Theft, 2005: National Crime Victimization Survey" U.S. Department of Justice, (November 2007): 1-8.

Baum, K., "Identity Theft, 2004: First Estimates from the National Crime Victimization Survey" U.S. Department of Justice, (April 2006): 1-8.

Brenner, B., "How Russia became a malware hornet's nest," *SearchSecurity.com* (October 2007): 1-2. http://searchsecurity.techtarget.com/originalContent/ 0,289142,sid14_gci1275987,00.html last accessed January 10 2008.

Brown., David C.G., and George, Kourakos., "Public Policy Forum RoundTable on Identity Theft and Identity Fraud", 2003, 26 June, Ottawa, pp. 1-23, http://www.pp forum.ca/common/assets/publications/en/identity_theft_fraud.pdf, accessed 10-6-06).

Brungs, A., and Jamieson, R., "Identification of Legal Issue for Computer Forensics" *Information Systems Management*, (22)2, (Spring 2005): 57-66.

Buell, D. A., and Sandhu, R., "Identity management" *IEEE Internet Computing*, (November/December 2003): 26-28.

Cavoukian, A., "7 Laws of Identity: The case for privacy-embedded laws of identity in the digital age" (2007): 1-24. (accessed February 6 2008, http://www.identityblog.com/wp-content/resources/7_laws_whitepaper.pdf).

Commission of the European Communities., "Towards a general policy on the fight against cyber crime," *Commission of the European Communities*, (June 2007) 1-48. http://www.coe.int/t/e/legal_affairs/legal_co-

operation/combating _economic_crime/6_cybercrime/t-cy/T-CY%20_2007_%2002%20-%20e%20-%20Cybercrime%20and%20the%20EU.pdf

Commission of the European Communities., "Convention on Cybercrime" (ETS No. 185) Commission of the European Communities Online, (2004): 1. http://conventions.coe.int/Treaty/en/Summaries/ Html/185.htm, January 16, 2008

Credit Industry Fraud Avoidance System (CIFAS) 2007 online.

Cuganesan, S., and D. Lacey, "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.

Damiani, E., De Capitani di Vimercati, S., and Samarati, P., "Managing Multiple and Dependable Identities," *IEEE Internet Computing*, 7(6), (2003): 29–37.

Deloitte., "2005 Global Security Survey," *Deloitte, Global Financial Services Industry,* (2005) (available at http://www.deloitte.com/dtt/cda/doc/content/dtt _financial services_2005GlobalSecuritySurvey_2005-07-21.pdf).

Druker, S. J., and Gumpert, G., eds. *RealLaw@Virtual Space: Communication Regulation in Cyberspace* Hampton Press, Inc. Cresskill, New Jersey, 2005.

Dunn, M., Krishna-Hensel, S. F., and Mauer, V., (eds) *The Resurgence of the State: Trends and processes in Cyberspace Governance*, Ashgate Publishing Company, USA, 2007.

Durante, A., "How the nature of identity will shape its deployment," *Digital ID World*, (November/December 2003): 1-3.

Economist.com., "A walk on the dark side: These badhats may have bought your bank account," *The Economist Group*, August, (2007): 1-2.

Economist, The., "Complying with the rules for identity management," *An Economist Intelligence Unit,* briefing paper sponsored by IdenTrust, (2006): 1-28.

Econsumer online 2008 (accessed February 5 2008, http://www.consumer.gov/econsumer/english/index.html).

Gibson, W., Neuromancer. New York: Ace Books, 1984.

Hayashi, M., "The information revolution and the rules of jurisdiction in public international law" 59-83 in *The resurgence of the state: Trends and processes in cyberspace governance* Dunn, M., Krishna-Hensel, S. F., Mauer, V. eds., Ashgate, England, 2007.

Gerke, M., "Internet-Related Identity Theft," *Council of Europe*, November, 2007, pp.1-32. http://www.idfraudconference-pt2007.org/cms/files/conteudos/image/ 567% 20port%20id-d-identity%20theft%20paper%2022%20nov%2007.pdf

Gordon, L., and Loeb, M., "The Economics of Information Security Investment," *ACM Transactions on Information and System Security* 5(4), (2002): 438-457.

Grabosky P & Sutton A., *Stains on a white collar*. Sydney: Federation Press, 1989.

Henry, P. A., "Will the Tide Finally Turn for Network Security?" *Cyber Security Industry Alliance Newsletter*, (2)7, (March 2006): 1-3, (accessed February 5 2008).

Hinde, S., "Security Surveys," *Computers & Security* 21(4), (2002): 310-321.

Ilett, D., "US to force firms to 'fess up on data loss" *Security Strategy*, 2006, 3 April, (http://software.silicon.com/security/0,39024655,39157787,00.htm, accessed 01-6-06).

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

Jamieson, R J., Winchester, D W., and Smith, S., "Development of a Conceptual Framework for Managing Identity Fraud," *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS-40)*, CD-ROM, IEEE Computer Society, (January 2007): 1-10.

Jamieson, R., Stephens, G., and Winchester, D., "An Identity Fraud Model Categorising Perpetrators, Channels, Methods of Attack, Victims and Organisational Impacts," *PACIS conference*, New Zealand, (July 2007a): 1-14.

Jamieson, R J., Stephens, G., and Winchester, D W., "Managing Identity Fraud: For Government and Organisations", *Unpublished working paper SISTM, UNSW,* Presented at the Australian Public Sector Anti-Corruption Conference (APSAC) 2007, Sydney, (October 2007b): 1-45.

Javelin Strategy & Research., "U.S. identity theft losses fall: study" (February 2007). http://www.javelinstrategy.com/2007/02/01/us-identity-theft-losses-fall-study/

Javelin Strategy & Research., "New Research Confirms Identity Fraud Is On Decline" Javelin Online, (February 11 2008): 1-4. http://www.javelinstrategy.com/ 2008/02/11/new-research-confirms-identity-fraud-is-on-decline/#more-1057

Javelin Strategy & Research., "2007 Identity fraud survey report: How Consumers Can Protect Themselves," *Javelin Strategy & Research,* Consumer Version, (February 2007): 1-22. http://www.acxiom.com/AppFiles/Download18/ Javelin_ID_Theft_Consumer_Report-627200734724.pdf

Javelin Strategy & Research., "2006 Identity fraud survey report," *Javelin Strategy & Research*, Consumer Version, (January 2006): 1-20. http://www.javelinstrategy.com/products/99DEBA/27/delivery.pdf

Kanellis, P., Kiountouzis, E., Kolokotronis, N., and Martakos, E., eds. *Digital crime and forensic science in cyberspace* Idea Group Publishing, USA, 2006.

King, L. "UK defense department loses 11,000 military ID cards" *Computerworld UK*, March 13 2008 (accessed 14 March 2008 http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9068218)

Kleist, V. F., "Building Technologically Based Online Trust: Can the Biometrics Industry Deliver the online trust silver bullet" *Information Systems Management*, (24)4, (Fall 2007): 319-329.

Kronish, C. G., "US Data Protection Laws, with a focus on California" *Bird & Bird Law Firm* (2007): 1-3. (accessed February 2008, http://www.twobirds.com/ english/publications/articles/US_DP_Laws _focus_California.cfm).

Lemos, R., "*International cybercrime treaty finalized*" CNET News.com, (June 2001): 1-3. (accessed February 2008 http://www.news.com/2100-1001-268894.html).

Lim, Y F., 2007. *Cyberspace law: commentaries and materials* Second Edition. Oxford University Press, Victoria, Australia.

Lininger, R., and Vines, R. D., *Phishing: Cutting the identity theft line* Wiley Publishing, Inc, Indiana, 2005.

Lockhart, S., Jamieson, R., Winchester, D., and Sarre, R., "Responding to Identity Fraud: Issues for Australian Policy-makers," *Report for the Australian Research Council,* Grant 2005-2008, (November 2007): 1-28.

McCusker, R., "Transnational organised cyber crime: distinguishing threat from reality" *Crime, Law and Social Change* (46), (March 2006): 257–273.

McLaughlin, L., "Online Fraud Gets Sophisticated," *IEEE Internet Computing*, 7(5) (September/October 2003): 6-8.

Milne, G. R., "How Well Do Consumers Protect Themselves from Identity Theft?," *Journal of Consumer Affairs*, (37)2, (Winter 2003): 388-402.

NVivo *qualitative data analysis software* QSR International Pty Ltd. (Version 2), 2002.

O'Connell, K., "Russian Company Outed as Mother of all Cybercrime," October, (2007): 1-2. http://www.ibls.com/internet_law_news_portal_view.aspx?s= latestnews &id=1887, last accessed Jan 10 2008.

Paltridge, S., Roberts, S., and Beuzekom, B., "Scoping study for the measurement of trust in the online environment" *OECD, Organisation for Economic Co-operation and Development*, (December 2005): 1-75. http://www.oecd.org/dataoecd /26/15/35792806.pdf

Paul, S. R., "Identity Theft: Outline of Federal Statutes and Bibliography of Select Resources," *Law and Technology Resources for Legal Professionals*, February, (2006): 1-16. http://www.llrx.com/node/646/print, last accessed January 9 2008.

Phair, N., *Cybercrime: The reality of the threat* Kambah, A.C.T Australia, 2007.

Pfitzmann, A., and Hansen, M., "Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management: A consolidated proposal for terminology" Working paper TU Dresden, (Version v0.28) (May 2006): 1-54, (accessed February 2008, http://dud.inf.tu-dresden.de/literatur/ AnonTerminology_v0.28.pdf)

Privacy Rights Clearinghouse., "A Chronology of Data Breaches," *Privacy Rights Clearinghouse* 2008. http://www.privacyrights.org/ar/ChronDataBreaches.htm

Rubel, S. K., "Security Breach Bills and Passed Legislation in the 50 State Legislatures Plus New York City" *privacylaws@sbcglobal.net*, (2005): 1-72.

Schwartz, P. M. and Janger, E. J., "Notification of Data Security Breaches" *Michigan Law Review*, 105, (2007): 913- 984

Skogsrud, H., Benatallah, B., and Casati, F., "Model-Driven Trust Negotiation for Web Services," *IEEE Internet Computing*, 7(6), (2003): 45- 52.

Singer. J. G., "What Strategy Is Not," *MIT Sloan Management Review*, 49(2) (Winter 2008): 96.

Smith, R. G., and Urbas, G., *Controlling fraud on the internet: A CAPA perspective*. Panther Publishing and Printing, Canberra, 2001.

Sofaer, A. D., and Goodman, S. E., (eds) *Transnational Dimension of Cyber Crime and Terrorism* Hoover Institution Press, California, 2001.

Spang-Hanssen, H., ed. *Cyberspace & international law on jurisdiction: Possibilities of dividing cyberspace into jurisdictions with help of filters and firewall software*. Djof Publishing, Copenhagen, Denmark, 2004.

Swartz, Bruce., "Helping the World Combat International Crime" Global Issues, (6)2, (August 2001): 9-11.

Synovate., "Federal Trade Commission: 2006 identity theft survey report" *Federal Trade Commission*, (November 2007): 1-108.

The Fraud Advisory Panel., Identity Theft: Do you know the signs? A guide for businesses and individuals, The Fraud Advisory Panel London, 2003, pp. 1-24.

UK Home Office, "Updated estimate of the cost of identity fraud to the UK economy", (2006). 2 February, pp. 1-4. (http://www.identity-theft.org.uk/ID%20 fraud%20Table.pdf, accessed 01-6-06).

Wall, D. S., ed. *Cyberspace crime* Dartmouth Publishing Company, England, 2009.

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

Published by the Forum on Public Policy