




NATIONAL
IDENTITY
SECURITY
STRATEGY



***Improving the Measurement of
Identity Crime and Misuse in
Australia:*** Recommendations from
the National Identity Crime and
Misuse Measurement Framework
Project

• • •
IDENTITY SECURITY

Contents

| | |
|---|----|
| Executive Summary..... | 3 |
| Overview of Recommendations..... | 4 |
| A future Identity Crime Measurement Framework..... | 4 |
| Identity crime recording by government agencies..... | 4 |
| Prosecutions for identity crime..... | 4 |
| Identity crime against Australians | 5 |
| Identity crime against Australian business | 5 |
| Online identity crime | 5 |
| Background | 6 |
| The need for an evidence base..... | 6 |
| Conceptual Model of Identity Crime | 7 |
| Identity crime recording by government agencies..... | 9 |
| Commonwealth..... | 10 |
| Prosecutions for identity related crime | 11 |
| Identity crime against Australians | 12 |
| Identity crime against Australian business | 13 |
| Online Identity Crime..... | 14 |
| Conclusion..... | 15 |
| References | 16 |
| Appendix A – Measurement Framework Pilot Indicators..... | 18 |
| Appendix B – Minimum and Complete Variable List for Ongoing Data Collection around Identity Crime and Misuse in Australia | 21 |

Executive Summary

Identity crime, those offences in which a perpetrator uses a fabricated, manipulated, or stolen/assumed identity to help them commit a crime, has become one of the most prevalent crime types in Australia and a key enabler of serious and organised crime.

Developing a more comprehensive evidence base around identity crime and misuse in Australia is a priority under the National Identity Security Strategy (NISS) (COAG 2012). To guide this work, the Attorney-General's Department (AGD) commissioned the Australian Institute of Criminology (AIC) to develop a framework that included 20 different measurement indicators (Bricknell & Smith 2013).

A Conceptual Model was then developed to align groups of indicators against five separate components of identity crime and related activities, from the acquisition and use of fraudulent identities, to the consequences, remediation and prevention of this crime type. With the endorsement of the National Identity Security Coordination Group (NISCG), a pilot exercise was undertaken to collect available data and information about identity crime. The purpose was to assess the feasibility of establishing a formal identity crime and misuse monitoring program.

Complete findings from this pilot exercise are presented in a companion report titled; *Identity Crime and Misuse in Australia: Key Findings from the National Identity Crime and Misuse Measurement Framework Pilot* (AGD 2014). The pilot exercise has shown that it may be possible with adequate resourcing to collect data and information to estimate the overall prevalence of identity crime in Australia, and to examine various different types of identity crimes such as benefits, taxation, immigration, passport, financial (credit card), driver's licence and conveyancing identity-related frauds. The pilot exercise was also able to quantify certain outcomes from these incidents, such as the financial losses suffered by individuals and some government agencies, as well as the estimated number of offences detected by police and prosecuted through the courts.

However, the pilot exercise also found that there are many gaps in data and information that need to be addressed before a complete and comprehensive evidence base can be established. This report presents the recommendations for improving the quality and availability of data, as well as identifying some of the steps required to enhance the monitoring of identity crime and misuse in Australia on an ongoing basis.

Certain agencies reported that they either did not routinely collect data on incidents of identity crime, or could not provide the data they did collect within the time and resources available during the pilot exercise. For example, no road transport agencies, only two out of nine police agencies, two out of eight registries of births deaths and marriages, and three out of eight consumer affairs department could provide relevant data, within the time and resources available.

At a Commonwealth level, similar deficiencies in data availability were identified. However, Commonwealth agencies responsible for delivering key government services, such as the Department of Human Services and the Australian Taxation Office, collected and were able to provide valuable data for the purpose of measuring identity crime. Moreover, Commonwealth agencies that issue identity credentials, such as the Australian Passport Office within the Department of Foreign Affairs and Trade, and the Department of Immigration and Border Protection, also provided detailed data and information.

Based on the success of the pilot exercise, it is proposed that an annual identity crime measurement report be provided to Commonwealth and state and territory ministers on the nature, extent and impacts of identity crime in Australia. These reports would help inform policy and operational

responses to identity crime. The reports would also be made public to help raise community awareness of identity crime and how it can be prevented.

This report also includes recommended measures to improve the quality and availability of information on identity crime that is held by government agencies and the private sector.

Responsibility for implementation of the measurement framework, including the coordination of work to improve current data sources, should fall with the NISCG. This group, which comprises officials from relevant Commonwealth, state and territory agencies, is responsible to Ministers for the implementation of the National Identity Security Strategy.

Overview of Recommendations

A future Identity Crime Measurement Framework

Recommendation 1: That the National Identity Security Coordination Group (NISCG) develops an annual identity crime measurement report for relevant Commonwealth and state and territory ministers on the nature, extent and impacts of identity crime in Australia.

Recommendation 2: The identity crime measurement report should adopt and refine the methodology used in the pilot exercise, including the conceptual model and measurement indicators. Annual reports should be provided at the beginning of each calendar year, providing an analysis of data relating to the previous financial year.

Identity crime recording by government agencies

Recommendation 3: That the NISCG develop a nationally agreed minimum data set(s) of information that government agencies should capture when recording incidents of identity crime or misuse, together with an approach to encouraging implementation of the data set by relevant agencies. This should include agencies with responsibilities for: registering births, deaths and marriages, driver licensing, consumer affairs, human services, revenue collection, immigration and border management (including passports) and law enforcement.

Recommendation 4: That the Attorney-General's Department, with assistance from the Australian Federal Police and state and territory police agencies, develop processes for monitoring the cost, quality and availability of fraudulent identity credentials; and develop protocols for sharing this information directly with the government agencies that issue or rely upon those credentials. This information should also be made available in summary form for inclusion in future measurement framework reports.

Recommendation 5: That the Office of the Australian Information Commissioner considers collecting and publishing additional information on reported data breaches that involve the theft or loss of personal information. This could include the type of breach, number of records involved and how the incident was detected.*

(*Note: With the disbanding of the OAIC on 31 December 2014, this function will be performed by the Australian Privacy Commissioner.)

Prosecutions for identity crime

Recommendation 6: That the Australian Bureau of Statistics (ABS) review the Australian and New Zealand Standard Offence Codes (ANZSOC) to discriminate between specific identity crime

offences (such as stealing or selling personal information or possessing/manufacturing a fraudulent identity credential) and other fraud or related offences.

Recommendation 7: That these new ANZSOC codes be incorporated into data recording systems of police agencies and criminal courts over time, to enable more effective measurement of identity crime.

Recommendation 8: That the ABS develop a pilot project to analyse a sample of criminal courts cases involving multiple crime types to estimate the number offences that were enabled through the fraudulent use of personal information.

Identity crime against Australians

Recommendation 9: That an annual survey be administered to a representative sample of the Australian community to ascertain experiences of, and attitudes towards, identity crime and fraudulent misuse of personal information, with a view to measuring trends over time.

Identity crime against Australian business

Recommendation 10: That the NISCG explore additional data sources to refine measurement indicators on identity crime within the private sector. Potential data sources may include financial industry organisations such as the Australian Bankers Association, the Australian Payments Clearing Association and the forthcoming National Fraud Exchange.

Online identity crime

Recommendation 11: That the NISCG explore additional data sources to refine measurement indicators on online identity crime. Potential data sources may include: CERT Australia's annual Cyber Crime and Security Survey, the proposed Australian Cybercrime Online Reporting Network; and any future work to develop measurement frameworks for cybercrime or cyber security.

Background

Developing effective policy and operational responses to identity crime requires comprehensive and reliable evidence. Currently in Australia there is no systematic, regular collection of information about identity crime, its impacts and costs.

To address this gap in knowledge, the National Identity Security Coordination Group (NISCG) agreed that a priority for the 2013-14 financial year, should be to develop an ongoing national identity crime measurement project. This proposal was then endorsed by the Council of Australian Governments (COAG) and the task of coordinating this project was given to the Commonwealth Attorney-General's Department (AGD).

To test the feasibility of developing an ongoing national monitoring programme around identity crime and misuse, AGD commissioned the Australian Institute of Criminology (AIC) to develop a measurement framework that identified 20 high level measurement indicators (see Appendix A) that were aligned with these key objectives of the NISS (Bricknell & Smith 2013: the AIC Report). The measurement indicators were then approved by the NISCG.

The suitability of these measurement indicators was then field tested by the AGD through a pilot data collection exercise. The AGD worked closely with 54 different Commonwealth, State and Territory government agencies to source data and information relevant to the specific indicators. Findings from this pilot exercise are presented in a companion report titled; *Identity Crime and Misuse in Australia: Key Findings from the National Identity Crime and Misuse Measurement Framework Pilot* (AGD 2014) (the Findings Report).

The need for an evidence base

There is a growing body of statistical evidence, attitudinal data and certain threat-based intelligence to support the proposition that identity crime and misuse is a significant and growing problem in Australia. For example, a survey undertaken by the AIC as part of the Measurement Framework pilot project found that 9.4 per cent of respondents reported having had their personal information misused in the previous 12 months; with five per cent reporting that they lost money as a result (Smith & Hutchings 2014). It was also found that the identity crime victimisation rate is higher than for assault, robbery, break-ins and motor vehicle theft (ABS 2014). These findings indicate that identity crime is one of the most prevalent offence types affecting Australians each year.

Developing a formal measurement program to collect information and data about the theft and misuse of personal identifying information will improve understanding of the various types of identity crime, as well as identifying emerging trends and issues that raise concerns for Australia's inter-dependent identity infrastructure.

Without the regular collection of detailed information about identity crime, the true nature and impact of these incidents will remain unknown, and preventative measures will largely continue to be developed on a reactionary basis. Establishing a comprehensive and reliable evidence base will ensure that effective strategies are available to address one of Australia's most prevalent and corrosive crime types, and that appropriate assistance and support services are made available to victims.

National Identity Crime Measurement Framework (NICAM Framework)

Recommendation 1: That the National Identity Security Coordination Group (NISCAG) develops an annual identity crime measurement report for relevant Commonwealth and state and territory ministers on the nature, extent and impacts of identity crime in Australia.

Recommendation 2: The identity crime measurement report should adopt and refine the methodology used in the pilot exercise, including the conceptual model and measurement indicators. Annual reports should be provided at the beginning of each calendar year, providing an analysis of data relating to the previous financial year.

The pilot exercise confirmed the feasibility of using a measurement framework to quantify the size and nature of identity crime in Australia, with analysis of the data providing insights into the various identity crime methodologies and targets used by criminals.

Australia's identity management infrastructure is highly dynamic and characterised by many inter-dependencies; in that around 20 government agencies manage over 50 million core identity credentials, and that many agencies are relying on the identity verification processes of other agencies to ensure that individuals are who they claim to be.

The result is that vulnerability in one type of identity credential, or the verification processes that sit behind it, can have serious downstream consequences for the integrity of the system as a whole. Conducting ongoing measurement of identity crime will provide agencies with a more comprehensive evidence base to develop new and potentially more effective responses to identity crime.

Conceptual Model of Identity Crime

The Conceptual Model developed as part of the pilot exercise was designed to separate the NICAM Framework into five key components, each focussing on a specific set of activities relating to identity crime (see Figure 1 below).

Measurement indicators were then aligned to the relevant component of the Model. The indicators are included at Attachment A. The benefit of this approach, as opposed to an approach of listing offence types that is often adopted in other attempts at measuring crime, is that it provides a more holistic picture of identity crime, its consequences, as well as remediation and prevention activity.

The data and information that have been collected for these measurement indicators provided sufficient evidence to support their continued use in future measurement of identity crime. Any ongoing measurement should continue to adopt this conceptual model to help guide the collection of data under each of the groups of indicators.

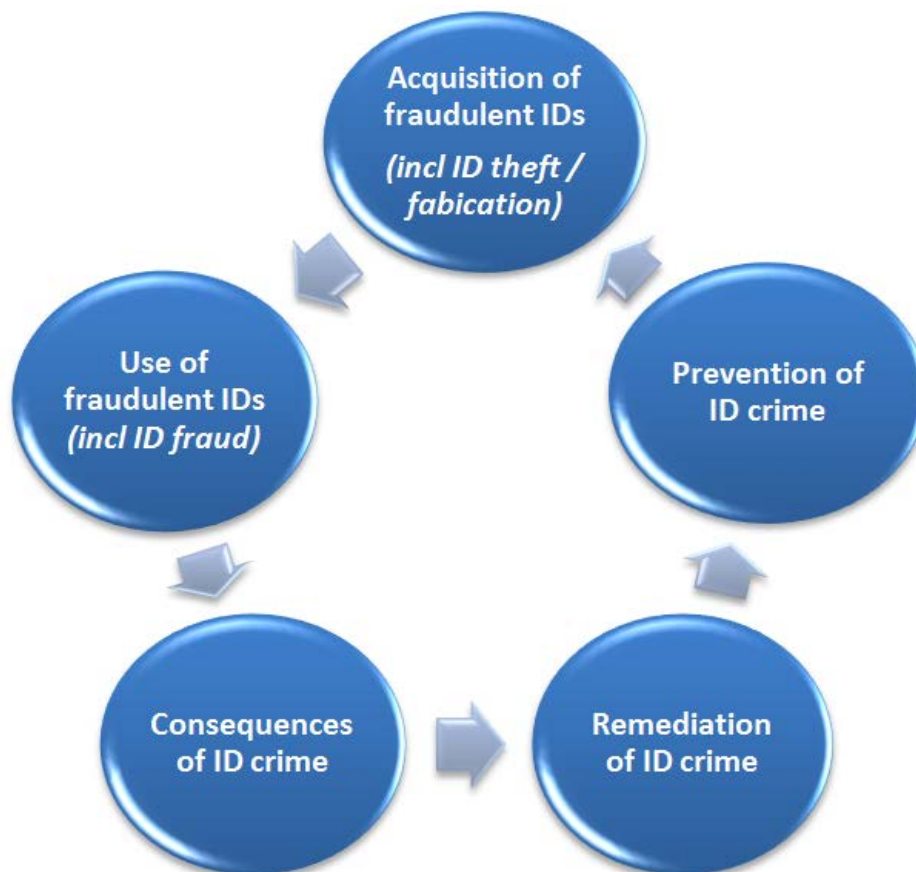
Providing a public annual report for the measurement of identity crime will both describe the current problem of the illicit activity in the context of the conceptual model and attempt to detail the overall quantum of the costs and consequences. It will mean that the reports are providing the Australian community with a meaningful picture of where the problems are, what are the costs and consequences, and whether current prevention and remediation actions are addressing the needs of the community.

It will be important to coordinate the data collection process for the development of future reports with the efforts of other relevant agencies so as to minimise potential confusion or duplication of effort. This includes requests for data or other information from the Australian Crime Commission and the Australian Bureau of Statistics (ABS), including those relating to the Report on Government Services process.

Aside from a lack of standardisation between organisations in terms of how identity crime incidents are recorded, the Key Findings report also identified that some agencies use different definitions of identity crime than others. In working towards improving the collection of data, agencies should endeavour to incorporate the standard definitions developed by the Australasian Centre for Policing Research (2006), and subsequently adopted by the Australian Law Reform Commission (2008) and Australian Federal Police (2014). This will ensure that different agencies are recording information about the same types of incidents.

Finally, the Key Findings report also showed that a large proportion (in the region of 80-90%) of recorded identity crime incidents take the form of credit card fraud. To commit credit card fraud, the offender requires not only the credit card numbers but also the card holder's name or other personal information and, as such, these incidents should be included within the definition of identity crimes for the purpose of future measurement. Data collected from participants during the AIC Survey indicate that more than half of respondents considered credit card details to be personal information and when asked about experiences of identity crime, many reported incidents of credit card fraud.

Figure 1: Identity Crime Conceptual Model



Identity crime recording by government agencies

Recommendation 3: That the NISCG develop a nationally agreed minimum data set(s) of information that government agencies should capture when recording incidents of identity crime or misuse, together with an approach to encouraging implementation of the data set by relevant agencies. This should include agencies with responsibilities for: registering births, deaths and marriages, driver licensing, consumer affairs, human services, revenue collection, immigration and border management (including passports) and law enforcement.

Many incidences of identity crime and misuse, particularly where it enables fraud against governments may not be prosecuted. This means that data from agencies beyond law enforcement is necessary to build a complete picture of the nature of identity crime.

However, findings from the pilot exercise show that for some measurement indicators it was not possible to collect sufficient data to make definitive conclusions about the precise nature and characteristics of identity crime and related activities. For example, only three large Commonwealth service delivery agencies (Department of Human Services (DHS), Australian Taxation Office (ATO) and Department of Immigration and Border Protection (DIBP)) and three state government agencies (the Queensland Police Service and NSW and WA Registrars of Births, Deaths and Marriages (BDMs), could provide statistics that were relevant to quantifying the number of recorded incidents of identity crime. Similarly, in relation to trying to measure the direct cost of identity crime to government agencies, only DHS and the ATO could provide data, while no state government agency could provide any data on costs of identity crime.

This lack of data makes it difficult to identify gaps and vulnerabilities in Australia's federated identity system, particularly where it is needed to design policies and mitigation strategies.

Additional data about vulnerabilities would also help justify spending and effort on risk mitigation, including from central agencies for cases where upgrades cannot be resourced from within agency budgets.

To conduct ongoing identity crime measurement, it will be necessary for relevant agencies named below to take steps to improve the quality and availability of data around identity crime and misuse. This should involve the collection of a minimum set of data for each reported incident, including details such as: the type of identity crime, the identity credential used, and any resulting financial loss to the agency.

A suggested minimum data set is outlined in Appendix B, which may need to be refined by relevant agencies before being endorsed by the NISCG. The feasibility of collecting such minimum data sets and the potential costs and benefits to credential issuing agencies collecting should be considered during this process.

In many cases collection of this information will involve changes to agency business processes and ICT systems. While this will involve the allocation of time and resources, agencies could look for opportunities to implement any changes that may be needed as part of regular business process and system refresh and upgrades. The NISCG should encourage relevant agencies to implement these changes in time to enable data collection for the 2016/17 financial year.

Relevant agencies that could be expected to implement the minimum data set, once agreed, include:

Commonwealth:

Service Delivery: Department of Human Services (DHS) and Australian Taxation Office (ATO).

Credential Issuing: Department of Immigration and Border Protection (DIBP) and Department of Foreign Affairs and Trade (DFAT).

Law Enforcement: Australian Federal Police (AFP)

State/Territory:

Service Delivery/Credential Issuing: All Registries of Births, Deaths and Marriages (RBDMs), Road Transport Agencies (RTAs) and Consumer Affairs / Protection agencies.

Law Enforcement: All state and territory policing agencies.

Recommendation 4: That the Attorney-General's Department, with assistance from the Australian Federal Police and state and territory police agencies, develop processes for monitoring the cost, quality and availability of fraudulent identity credentials; and develop protocols for sharing this information directly with the government agencies that issue or rely upon those credentials. This information should also be made available in summary form for inclusion in future measurement framework reports.

Only a small number of agencies were able to provide information on the utilisation of fraudulent identity credentials (AFP, NSW Police and Department of Foreign Affairs and Trade – Australian Passport Agency (DFAT)). This information was collected as part of specific operational activities, rather than a more systematic basis as an indicator of the nature or extent of identity crime.

Collection of this information on a comprehensive, national basis will help develop a more complete picture of the size of identity crime, including the types of fraudulent credentials used to facilitate these offences and the specific targets for the malicious use of fraudulent identities. Over time, it will also be possible to identify trends in relation to these various elements.

The regular collection and dissemination of intelligence by Commonwealth, State and Territory law enforcement agencies on the cost, nature and extent of fraudulent credentials would provide credential issuing agencies with a measure of the extent to which certain credentials are being used to facilitate identity crime. This is also a valuable indication as to the vulnerability of their credentials and should inform any future changes to the security features or issuing processes for these credentials.

Finally, the regular flow of this information back to credential issuing agencies will also help to identify whether there are weaknesses in one type of credential that may have flow-on effects for other agencies within Australia's inter-dependent identity management infrastructure.

Recommendation 5: That the Office of the Australian Information Commissioner considers collecting and publishing additional information on reported data breaches that involve the theft or loss of personal information. This could include the type of breach, number of records involved and how the incident was detected.*

The pilot findings revealed that there is currently a lack of detailed information on the nature and size of data breaches in Australia, incidents where sensitive and/or personal information held by an organisation is accidentally lost or maliciously stolen. While the Office of the Australian Information Commissioner (OAIC) reports on the number of voluntarily reported data breaches each year, there is no regular, comprehensive source of information to quantify the precise nature of these breaches, including whether the incident involved the theft or loss of personal information. This level of information was not available from the OAIC as it does not uniformly require or capture this amount of detail from organisations or agencies reporting a data breach.

Studies by private sector organisations, such as the Ponemon Institute (2012), do provide some more detailed insights, however these studies examine only a sub-set of Australian organisations that may experience data breaches. The regular collection of more detailed information about data breaches would help to determine not only whether these incidents are increasing in frequency and/or severity, but would also assist agencies to identify common vulnerabilities and deploy preventative measures.

*(*Note: With the disbanding of the OAIC on 31 December 2014, this function will be performed by the Australian Privacy Commissioner.)*

Prosecutions for identity related crime

Recommendation 6: That the Australian Bureau of Statistics (ABS) review the Australian and New Zealand Standard Offence Codes (ANZSOC) to discriminate between specific identity crime offences (such as stealing or selling personal information or possessing/manufacturing a fraudulent identity credential) and other fraud or related offences.

Recommendation 7: That these new ANZSOC codes be incorporated into data recording systems of police agencies and criminal courts over time, to enable more effective measurement of identity crime.

There is no standardised approach to the collection of statistics on identity crime offences in Australia. The methodology for quantifying the number of identity crimes adopted for the pilot exercise involved collection of any available statistics on specific identity crime offences, and also an estimate of the number of fraud and other offences that were enabled through the use of a fraudulent identity.

This methodology was employed using data on offences recorded by the Queensland Police Service (the only state and territory police agency that was able to provide such data), as well as prosecution data from the Commonwealth Director of Public Prosecutions (CDPP) and the ABS (for Commonwealth, state and territory prosecutions). Given the constraints of this methodology and limitations in the available data, this approach does not necessarily produce an accurate picture of the true number of identity crime offences.

Historically, a similar lack of standardisation existed with the collection of statistics on violent offences. To address this deficiency, the ABS in conjunction with State and Territory criminal justice agencies developed greater consistency across jurisdictions in terms of definitions and recording practices around violent crimes.

Contributing to the success of this approach was the application of the ANZSOCs (standard offence codes) (ABS 2011), which ensured police statistical units and criminal courts staff were all coding offences in the same way. The outcome of this approach was that data quality greatly improved. As data was being collected in a more consistent and standardised manner, it became possible to make comparisons across jurisdictions and therefore better identify whether certain state-based initiatives were reducing violent offending.

It would be beneficial if the ABS could undertake a similar standardisation process with criminal justice agencies around identity crime offences. In particular, consideration should be given to developing a specific ANZSOC for identity crimes that could then be incorporated into existing data recording systems operated by police agencies and criminal courts staff. With the adoption of this new statistical code, it will be possible for these agencies to separate identity crimes from broader offence categories (such as fraud) and quantify the true number of identity crimes on a regular basis.

Developing and implementing a new ANZSOC for identity crime offences will require the support of the ABS, police services and the criminal courts. It is envisaged that this process, including relevant approvals from police agencies and the courts across Australian jurisdictions, will likely take at least 18 months, with new data available over a number of years.

Recommendation 8: That the ABS develop a pilot project to analyse a sample of criminal courts cases involving multiple crime types to estimate the number offences that were enabled through the fraudulent use of personal information.

While developing standard offence codes for identity crimes will provide the ability to quantify the specific number of these offences, it will not provide an indication of the number of other offences that are enabled through the use of a fabricated, stolen or manipulated identity. The pilot exercise revealed instances where prosecutions for offences such as drug trafficking and money laundering, which involved the use of fraudulent identities to facilitate the offence, did not provide any indication that these were identity-related crimes.

One practical approach to estimating the number of offences enabled through the use of a fraudulent identity is to analyse a sample of cases, and then extrapolate the findings to a national figure. A pilot project could analyse a sample of cases (perhaps 1000 cases over a 12 month period) to produce estimates of the number and/or proportion of offences that are enabled through the use of a fraudulent identity

Identity crime against Australians

Recommendation 9: That an annual survey be administered to a representative sample of the Australian community to ascertain experiences of, and attitudes towards, identity crime and fraudulent misuse of personal information, with a view to measuring trends over time.

As part of the pilot exercise, the AGD and DFAT commissioned the AIC to undertake a 5,000 person online community survey to build a better understanding of the prevalence of identity crime and misuse. In addition to asking respondents about specific incidents of victimisation, amounts lost and amounts recovered, the survey also asked participants about their perceptions of identity crime more generally, as well as behavioural change resulting from the incident (Smith & Hutchings 2014).

The headline finding from the survey was that 9.4 per cent of respondents reported having had their personal information misused in the previous 12 months, with five per cent reporting having lost money as a result (Smith & Hutchings 2014). Of those who lost money, the vast majority (around 90 per cent)

were victims of credit card fraud. The remaining 10 per cent of victims experienced other cases of misuse of personal information including identity theft.

Conducting an annual identity crime survey will significantly enhance the value of the annual measurement of identity crime. The identity crime survey will allow an accurate quantification of the level of community concern about identity crime and trend information as to changes reported annually.

Identity crime against Australian business

Recommendation 10: That the NISCG explore additional data sources to refine measurement indicators on identity crime within the private sector. Potential data sources may include financial industry organisations such as the Australian Bankers Association, the Australian Payments Clearing Association and the forthcoming National Fraud Exchange.

The pilot exercise found that the only reliable, publicly available sources of information on the direct costs of fraud to businesses were payment fraud data produced by the Australian Payments Clearing Association (APCA) and a series of the KPMG Fraud and Misconduct surveys (KPMG 2009, 2010, 2013). To quantify the costs of identity crime and misuse to businesses, it was necessary to estimate the proportion of fraud costs identified in the KPMG survey that were attributable to identity crimes. These KPMG surveys are administered to only around 220-280 businesses from both Australian and New Zealand, and there are no specific questions regarding identity crime. As a result, the findings are indicative estimates only and are not ideal for quantifying the direct costs of identity crime and misuse to Australian businesses.

Addressing the deficiency in available data could be achieved through a dedicated identity crime survey administered to a representative sample of small, medium and larger private sector organisations. The survey questions could be adapted from those already developed for previous similar surveys of individuals, or alternatively could be adapted from the one-off Australian Business Assessment of Computer User Security (ABACUS) survey conducted in 2005/06 by the AIC (Richards 2009).

Any broader based business survey would be in addition to CERT Australia's annual *Cyber Crime and Security Survey* (AGD 2012). A survey based on the ABACUS methodology would require additional resources from relevant agencies and/or sponsorship from interested private sector organisations. It is proposed that the NISCG investigate options for conducting such a survey.

Other potential data sources could include the Australian Bankers Association, APCA and the forthcoming National Fraud Exchange (NFX). The NFX is expected to involve member institutions from the financial sector establishing coordinated systems to allow the structured exchange, collection and analysis of fraud data. Anticipated benefits include the reduction of fraud losses, the ability to address vulnerabilities, and improved productivity through the increased capacity to share data and analysis.

A similar system is operated by the United Kingdom's Credit Industry Fraud Avoidance Scheme (CIFAS). CIFAS is a not-for-profit organisation dedicated to the prevention of fraud and financial crime. It has membership across the financial, telecommunications, insurance, retail and public sectors.

The CIFAS National Fraud Database contains records of frauds, including identity frauds, which have been perpetrated or attempted against its member organisations. In order to be recorded on the CIFAS Database a case must satisfy a standard of proof. This means there must be sufficient evidence to take the case to the police, although it is not mandatory to do so.

CIFAS uses this information to publish annual reports on the UK's 'fraud landscape' and quarterly bulletins with statistics the nature and extent of fraud in the United Kingdom. The latest bulletin was published on 14 March, 2014 and indicated that 'frauds where criminals misuse the personal data of victims still accounted for over 60% of all fraud in the UK in 2013' (CIFAS 2014). The CIFAS model would appear to represent international best practice in terms of a public-private collaboration to help prevent financial and identity related crime. Elements of this approach could be adopted in Australia, over time, as initiatives such as the National Fraud Exchange (NFX) mature.

Online Identity Crime

Recommendation 11: That the NISCG explore additional data sources to refine measurement indicators on online identity crime. Potential data sources may include: CERT Australia's annual Cyber Crime and Security Survey, the proposed Australian Cybercrime Online Reporting Network; and any future work to develop measurement frameworks for cybercrime or cyber security.

The Findings Report contained information on the online security practices from of Australians and Australian businesses from a range of published sources. These included global surveys by major ICT companies Microsoft (2014) and Norton (Symantec) (2013) as well as government agencies such as the Australian Communications and Media Authority and CERT Australia's annual *Cyber Crime and Security Survey*. In addition this publicly available data, there is a range of work that is currently underway within government agencies that over time might provide additional sources of data.

These include the Australian Cybercrime Online Reporting Network (ACORN), due to commence operation later in 2014, and work on developing possible measurement frameworks for cybercrime and cyber security by the ABS and AGD respectively. To avoid potential duplication of effort with these initiatives, the future development of measurement indicators for online identity crime should, as far as possible, look to leverage this work.

Conclusion

The National Identity Crime Measurement Framework Pilot Project would not have been possible without the input and assistance of a large range of agencies across the Commonwealth, states and territories. In addition to assistance provided by the AIC in developing the methodology for the project, 54 agencies were approached with requests to identify any relevant information; 18 were able to respond with data that was used to compile the Key Findings report.

Many agencies also provided positive feedback and encouragement, as well as useful suggestions for improving the measurement of identity crime. Some of these suggestions were able to be included in the Findings or this Recommendations report, while others will be useful for informing ongoing work to refine the measurement process into the future.

This report outlines a roadmap for improving data collection, measurement and reporting of identity crime, one of the most prevalent crimes in Australia and a key enabler of serious and organised crime. These recommendations are primarily focussed on the systems of government agencies – reflecting the scope of the initial pilot exercise – but also recognise the need to further engage the private sector as a critical source of information and insights into the nature of identity crime and its impacts.

Implementation of this roadmap will require a sustained effort by a range of government agencies and non-government organisations over a number of years. This will in turn need the development of new and innovative approaches, a willingness to share information with a greater range of partner organisations, commitment of resources – all as part of the broader implementation of the National Identity Security Strategy (NISS) and related efforts to combat identity crime in Australia.

Once achieved, it will create a comprehensive and reliable evidence base to inform the development of future policy and operational responses to take forward the implementation of the NISS and related efforts to combat identity crime.

References

- Attorney-General's Department (AGD), (2014), *Identity Crime and Misuse in Australia: Key Findings from the National Identity Crime and Misuse Measurement Framework Pilot*, A key priority under the National Identity Security Strategy: Canberra.
- Attorney-General's Department, (2012), *Cyber Crime & Security Survey Report 2012*, Canberra: <http://www.canberra.edu.au/cis/storage/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf>
- Australasian Centre for Policing Research (ACPR), (2006), *Standardisation of definitions of identity crime terms: A step towards consistency*, Report Series No. 145.3, South Australia: <http://www.anzpaa.org.au/anzpire/acpr-publications>
- Australian Bureau of Statistics, (2014), *Crime Victimisation, Australia, 2012-13*, ABS Cat. No. 4530.0, Canberra: <http://www.abs.gov.au/ausstats/abs@.nsf/Lookup/D7B1A6CCDEF87612CA257B16000E06DE?opendocument>
- Australian Bureau of Statistics, (2011), *Australian and New Zealand Standard Offence Classification (ANZSOC), 2011*, ABS Cat. No. 1234.0, Canberra: <http://www.abs.gov.au/AUSSTATS/abs@.nsf/ProductsbyCatalogue/E6838CDEE01D34BCA25722E0017B26B>
- Australian Federal Police (AFP), (2014), *Identity Crime*, AFP website: <http://www.afp.gov.au/policing/fraud/identity-crime>
- Australian Law Reform Commission, (2008), *For Your Information: Australian Privacy Law and Practice*, ALRC Report 108, Canberra: <http://www.alrc.gov.au/publications/report-108>
- Bricknell, S and Smith, R. G., (2013), *Developing a monitoring framework for identity crime and misuse*, (AIC Report) Australian Institute of Criminology, Canberra.
- Credit Industry Fraud Avoidance Scheme (CIFAS), (2014), *Fraudscape 2014*, http://www.cifas.org.uk/fraudscape_twentyfourteen
- Council of Australian Governments (COAG), (2012), *National Identity Security Strategy*, <http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Pages/NationalIdentitySecurityStrategy.aspx>
- KPMG, (2013), *A survey of fraud, bribery and corruption in Australia and New Zealand 2012*, <http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Fraud-Survey/Pages/fraud-bribery-corruption-survey-2012.aspx>
- KPMG, (2010), *Fraud and Misconduct Survey 2010*, <http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Fraud-Survey/Pages/Fraud-Survey-2010.aspx>
- KPMG, (2009), *Fraud Survey 2008*, <http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Fraud-Survey/Pages/Fraud-Survey-2008.aspx>

Microsoft, (2014), *2013 Microsoft Computing Safety Index*:
<http://www.microsoft.com/security/resources/mcsi.aspx>

Norton, (2013), *2013 Norton Report – Country Report: Australia*, Symantec:
<http://www.symantec.com/content/en/us/about/presskits/b-norton-report-2013-australia.pdf>

Ponemon Institute, (2012), *2011 Cost of Data Breach Study: Australia*,
<http://www.ponemon.org/library/2011-cost-of-data-breach-australia>

Richards, K, (2009), *The Australian Business Assessment of Computer User Security (ABACUS): a national survey*, Research and Public Policy Series 102, Australian Institute of Criminology: Canberra.
<http://www.aic.gov.au/documents/3/B/3/%7B3B3117DE-635A-4A0D-B1D3-FB1005D53832%7Drpp102.pdf>

Smith, R. & Hutchings, A., (2014), *Identity crime and misuse in Australia: Results of the 2013 online survey*, Research & Public Policy Series, Australian Institute of Criminology: Canberra.

Appendix A – Measurement Framework Pilot Indicators

| Table A1 – Pilot project measurement indicators of identity crime and misuse and data sources | | |
|---|---|---|
| Indicators | Description | Data source |
| 1. Acquisition of Fraudulent IDs | | |
| 1.1 The price of fraudulent identity credentials | The cost to illicitly acquire real Australian credentials or identities. | Data from law enforcement (and other government) agencies on the cost to illicitly acquire the most common identity credentials such as: <ul style="list-style-type: none"> • Driver licences • Australian passport • Medicare card • Birth certificate |
| 1.2 Number of reported data breaches | Acts as a proxy measure of organisational cyber security arrangements for protecting personal information. | Privacy (Information) Commissioners. Ponemon Institute Verizon |
| 2. Use of Fraudulent IDs | | |
| 2.1 Number of identity crime and misuse incidents recorded by government agencies. | Estimates the known (or detected) incidence of identity crime and or misuse, based on incidents recorded in Australian governments administrative and law enforcement datasets. | AFP ATO DFAT DHS DIBP ACCC Births, Death & Marriages Consumer Affairs / Protection Police (State & Territory) Privacy Commissioners Road & Traffic Authorities |
| 2.2 Number of prosecutions for identity crime and other related offences | The number of prosecutions for identity related offences is used as a proxy for the number of serious incidents of identity crime and misuse that occur in Australia. | CDPP ABS Police (State & Territory) |
| 2.3 Number of people who self-report being victims of identity crime or misuse | Estimate of the victimisation rate based on self-report data, collected in specialised crime victimisation or consumer surveys. | AIC survey ABS surveys AGD surveys |
| 2.4 Number of people who perceive identity crime and misuse as a problem | Estimate the number and proportion of people who perceive identity crime and misuse as a problem based on data collected from attitudinal surveys | ABS AGD |

Table A1 – Pilot project measurement indicators of identity crime and misuse and data sources

| Indicators | Description | Data source |
|--|---|--|
| 2.4 The types of personal information most susceptible to identity theft or misuse | Estimate the types of personal information and identity credentials that may be more vulnerable to theft or misuse, based on data collected from attitudinal surveys. | ABS AGD |
| 3. Consequences of ID Crime | | |
| 3.1 Direct costs of identity crime and misuse to government agencies | Estimates of the cost of identity crime and misuse to government agencies. | AFP ATO DFAT DHS DIBP ACCC Births, Death & Marriages Consumer Affairs / Protection Police (State & Territory) Privacy Commissioners Road & Traffic Authorities |
| 3.2 Direct costs of identity crime and misuse to business | Estimates of the cost of identity crime and misuse to businesses. | Unisys Symantec KPMG |
| 3.3 Direct financial losses to victims of identity crime and misuse | Estimates of the cost of identity crime and misuse to individuals. | ABS AGD AIC |
| 3.4 Number of identity crime victims experiencing non-financial consequences | Seeks to quantify the non-monetary harm caused by identity crime victimisation. | Academic literature |
| 4. Remediation of ID Crime | | |
| 4.1 Average time by victims spent in remediation activity (i.e. recovering their identity) | Estimates the time victims (broadly individual, business and government victims) spend trying to resolve the issue of having their identity stolen or misused. | ABS AIC AGD Police (State & Territory) Consumer Affairs / Protection |
| 4.2 Number of enquiries to government agencies regarding assistance to recover identity information | Identifies the number of enquiries made to government agencies about identity recovery measures. | OAIC AGD State Consumer Affairs agencies |
| 4.3 Number of applications for Victims' Certificates (issued by the courts) | Assesses the application rate for Victims' Certificates in each applicable Australian jurisdiction. | AGD ABS CDPP |

Table A1 – Pilot project measurement indicators of identity crime and misuse and data sources

| Indicators | Description | Data source |
|--|--|---|
| 5. Prevention of ID Crime | | |
| 5.1 Number of identity credentials able to be verified using the DVS | The number of identity credentials that can be validated through the Document Verification Service | AGD |
| 5.2 Number of government agencies using the DVS | The number of government agencies using the Document Verification Service to determine the validity of a document | AGD |
| 5.3 Number of private sector organisations using the DVS | The number of private sector organisations using the Document Verification Service to determine the validity of a document | AGD |
| 5.4 Number of DVS transactions each year | The number of validation transactions through the DVS each year | AGD |
| 5.5 The proportion of individuals, business and governments that adopt robust online security practices to protect personal information | Measures the extent to which the Australian population (as individuals or by designated sector) have acted to minimise risk by using computer security protection. | AGD (CERT) ACMA Microsoft Sophos |

Appendix B – Minimum and Complete Variable List for Ongoing Data Collection around Identity Crime and Misuse in Australia

Table B1: Minimum Variable List for Ongoing Data Collection around Identity Crime and Misuse in Australia

| | Variable Number | Variable Name | Variable Description |
|-----------------------------|-----------------|--------------------------------|--|
| Minimum Variable List (1-6) | 1 | Incident Identification Number | Each recorded incident should be given a unique identification number, to allow agencies to search through cases, and to allow the production of an incident count. |
| | 2 | Incident Date | The date, month and year of each recorded incident. |
| | 3 | Incident Type | This variable is intended to allow agencies to distinguish between the various types of identity crime they experience. In the case of the Department of Human Services, the options under this variable may include identity fraud against: <ul style="list-style-type: none"> • Family assistance payments; • Pension payments; • Disability/sickness payments; • Carer payments; • Education/study assistance; • Partner payments; • Household assistance; • Other (i.e. not elsewhere classified). Each agency will need to specify the different options that are included under this variable. |
| | 4 | Incident Direct Loss to Agency | Record the precise (or best estimated) dollar figure that was lost by the agency as a result of the identity crime. |
| | 5 | Identity Credential Involved | Capture information about the type of identity credential that was used to facilitate the identity crime. <ul style="list-style-type: none"> • Medicare card; • Driver licence; • Proof of age card; • Birth certificate; • Marriage/divorce certificate; • Immicard; • Australian passport; • Passport from another country; • Other (i.e. not elsewhere classified). |
| | | | |

Table B1: Minimum Variable List for Ongoing Data Collection around Identity Crime and Misuse in Australia

| | Variable Number | Variable Name | Variable Description |
|--|-----------------|----------------------------------|--|
| | 6 | Type of Fraudulent Identity Used | <p>This variable is intended to isolate the specific type of fraudulent identity information that was used in the crime (where information is available).</p> <ul style="list-style-type: none"> • Manipulated genuine identity (i.e. parts of a legitimate identity stolen); • Stolen genuine identity (i.e. the complete identity of another person stolen); • Partially fabricated identity (i.e. some part of the identity is genuine and some part is fake); • Completely fabricated identity (i.e. the identity is completely fake). |

Table B2: Complete Variable List for Ongoing Data Collection around Identity Crime and Misuse in Australia

| | Variable Number | Variable Name | Variable Description |
|-------------------------------|-----------------|---------------------------|---|
| Complete Variable List (1-19) | 7 | Alleged Offender's Gender | <p>The gender of the alleged offender:</p> <ul style="list-style-type: none"> • Male • Female • Transgender • Other |
| | 8 | Alleged Offender's Age | <p>The alleged offender's age (if known). (Note: Variable 7 & 8 are designed to allow agencies to build an offender profile that may assist with the targeting of preventative measures).</p> |
| | 9 | Incident Detected | <p>The purpose of this variable is to collect information about how the incident of identity crime or misuse was detected. Variable options could include the following:</p> <ul style="list-style-type: none"> • Internal review/audit; • As part of broader investigation; • By referral from another organisation/agency; • Tip-off from member of public; • Other (i.e. not elsewhere classified). |
| | 10 | Incident Indirect Loss | <p>Record the estimated dollar figure associated with detecting, investigating and prosecuting the identity crime. This information could be recorded in estimated ranges:</p> <ul style="list-style-type: none"> • 0 - \$2,999; • \$3,000 - \$5,999; • \$6,000 - \$8,999; • \$9,000 - \$11,999; • \$12,000 - \$14,999; • \$15,000 - \$17,999; • \$18,000 and above. |

Table B2: Complete Variable List for Ongoing Data Collection around Identity Crime and Misuse in Australia

| | Variable Number | Variable Name | Variable Description |
|--|------------------------|--|--|
| | 11 | Incident Outcome | This variable is intended to capture information about how the matter was dealt with once it was identified. Options under this variable might include: <ul style="list-style-type: none"> • Referred for ongoing monitoring; • Referred for internal investigation; • Referred to law enforcement; • Referred to Director of Public Prosecution; • Other outcome; • No further action required. |
| | 12 | Name of Fraudulent Identity | This variable should be used to record the name used as part of the fraudulent identity. This would provide agencies with the ability to share this information to ensure that the same fraudulent name is not being used against multiple different targets. |
| | 13 | Date of Birth of Fraudulent Identity | This variable should be used to record the date of birth used in the fraudulent identity. This would provide agencies with the ability to share this information to ensure that the same fraudulent date of birth is not being used against multiple different targets. |
| | 14 | Date of Call for Assistance from ID Crime Victim | Record the date of all calls for assistance from victims of identity crime or misuse. |
| | 15 | Name of ID Crime Victim | Record the name of the ID crime victim requesting assistance. |
| | 16 | Gender of ID Crime Victim | Record the gender of the ID crime victim requesting assistance. |
| | 17 | Date of Birth of ID Crime Victim | Record the date of birth of the ID crime victim requesting assistance. |
| | 18 | Amount Lost by Victim of ID Crime | Record the precise dollar figure reported lost by the victim of identity crime or misuse. |
| | 19 | Response Provided to Victim of ID Crime | This variable is intended to capture information about how the victim of ID crime was dealt with once they had reported the matter. <ul style="list-style-type: none"> • Referred for ongoing monitoring; • Referred for internal investigation; • Referred to law enforcement; • Referred to iDcare; • Other outcome; • No further action required. |