Australian Government
Australian Institute of Criminology

Evaluation of the Australian Cybercrime Online Reporting Network

Anthony Morgan
Christopher Dowling
Rick Brown
Monique Mann
Isabella Voce
Marc Smith

October 2016

Contents

Tables

Figures

Acknowledgements

This research was commissioned and funded by CrimTrac as part of a broader program of collaborative research. The support and assistance of Kristen Warden in managing the project on behalf of CrimTrac is gratefully acknowledged.

The evaluation was overseen by an Evaluation Working Group comprising representatives from CrimTrac, New South Wales Police Force (NSWPF), Queensland Police Service (QPS), WA Police (WAPOL), the Australian Crime Commission (ACC) and Attorney-General's Department (AGD). The Australian Institute of Criminology would like to acknowledge the support of this group in developing the evaluation, facilitating access to data and interview participants and providing feedback on research outputs.

Finally, the evaluation would not have been possible without the willing participation of staff from NSWPF, QPS, WAPOL, the ACC, AGD and Australian Federal Police who participated in interviews and provided valuable data that formed the basis of the evaluation.

Disclaimer

On 1 July 2016 the ACC and CrimTrac merged to become the Australian Criminal Intelligence Commission (ACIC). Given the evaluation relates to the period up to 30 June 2016, and the two agencies performed different roles in the management and implementation of the ACORN, this report refers separately to CrimTrac and the ACC.

Further, the Australian Institute of Criminology merged into the ACC (and then ACIC) in late 2015. Importantly, the AIC remains independent of the now ACIC. This evaluation therefore represents the views of the research team, who are members of the AIC, and does not necessarily represent the views of the ACIC or broader Commonwealth Government.

Finally, the majority of the data used as part of the evaluation were collected prior to or in early 2016. The merge of the ACC and CrimTrac has resulted in changes to the way in which the ACORN and cybercrime intelligence is managed. Further, there have been regular meetings of the ACORN Steering Group and Joint Management Group that have overseen the implementation of the ACORN, identifying issues and developing strategies to address them, where possible. In addition, work is underway to develop a business case for an updated version of the ACORN ICT infrastructure. Descriptions of the process by which the ACORN and police partner agencies handle reports are therefore current up to early 2016, and will not reflect any recent changes. However, data on outcomes are unlikely to be affected.

Acronyms

AGD	Attorney-General's Department
ABS	Australian Bureau of Statistics
ACC	Australian Crime Commission
ACCC	Australian Competition and Consumer Commission
ACIC	Australian Criminal Intelligence Commission
ACORN	Australian Cybercrime Online Reporting Network
AFP	Australian Federal Police
AIC	Australian Institute of Criminology
ANZPAA	Australia New Zealand Policing Advisory Agency
CERT	Computer Emergency Response Team
CICIU	Cyber and Identity Crime Investigation Unit
ESNA	E-Security National Agenda
IC3	Internet Crime Complaint Centre
LAC	Local Area Command
NFA	National Fraud Authority
NPCC	National Plan to Combat Cybercrime
NSWPF	New South Wales Police Force
Orb	Online reporting button
QPS	Queensland Police Service
UNODC	United Nations Office on Drugs and Crime
USD	United States Dollar
WAPOL	Western Australia Police

Executive summary

The Australian Institute of Criminology (AIC) was commissioned by CrimTrac to conduct an evaluation of the Australian Cybercrime Online Reporting Network (ACORN). The ACORN is a national online facility that receives cybercrime reports from members of the public, provides information to Australian law enforcement agencies and provides crime prevention advice to the public. The overall aim of the ACORN was to improve strategic, operational and tactical responses to cybercrime.

The AIC's approach to the evaluation was developed in collaboration with an Evaluation Working Group (EWG) comprising representatives from the Attorney-General's Department (AGD), Australian Crime Commission (ACC), Queensland Police Service (QPS), NSW Police Force (NSWPF), Western Australia Police (WAPOL) and CrimTrac.

The evaluation has been wide ranging, obtaining the views of more than 1,600 ACORN users who submitted a report through an online survey and more than 3,500 members of the general public through a survey conducted before and after the implementation of the ACORN. In addition, working closely with the ACC, NSWPF, QPS and WAPOL enabled the AIC to collect data on the handling of cybercrime reports, intelligence activity and enforcement activity and obtain the views of a wide range of stakeholders. Together, these data provide a unique and important insight into effectiveness of the ACORN in improving law enforcement response to cybercrime.

Finding 1: There have been more than 65,000 reports submitted to the ACORN since it was first implemented, with a recent upward trend in the number of reports

Between November 2014 and June 2016 there were more than 65,000 reports submitted to the ACORN. Online scams and fraud were the most common type of cybercrime reported (48% of all reports), followed by issues buying and selling online (21%).

There was a peak in reporting to the ACORN in May 2015, likely due to the significant investment in a communication and marketing campaign that supported the implementation of the ACORN in early 2015. While the trend was otherwise relatively stable throughout 2015, there was a four percent increase in the number of reports submitted in the first half of 2016, indicating a recent upward trend in reporting.

Finding 2: There was little evidence that the ACORN has led to an increased prevalence among victims of reporting cybercrime victimisation to police

Victimisation rates for the four major categories of cybercrime reportable to the ACORN remained relatively stable between the pre- and post-implementation public survey. Rates of reporting to police also remained stable, with the exception of an increase in the rate of reporting for issues buying or selling online.

Notwithstanding the very small numbers, this did not appear to be the result of the ACORN, with only four percent of victims of issues buying and selling online reporting to the ACORN. Rates of reporting to the ACORN among victims ranged from two percent for victims of attacks on computer systems to one in ten victims of online scams and frauds.

Finding 3: There has been little change in terms of public awareness of where to report cybercrime

The ACORN aims to make it easier for victims to report cybercrime by providing an easy and accessible method for reporting that is dedicated to cybercrime offences. There was little difference between the pre- and post-implementation survey responses in terms of the proportion of victims who did not report the most recent incident due to being unsure of which agency to contact.

Further, more than one-third of all victims, including more than half of all victims of cyber bullying, sexting, online harassment and stalking, reported the most recent incident of cybercrime to police, in addition to reporting it to the ACORN. A large proportion of victims who report to the ACORN have attempted to report to police through a more traditional mode of reporting in the first instance. Overall, these results suggest there has been little change in terms of public awareness of where to report cybercrime. If anything, it may have created some confusion and impacted levels of satisfaction among victims, at least in the short-term.

Finding 4: There are relatively high levels of satisfaction with the process of reporting to the ACORN

ACORN users appear to be largely satisfied with the ACORN user interface. While there is some variability between users, there is a high level of satisfaction with the reporting process in terms of the ease with which reports can be made, the relevance of information requested, the accessibility of the system and the time taken to enter reports.

However, views were mixed in terms of how the ACORN compared with alternative methods of reporting cybercrime. Around half of all victims felt that it was easier to report to the ACORN and that reporting the ACORN was more convenient and faster than other methods.

Finding 5: Overall levels of satisfaction among cybercrime victims with the outcome of submitting a report to the ACORN are low, particularly among those ACORN users who were not satisfied with the process or whose expectations were not met

Less than one-third of all victims who reported to the ACORN were satisfied with the outcome. There was evidence that cybercrime victims who reported to the ACORN were less satisfied than cybercrime victims who reported to police through more traditional modes (by phone, in person etc). The same was also true when compared with victims of theft offences.

Consistent with past research, satisfaction with the process of reporting was an important predictor of satisfaction with the outcome of reporting. Nearly half of all victims who were satisfied with the process of reporting were satisfied with the outcome, compared with around one in eight victims who were not satisfied with the process.

More importantly, however, was that four in five victims reporting to the ACORN expected that they would be notified that their report had been investigated. Around one in six actually were, and one in four victims reported that they had not received any information about their report. Victims who were notified that their report had been investigated were much more likely to be satisfied with the outcome. However, there was much fewer of them.

More than three quarters of all victims who reported to the ACORN said that the outcome did not meet their expectations. Not surprisingly, very few of these victims (15%) were satisfied with the outcome.

Finding 6: Victims of issues buying and selling online and of cyber bullying, online harassment, sexting and/or stalking tend to be less satisfied with the ACORN than other victims

Overall rates of satisfaction with the outcome of reporting to the ACORN were lowest among victims of issues buying and selling online and of cyber bullying, online harassment, sexting and/or stalking. They tended to be less satisfied with the process of reporting to the ACORN, but had higher expectations of offenders being apprehended and were more likely to report that their expectations had not been met. This is probably because victims of issues buying and selling online were far more likely than any other victims to report to the ACORN to recover lost money, while victims of cyber bullying, online harassment, sexting and/or stalking were significantly more likely to report so that police could investigate the crime.

Finding 7: Awareness of the ACORN among the general public is still relatively low, but people who are aware of the ACORN are more positive about the government's response to cybercrime

In the post-implementation public survey, conducted nearly 15 months after the ACORN had been implemented, only 14 percent of respondents reported that they were aware of the ACORN. Importantly, those respondents who were aware of the ACORN were generally more positive about the Australian Government's response to cybercrime. They were more supportive of the Australian Government's response and had higher levels of satisfaction and confidence in the response. They were also more likely to believe the Australian Government was doing more to respond to cybercrime than it was 12 months ago and that it was committed to combatting cybercrime.

Finding 8: Each of the police partner agencies implemented the ACORN in different ways, but they all reported a significant rise in the number of reports received and associated resource implications

The number of reports automatically referred to law enforcement agencies has gradually increased since the ACORN was first implemented, with nearly three quarters of all reports submitted in 2015-16 automatically referred. Reports referred by the ACORN are received and handled by specialist units in each agency, and these units have implemented the ACORN in different ways. In WAPOL, reports are assessed by the Technology Crime Investigation team and investigations are commenced where there is some prospect of a positive outcome. Other reports are 'written off' and victims are notified of this decision. The role of the NSWPF Fraud and Cybercrime Squad and QPS Fraud and Cyber Group has largely been to enter ACORN report data into that agency's own information management system and enable local area commands (LAC) to commence investigations—the latter has also prioritised high-risk reports received through the ACORN, including offences against children and domestic violence.

Irrespective of the model that has been adopted, the ACORN has contributed to a significant increase in the number of reports received and handled by specialist units within the three participating agencies. While each agency has adopted a different method for reviewing, prioritising and handling reports, all three police partner agencies reported significant resource implications associated with this increase. This has resulted in significant delays in entering and responding to cybercrime reports in some jurisdictions.

There have been some limitations with the ACORN system that have impacted on law enforcement outcomes and resulted in some duplication of effort, including the limited interoperability with police information systems, the format of reports produced, the amount of information that is collected and the capacity of the system to automatically group reports over time.

Finding 9: The ACORN has largely shifted responsibility for referring reports between business areas and agencies, rather than reduce the time spent by law enforcement referring reports

Prior to the ACORN, cybercrime reports could be referred to or from LACs to a specialist cybercrime unit, depending on who was best placed to conduct an investigation, or from one agency to another once the offender's location has been determined—often once an investigation had commenced. The ACORN was expected to address some of these inefficiencies by automatically grouping and referring reports to the appropriate jurisdiction, based on the information supplied by the victim reporting the incident.

The trend towards encouraging all victims attempting to report cybercrime through traditional mechanisms (by telephone or in person) to report via the ACORN, the automated referral of reports to state and territory police by the ACORN, and the centralisation of report handling within specialist units, has altered these referral pathways. Most importantly, responsibility for referring reports now rests with the specialist units who receive and handle reports submitted to the ACORN.

Both NSWPF and QPS indicated that the referral of reports to LACs had presented a significant administrative burden, and required dedicated personnel to be appointed to the role of entering reports into the local information management system to facilitate referrals. WAPOL reported a relatively small decline in the proportion of investigations commenced by the Technology Crime Investigation team that were finalised and referred to another business area or agency, but these also doubled in number.

Finding 10: The number of cybercrime intelligence products has increased following the introduction of the ACORN, which has required more analyst time but also resulted in more efficient intelligence activity

Overall, the increase in cybercrime reports resulting from the introduction of the ACORN has led to an increase in the level of intelligence activity (based on the number of products produced). While the number of intelligence products has been highly variable, and not all of the reports draw upon the ACORN or relate to the categories of cybercrime reportable to the ACORN, the number of strategic and tactical intelligence products produced by specialist cybercrime units within the ACC, NSWPF and QPS has increased.

Based on data supplied by the ACC and NSWPF, the ACORN has contributed to an increase in overall time spent by analysts preparing cybercrime intelligence products. However, in both cases, the increase in the total amount of time spent by intelligence analysts on cybercrime intelligence activities was not proportionate to the increase in the number of products, meaning that the estimated number of hours per intelligence product declined significantly—by around half. This may be due to the grouping of reports, or the ease with which patterns in offences can be identified.

Finding 11: The number of investigations into cybercrime offences has increased, and it appears this has contributed to increased resourcing for cybercrime investigations

Similar to intelligence activity, the increase in the number of cybercrime reports has contributed to a significant increase in the number of investigations commenced. NSWPF reported a significant increase in the number of investigations commenced, largely within LACs, while the the WAPOL Technology Crime Investigation team reported a three-fold increase in the number of investigations commenced. This ranged from a two-fold increase for attacks on computer systems, to a nine-fold increase in the number of investigations into online scams and fraud.

Senior police raised concerns about the resource implications associated with an increase in investigations, particularly as they relate to low-level cybercrime offences. Data on the average number of hours spent by NSWPF and WAPOL investigators investigating the categories of cybercrime reportable to the ACORN suggested that the ACORN has contributed to increased resourcing for investigations, at least within centralised specialist areas. A shift towards greater resourcing for cybercrime investigations is a positive outcome and, at least to some extent, something the ACORN set out to achieve.

Nevertheless, there is still a significant backlog of reports in some jurisdictions resulting in long delays in terms of commencing investigations—this has an impact on both the likelihood of a positive investigation outcome and satisfaction of the person making the report. There was anecdotal evidence of victims submitting multiple reports for the same incident due to perceived inaction by police.

Finding 12: There have been examples of positive investigation outcomes resulting from the grouping of reports by the ACORN and ability to identify patterns of offences, but challenges persist

There have been examples of successful outcomes resulting from the grouping of reports to the ACORN and ability to identify patterns of offences. WAPOL reported several investigations that had resulted in an offender being identified and, in some cases, apprehended.

However, this represented less than one percent of all investigations. The proportion of investigations finalised where there was no further action because no offence had occurred nearly doubled, while there was a five-fold increase in the number of investigations per quarter with this outcome. These results may not be indicative of patterns in other jurisdictions, but they highlight the challenges associated with relying on information reported by members of the public.

Widely acknowledged challenges associated with policing cybercrime also persist, such as the difficulties identifying where offenders reside and investigating overseas offenders, limited police understanding and knowledge of cybercrime, police staff rotation policies and under resourcing for policing technology-enabled crime.

Finding 13: There has been a high level of engagement with the prevention advice available from the ACORN among those users who submit a report

ACORN users who report a cybercrime incident are also able to access targeted prevention advice, which relates specifically to the type of cybercrime reported by the user. Around three quarters of victims who reported to the ACORN read the targeted prevention advice at the time of submitting a report. Further, around one in four users reported having accessed the general prevention advice at any time, typically in the three months after submitting a report.

The vast majority of users reported both types of prevention advice as being easily understood, while around two-thirds of all users felt it was useful were satisfied with the information. Around half of all users felt the information was relevant and, in the case of targeted prevention advice, that the recommended strategies would reduce their risk of repeat victimisation.

Finding 14: Many victims who report to the ACORN implement strategies recommended in the prevention advice, but there is little evidence that the prevention advice has had an impact on repeat victimisation rates

Around two-thirds of victims who read the targeted prevention advice reported having started using or using more frequently at least one prevention strategy since having submitted a report to the ACORN. The exception to this was victims of cyber bullying, sexting, online harassment and/or stalking, with less than half reporting having started using or using more frequently at least one prevention strategy.

Overall rates of reporting repeat victimisation to the ACORN were relatively low, irrespective of the type of cybercrime experienced. One in six ACORN users who were a repeat victim in the three months after submitting the original report reported the subsequent and most recent incident to the ACORN. There was little difference in the repeat victimisation rates for those ACORN users who had read the targeted prevention advice and those who did not, suggesting that it has had little impact on the rates of repeat victimisation among victims who report to the ACORN.

Introduction

Over the past three decades, cybercrime has developed into a major form of transnational organised crime with significant consequences for a growing number of victims in Australia (Standing Committee on Communications 2010). Cybercrime offenders can inflict catastrophic loss or damage to individuals, companies and governments at little cost and from remote locations (Broadhurst 2006; Broadhurst et al 2014).

Cybercrime is a broad term that encompasses a wide range of offences. It refers to crimes that are directed at computers and devices connected to the internet or the communications technology supporting them (such as hacking, denial of service attacks and the unauthorised access to, modification or impairment of electronic communications or computer systems or data). It also includes those crimes where the internet, communications technology or information technology is an integral part of the commission of the offence (such as online fraud, identity theft and distribution of child exploitation material). It excludes forms of criminal conduct in which the use of a computer is merely incidental to the offending.

While it is difficult to measure the costs of cybercrime to Australia, government agencies estimate that cybercrime costs the Australian community billions of dollars a year (Attorney-General's Department (AGD) 2009; 2013). The private sector estimates the annual global cost of cybercrime in 2013 at $113 billion (USD), and the annual Australian cost of cybercrime at approximately one billion (USD) (Johnson 2013; Symantec 2014).

Available data on victimisation indicates that cybercrime victimisation rates are significantly higher than traditional crime victimisation rates. Victimisation rates for online credit card fraud, identity theft, responding to phishing attempts or unauthorized access to email accounts are estimated at between one and 17 per cent of the online population (United Nations Office of Drugs and Crime (UNODC) 2013). The 2013 Norton Report placed the 2013 annual rate of victimisation of cybercrime as high as 50 percent of online adults (Symantec 2014). By comparison, in 2012-13 less than three percent of the Australian population were a victim of physical assault, less than three percent of households were a victim of home break-ins and six percent of households were victims of at least one incident of malicious damage (Australian Bureau of Statistics (ABS) 2014).

Australian approach to cybercrime

In response to this growing evidence, there has been a concerted effort by the Australian Government (and its international counterparts) to develop a coordinated response to cybercrime. The Australian Government's approach to cybercrime was guided by the E-Security National Agenda (ESNA). The ESNA was periodically reviewed from 2004 to 2008 to reflect the increasing threat of cybercrime and the development and expansion of the use of information communication technology over this period (Standing Committee on Communication 2010). In 2009, the Cyber Security Strategy was launched, bringing all cybercrime policy together into one framework, and replacing the ESNA. This was superseded by an updated Cyber Security Strategy, released in April 2016.

The current Cyber Security Strategy is built around five key themes:

- A national cyber partnership. This recognises the importance of government working with the business sector to address cyber threats, including cybercrime, with a commitment to jointly set a strategic agenda. There is also a commitment to relocate the Australian Cyber Security Centre (ACSC) to help foster greater partnership-working between Government and the private sector. Formed in November 2014, the ACSC brings together law enforcement and security agencies from across the Commonwealth.
- Strong cyber defences. This includes strengthening the capabilities of the Australian Signal's Directorate and increasing the capacity of the National Computer Emergency Response Team - CERT Australia. Launched in 2010, CERT Australia's mandate is to provide Australian businesses with advice and support in mitigating cyber threats. It focuses on cyber security issues affecting major Australian businesses, Australia's critical infrastructure and other systems of national interest, rather than on cybercrime affecting the public or small / medium sized businesses. (Standing Committee on Communications 2010).
- Global responsibility and influence. The strategy sets out a commitment to champion an open, free and secure internet. This also includes a commitment to building capacity to tackle cybercrime that originates overseas.
- Growth and innovation. This places a particular emphasis on cyber security innovation that will be fostered through a new Cyber Security Growth Centre. This Centre will work with Government, business and the research community to define and prioritise national cyber security issues.
- A cyber smart nation. This will include establishing centres of cyber security excellence in universities as well as encouraging greater uptake of subjects at school that will feed into cyber security studies. The Strategy also reinforces the Government's commitment to raising national cyber security awareness, with the Attorney General's Department tasked to develop a national cyber awareness raising campaign to help Australians be more aware of cyber risks and know how to stay secure online.

The Strategy also includes a range of measures designed to bolster the Commonwealth's operational approach to cybercrime, including increasing the number of specialists conducting threat detection and technical analysis of cybercrime matters within the Australian Federal Police (AFP) and Australian Criminal Intelligence Commission (ACIC) and increasing overseas partnerships to target the source of cyber security threats.

Importantly, no law enforcement or policy agency has sole responsibility for cybercrime (Parliamentary Joint Committee on the Australian Crime Commission Inquiry into Cybercrime 2004). Within Australia, responsibility for cybercrimes committed against individuals, businesses and government systems rests with state and territory police agencies. Infrastructure, data systems of national interest and Australian Government systems are the responsibility of Commonwealth agencies, such as the AFP (AGD 2013). A number of Australian Government agencies are also responsible for developing responses to cybercrime in Australia (AGD 2013; CERT Australia 2012).

Given the range of agencies involved in addressing this growing problem, a 2010 Senate Inquiry into cybercrime found that a more strategic and coordinated response to cybercrime was required. To help achieve this, the Inquiry recommended that a national cybercrime reporting centre be developed and that it should provide a single portal for standardised online reporting of cybercrime across a range of categories. Further, that the data be collected in a systematic way to enable aggregation for intelligence purposes, referral to appropriate agencies and the provision of public information about cybercrime prevention strategies.

As a result, the development of a reporting centre became an important feature of the Attorney-General's Department National Plan to Combat Cybercrime (NPCC). This Plan was developed in 2013 and sits under the national Cyber Security Strategy (AGD 2013). The NPCC identified priority areas and outlines initiatives to respond to the problem of cybercrime in Australia. There were four key principles guiding the NPCC:

- developing a better understanding of the problem of cybercrime and how it affects Australia;
- developing national and international partnerships to respond to cybercrime;
- a focus on crime prevention; and
- balancing security, freedom and privacy on the internet.

A key initiative under the NPCC was the development of an online reporting system that would make it easier for the public to report cybercrime and access information on prevention and that would provide the data necessary to inform more effective operational and policy responses.

Online reporting systems

Cybercrime investigation and enforcement presents a number of challenges for police. The size of the internet means the investigation of cybercrimes is technical and complex and often involves different agencies across multiple jurisdictions (Hunton 2010; 2011a; 2011b; 2012). Cybercrimes frequently cross national, and state and territory borders. This means that police must negotiate formal and informal channels of communication and cooperation, in order to share information and conduct joint investigations (Urbas 2012). A lack of coordination and cooperation between agencies is one of the most problematic issues in cybersecurity (Levi & Williams 2013). Further, an absence of policies around information sharing has created difficulties for police (Kellermann 2010). The challenges presented by cybercrime mean that police and other agencies must have effective and efficient means of sharing information.

Another challenge facing police is the underreporting of cybercrime by victims. A recent study completed by the United Nations Office on Drugs and Crime (UNODC) identified that 90 percent of countries that responded to their survey reported that cybercrime offences are most commonly brought to the attention of law enforcement through reporting by victims (UNODC 2013). Despite victim reporting being the most frequent method by which cybercrime is brought to the attention of authorities, cybercrime is believed to be significantly underreported (UNODC 2013). This may be due to victim shame and embarrassment, confusion about which agency to contact or whether they have actually been a victim of a crime. Importantly, this hampers efforts to properly understand the extent, patterns and drivers of cybercrime offences.

In order to address the issue of victim underreporting and sharing of information between jurisdictions, a number of developed countries have recently established online reporting portals that enable members of the general public to make reports to police:

- In the United States, the Federal Bureau of Investigation and the National White Collar Crime Centre established the Internet Crime Complaint Centre (IC3) to receive reports of cybercrime victimisation. This system is an expanded version of the Internet Fraud Complaint Centre. The mission of the IC3 is to 'receive, develop, and refer criminal complaints' relating to cybercrime victimisation and to provide 'a convenient and easy-to-use reporting mechanism that alerts authorities of suspected criminal or civil violations' (IC3 2014).
- In the United Kingdom, the City of London Police and the National Fraud Intelligence Bureau have implemented Action Fraud, which was developed as the national reporting centre for cybercrime and fraud (Action Fraud 2014). Action Fraud provides a web based platform and hotline allowing members of the public to report incidents of cybercrime and fraud and receive advice.
- New Zealand has implemented the Online Reporting Button (Orb) to enable the public to report incidents of cybercrime. The Orb receives reports from the public for a range of online

offences, including objectionable material, issues with online traders, privacy breaches, scams or fraud, computer system attacks, spam messages, offending against children, and child exploitation material (Netsafe 2014).

- The International Consumer Protection and Enforcement Network developed the eConsumer.gov site. This site provides an online reporting portal allowing consumers around the world to report scams that involve foreign companies. The data collected is aggregated and used to analyse trends (Standing Committee on Communications 2010).

In Australia, online cybercrime reporting systems have been established in the field of consumer protection since 2006. The Australian Competition and Consumer Commission (ACCC) have established a reporting platform known as SCAMwatch (ACCC 2014). SCAMwatch enables members of the public to report suspected or actual scams to the Australian Competition and Consumer Commission, including those that are based online. Information from reports received by SCAMwatch is used to monitor scams across Australia and inform the public of new scams by providing educational material on the website.

There have also been initiatives developed at the state and territory level. For example, the Queensland Police Fraud and Corporate Crime Group have developed and implemented online reporting portals in response to the problem of 'Nigerian Fraud' and fraud conducted on online auction sites (Standing Committee on Communications 2010). An example of the latter is the eBay project which enabled members of the public to report online auction fraud. This was initially limited to eBay users, but was later extended to all online auction sites. The reports are then referred to the relevant police agency. The eBay project also provided an aggregated database of fraud committed on auction sites (Standing Committee on Communications 2010).

Research has shown that alternative crime reporting modes are popular with the general public, increase reporting and have been found to improve the completeness of crime reports, without compromising accuracy. Lasley (1995) demonstrated that online reporting of crime resulted in higher reporting rates than telephone reporting for both low and moderate levels of crime seriousness. Age has a significant influence on internet reporting, which is supported more by younger age cohorts (Alarid & Novak 2008). Lack of internet knowledge or capability may impact on reporting for older age groups. Finally, Iriberri and Navarrete (2013) evaluated the effectiveness of an interactive e-government system for reporting crime. The results of their evaluation indicate that the online reporting system resulted in more complete crime reports being made with comparable report accuracy.

Australian Cybercrime Online Reporting Network

The Australian Cybercrime Online Reporting Network (ACORN), an Australian Government initiative launched in November 2014, is a national online facility that receives cybercrime reports from members of the public, provides information to Australian law enforcement agencies and provides crime prevention advice to the public. The overall aim of the ACORN is to improve strategic, operational and tactical responses to cybercrime. To achieve this aim, the ACORN has four key objectives:

- provide a centralised, national online facility that would receive reports from members of the public;
- refer reports to the police and regulatory agencies for further consideration;
- collect and aggregate data from reports to assist police, regulatory and other government agencies to develop improved strategic and tactical responses to cybercrime; and
- provide ACORN users with general and targeted educational advice.

The ACORN was expected to become a vital tool that would improve the reporting, gathering and analysis of data to combat cybercrime in Australia and encompassed service delivery, referral and data aggregation functions. There have been multiple stakeholders involved in the development, management and use of the ACORN. The ACORN information technology infrastructure is maintained by CrimTrac (now the Australian Criminal Intelligence Commission), and law enforcement agencies investigate cybercrime based on the reports received. The ACC (also now the Australian Criminal Intelligence Commission) manage and use the ACORN data to generate intelligence products for law enforcement and other government agencies. The AGD was responsible for the communication strategy and marketing of the ACORN to potential users. All of these stakeholders have a vested interest in the success of the ACORN in terms of improving Australia’s response to cybercrime.

Evaluation methodology

The approach used by the Australian Institute of Criminology (AIC) to evaluate the ACORN was underpinned by a program logic model that was developed in collaboration with an Evaluation Working Group (EWG). The EWG comprised representatives from the AGD, Australian Crime Commission (ACC), Queensland Police Service (QPS), NSW Police Force (NSWPF), Western Australia Police (WAPOL) and CrimTrac. The logic model described the outputs and outcomes that were expected to be delivered by the ACORN and the relationship between these outputs and the hierarchy of short, medium and longer-term outcomes. This provides the focus for the evaluation and is reflected in the structure of this report.

While the evaluation has adopted a national focus, three police partner agencies—NSWPF, QPS and WAPOL—were selected for more detailed examination. This was for two main reasons. First, because additional primary data on police handling and response to reports submitted to the ACORN was required, which had important resource implications (both for the AIC and police partner agencies). Second, recognising that each police partner agency has differing levels of resourcing, capacity and mechanisms for producing cybercrime intelligence and investigating reported offences, this enable the implementation and impact of the ACORN to be assessed in multiple settings.

The AIC's evaluation aimed to address a number of overarching evaluation questions about the impact of the ACORN. These are summarised in Table 1. The evaluation was conducted in two stages (a pre-post design). Stage one was a pre-implementation evaluation and examined the state of cybercrime reporting, intelligence gathering, investigation and prevention prior to the implementation of the ACORN. Stage two was a post-implementation evaluation and assessed the impact of the ACORN across these outcome domains in the 18 months post-implementation.

An evaluation framework was also developed to help guide the evaluation and was agreed by the EWG prior to commencement. This outlined the specific evaluation questions relating to the various outputs and outcomes described in the logic model, along with appropriate performance indicators, data sources and data collection methods that were used to measure these pre and post-implementation. The performance indicators and data collection methods are vital components the AIC’s evaluation of the ACORN and should be read in conjunction with the research methods described below.

Table 1 Overarching evaluation questions, by objective

Objective	Overarching evaluation questions
Provide a centralised, national online facility that would receive reports from members of the public	Has the ACORN provided a user friendly accessible system available to take reports from the public? What impact has the ACORN had on the frequency with which cybercrime incidents are reported by the public? Has the ACORN led to improved public satisfaction with the process of reporting cybercrime incidents? Has the ACORN helped build public confidence with action being taken to address cybercrime?
Refer reports to the police and regulatory agencies for further consideration	Has ACORN increased the volume of reports received by law enforcement agencies, including reports that meet the ACORN business rules? Has ACORN resulted in productivity savings for law enforcement agencies associated with the automated referral of reports by ACORN?
Collect and aggregate data from reports to assist police, regulatory and other government agencies to develop improved strategic and tactical responses to cybercrime	To what extent has the ACORN automatically grouped reports to produce patterns (both offences and offenders)? Has the ACORN provided more accurate data on the frequency, scale and impact of cybercrime? To what extent does ACORN provide information that is more actionable because it constitutes multiple offences/ victims? Has ACORN resulted in more detailed intelligence packages? To what extent has the ACORN assisted with the production of a national picture and to identify targets across boundaries? Has the ACORN enabled faster recognition of emerging problems and cybercrime trends resulting in proactive enforcement action being taken? Has ACORN resulted in more operational intelligence packages? To what extent has the ACORN helped to create operational intelligence packages that develop better quality targets? Has the ACORN made available better quality information on the nature and extent of cybercrime to policy makers? Has the number of targets against which enforcement action is taken increased due to the ACORN?
Provide ACORN users with general and targeted educational advice	Has the ACORN provided general and targeted crime prevention advice to members of the public, and to what extent has this information been accessed and read by users? Has the ACORN helped to increase public awareness and use of strategies to reduce the risk of cybercrime victimisation? Has the ACORN contributed to a reduction in repeat victimisation by providing prevention advice to victims?

Analysis of ACORN report data

Data were provided by the Australian Criminal Intelligence Commission on high level indicators relating to the performance of the ACORN. Specifically, the AIC was provided with aggregated data on the total number of reports submitted to the ACORN each month, by cybercrime type, since the implementation of the ACORN in November 2014. In addition, data on the number of reports referred by the ACORN to each state and territory were also provided. Together, this information was used to assess the use of ACORN by members of the public to report cybercrime incidents to police, and to inform the review of report handling by police partner agencies.

Survey of the general public

A survey of the general public was conducted to determine the level of cybercrime victimisation, reporting activity, satisfaction with the process of reporting cybercrime and overall perceptions of the government's response to cybercrime in the 12 months prior to the launch of ACORN and 12 months post-implementation. The survey, which was designed by the AIC, used the same categories of cybercrime reportable to ACORN and addressed the following areas:

- awareness and understanding of cybercrime;
- previous cybercrime victimisation (for categories of cybercrime reportable to ACORN);
- previous reporting behaviours and satisfaction with reporting processes (for categories of cybercrime reportable to ACORN);
- perceptions of cybercrime, including perceived risk, government initiatives and responses;
- knowledge of relevant cybercrime educational websites and resources;
- knowledge and use of individual prevention strategies; and
- knowledge and perceptions of ACORN, including the likelihood of using and actual use of ACORN.

Results from the two surveys were then compared to determine whether there have been any changes in the proportion of victims reporting cybercrime incidents to police, victim satisfaction with reporting processes and outcomes and views among the general population regarding the government’s response to cybercrime.

The public survey was administered to an online survey panel by i-Link Research Solutions in September 2014 and again in January 2016. Additional time was allowed due to the initial soft release of the system. The sample for each survey consisted of around 1,800 Australians aged 18 years and over who had internet access and who had registered with the online survey panel provider (Table 2). The sampling frame and survey hosting was undertaken by i-Link Research Solutions, with the de-identified data then provided to the AIC for analysis and reporting.

The data were then weighted according to age and sex using data from the Australian Bureau of Statistics (ABS). The process of weighting involved the application of a formula to data provided by each respondent to make each response proportionate to the broader population from which the sample was derived. For example, males aged 70 years and over accounted for 4.12 percent of respondents to the survey, but account for 5.64 percent of the broader Australian population (ABS 2014). A ratio of 1.37 was therefore applied to the responses for this cohort. This ensures that the results of the survey are generalisable to the wider population. Demographic characteristics of survey respondents using the weighted data are presented in Table 2. Importantly, 97 percent of respondents to the pre-implementation survey and 98 percent of respondents to the post-implementation survey reported using the Internet at least once a day (ie are regularly online). All of the results presented in this report refer to the weighted data.

Table 2 Demographic characteristics of survey respondents, pre- and post-implementation surveys (weighted data)

	Pre-implementation		Post-implementation	
	n	%	n	%
Sex				
Male	908	51	940	51
Female	885	49	913	49
Age				
18-24	226	13	228	12
25-29	174	10	177	10
30-34	166	9	176	9
35-39	157	9	158	9
40-44	165	9	166	9
45-49	153	9	157	8
50-54	155	9	157	8
55-59	139	8	146	8
60-64	124	7	129	7
65-69	108	6	116	6
70+	226	13	243	13
Highest level of education				
Less than year 12 or Secondary School	311	17	340	18
Year 12 or equivalent	384	21	370	20
Vocational qualification	502	28	512	28
Bachelor degree	420	23	442	24
Postgraduate degree	176	10	190	10
Income				
$0-18,200	282	16	263	142
$18,201-37,000	446	25	463	25
$37,001-80,000	540	30	560	30
$80,000-180,000	271	15	304	16
$180,001 +	46	3	32	2
I'd rather not say	209	12	232	13
Total respondents	***1,793***		***1,853***	

Totals may not equal 100 due to weighted data and rounding

Data were weighted according to ABS population data (for the relevant year) to reflect distribution of age and sex across the entire population

Source: ACORN Public Survey [AIC data file]

Interviews with stakeholders

The AIC conducted a series of interviews with senior staff, intelligence analysts and investigators involved in the development, management and operation of the ACORN. Interview participants were identified in consultation with the EWG. Nineteen agency representatives were interviewed as part of the pre-implementation evaluation, and 31 agency representatives were interviewed during the post-implementation period. Where possible, agency representatives interviewed prior to the implementation of the ACORN were interviewed again during the second stage of interviews. A summary of the roles of representatives who participated in an interview post-implementation is presented in Table 3.

Table 3 Summary of interview participants (post-implementation)

NSW Police Force	WA Police	Queensland Police Service	Commonwealth government

Senior Representatives, Fraud and Cybercrime Squad;
Senior Intelligence Analysts, Cybercrime Unit, Fraud and Cybercrime Squad;
ACORN Referral Team, Fraud and Cybercrime Squad;
Representatives from Northshore Local Area Command and Chatswood police station
	Senior Representatives, Technology Crime Investigations, Technology Crime Services;
	Team Leaders and Digital Evidence Managers, Technology Crime Services; and
	Investigators, Technology Crime Investigations, Technology Crime Services.
		Senior Representative from the Fraud and Cyber Crime Group;
		District Representative and Crime Manager from North Brisbane District;
		Referral Team for Cyber and Identity Crime Investigation Unit;
		Referral Team for Policelink and programs group;
		Representatives from State Intelligence, Intelligence, Counter Terrorism and Major Events Command;
		Team Leader, Fraud Intelligence Unit; and
		Team Leader, Cyber and Identity Crime Investigation Unit.
			Representatives from the ACIC, including client managers responsible for the ACORN, and intelligence analyst seconded to the Australian Cyber Security Centre (ACSC);
			Representative from the Cybercrime Unit at AGD; and
			Senior representatives from the Australian Competition and Consumer Commission (ACCC); and
			Intelligence analysts from the Consumer and Small Business Strategies Branch, (ACCC).

Interviews with senior representatives

Interviews were conducted with senior representatives from the ACC, AGD, AFP, NSWPF, QPS, WAPOL. Interview participants were engaged on the basis that they were responsible for overseeing their agency's response to cybercrime. The purpose of these interviews during the was to better understand stakeholder views regarding the need for the ACORN prior to implementation, the limitations and challenges associated with the implementation of ACORN and the implications of the ACORN for law enforcement and the response of the agency to cybercrime.

Interviews with intelligence analysts

Interviews were also conducted with intelligence analysts from two of the three participating police agency partners (NSWPF and QPS) as well as the ACC. WAPOL does not currently have a dedicated cybercrime intelligence analyst. Analysts were interviewed on the basis that they were responsible for reviewing cybercrime reports and preparing both tactical and strategic intelligence for investigators. Interviews with intelligence analysts explored issues related to:

- the need for ACORN and the gap that it addresses;
- intelligence handling processes for cybercrime offences;
- the perceived quality of information on cybercrime offences, offenders and victims (as well as risks and emerging threats) available to intelligence analysts; and
- the impact of the ACORN for intelligence analysts.

Interviews with investigators

Cybercrime investigators were also interviewed to better understand law enforcement responses to cybercrime before and after the implementation of the ACORN. Interviews were conducted with investigators from specialist units in NSWPF, QPS and WAPOL, and a sample of investigators in local area commands. The interviews explored a range of issues, including:

- the type of activities undertaken by law enforcement in response to cybercrime;
- barriers to effective police investigations;
- new and emerging cybercrime threats;

- perceptions regarding the availability of intelligence;
- how intelligence helps to inform the prevention and enforcement response to cybercrime by police agencies, and;
- the impact of the ACORN on the investigation of cybercrime offences.

Survey of law enforcement agencies

A survey instrument was developed to provide a snapshot of the nature and extent of cybercrime reporting to police pre and post-implementation of the ACORN. The survey was distributed to specialist cybercrime units within NSWPF, QPS and WAPOL. All three agencies completed this survey for the periods 1 July 2014—30 September 2014 and 1 July 2015—30 September 2015. The survey was based on the same categories of cybercrime used by ACORN and required the respondents to report:

- the number of reports received from members of the public;
- the number of reported cybercrime offences that met the ACORN business rules;
- investigation outcomes for offences reported by members of the public;
- reported incidents referred to other business areas or agencies, where they were referred, and the average time spent referring reports; and
- reported incidents referred from other business areas or agencies, where they were referred from, the investigation outcomes for referred reports and the average time spent re-referring reports.

Results from the two surveys have been compared to measure changes in the nature and extent of cybercrime reporting to law enforcement agencies and, where possible, the extent to which reports are referred to and from other business areas and agencies.

Quarterly monitoring tool to measure intelligence activity

A quarterly monitoring tool was developed by the AIC to gather information about cybercrime intelligence activity on a regular basis. The questionnaire was based on the same categories of cybercrime used by the ACORN and collected information regarding:

- the number and type of intelligence reports produced for cybercrime offences; and
- the amount of time spent gathering, reviewing and producing both tactical and strategic intelligence reports.

Data were collected on a quarterly basis between July 2014 and September 2015, which allowed data for the pre-implementation period to be compared with up to 12 months post-implementation. These data were used to assess whether there had been improvements in the number of intelligence products produced, the information available to intelligence analysts and the time taken to produce and disseminate intelligence to investigators.

Quarterly monitoring tool to measure enforcement activity

A quarterly monitoring tool was also developed by the AIC to gather information about cybercrime enforcement activity on a regular basis. The questionnaire was based on the same categories of cybercrime used by the ACORN and collected information regarding:

- the number of investigations commenced and finalised in the relevant quarter, along with the outcomes of those finalised investigations;
- the number of offenders arrested and charged, including the number of charges;
- the estimated police resources involved in the investigation of cybercrime offences;
- the nature of any other activity related to the prevention and investigation of cybercrime.

As with the intelligence monitoring tool, data were collected on a quarterly basis between July 2014 and September 2015, which allowed data for the pre-implementation period to be compared with up to 12 months post-implementation. These data were used to assess whether the improved intelligence available from the ACORN had led to an increase in enforcement activity and improved outcomes for investigations.

Survey of ACORN users

Individuals who had submitted a report to the ACORN and consented to participate in the evaluation were invited to complete an online survey. At the end of every month, CrimTrac provided the AIC with a list of ACORN users who indicated that they were willing to be contacted by the AIC to participate in the survey. The AIC emailed prospective participants three months after they had submitted their report to invite them to participate in the survey. The survey included questions addressing the following areas:

- how easy the website was to find and navigate (usability and accessibility);
- overall satisfaction with the reporting process and outcome of submitting a report;
- whether they had accessed the prevention advice (targeted or general) as a result of using ACORN;
- whether they had adopted any prevention strategies in the period since they submitted a report; and
- whether they had been a victim of cybercrime in the period immediately before and after they submitted a report.

Table 4 Response rate for survey of ACORN users

Category	Invited (n)	Completed (n)	Response rate (%)
Online scams and fraud	3,669	1,043	28
Issues buying and selling online	1,164	297	26
Attacks on computer system and virus	613	173	28
Cyberbullying, sexting, online harassment and stalking	583	141	24
Total	6,029	1,654	27

Invited participants does not include bounce backs and undelivered emails and users who did not consent to participate in the evaluation

Source: ACORN Victim Survey [AIC datafile].

The survey was administered for four consecutive months and over 6,000 invitations to participate in the survey were sent to individuals who had reported to the ACORN between April and July 2015. The number of invitations sent, and completed responses received, for each type of cybercrime is summarised in Table 4. The overall response rate for the survey of ACORN users was 27 percent, while response rates for individual cybercrime categories ranged from 24 percent for cyberbullying, sexting, online harassment and stalking to 28 percent for online scams and fraud and attacks on computer systems.

Limitations

There are a number of limitations that need to be considered in reviewing the findings from the AIC's evaluation. First, it was necessary to focus data collection on the specialist units within each participating law enforcement agency that has primary responsibility for leading each agency's response to cybercrime. This was due to both logistical and resource constraints. Except where stated, results from the survey of law enforcement and quarterly monitoring tools relate to these specialist units, rather than police partner agencies as a whole. This means that estimates of the number of reports received and time spent by each agency in relation to cybercrime will underestimate the full burden of cybercrime on law enforcement.

Second, the survey of law enforcement agencies was designed to overcome the lack of established systems for recording data on cybercrime incidents reported to police. However, it relied on police either having access to the data (based on systems maintained locally) or recalling the information. While limited to a three-month period to limit issues relating to recall, this may impact on the reliability of the information provided. Similarly, information provided as part of the quarterly monitoring tools also relied upon police having access to that data or recalling the information. Similar issues may therefore exist with regards to the reliability of the information provided.

Third, while the survey and quarterly monitoring tools used the agreed definitions for cybercrime categories from the ACORN, different definitions may have been applied within each jurisdiction prior to November 2014. Reporting, intelligence and enforcement activity reported to the AIC may also be influenced by existing resources and local practices. For this reason, direct comparisons between agencies that have provided the data for the pre-implementation stage of the evaluation have been avoided.

Fourth, the first round of quarterly monitoring tools administered during the post-implementation period were completed for the period October to December 2014, which overlapped the actual implementation date for the ACORN. This may have impacted the results from this first quarter in terms of the efficiency and effectiveness of investigation and enforcement activity. However, both trend data and averages for the entire post-implementation period are presented to address this problem. In any case, while the ACORN was implemented in November 2014, it took some time for the processes to support the operation of the system to be embedded in each police partner agency and, like any new program, there was invariably a period of refinement and adjustment as the ACORN was established. Related to this point, the fact that the ACORN was initially launched with a soft release (ie there was no initial media launch to coincide with the website going live) meant that there was an additional lag period in terms of the impact of the system on law enforcement. Where applicable, these limitations are acknowledged when discussing the results.

Fifth, the survey of ACORN users was sent to all users who consented to participate in the AIC's evaluation. The overall response rate (27%) was adequate, and the number of completed surveys (n=1,654) was sufficient to conclude that responses were accurate to within two percentage points. However, respondents to the survey self-selected to actually complete the survey, and there was the potential for selection bias. Specifically, respondents may have been more likely to complete the survey if they had very positive or very negative experiences.

Finally, while the public survey was designed to be representative of the Australian population in terms of the age and sex of respondents, and while the sample is large enough to draw valid conclusions from the national results, there was some undersampling of respondents from states and territories. The overall sample size also prohibits conclusions being drawn from state and territory results (for all states and territories). There are important differences between jurisdictions in terms of reporting processes and the response to cybercrime and these may have influenced the responses from respondents in different states and territories. These must also be acknowledged.

Cybercrime reporting

The first objective of the ACORN was to provide a centralised, national online facility that could receive reports from members of the public. This is a high level objective that supports the three remaining objectives. However, this objective is also associated with two long-term outcomes. The first relates to improved satisfaction among those who report cybercrime because of the accessibility and ease of use of the system. There is evidence that the ease of reporting can improve satisfaction with both the process of reporting and the outcome of a case (Brown & Evans 2014; Ekblom & Heal 1982; FitzGerald et al. 2002; Skogan 2005). The second outcome relates to confidence among the general public that cybercrime is being taken seriously by the government, by virtue of the fact that it has invested in establishing ACORN. The rate of reporting among cybercrime victims, the modes of reporting used, satisfaction with the reporting process and outcomes and overall perceptions of the government's response to cybercrime are examined in this section.

The ACORN accepts reports for a number of specific categories of cybercrime. It enables members of the public to make online reports for online fraud and scams (including email spam, phishing and identity theft), Issues buying or selling online, attacks on computer system and virus and cyber-bullying (Table 5). If a member of the public attempts to report a category of cybercrime that is not accepted by ACORN they are directed to the relevant agency, or to preventative advice. For example, if a member of the public attempts to report online child exploitation material they are directed to report to the Office of Children's eSafety Commissioner, or if the child is in immediate danger, to call 000 for an emergency response. Similarly if a member of the public attempts to report offensive, illegal and prohibited content that advocates a terrorist act they are directed to report to the Report Online Extremism tool.

Table 5 Categories of cybercrime reportable to the ACORN

Category	Description
Online scam or fraud	A scam or fraud refers to an attempt by a 'scammer' to lure and trick a victim into giving money or personal information (excludes issues buying and selling online).
Issues buying and selling online	Scammers frequently target online shoppers, for example, by selling fake or faulty products on auction websites.
Attacks on computer system or virus	An *attack* refers to hacking, or being infected by a virus or malicious software. A *computer system* may be any electronic device (home computer, tablet, mobile phone, or router), network or website.
Cyber bullying, sexting, online harassment or stalking	Cyber bullying, sexting, online harassment or stalking refers to someone engaging in offensive, menacing or harassing behaviour online. The behaviour may include abusive texts or emails, hurtful messages, images or videos, imitating others online, or a blackmail attempt.

Source: CrimTrac (2014)

Reports submitted to the ACORN

Data were provided by the ACIC on the number of reports made to the ACORN. Between November 2014 and June 2016 there were more than 65,000 reports submitted to the ACORN, including those reports in which the person was directed to another reporting method (Table 6). Online scams and fraud were the most common type of cybercrime reported (48% of all reports), followed by issues buying and selling online (21%). One in ten reports did not fall into one of the main categories of cybercrime. Reports relating to offensive, illegal and prohibited content and child offences, which are not reportable to the ACORN, accounted for six percent of all reports.

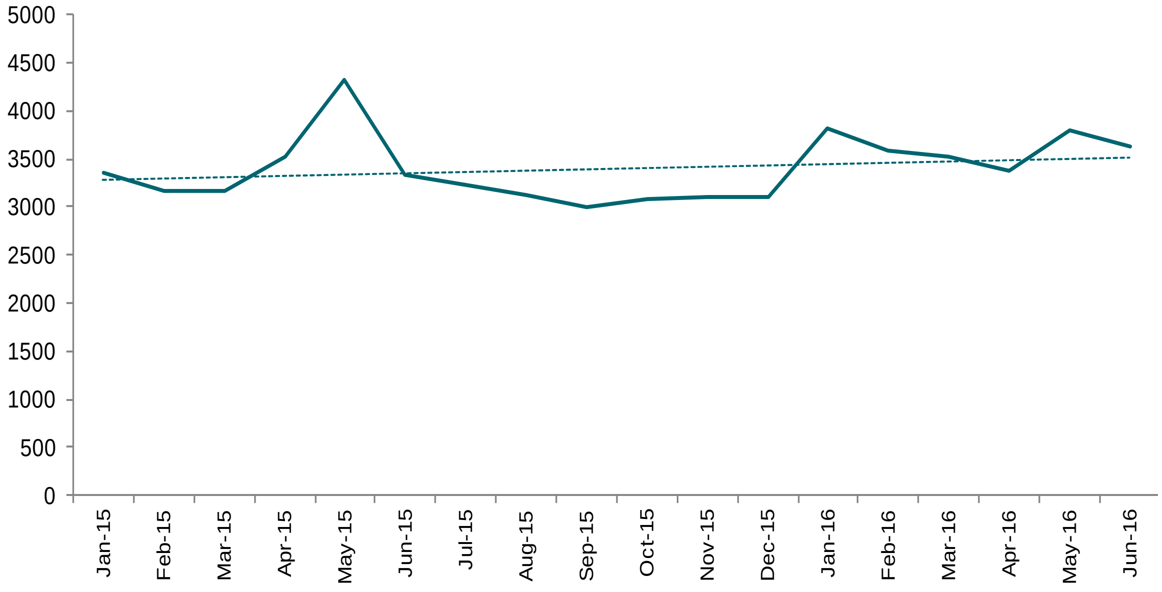
Table 6 Reports submitted to the ACORN, by cybercrime type, November 2014 - June 2016

	n	%
Online scams and fraud	31,638	48
Issues buying and selling online	13,860	21
Cyberbullying, sexting, online harassment and stalking	4,929	8
Attacks on computer system and virus	4,383	7
Illegal material	2,485	4
Children offences	1,384	2
Other	6,607	10
Total Reports	65,286	100

Source: Australian Criminal Intelligence Commission 2016 [data file]

Trend data are reported for the period January 2015 to June 2016, to account for the initial soft release period following the launch of the ACORN in November 2014. The total number of reports by month, including those reports in which the person was directed to another reporting method, is presented in Figure 1. This shows that there has been considerable variability in the number of reports made during the observation period, with a small upwards trend in the first half of 2016. There was a significant peak in reporting to the ACORN in May 2015, likely due to the significant investment in a communication and marketing campaign that supported the implementation of the ACORN in early 2015.

Figure 1 Number of reports made to the ACORN, by month

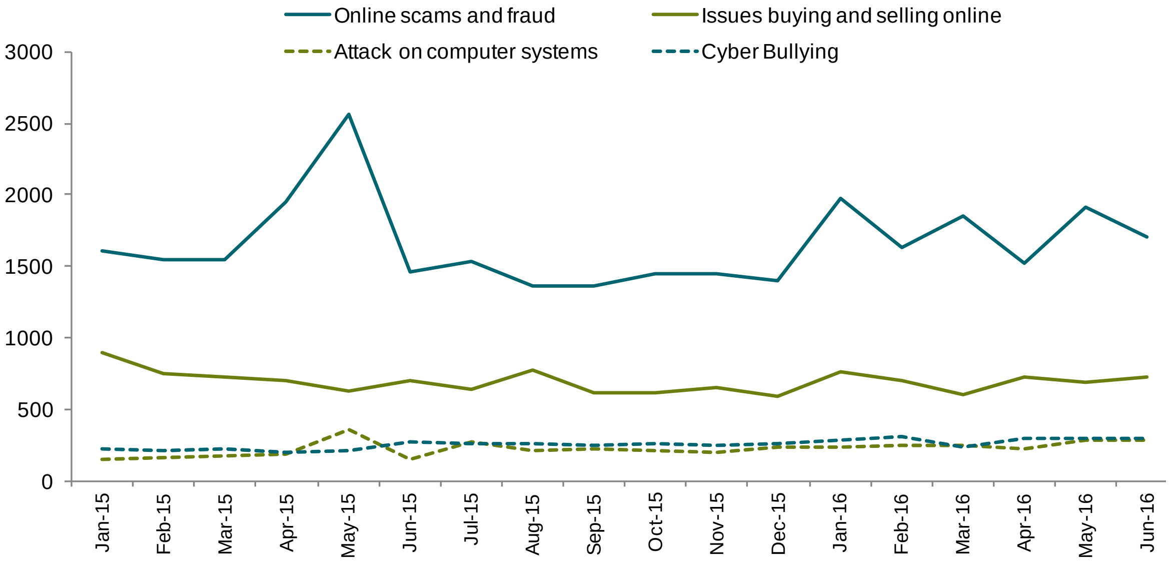


Source: Australian Criminal Intelligence Commission 2016 [data file]

To better understand overall patterns in reporting, while accounting for seasonal variation, the number of reports made in the first half of 2016 was compared with the same six-month period in the previous year. The percentage difference was then calculated. In the first half of 2016, there was a four percent increase in the number of reports submitted, indicating a recent upward trend in reporting.

Further analysis of these trend data revealed different patterns among the different types of cybercrime (Figure 2). The significant spike in the number of reports in May 2015 was almost entirely due to a sharp increase in the number of online scam and fraud reports. After plateauing in mid-2015, the number of reports has fluctuated considerably. The number of reports for issues buying and selling online remained relatively stable throughout the observation period, with a small decrease (5%) in early 2016. The two least common major categories of cybercrime, attacks on computer systems and cyber bullying, sexting, online harassment and stalking, which accounted for seven percent and eight percent of all reports, respectively, have both increased significantly in 2016. There was a 28 percent increase in the number of reports relating to attacks on computer systems and in the number of reports for cyber bullying, sexting, online harassment and stalking between January and June 2016, when compared with 2015.

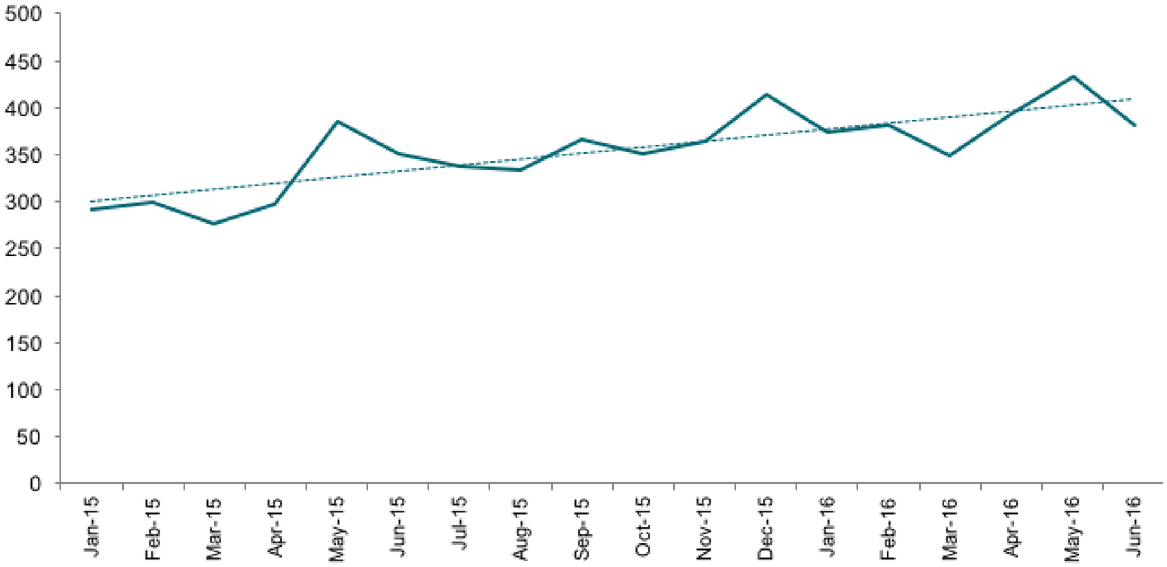
Figure 2 Number of reports submitted to the ACORN, by cybercrime type (major categories only) and month



Source: Australian Criminal Intelligence Commission 2016 [data file]

Also notable has been the trend in reports that fall into the ‘other’ category (Figure 3). This includes reports where the user indicates that the crime does not fall into one of the other selectable categories (reportable or not reportable). Accounting for around ten percent of all reports since the ACORN’s inception, there has been a gradual increase in the number of reports for ‘other’ types of cybercrime, with a 22 percent increase between January and June 2016 when compared with the same period in 2015. This is notable because of the limitations of free text fields in a system that relies on automated referrals, and also because of the potential for users to report non-reportable or potentially serious cybercrime offences in this category.

Figure 3 Number of reports submitted to the ACORN, other category, by month



Source: Australian Criminal Intelligence Commission 2016 [data file]

Cybercrime victimisation and reporting rates

A key focus of the public survey was on collecting information on the prevalence of cybercrime victimisation among the general population, along with estimates of reporting rates prior to and following the introduction of the ACORN. Results from the two surveys have been compared to assess whether there has been an overall increase in the proportion of victims who report cybercrime, particularly to police, as a result of there being an online reporting system accessible to members of the public. This may have been as a result of a re-direction of reports from other more traditional modes of reporting to police, or it may reflect the latent demand that existed prior to the ACORN.

The results are presented in Table 7. This shows that there was little change in rates of victimisation between the pre- and post-implementation periods. The proportion of survey respondents who reported being a victim of cybercrime in the previous 12 months remained steady for online scams and fraud (5% c/f 6%), issues and buying and selling online (6% c/f 7%), and cyber bullying, sexting, online harassment and stalking (7% c/f 8%). There was a small decrease in the proportion of respondents who reported being a victim of an attack on a computer system (28% c/f 35%). The survey was based on the counting rules for the ACORN; however, for online scams or fraud the victimisation rate was based on the proportion of respondents who had received multiple invitations from the same scammer *and* taken further action. This enabled direct comparison with the pre-implementation survey. The actual victimisation rate for online scams and frauds in the post-implementation period using the ACORN business rules was 40 percent—the majority of whom have not taken further action.

Some care must be taken in interpreting the results for reporting rates among victims of cybercrime, particularly in terms of reporting to police, because of the relatively low number of respondents. There was a small increase in the proportion of victims who reported online scams or fraud to anyone (73% c/f 64%), and decrease in the proportion of cyber bullying, sexting, online harassment and/or stalking victims (28% c/f 34%). There was no measurable change in reporting to police for these categories of cybercrime; however, there was an increase in the proportion of victims of issues buying and selling online who reported the most recent incident to police (17% c/f 6%). Notwithstanding the very small numbers, this did not appear to be the result of the ACORN, with only four percent of victims (n=5) of issues buying and selling online reporting to the ACORN. Rates of reporting to the ACORN among victims ranged from two percent for victims of attacks on computer systems to one in ten (11%) of victims of online scams and frauds.

This may in part be explained by the relatively low level of awareness of the ACORN among survey respondents. In the post-implementation survey, conducted nearly 15 months after the ACORN had been implemented, only 14 percent of respondents reported that they were aware of the ACORN. Four percent of respondents to the pre-implementation survey reported being aware of the ACORN prior to it being launched.

Table 7 Cybercrime victimisation and reporting rates, pre- and post-implementation of the ACORN %(n)

	Victim in the previous 12 months		Victims who reported the most recent incident[a]		Victims who reported the most recent incident to police[ab]		Victims who reported the most recent incident to ACORN[a]
	Pre	Post	Pre	Post	Pre	Post	
Online scams or fraud[c]	6 (103)	5 (99)	64 (66)	73 (73)	27 (22)	23 (23)	11 (11)
Issues buying and selling online	7 (120)	6 (119)	79 (95)	80 (95)	6 (8)	17 (21)	4 (5)
Attacks on computer system	35 (624)	28 (524)	28 (176)	28 (147)	4 (24)	4 (22)	2 (9)
Cyber bullying, sexting, online harassment and stalking	8 (136)	7 (133)	34 (46)	28 (38)	12 (16)	14 (19)	6 (8)

a: Proportions are of total victims, not total survey respondents.

b: Includes reporting to police by phone, in person, using a police website or via Crimestoppers. Includes reports to ACORN in post-implementation data.

c: Online scam and fraud victims were defined as those who had been contacted more than once by a scammer AND had taken further action in response to the invitation (including responding to the email or giving out personal information or money).

Data were weighted according to ABS population data to reflect distribution of age and sex across the entire population. Weighted figures may not equal totals due to rounding. Respondents could report more than one form of cybercrime victimisation.

Source: ACORN Public Survey [AIC data file]

While there is general acceptance that cybercrime offences are under reported by victims, the extent of this under reporting compared with more traditional forms of crime is rarely assessed. This has implications in terms of understanding the potential latent demand for reporting cybercrime to police. The post-implementation survey therefore included similar questions about victimisation and reporting relating to theft offences. Theft offences were selected as the comparison because it is the most common type of property offence among non-cybercrime offences, with almost 700,000 recorded victims of unlawful entry involving the taking of property, motor vehicle theft and other theft combined in 2015 (ABS 2016). Online scams and fraud was compared with theft offences because of the similar nature of both crime types (with the exception of online scams and fraud being computer enabled) and because online scams and fraud accounted for the largest number of reports to the ACORN.

Two comparisons are made with theft offences—online scams and fraud using the business rules for the ACORN, in which the victim received multiple invitations from same scammer or had taken further action, and online scams or fraud in which the victim had received multiple invitations from same scammer and taken further action. Based on the former definition, online scam or fraud was far more prevalent among respondents to the post-implementation survey than theft in the previous 12 months (40% c/f 8%) (Table 8). Victims of theft were around twice as likely to report the most recent incident to someone else as victims of online scams or fraud (67% c/f 35%), and far more likely to report to the police (30% c/f 7%). However, rates of reporting for online scams and fraud in which further action was also taken, including reporting to someone else (73% c/f 67%) and reporting to police (23% c/f 30%), were more comparable to theft offences. Notwithstanding the small sample size, these results suggest there is greater scope to increase the number of reports to the ACORN relating to online scams or fraud in which the victim received multiple invitations from the same scammer than with online scams in which the victim has taken further action. The implications for police in responding to reports in which there was no financial loss to the victim is discussed in later sections of this report.

Table 8 Victimisation and reporting rates, post-implementation of the ACORN, cybercrime and theft offences %(n)

	Victim	Victims who reported the most recent incident[a]	Victims who reported the most recent incident to police[ab]
Online scam or fraud			
Multiple invitations from same scammer OR taken further action in the previous 12 months	40 (738)	35 (260)	7 (48)
Multiple invitations from same scammer AND taken further action in the previous 12 months	5 (99)	73 (73)	23 (23)
Theft offences			
Victim in the previous 12 months	8 (147)	67 (98)	30 (44)

a: Proportions are of total victims, not total survey respondents.

b: Includes reporting to police by phone, in person, using a police website, via Crimestoppers or ACORN.

Data were weighted according to ABS population data to reflect distribution of age and sex across the entire population. Weighted figures may not equal totals due to rounding. Respondents could report more than one form of victimisation.

Source: ACORN Public Survey [AIC data file]

The survey also explored reasons for not reporting among those victims who did not report the most recent incident (Table 9). Victims could identify more than one reason for not reporting. There was some variation between the different categories of cybercrime; however, the most common reasons were that victims did not think anything would be done (34%-39%), believed that it was not worth the effort (34%-46%) and were unsure of which agency to contact (28%-53%).

Table 9 Reasons for not reporting the most recent incident, pre- and post-implementation of the ACORN, by cybercrime type %(n)

	Online scams or fraud[a]		Issues buying or selling online		Attacks on computer system		Cyber bullying, sexting, online harassment and/or stalking	
	Pre (n=37)	Post (n=26)	Pre (n=25)	Post (n=24)	Pre (n=448)	Post (n=377)	Pre (n=90)	Post (n=95)
Not worth the effort	31 (11)	34 (9)	55 (14)	46 (11)	31 (139)	36 (135)	55 (49)	43 (41)
Unsure of which agency to contact	40 (15)	40 (10)	38 (10)	28 (7)	52 (235)	53 (202)	36 (33)	34 (33)
Did not think anything would be done	40 (15)	35 (9)	46 (12)	34 (8)	34 (153)	34 (130)	30 (27)	39 (37)
Did not think what happened was illegal	11 (4)	8 (2)	18 (5)	7 (2)	6 (28)	9 (35)	13 (12)	24 (23)
Fear of repeat victimisation	8 (3)	7 (2)	3 (1)	5 (1)	2 (7)	4 (15)	12 (11)	15 (14)
Other	11 (4)	19 (5)	3 (1)	8 (2)	21 (95)	18 (69)	10 (9)	19 (18)

a: Online scam and fraud victims were defined as those who had been contacted more than once by a scammer AND had taken further action in response to the invitation (including responding to the email or giving out personal information or money)

Data were weighted according to ABS population data to reflect distribution of age and sex across the entire population. Weighted figures may not equal totals due to rounding. Respondents could identify more than one option

Source: ACORN Public Survey [AIC data file]

There was some variation in terms of the reasons given for not reporting between the pre- and post-implementation surveys. Of particular relevance to the ACORN was the proportion of victims who did not report because they were unsure of which agency to contact. The ACORN aims to make it easier for victims to report cybercrime by providing an easy and accessible method for reporting that is dedicated to cybercrime offences. There was little difference between the pre- and post-implementation survey responses in terms of the proportion of victims who did not report due to being unsure of which agency to contact. There was a small decrease among victims of issues buying and selling online (28% c/f 38%), although this was based on a very small sample of respondents. Overall, these results suggest there has been little change in terms of public awareness of where to report cybercrime.

A comparison between victims of online scams or fraud and theft offences who did not report the most recent incident in the period post-implementation of the ACORN revealed little difference in terms of the reasons for not reporting (Table 10). However, when compared with the larger group of victims of online scams or fraud who received multiple invitations from the same scammer, victims of theft offences were significantly less likely to report being unsure of which agency to contact (34% c/f 58%).

Table 10 Reasons for not reporting the most recent incident, pre- and post-implementation of the ACORN, online scams and fraud and theft offences %(n)

	Online scams or fraud (n=26)	Theft (n=49)
Not worth the effort	34 (9)	31 (15)
Unsure of which agency to contact	40 (10)	34 (17)
Did not think anything would be done	35 (9)	44 (22)
Did not think what happened was illegal	8 (2)	5 (3)
Fear of repeat victimisation	7 (2)	6 (3)
Other	19 (5)	12 (6)

Data were weighted according to ABS population data to reflect distribution of age and sex across the entire population. Weighted figures may not equal totals due to rounding. Respondents could identify more than one option.

Source: ACORN Public Survey [AIC data file]

Reporting to multiple individuals or organisations

Victims who reported to the ACORN and who responded to a follow-up survey were asked where else they reported the most recent incident (Table 11). More than half of all victims (58%) reported having also reported the most recent incident to another agency or individual. Importantly, 22 percent of all victims who reported to the ACORN—and as many as 39 percent of victims of issues buying and selling online—indicated they had also reported the incident to a police station (in person), while 15 percent reported the incident to police over the phone. Overall, 37 percent of all victims, including more than half (54%) of all victims of cyber bullying, sexting, online harassment and stalking, reported the most recent incident of cybercrime to police, in addition to reporting it to the ACORN. Given the significant proportion of victims (14%) who indicated that the *main* reason for reporting to the ACORN was that they had been directed to by police, these results suggest that a large proportion of victims who report to the ACORN may have attempted to report to police through a more traditional mode of reporting in the first instance. Alternatively, they may have reported to police through some other means after they submitted the ACORN report. This has significant implications in terms of victim satisfaction with reporting. It also indicates that a large proportion of reports received by the ACORN constitute reports that would have otherwise been received by police through some other mechanism, rather than representing a latent demand for reporting cybercrime.

Table 11 Additional modes of reporting pursued by victims who reported to the ACORN

	Online scams or fraud[a]		Issues buying or selling online		Attacks on computer system		Cyber bullying, sexting, online harassment and/or stalking		All reports to the ACORN	
	n	%	n	%	n	%	n	%	n	%
Police (excluding the ACORN)										
Police station (in person)	228	22	116	39	31	18	43	30	372	22
Police by phone	139	13	38	13	30	17	35	25	242	15
Police website	47	5	17	6	7	4	12	8	83	5
Crime stoppers	20	2	5	2	3	2	12	8	40	2
Total reported to police	362	35	106	36	61	35	76	54	605	37
Non-police										
Bank or financial institution	244	23	78	26	34	20	7	5	363	22
A friend or family member	144	14	42	14	22	13	46	33	254	15
The business that was involved in the fraud or scam	115	11	60	20	13	7	15	11	203	12
SCAMwatch	96	9	17	6	12	7	3	2	128	8
Internet service provider	46	4	9	3	18	10	23	16	96	6
Australian Competition and Consumer Commission	27	3	24	8	1	<1	2	1	54	3
Lawyer	21	2	4	1	4	2	19	13	48	3
Australian Communications and Media Authority	6	<1	0	0	0	0	2	1	8	<1
Don’t know / cannot recall	6	<1	1	<1	1	<1	0	0	8	<1
Other	94	9	37	12	26	15	19	14	176	11
Total reported to agency or individual other than ACORN[b]	574	55	185	62	100	58	100	71	959	58

a: Online scam and fraud victims were defined as those who had been contacted more than once by a scammer AND had taken further action in response to the invitation (including responding to the email or giving out personal information or money)

b: Respondents could identify more than one option

Percentages may not equal 100 due to rounding.

Source: ACORN Victim Survey [AIC data file]

Public expectations and satisfaction with reporting

The ACORN aims to improve satisfaction among those who report cybercrime because of the accessibility and ease of use of the system. This offers a number of important benefits, including increasing the likelihood that victims will report future incidents using the ACORN, increasing the likelihood that ACORN will be recommended to friends and family and the potential to increase overall satisfaction with the outcome of a report. In addition, given the ACORN represents a shift away from traditional modes of reporting to police, and there is interest in online reporting to police for a range of offence types, it is important to assess whether ACORN users are satisfied with the process and outcome of submitting a report. A common theme during the interviews with law enforcement personnel during the pre-implementation stage of the evaluation was the perceived risk of dissatisfaction among cybercrime victims who report to the ACORN and do not receive an individual response to their report.

Results from the follow-up survey of victims who reported to the ACORN show that, overall, victims were satisfied with the accessibility of the ACORN and the process of submitting a report

(Table 12). Three quarters of victims (77%) reported that the ACORN was easy to find and use, 82 percent of victims were able to provide all of the information requested by the ACORN, 74 percent of victims indicated that the questions asked by the ACORN were relevant and two thirds (63%) reported that the ACORN collected enough information about their case. However, views were mixed in terms of how the ACORN compared with alternative methods of reporting cybercrime. Fifty-one percent of victims agreed that it was easier to report to the ACORN, while 49 percent of victims indicated that reporting the ACORN was more convenient and also faster than other methods.

Table 12 Victims who agreed or strongly agreed with the following statements

	Online scams or fraud		Issues buying and selling online		Attacks on computer system		Cyber bullying, sexting, online harassment and/or stalking		All reports to the ACORN	
	n	%	n	%	n	%	n	%	n	%
The ACORN website was easy to find	753	79	191	71	119	75	102	75	1,165	77
The ACORN easy to use	748	78	198	74	125	79	95	74	1,166	77
I was able to provide all of the information requested by the ACORN	778	82	227	84	134	85	96	74	1,235	82
The ACORN collected enough information about my case	593	63	179	67	103	65	75	58	950	63
The questions were relevant	696	73	197	74	119	75	99	77	1,111	74
There was repetition in the questions asked	156	17	54	21	27	18	33	25	270	18
Submitting a report to the ACORN took too long	168	18	58	22	33	21	26	20	285	19
It was difficult to get help to complete	96	10	23	9	13	8	23	18	155	10
Reporting to the ACORN was more convenient[a]	280	49	81	44	45	45	55	57	461	49
It was easier to report to the ACORN[a]	289	51	88	48	45	46	57	58	479	51
It was faster to report to the ACORN[a]	283	50	79	43	45	46	53	54	460	49
I was satisfied with the process of reporting to the ACORN	598	63	133	50	96	61	72	56	899	60

a: Compared with reporting to the other agencies, institutions or individuals

Table indicates the number and percentage of victims who 'Agreed' or 'Strongly Agreed' with ACORN satisfaction statements. Excludes cases with missing data.

Source: ACORN Victim Survey [AIC data file]

There were some differences between the different categories of cybercrime in terms of the level of satisfaction of victims with the reporting process. Most notably, the proportion of victims of cyber bullying, sexting, online harassment and stalking who were able to provide all of the information required (74%) and who believed the ACORN collected enough information about their case (58%) was lower than for other victims. Conversely, they were more likely report the ACORN as being more convenient and easier to use than other methods, but also nearly twice as likely to report finding it difficult to get help to complete the report. Overall, 60 percent of victims were satisfied with the process of reporting to the ACORN. Levels of satisfaction ranged from 50 percent of victims of issues buying and selling online to 63 percent of victims of online scams or fraud.

Understanding victims' reasons for reporting to the ACORN is important in understanding their expectations regarding the outcome of their report and how this might influence their level of satisfaction. Victims who reported to the ACORN were also asked the main reason they submitted a report for the most recent incident (Table 13). They could only select one reason. The most common reason given was to notify police so action could be taken to investigate crime (40% of all victims), followed by protecting others from future crimes (22%) and being directed to by police (14%). With regards to the latter reason, police partner agencies advised that officers have been encouraged to tell victims who are reporting to a police station or on the phone to instead report to the ACORN.

Victims of cyber bullying, sexting, online harassment and/or stalking were more likely to report having submitted a report to the ACORN to notify police so investigative action could commence (56%), and much less likely to submit a report to protect others (9%). One in eight victims indicated that it was to protect themselves from future offending. Victims of issues buying and selling online were more likely than other victims to want to protect themselves from future crimes, and also significantly more likely to be motivated by a desire to recover lost money. These responses reflect the different characteristics of the major categories of cybercrime, including the type of harm experienced and the victim's relationship to the perpetrator, which have implications for how and why victims use the ACORN.

Table 13 Reasons for reporting the most recent incident to the ACORN, by cybercrime type

	Online scams or fraud		Issues buying and selling online		Attacks on computer system		Cyber bullying, sexting, online harassment and/or stalking		All reports to the ACORN	
	n	%	n	%	n	%	n	%	n	%
To notify police so action could be taken to investigate the crime	372	39	95	35	70	44	73	56	610	40
To protect others from future crimes	263	25	50	19	30	19	11	9	327	22
I was directed to by the police	132	14	39	15	22	14	22	17	215	14
To recover lost money	70	7	75	28	3	2	2	2	150	10
To protect myself from future crimes	80	8	3	1	21	13	15	12	119	8
I was directed to by my financial institution	35	4	4	1	5	3	1	1	45	3
I was directed to by my legal representative	1	<1	-	-	2	2	3	2	6	<1
For insurance purposes	1	<1	1	<1	0	0	0	0	2	<1
Other	35	4	2	<1	6	4	3	2	42	3

Excludes cases with missing data. Percentages may not equal 100 due to rounding. Respondents could identify one option.

Source: ACORN Victim Survey [AIC data file]

Levels of satisfaction with the outcome of reporting to the ACORN among cybercrime victims were substantially lower than levels of satisfaction with the process of reporting (Table 14). Less than one-third of all victims (29%) were satisfied with the outcome of their report. Victims of cyber bullying, sexting, online harassment and stalking were the least satisfied (21%), followed by victims of issues buying and selling online (24%).

However, around two-thirds of victims (66%) indicated that they would use the ACORN again. This ranged from 53 percent of victims of issues buying and selling online, to 74 percent of victims of attacks on computer systems. Similarly, around two-thirds of victims (63%) who reported to the ACORN indicated that they would recommend it to family and friends if they needed to report cybercrime. Victims of online scams or fraud (65%) and attacks on a computer system (70%) were more likely to express a willingness to recommend the ACORN than victims of issues buying and selling online (52%) and cyber bullying, sexting, online harassment and stalking (57%).

Table 14 Satisfaction with the outcome of reporting to the ACORN, by cybercrime type

	Online scams or fraud		Issues buying and selling online		Attacks on computer system		Cyber bullying, sexting, online harassment and/or stalking		All reports to the ACORN	
	n	%	n	%	n	%	n	%	n	%
Satisfied with the outcome of the reporta	287	30	65	24	50	32	27	21	429	29
Would use the ACORN to report cybercrime in the futureb	660	69	140	53	118	74	79	61	997	66
Would recommend the ACORN website to my friends or family if they needed to report cybercrime in the futureb	622	65	138	52	112	70	73	57	945	63

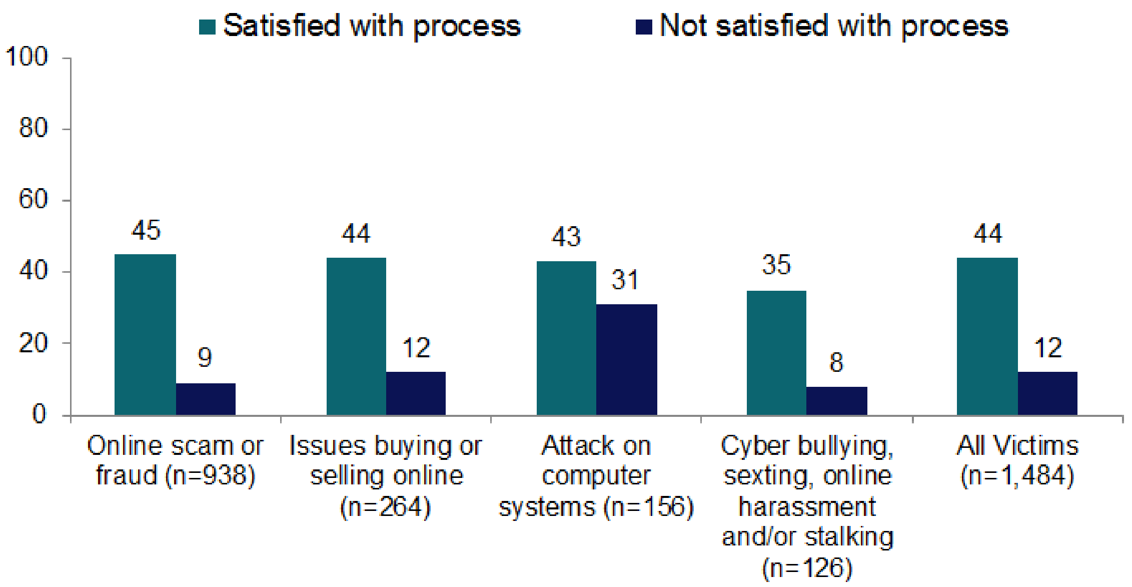
a: Number and percentage of victims who were satisfied or very satisfied with the outcome

b: Number and percentage of victims who agreed or strongly agreed

Excludes cases with missing data.

Source: The ACORN Victim Survey [AIC data file]

Figure 4 Satisfaction with report outcome, by satisfaction with process of reporting (%)



Excludes cases with missing data.

Source: The ACORN Victim Survey [AIC data file]

Further analysis of ACORN users' satisfaction with the process and outcome of reporting revealed that, as expected, users who were satisfied with the process of reporting were significantly more likely to be satisfied with the outcome of the report (Figure 4). Overall, 44 percent of users who were satisfied with the process of reporting were satisfied with the outcome, compared with just 12 percent of users who were not satisfied with the process of reporting. These results were consistent across all cybercrime types, with the exception of attacks on computer systems (43% c/f 31%). Aspects of reporting with which users were less satisfied, such as the amount and relevance of information collected, or the speed and ease of reporting relative to other methods, may therefore have a significant bearing on how satisfied ACORN users are with the outcome of a report.

However, these results do not on their own explain the low levels of satisfaction with the outcome of reporting to the ACORN. Prior to the launch of the new system, police partner agencies raised concerns regarding the likely expectations of users who report to the ACORN and the potential for these expectations to exceed what was possible in terms of a law enforcement response to individual reports. To better understand ACORN users' expectations regarding the outcome of their report, a hierarchy was created whereby users were able to select from options ranging from an expectation that they would be notified that the report had been received through to being notified that the report had been received, investigated, action taken and an offender arrested (Table 15). One in five (19%) users reported that they expected to be notified that a report had been received, while a further one in four (24%) reported that they expected to be notified that a report had been received and investigated. More than half of all users (57%) expected police to take some sort of action in response to their report, including 19 percent of users who expected police to arrest the offender. Victims of issues buying and selling online and cyber bullying, sexting, online harassment and/or stalking had the highest overall expectations in terms of an offender being apprehended (28% and 26%, respectively).

Table 15 Expected and actual outcomes of reports to the ACORN, by cybercrime type

	Online scams or fraud		Issues buying and selling online		Attacks on computer system		Cyber bullying, sexting, online harassment and/or stalking		All reports	
Expectation	n	%	n	%	n	%	n	%	n	%
Expected to be notified the report was received	210	22	30	11	39	25	13	10	292	19
Expected to be notified the report was received and investigated	244	26	42	16	42	26	34	26	362	24
Expected to be notified the report was received, investigated and action taken	341	36	121	45	55	35	49	38	566	38
Expected to be notified the report was received, investigated, action taken and an offender arrested	157	17	76	28	23	14	33	26	289	19
Outcome										
Did not receive any information of the outcome	243	26	79	29	28	18	35	27	385	26
Notified the report was received	568	60	122	46	104	67	66	51	860	57
Notified the report was received and investigated	107	11	49	18	18	12	24	18	198	13
Notified the report was received, investigated and action taken	31	3	17	6	6	4	5	4	59	4
Notified the report was received, investigated, action taken and an offender arrested	2	<1	1	<1	-	-	-	-	3	<1

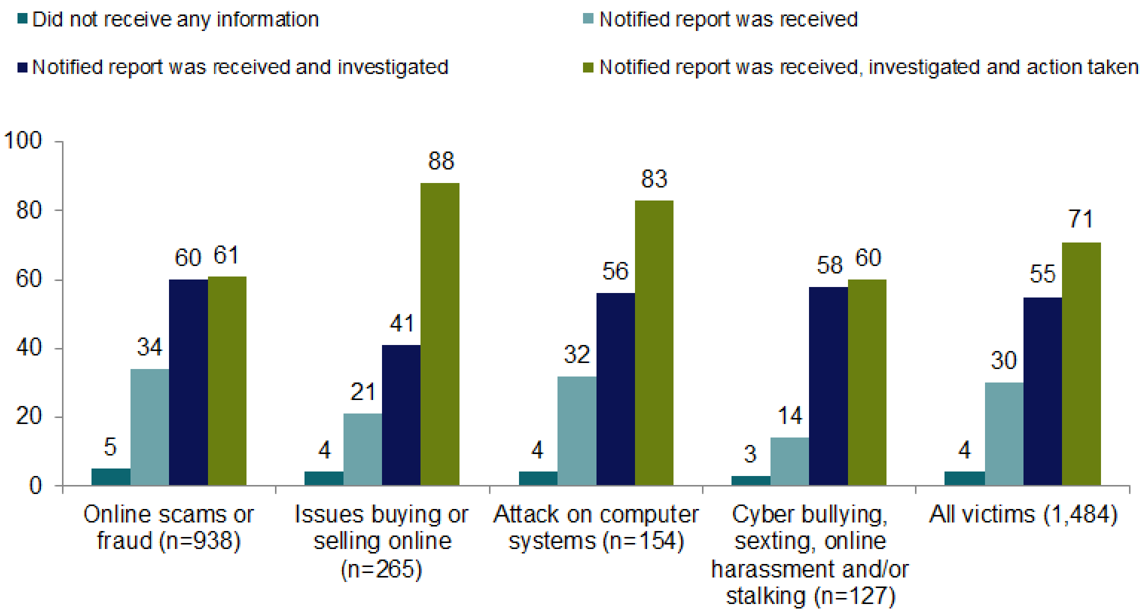
Percentages may not equal 100 due to rounding. Respondents could identify one option only. Excludes cases with missing data.

Source: ACORN Victim Survey [AIC data file]

The outcomes of reports submitted to the ACORN are also presented in Table 15. It should be noted from the outset that these outcomes are based on the information provided to the victim by a police partner agency, and may not reflect all of the action taken by police in response to a report. Further, action may be taken by police in response to groups of reports, which may not necessarily be attributed to individual reports by victims. However, the information provided to victims is relevant because of the potential impact on levels of satisfaction.

When users submit a report to the ACORN, they receive a report confirmation email with a unique ACORN reference number. Reports may then be forwarded, either automatically or following assessment, to the relevant federal, state, local, or international law enforcement or regulatory agencies for consideration and, potentially, investigation. An investigator may then contact the person who submitted the report for more information, should an investigation proceed and the person provided their contact details. More than half (57%) of all ACORN users who submitted a report were notified that the report had been received—most likely the email sent to users to confirm receipt. One quarter (26%) of all users who submitted a report indicated that they did not receive notification of a report being received. This means they either did not see the email confirming receipt, or that they expected further contact from a law enforcement agency confirming that they had received the report. Thirteen percent of users indicated that they had been advised the report was being investigated, while four percent were notified that some further action had been taken as a result. Three people reported being notified that an offender had been arrested.

Figure 5 Satisfaction with report outcome, by outcome of report (%)



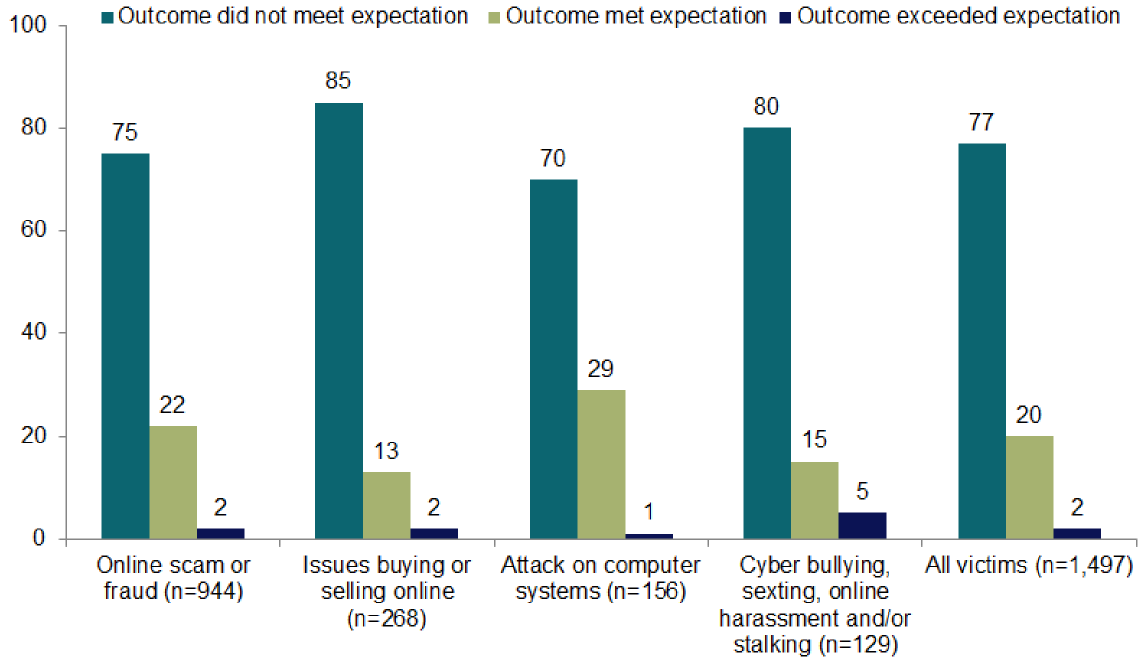
Respondents could identify one option only. Excludes cases with missing data.

Source: The ACORN Victim Survey [AIC data file]

There was considerable variation in terms of the level of satisfaction with the outcome of the report between ACORN users, depending on whether they had received any information about the report outcome, were notified that it had been received, or had been notified that an investigation had commenced and/or some action had been taken (Figure 5). Four percent of all users who indicated that they did not receive any information about the outcome of the report were satisfied with the outcome. Thirty percent of users who were notified that their report had been received were satisfied with the outcome of the report, although this ranged from 14 percent of cyber bullying, sexting, online harassment and/or stalking victims to 34 percent of victims of online scams or fraud. Being notified that the report had been received and investigated, or that action had been taken, was associated with significantly higher levels of satisfaction (55% and 71% of all users, respectively), although this was based on a much smaller number of respondents. In short, the better the outcome from a law enforcement perspective, the more satisfied users were with the outcome.

The nature of cybercrime, and the challenges this presents for police investigating cybercrime offences, means that many reports are unlikely to be investigated. This advice is included on the ACORN website. While the outcome of investigations is still important, it is arguably more important to ensure that the ACORN users have realistic expectations about the outcome. Comparing actual with expected outcomes revealed that the vast majority of users felt that the outcome did not meet their expectations; specifically, their response to the question about the actual outcome was lower on the hierarchy than their question about the expected outcome (Figure 6). Three quarters (77%) of all victims who submitted a report to the ACORN indicated that the outcome did not meet their expectation, one in five (20%) reported that the outcome met their expectation, while two percent of all ACORN users reported that the outcome had exceeded their expectations.

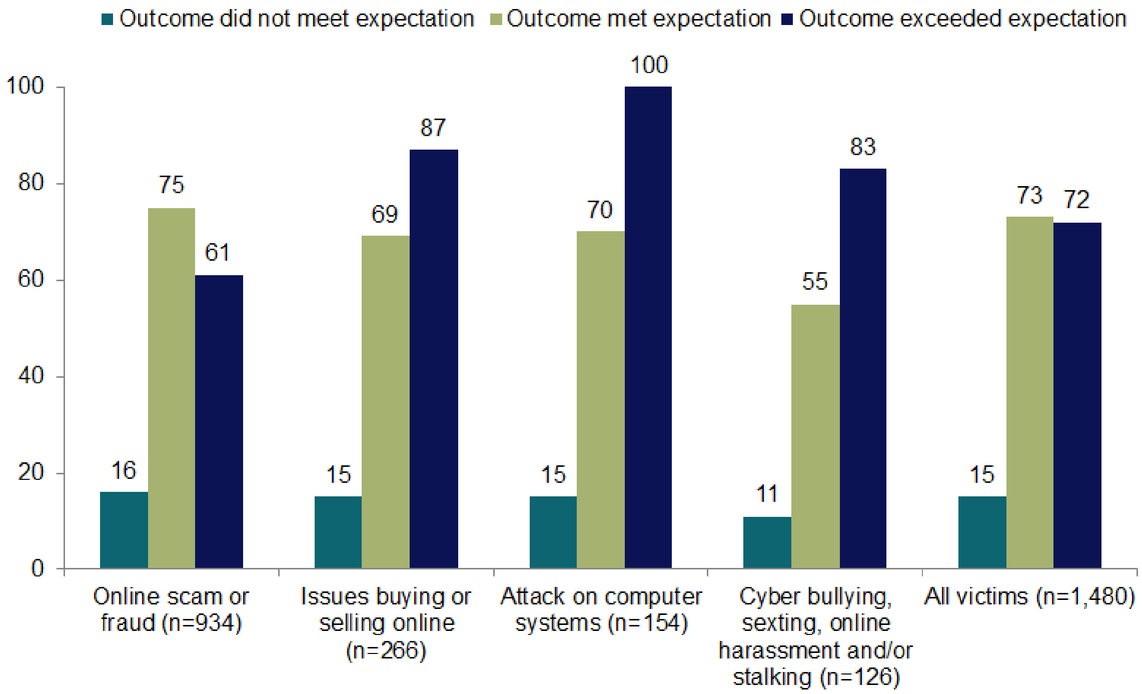
Figure 6 Actual versus expected outcome, by cybercrime type (%)



Source: The ACORN Victim Survey [AIC data file]

Overall, levels of satisfaction among ACORN users whose expectations were not met were significantly lower than users whose expectations were met or exceeded (Figure 7). Fifteen percent of users whose expectations were not met were satisfied with the outcome of their report. Victims of cyber bullying, sexting, online harassment and/or stalking whose expectations were not met had the lowest levels of satisfaction (11%). Close to three quarters of users whose expectations were met (73%) and users whose expectations were exceeded (72%) were satisfied with the outcome. These results clearly show that a large proportion of victims who report to the ACORN have unrealistic expectations regarding the likely outcome of their report and that this has a negative impact on satisfaction levels among users reporting to the ACORN.

Figure 7 Satisfaction with report outcome, by relationship between expected and actual outcome (%)



Source: The ACORN Victim Survey [AIC data file]

To better understand whether this issue is unique to the ACORN, the expected and actual report outcomes for those victims who reported online scams or fraud to the ACORN, and their satisfaction with the process and outcome of their report, were compared with victims of online scams or fraud who reported to police (through a method other than the ACORN), and victims of theft who reported to police (Table 16). Despite the small sample size, and missing data, there were some notable differences. Victims of online scams or fraud who reported to the ACORN were much less likely to receive a notification that their report had been received (40%) than victims of online scams or fraud who reported to police through some other method (77%) and victims of theft who reported the most recent incident to police (59%). Levels of satisfaction with the process of reporting were similar for victims of online scams or fraud who reported to the ACORN (71%) and to police (77%), and lower among victims of theft reporting to police (58%). Most importantly, while levels of satisfaction with the outcome of reporting the most recent incident were marginally lower among victims who reported to the ACORN than victims of theft offences who reported to police (41% c/f 51%), levels of satisfaction with the outcome were significantly higher among victims of online scams or fraud who reported to police through some other method.

Table 16 Expected and actual outcomes of reporting and levels of satisfaction among victims of online scams or fraud and theft offences %(n)

	Reported to ACORN	Reported to police	
Expectation[ab]	Online scams or fraud (n=23)[c]	Online scams or fraud (n=25)[d]	Theft (n=44)
Expected to be notified the report was received	45 (5)	28 (4)	24 (8)
Expected to be notified the report was received and investigated	18 (2)	55 (9)	22 (8)
Expected to be notified the report was received, investigated and action taken	27 (3)	18 (3)	33 (11)
Expected to be notified the report was received, investigated, action taken and an offender arrested	10 (1)	-	20 (7)
Outcome[b]			
Notified the report was received	16 (4)	18 (5)	17 (7)
Notified the report was received and investigated	24 (6)	36 (9)	26 (11)
Notified the report was received, investigated and action taken	-	19 (5)	4 (2)
Notified the report was received, investigated, action taken and an offender arrested	-	3 (1)	12 (5)
Did not receive any information of the outcome	60 (14)	23 (6)	41 (18)
Satisfaction			
The overall process of reporting	71 (17)	77 (19)	58 (25)
How quickly you were able to make the report	71 (17)	84 (21)	78 (34)
How easy it was to get help with the report if it was required	59 (12)e	79 (19)	63 (27)e
The level of assistance you received in making a report	72 (15)e	76 (18)e	55 (24)
The outcome of your report	41 (9)	70 (17)	51 (22)

a: Respondents could identify one option only.
b: These items were missing data.
c: Only includes victims who reported the most recent crime to ACORN. Excludes victims who reported to police by phone, in person, using a police website or via Crimestoppers. Victims may also have reported to other authorities or individuals other than police.

d: Only includes victims who reported to police by phone, in person, using a police website or via Crimestoppers. Excludes online scam or fraud victims who reported to the ACORN. Victims may also have reported to other authorities or individuals other than ACORN.

e: Excludes cases with missing data

Number and percentage of victims who 'Agreed' or 'Strongly Agreed' or were 'Very Satisfied' or 'Satisfied'. Data were weighted according to ABS population data to reflect distribution of age and sex across the entire population. Weighted figures may not equal totals due to rounding. Respondents could report more than one form of victimisation.

Source: ACORN Public Survey [AIC data file]

Consistent with quantitative findings, police reported an unrealistic expectation among victims that all reports would invariably be investigated and funds returned. Further, police reported that many victims have limited knowledge of criminal justice system processes, and do not understand that, in the rare event an offender is actually identified, they will need to make a formal statement in addition to an ACORN report and go to court, in order to recoup lost funds. These concerns were also raised during the pre-implementation stage of the evaluation, whereby police expressed a concern that these unrealistic expectations would lead to low levels of satisfaction among victims after making a report to the ACORN.

In order to manage victim expectations, police recommended that the ACORN website more clearly advise victims that it may not be possible to investigate their report or recoup lost funds, particularly if the offender is located offshore, as is often the case. Two of the police partner agencies involved in the evaluation have developed standard email responses to victims when their report will not be investigated, sometimes referring them to a support group. It is noted that this encourages more realistic expectations among victims who report to the ACORN. Police from one jurisdiction also proposed a 'traffic light' system, to advise victims of the likelihood of recovering funds or of a successful investigation, based on the characteristics of their case (eg 'red' indicating that no action would likely be taken and that there was a low probability of lost funds being recovered, and so on).

In addition to the low probability of a complaint being investigated or funds being recovered, police also noted that they had difficulty ascertaining offence details in a number of reports to the ACORN. They reported that a large proportion of ACORN reports appeared to be unfounded (ie no actual offence had occurred), exaggerated the value of victims' losses, or otherwise contained insufficient information to justify further investigation. Furthermore, it was often not feasible to conduct interviews with all of the victims who reported in order to collect the additional information necessary to ascertain whether an offence had actually occurred, and justify further investigation. These issues were compounded by the significant (three to five month) delays in the processing of reports. In fact, police reported that it was not uncommon for victims to withdraw their complaints after reporting, due to the delay in being contacted for the purposes of investigation. These issues are explored further in later sections of this report.

Confidence in the Australian Government response to cybercrime

Providing a centralised, national online facility that would enable members of the public to easily report cybercrime to police was expected to improve public confidence in the action being taken to address cybercrime. The public survey therefore included a number of questions about respondent perceptions of the Australian Government’s response to cybercrime. Answers to these questions pre and post-implementation of the ACORN were compared, as were the responses of those respondents who were and were not aware of the ACORN.

There has been little change in the perceptions of the Australian Government’s response to cybercrime in the 15 months since the ACORN was implemented (Table 17). The only notable changes were a decrease in the proportion of respondents who felt the Australian Government was doing more to respond to cybercrime than it was 12 months ago (34% c/f 40%), and a smaller decline in the proportion who felt confident in the Australian Government’s response to cybercrime (34% c/f 37%).

Table 17 Perceptions of the Australian Government's response to cybercrime, pre- and post- implementation of the ACORN

	Pre-implementation (n=1,793)		Post-implementation (n=1,854)	
	n	%	n	%
I am concerned about the prevalence of cybercrime in Australia generally	1145	64	1206	65
The Australian Government should be doing more to address cybercrime	1111	62	1123	61
I am supportive of the Australian Government's response to cybercrime in general	976	54	1003	54
I am satisfied with the Australian Government's response to cybercrime	536	30	523	28
I have confidence with the Australian Government's response to cybercrime	659	37	625	34
The Australian Government is doing more to respond to cybercrime than it was 12 months ago	713	40	635	34
The Australian government is committed to combating cybercrime	808	45	837	45

Number and percentage of victims who 'Agreed' or 'Strongly Agreed' with statements about the Australian government's response to cybercrime. Data were weighted according to ABS population data to reflect distribution of age and sex across the entire population.

Source: ACORN Public Survey [AIC data file]

One explanation for this is that relatively few respondents were aware of the ACORN, which represents a major initiative and investment by the Australian Government and police partner agencies. Respondents who were aware of the ACORN were more likely to be concerned about the prevalence of cybercrime (70% c/f 64%) and believe the Australian Government should be doing more to address cybercrime (64% c/f 60%).

Importantly, those respondents who were aware of the ACORN were generally more positive about the Australian Government’s response to cybercrime (Table 18). They were more supportive of the Australian Government’s response (70 c/f 51) and had higher levels of satisfaction (43% c/f 26%) and confidence (49% c/f 31%) in the response. They were also more likely to believe the Australian Government was doing more to respond to cybercrime than it was 12 months ago (49% c/f 32%) and that it was committed to combatting cybercrime (63% c/f 42%).

While the ACORN is unlikely to be the only explanation for these differences, these results suggest that building awareness of the ACORN among members of the public (along with other initiatives) may help contribute to improved perceptions of the Australian Government’s response to cybercrime. Particularly as a large proportion of respondents neither agreed nor disagreed with the statements about cybercrime, indicating a relatively low level of awareness and understanding.

Table 18 Perceptions of the Australian Government's response to cybercrime, by ACORN awareness

	Not aware of ACORN (n=1,596)		Aware of ACORN (n=258)	
	N	%	N	%
I am concerned about the prevalence of cybercrime in Australia generally	1025	64	181	70
The Australian Government should be doing more to address cybercrime	958	60	165	64
I am supportive of the Australian Government's response to cybercrime in general	822	51	181	70
I am satisfied with the Australian Government's response to cybercrime	412	26	111	43
I have confidence with the Australian Government's response to cybercrime	498	31	127	49
The Australian Government is doing more to respond to cybercrime than it was 12 months ago	509	32	126	49
The Australian government is committed to combating cybercrime	675	42	162	63

Number and percentage of victims who 'Agreed' or 'Strongly Agreed' with statements about the Australian government's response to cybercrime. Data were weighted according to ABS population data to reflect distribution of age and sex across the entire population.

Source: The ACORN Public Survey [AIC data file]

Report handling and the impact on police resources

The second objective of the ACORN was to refer reports to the police and regulatory agencies for further consideration. Prior to the implementation of the ACORN, there was a cost to law enforcement agencies in dealing with reports of cybercrime they receive, both in terms of entering the reports that were received from the public into police information systems and in redirecting reports to the relevant business area or agency. ACORN aimed to (at least in part) address this by accepting cybercrime reports direct from the public and then forwarding them to the appropriate agency, thereby saving the need for agencies to review and refer cases on.

In this section of the report, results from the survey of law enforcement and monitoring tools completed by police agency partners are presented. Findings from the interviews with senior representatives, investigators and intelligence analysts relating to the handling of reports received through the ACORN and the impact of the ACORN on police resources are also discussed.

Referral of reports to police agencies

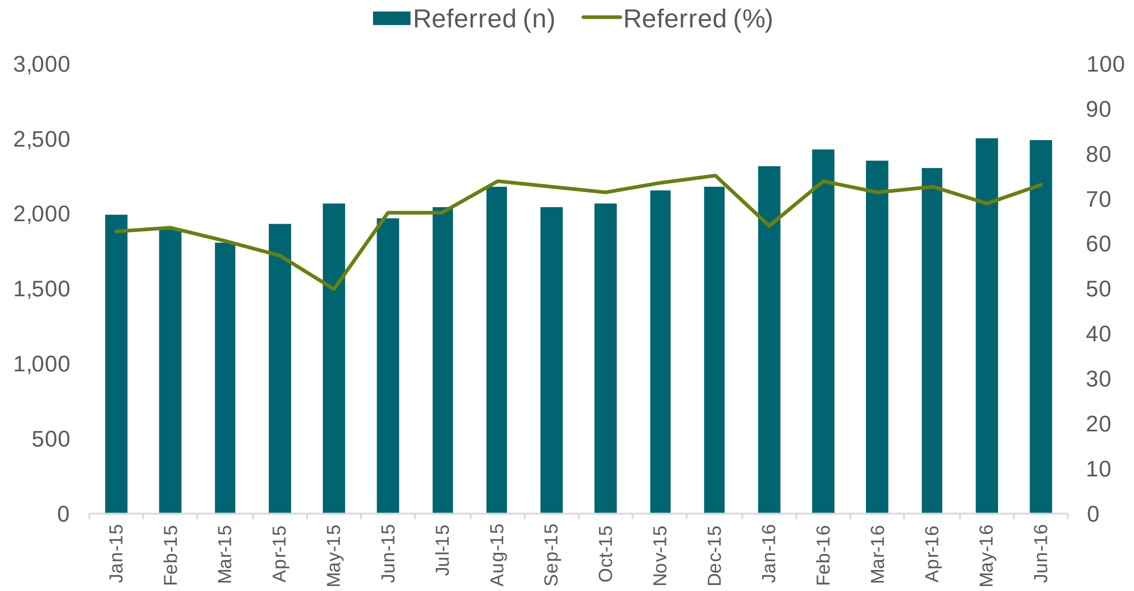
An important feature of the ACORN system is the capacity to automatically refer reports to the relevant jurisdiction for consideration and possible investigation. Reports that meet the ACORN business rules are automatically referred based on where the suspect is located, where the report contains sufficient information about the offender. Where the offender's identify or location is unknown, then the responsible agency will initially be determined by the location of the victim.

Reports may also be referred by the ACC, following manual interrogation of the data received by the ACORN. Reports that do not meet the business rules of the ACORN may still be referred if they provide evidence of imminent risk to the parties involved or relate to issues such as national security. These reports are assessed and referred on a case by case basis.

The number of reports automatically referred to police partner agencies, along with the proportion of all reports submitted to the ACORN that were automatically referred to police, are presented in Figure 8. This shows that the number of reports automatically referred gradually increased in the 18 months to June 2016. The proportion of reports automatically referred increased prior to August 2015 after a low in May 2015, after which it has remained relatively stable. More than 27,000 reports were automatically referred to police partner agencies between July 2015 and June 2016 (Table 19)—equivalent to 71 percent of all reports submitted to the ACORN (excluding those reports not reportable to the ACORN).

To better understand overall patterns in referrals by the ACORN, while accounting for seasonal variation, the number of reports automatically referred in the first half of 2016 was compared with the same six-month period in 2015. This showed that the number of reports automatically referred to law enforcement agencies increased by 23 percent in the first half of 2016, compared to the equivalent period in 2015. The proportion of all reports automatically referred increased by 11 percentage points during this same period.

Figure 8 Reports referred by the ACORN to police partner agencies, by month



Source: Australian Criminal Intelligence Commission 2016 [data file]

Victoria (26%), Queensland (25%) and NSW (22%) received the largest proportion of automated referrals in 2015-16 (Table 19). Together, these three jurisdictions accounted for three quarters of all reports automatically referred.

Table 19 ACORN report automated referrals, by state and territory, 2015-16

	n	%
Victoria	6,948	26
Queensland	6,683	25
NSW	6,049	22
WA	3,561	13
SA	2,615	10
ACT	494	2
Tasmania	391	1
NT	341	1
Total	27,082	100

Source: Australian Criminal Intelligence Commission 2016 [data file]

Report handling by police

Each of the police partner agencies nominated to participate in the evaluation have implemented the ACORN in different ways. This is important because the way in which the ACORN is implemented has influenced how reports are received and processed by each agency and has implications in terms of understanding the impact of the ACORN on the efficiency and effectiveness of the law enforcement response to cybercrime.

NSWPF Fraud and Cybercrime Squad takes every report received from the ACORN system and enters it into their local information system, to disseminate the reports to Local Area Commands (LACs) for local investigation. In this jurisdiction the ACORN is used as a 'mail delivery system', whereby all reports are processed and triaged by a centralised ACORN Referral Team (ART).

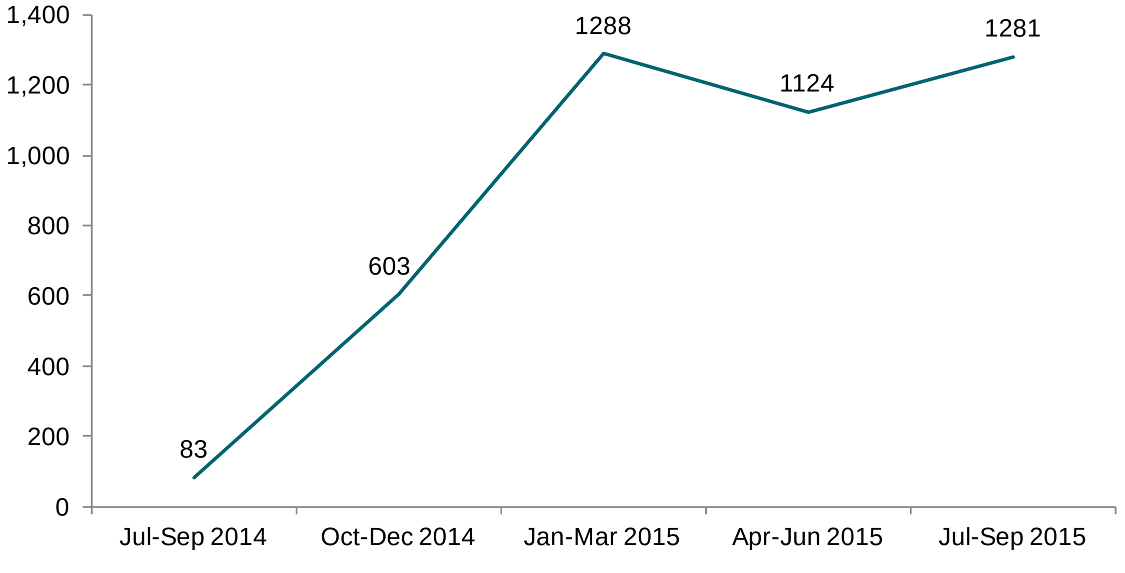
QPS has prioritised the identification of high-risk reports received through the ACORN, including offences against children and domestic violence (eg breaches of domestic violence orders committed online). The remaining reports are processed by the Fraud and Cyber Group and disseminated to crime managers who task local police districts with the investigation. This process is similar to NSWPF.

The focus of the Technology Crime Investigation team at WAPOL is on investigating reports from the ACORN. Relatively few reports are referred to other business areas for investigation. Reports are triaged by the Technology Crime Investigation team prior to commencing an investigation, with priority given to those reports that are expected to produce a favourable investigative outcome. Victims who have reported to the ACORN, but whose report will not be investigated, are notified of that fact.

While reports are automatically referred to each police partner agency, decisions about which reports are received, handled by the specialist unit and subject to further interrogation rest with the receiving agency. To provide a more accurate estimate of the number of reports received from members of the public, data were collected on a quarterly basis from each police partner agency on the number of reports received and handled between July 2014 and September 2015.

The number of reports received by the NSWPF Fraud and Cybercrime Squad is presented in Figure 9. There has been a significant upward trend in the number of reports received. Note that the ACORN was implemented midway through the second quarter of data collection. In the final four quarters of the observation period, there was an average of 1,074 reports received by the Fraud and Cybercrime Squad—a nearly 13-fold increase when compared to the September quarter in 2014, prior to the implementation of the ACORN.

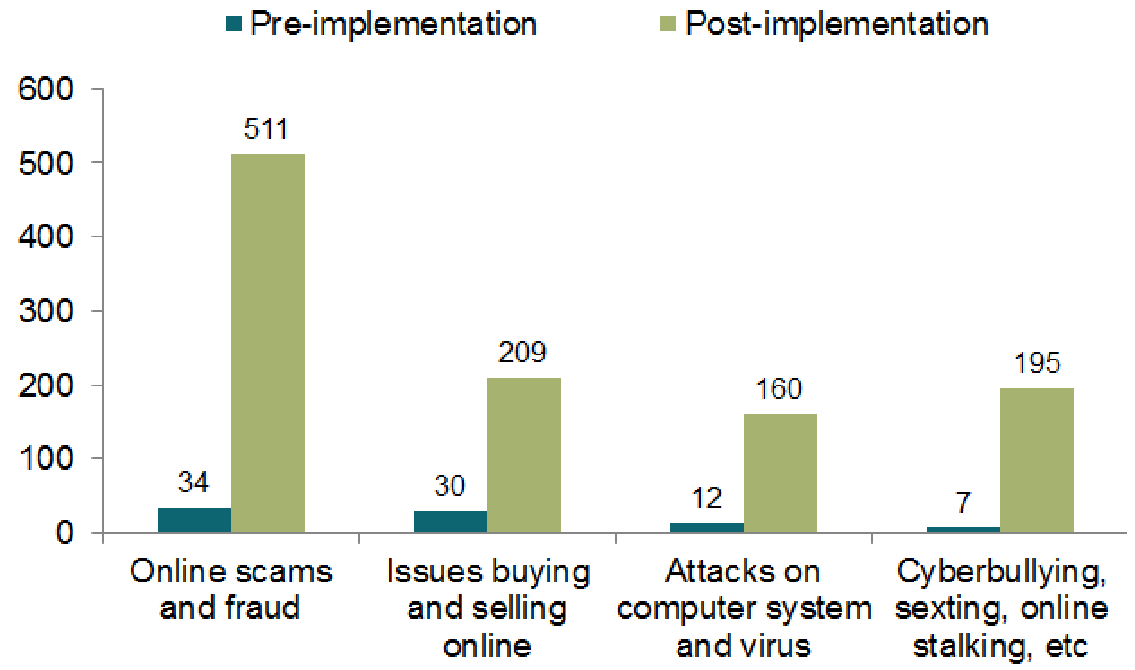
Figure 9 Number of cybercrime reports received and handled by the NSWPF Fraud and Cybercrime Squad, by quarter



Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

A summary of the number of reports received in the September 2014 quarter, prior to the ACORN, and the average number of reports per quarter in the four quarters post-implementation is presented in Figure 10. Nearly half of all reports received by NSWPF post-ACORN relate to online scams or fraud. However, there has been a significant increase in all forms of cybercrime reported to and received by the NSWPF. Particularly notable is the significant increase in reports received by the NSWPF Fraud and Cybercrime Squad that relate to cyberbullying, sexting, online stalking and harassment.

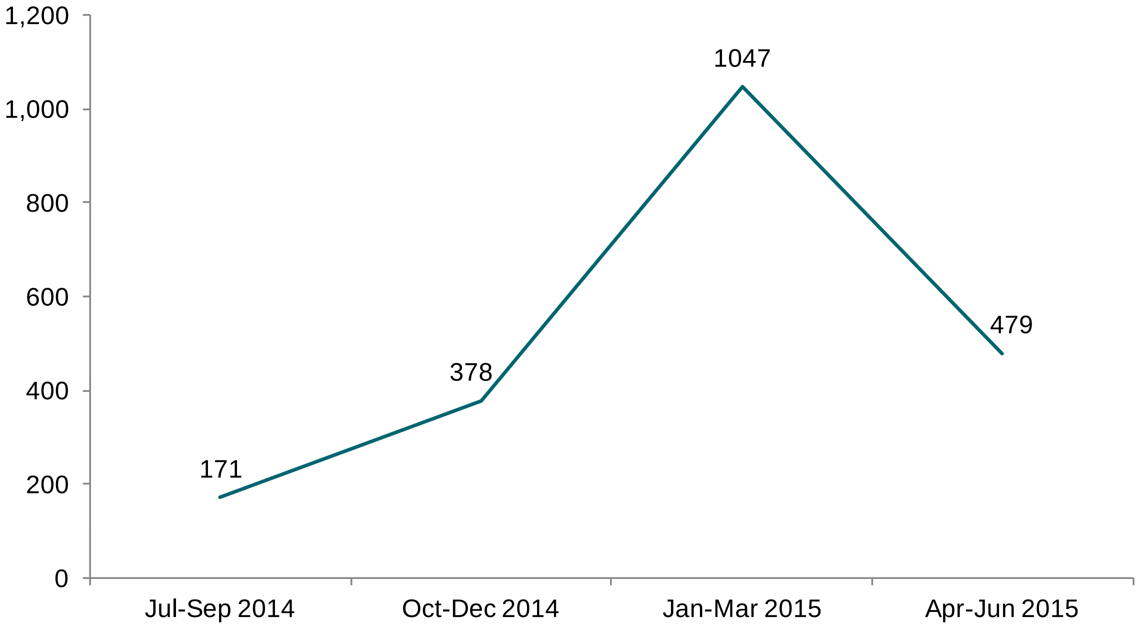
Figure 10 Reports received and handled by the NSWPF Fraud and Cybercrime Squad, by cybercrime type, pre- and post-implementation of the ACORN



Pre-implementation period refers to July-September 2014. Post-implementation period represents average number of reports per quarter in 12 months to September 2015.

Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

Figure 11 Number of cybercrime reports received and handled by the QPS Cyber and Identity Crime Investigation Unit, by quarter

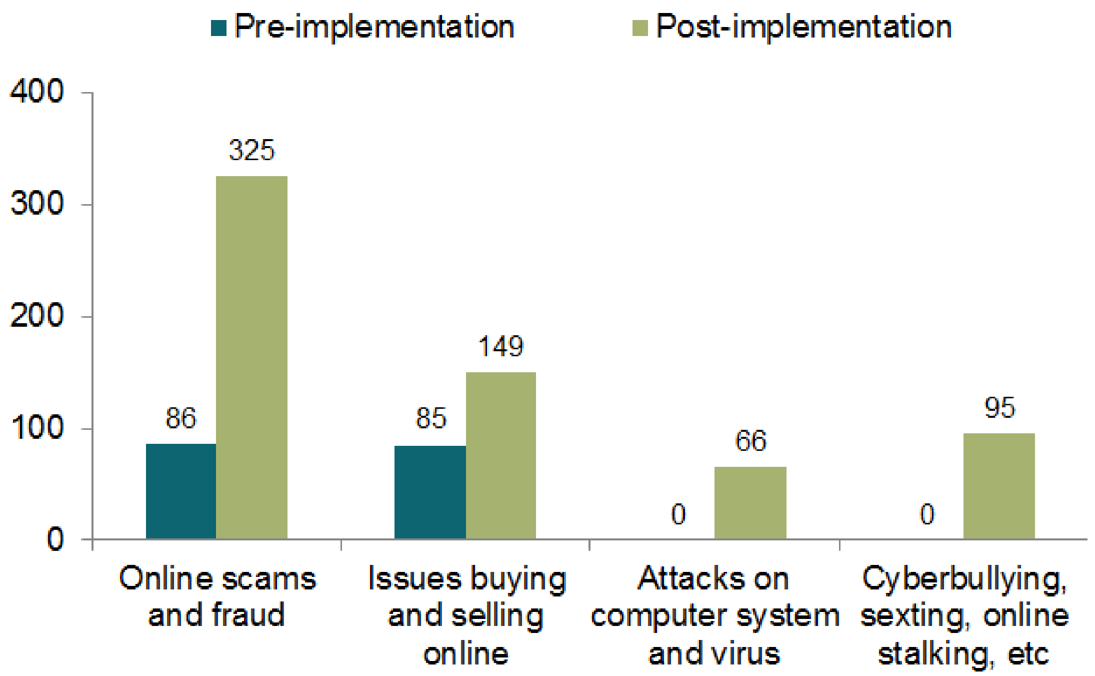


Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

The number of reports received and handled by the QPS Cyber and Identity Crime Investigation Unit is presented in Figure 11. Reliable data were not available for the September 2015 quarter. There has been an upward trend in the number of reports received and handled by the Unit, with a noticeable peak in the March 2015 quarter. In the final three quarters of the observation period, there was an average of 635 reports received by the Unit—a four-fold increase when compared to the September quarter in 2014.

A summary of the number of reports received and handled by the QPS Cyber and Identity Crime Investigation Unit prior to the ACORN, and the average number of reports per quarter in the three quarters post-implementation, is presented in Figure 12. Online scams and fraud accounted for more than half (51%) of all reports received and handled by the Unit. In the quarter prior to the implementation of the ACORN, the Unit did not receive any reports relating to attacks on computer systems or cyberbullying, sexting, online harassment and stalking. Post-implementation, the Unit received and handled an average of 66 and 95 reports per quarter, respectively.

Figure 12 Reports received by the QPS Cyber and Identity Crime Investigation Unit, by cybercrime type, pre- and post-implementation of the ACORN

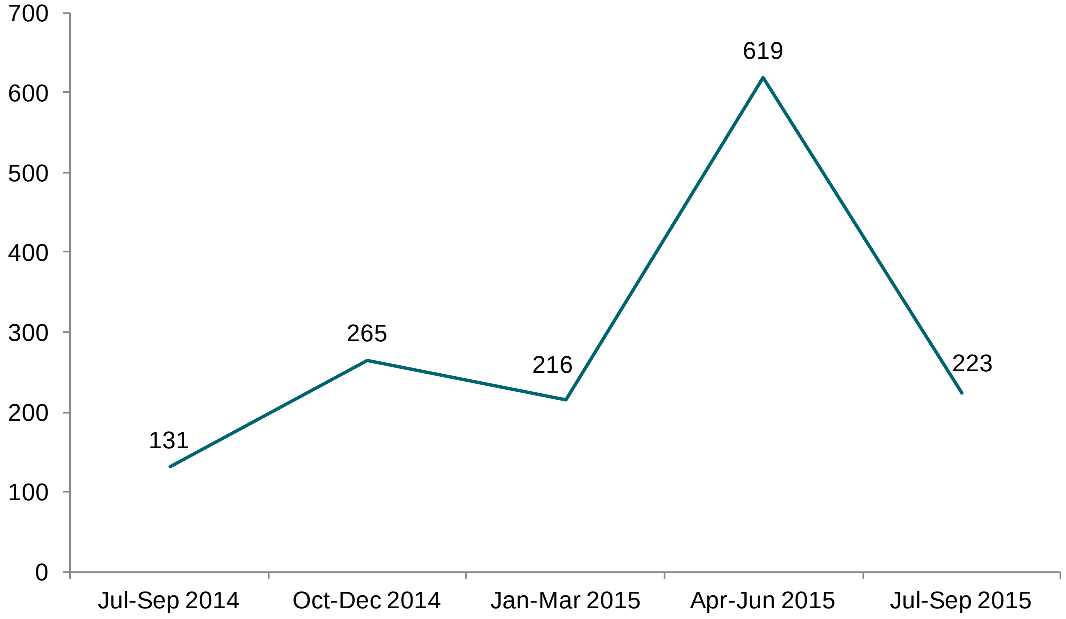


Pre-implementation period refers to July-September 2014. Post-implementation period represents average number of reports per quarter in 9 months to June 2015

S Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

The number of reports received and handled by the WAPOL Technology Crime Investigation team is presented in Figure 13. As in the other two jurisdictions, there has been an increase in the number of reports received, with a notable peak in the June 2015 quarter. However, the increase in the number of reports received and handled by WAPOL (when compared to NSWPF and QPS) reflects the different model of implementation that has been adopted. In the four quarters post-implementation of the ACORN there was an average of 331 reports received by the Technology Crime Investigation team—a 2.5-fold increase when compared to the September quarter in 2014.

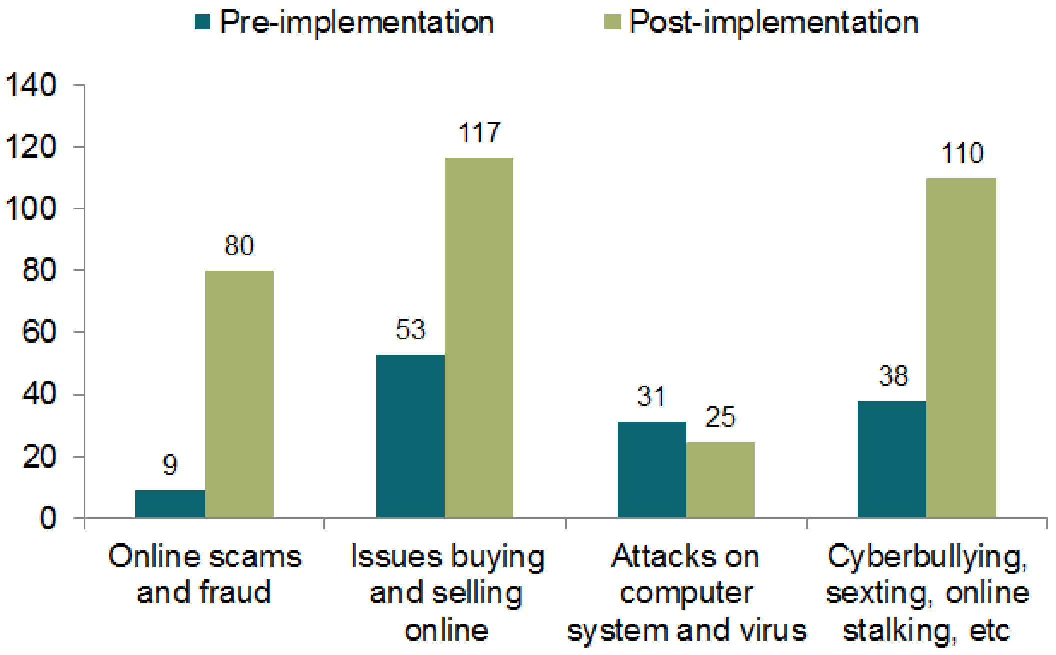
Figure 13 Number of cybercrime reports received and handled by the WAPOL Technology Crime Investigation team, by quarter



Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

While the average number of reports relating to attacks on computer systems received and handled by the Technology Crime Investigation team has remained relatively stable, there have been significant increases in the three other categories of cybercrime (Figure 14). Post-implementation of the ACORN, the most common type of report received and handled by the Technology Crime Investigation team was for issues buying and selling online (117 per quarter), followed by cyberbullying, sexting, online harassment and stalking (110). There was an eight-fold increase in the number of online scams and fraud reports received and handled by the team.

Figure 14 Reports received by the WAPOL Technology Crime Investigation team, by cybercrime type, pre- and post-implementation of the ACORN



Pre-implementation period refers to July-September 2014. Post-implementation period represents average number of reports per quarter in 12 months to September 2015.

Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

Taken as a whole, these results confirm that the ACORN has contributed to a significant increase in the number of reports received and handled by specialist units within the three participating agencies. While each agency has adopted a different method for reviewing, prioritising and handling reports, all three police partner agencies reported significant resource implications associated with this increase. Further, information provided by other police partner agencies suggests these issues have not been unique to NSWPF, QPS and WAPOL.

Resources allocated to referring reports

While the increase in cybercrime reports was expected, there were also mechanisms within the ACORN to improve the efficiency of report handling.

Prior to the implementation of the ACORN, there were several ways in which cybercrime reports may have been referred between business areas and agencies. It was possible that a report could be referred from a LAC, who received the original report, to a specialist cybercrime unit for investigation because they possessed the specialist knowledge and technical skills required to conduct the investigation. A report may have also been referred from a specialist unit to a LAC where they are well placed to conduct an investigation involving an offender or victim who resides within that LAC.

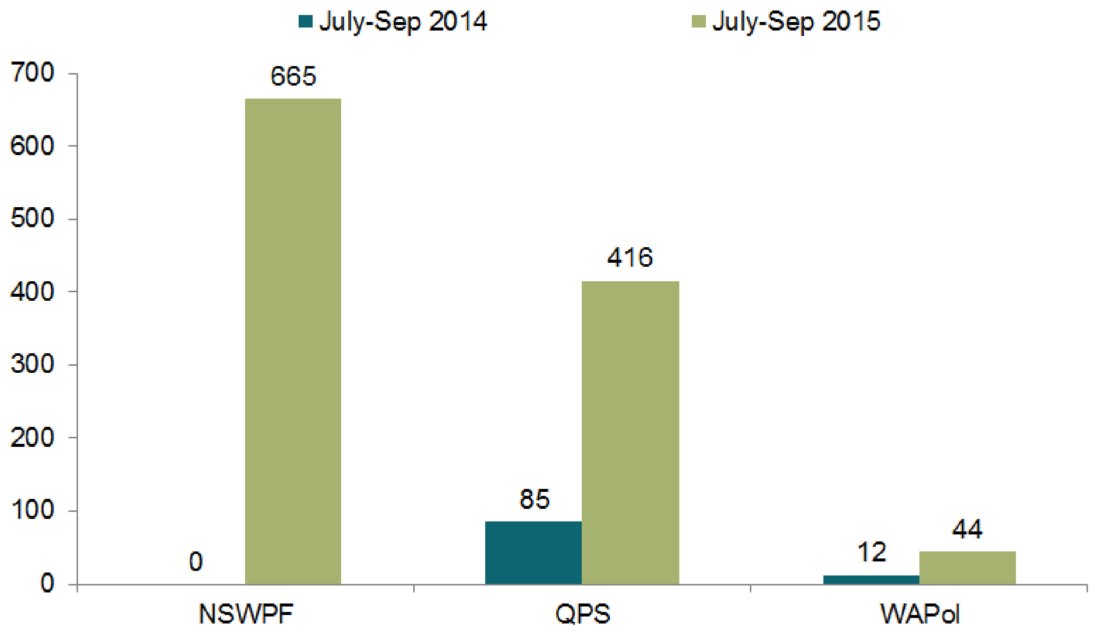
Reports may have also been referred between police agency partners based on the location of the offender. The jurisdiction in which an offender resides is responsible for leading the investigation. If the offender’s identify or location is unknown, then the agency responsible would be determined by the location of the victim (typically the agency to whom the report was first submitted). Cybercrime is unique in that it does not require the offender to be in close proximity to the victim—they may be based in another state or, as is frequently reported, overseas.

Interview participants reported that they often referred reports to another state and territory police agency, AFP or international jurisdiction for further investigation once the offender’s location is determined. This has important implications for police resources, as it frequently required the originating agency (the one receiving the original report from the victim) to initiate an investigation before they could refer the matter to the appropriate jurisdiction. Under pre-ACORN arrangements, all reports received by a state and territory agency were initially dealt with by that agency—in other words, there was no automated referral between jurisdictions, even where the offender’s location is known from the original report.

The ACORN was expected to address many of these inefficiencies by automatically grouping and referring reports to the appropriate jurisdiction, based on the information supplied by the victim reporting the incident. The trend towards encouraging all victims attempting to report cybercrime through traditional mechanisms (by telephone or in person) to report via the ACORN, the automated referral of reports to state and territory police by the ACORN, and the centralisation of report handling within specialist units, has altered these referral pathways.

Most importantly, responsibility for referring reports now rests with the specialist units who receive and handle reports submitted to the ACORN. The number of reports referred by these specialist units to other business areas or agencies has increased significantly as a result (Figure 15). In the September 2014 quarter prior to the implementation of the ACORN, the NSWPF Fraud and Cybercrime Squad did not refer any reports relating to the four main cybercrime categories to other business areas or agencies. In the September 2015 quarter post-implementation, it (and, specifically, the ART), referred 665 reports to LACs. Similarly, the QPS Cyber and Identity Crime Investigation Unit referred 85 reports in the quarter prior to the implementation of the ACORN, and a total of 416 referrals to LACs in the September 2015 quarter post-implementation—a five-fold increase in referrals.

Figure 15 Number of reports referred to other business areas or agencies, pre- and post-implementation, by police partner agency



Source: ACORN survey of law enforcement [data file]

There was a smaller increase in referrals by WAPOL's Technology Crime Investigation team (and much smaller number of referrals overall), consistent with the centralised model of investigation. In the September 2014 quarter, the team referred a total of 12 reports, compared with 44 reports received from the ACORN in the same period 12 months later. Of these 44 reports, 68 percent were referred to other state and territory police for further investigation, 23 percent were referred to another government agency, and nine percent were referred to another business area. In the September 2014 quarter, no reports were referred to other state and territory police, suggesting that (at least for WAPOL), the ACORN hasn’t overcome all of the challenges associated with identifying the jurisdiction with responsibility for investigating cybercrime reports.

Both NSWPF and QPS indicated that the referral of reports to LACs had presented a significant administrative burden, and required dedicated personnel to be appointed to the role of entering reports into the local information management system to facilitate referrals. There were limited reliable data to be able to quantify the time spent by police partner agencies referring reports to other business areas or agencies. However, QPS reported that, in the September 2015 quarter, officers spent a total of 168 hours per week referring reports to other business areas—equivalent to 4.2 FTE staff (based on a 40 hour working week).

Issues impacting on report handling and police resources

The volume of reports submitted to the ACORN and automatically referred to police partner agencies has exceeded expectations, which has exacerbated issues related to under resourcing. Police partner agencies stated that they were not prepared to deal with the volume of reports received by the ACORN and referred to their jurisdiction for investigation. While the number of reports received and handled by specialist units is significant, police representatives reported that there have been sustained periods whereby there is a backlog of reports that must be entered into local police information management systems, sometimes reaching thousands of reports and resulting in delays of up to three to five months before reports can be entered.

It was reported by all jurisdictions that the ACORN had added layers of administration to reporting offences and that there was a requirement for additional resources to assist in processing and triaging ACORN reports. Senior police from one jurisdiction recommended that a system of automatic processing and triaging that could take into account the quality and level of information entered by users would save significant time and resources.

There is a large volume of reports that do not meet the business rules and are not automatically referred to police agencies for investigation. At present, these reports are being manually reviewed to identify potential high-risk incidents or significant reports, which are then referred to the relevant jurisdiction or agency. This undermines the ACORN model of automated referrals, and imposes a significant burden on the ACC (now ACIC).

There have been some limitations with the ACORN system that have impacted on law enforcement outcomes and resulted in some duplication of effort, including the limited interoperability with state-based systems, the format of reports produced, the amount of information that is collected and the capacity of the system to automatically group reports over time. A key issue for police jurisdictions is limited interoperability between the ACORN and the local information management systems that exist in each jurisdiction (eg QPrime, COPS). ACORN reports must be taken from the ACORN system and exported into the local police information management system so that the relevant business area, LAC or police district can be tasked with investigating and responding to the report. This data transfer is not automated because of integration issues between multiple systems, and compromises productivity saving that would be gained through victims reporting directly to ACORN. This particularly affects NSWPF and QPS. Exporting reports from the ACORN to the local police information management system is a time and resource intensive process, as information needs to be manually transferred. One jurisdiction has written software that performs this function, as well as appointing additional staff where resources permit. Improved interoperability with police information management systems could lead to better investigation outcomes and outcomes for victims.

There is evidence of victims submitting multiple reports for the same incident due to perceived inaction by police and the delay in responding to victims, adding to the backlog of reports and creating further inefficiencies. Further, delays in processing reports have resulted in information being outdated. Police commented that this has consequences for investigations as the offenders have typically moved and money is unable to be recovered once the police commence investigating a report. Police reported that cybercrime offences are often time critical and investigation needs to commence immediately.

External factors have impacted on the implementation of the ACORN. For example, the unexpected reporting of family, domestic and sexual violence incidents via the ACORN, which must be prioritised for action, has influenced how police manage ACORN reports. The QPS Fraud and Cyber Group has a mandate to focus on fraud offences; however, due to the reporting of domestic violence offences in the 'other' ACORN category, the group is focused on triaging ACORN reports and responding to offences against the person (such as offending against children or domestic violence). There have reportedly been times where there have been up to 1,400 online scam and fraud reports that have not been processed, despite this being the main focus of the QPS Fraud and Cyber Group.

A number of suggestions for improvement in the functionality of the ACORN were made. Stakeholders expressed frustration at the report structure, commenting that it was difficult to read ACORN reports and that they could not distinguish between question and responses. This is compounded by free-text responses that appear as long blocks of text. Consistent feedback from the police jurisdictions was that improvements need to be made to the structure and overall readability of reports exported from the ACORN.

The free-text options available to victims should be reduced to ensure that reports are more concise and focus on the key issues. Further, police also recommended more specific dropdown options be provided that focus on establishing the necessary elements of an offence. One jurisdiction reported that the vast majority of reports received from the ACORN were unfounded (no offence could be identified) and were not a police matter.

Agencies cautioned that the data that is reported or contained within ACORN reports is not valid and that the questions need to be more focused and the provided responses should be able to be edited by police investigating the reports. For example, concerns were raised about the accuracy of victims' reported value of loss and that the police or those processing the report cannot make changes to this amount (as an 'assessed loss'). Police reported that victims often inflated the value of their loss, presumably to increase the chances that it would be prioritised and actioned, or inflate estimates of the value of personal information when identifying a monetary value of their loss when reporting to the ACORN.

Further, police recommended inclusion of a question about the victim's motivation or main reason for reporting to the ACORN. This is because some victims report solely to obtain a reporting number for insurance purposes or reimbursement from financial institutions or to obtain Centrelink emergency payments. Victims should be able to note in the report whether, for example, they want a report to be investigated, or are simply reporting to inform police of the scam (like SCAM watch), or for insurance purposes. This would allow reports in the latter two categories to be separated from those requiring investigation, increasing efficiency.

Representatives from one jurisdiction recommended that the ACORN user interface should be updated with additional columns to assist with the prioritisation and processing of reports. These included drop-down options for identifying the priority level of reports (high, medium or low), identifying whether the report had been previously referred (or re-referred) and any preliminary information, and the lead investigator or officer-in-charge responsible for processing the report.

Finally, interoperability and consistency with other reporting systems, particularly SCAMwatch and the integration of ACORN and SCAMwatch datasets was suggested by police as requiring further investigation.

Responding to cybercrime

The third objective of the ACORN was to collect and aggregate data from reports to assist police, regulatory and other government agencies to develop improved strategic and tactical responses to cybercrime. The ACORN attempted to provide law enforcement agencies with reports that were automatically grouped to create patterns of cybercrime activity. In doing so, cybercrime reports were expected to be more easily actioned by law enforcement agencies and result in quicker enforcement activity to tackle emerging problems, which would in turn lead to action being taken against a greater number of cybercrime targets. While beyond the scope of this evaluation, there was an expectation that this would lead to a reduction in cybercrime resulting from an increased risk of detection and an increase in the effort involved in offending against Australian targets.

There were also expected benefits in terms of intelligence. The ACORN was expected to create a greater quantity of information received by law enforcement agencies, which would in turn result in an increase in the number of intelligence products generated by law enforcement agencies, and an increase in the quality of intelligence relating to cybercrime threats. There was an expectation of savings associated with a reduction in the time taken to produce intelligence products, due to the improved quality of information available from the ACORN.

In this section of the report, results from the survey of law enforcement and monitoring tools relating to intelligence and enforcement activity are presented. Findings from the interviews with senior representatives, investigators and intelligence analysts, which addressed issues relating to cybercrime intelligence and enforcement, are also discussed.

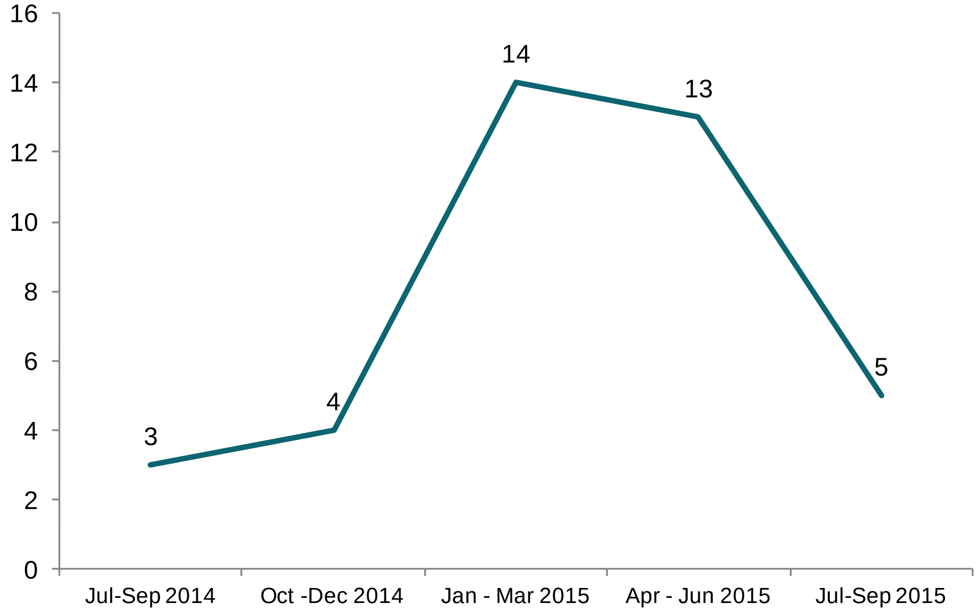
Intelligence activity

Increasing the effectiveness of cybercrime responses is contingent on the availability of timely, high quality strategic and tactical intelligence. For the purpose of this evaluation, tactical intelligence products were defined as products that direct and support operational activity and enforcement action, while strategic intelligence products identify broader or emerging trends. To assess the impact of the ACORN on the number of intelligence products produced by the specialist cybercrime units, data were collected on a quarterly basis on the intelligence activities undertaken by the ACC, NSWPF and QPS. This information was used to identify changes following the public launch of the ACORN.

In the first quarter of data collection, prior to the implementation of the ACORN, ACC's Fusion Discovery produced three intelligence products, all of which were focused on attacks on computer systems or viruses (Figure 16). This included two strategic intelligence products and one tactical intelligence product. The information used for all three intelligence packages was obtained through other intelligence activity.

Since then, there has been an increase in the number of cybercrime intelligence products produced by the ACC, with notable peaks in the March and June quarters. While it has varied across the observation period, the average number of intelligence products produced per quarter in the period following the implementation of the ACORN was three times that of the quarter pre-implementation (9 c/f 3). These products, which have been relatively evenly split between strategic and intelligence products, have drawn heavily on data received through the ACORN and have each related to one of the main categories of cybercrime.

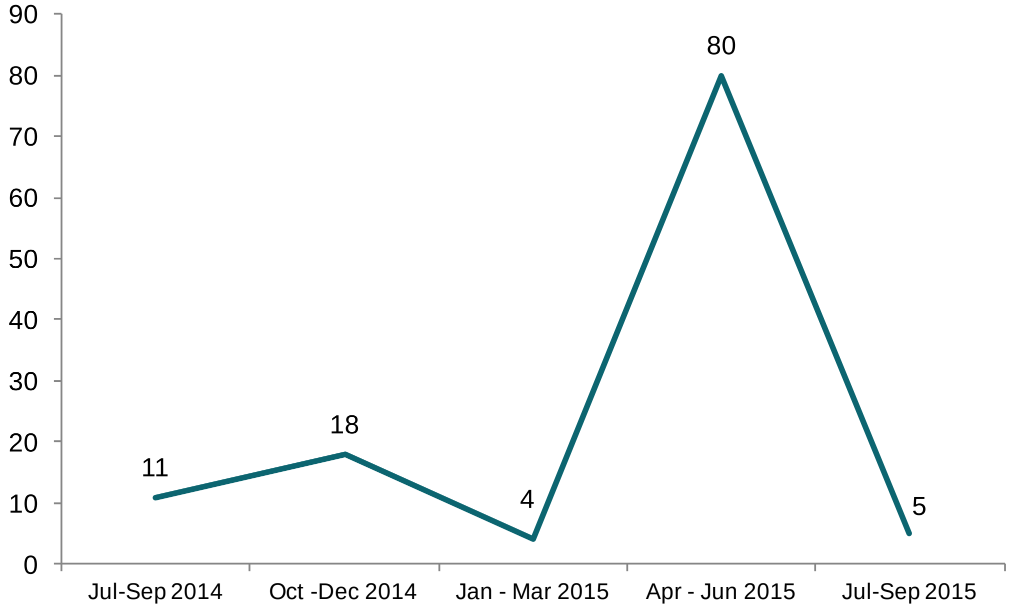
Figure 16 Number of cybercrime intelligence products produced, ACC, by quarter



Source: ACORN quarterly monitoring tool (intelligence), 1 July 2014—30 September 2015 [data file]

The number of intelligence products produced by the NSWPF Fraud and Cybercrime Squad was also highly variable (Figure 17). With the exception of the June 2015 quarter, there was little change in the number of products post-implementation. The spike in June 2015 was largely due to intelligence from ongoing investigations. There were more tactical than strategic intelligence products produced each month, with very few products reportedly drawing on reports received directly through the ACORN or relating to the main categories of cybercrime reportable to the ACORN.

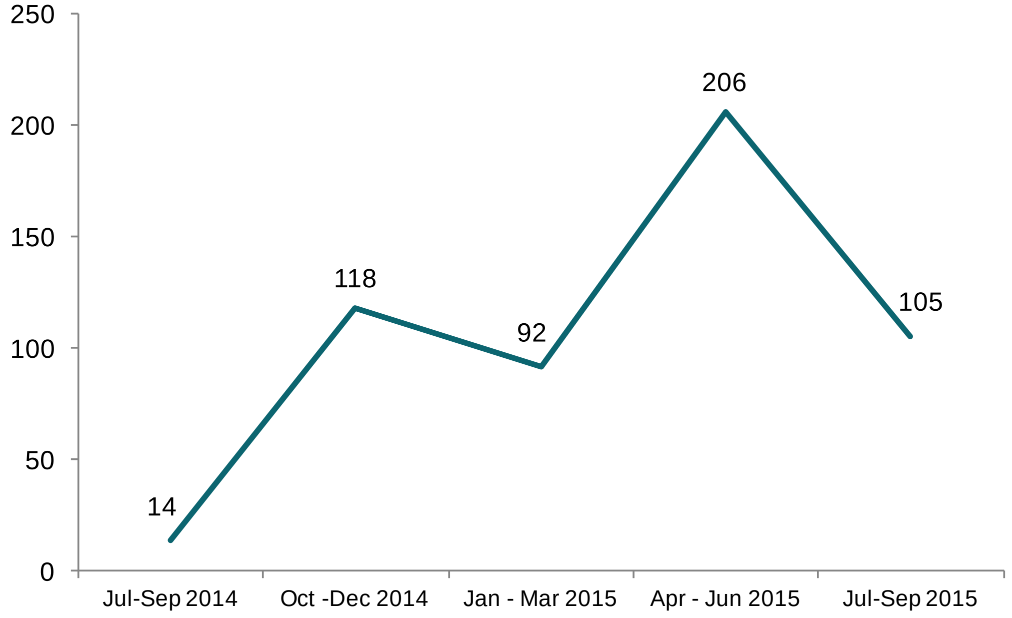
Figure 17 Number of cybercrime intelligence products produced, NSWPF, by quarter



Source: ACORN quarterly monitoring tool (intelligence), 1 July 2014—30 September 2015 [data file]

QPS Cyber and Identity Crime Investigation Unit reported a consistently higher number of cybercrime intelligence products, with a similar peak in June 2015 but an overall upward trend in the number of products generated (Figure 18). The average number of products created in the period post-implementation of the ACORN was more than nine times that of the quarter prior to implementation (130 c/f 14). Importantly, they reported drawing heavily on reports received through the ACORN, producing largely tactical intelligence products. They were able to provide a detailed breakdown of the source of intelligence used in prepared by the Unit in the September 2015 quarter. One-third (33%) relied on reports received through the ACORN, while a further 38 percent drew upon information provided by the public. The remainder were relatively evenly divided between other state and territory police, AFP, ACC, other government agencies, other intelligence activity and recent investigations.

Figure 18 Number of cybercrime intelligence products produced, QPS, by quarter



Source: ACORN quarterly monitoring tool (intelligence), 1 July 2014—30 September 2015 [data file]

Time spent on cybercrime intelligence activities

An anticipated productivity gain associated with the introduction of the ACORN was the improved efficiency of intelligence gathering, analysis and dissemination. The ACC, NSWPF and QPS provided information on the number and type of intelligence products produced each quarter, the number of intelligence analysts involved in cybercrime intelligence activities, and the time spent analysing, grouping, preparing and disseminating intelligence products. WAPOL reported that they did not currently have a dedicated cybercrime intelligence analyst and were therefore unable to provide data on intelligence activity. QPS were unable to provide data on the resources allocated by intelligence analysts for the entire observation period.

Information on the number of intelligence products produced in the September 2014 quarter prior to the implementation of the ACORN, and the average number produced in the four quarters post-implementation, is presented in Table 20. The number of intelligence products produced by both the ACC (9 c/f 3) and the NSWPF (27 c/f 11) increased following the introduction of the ACORN (although, as previously reported, the increase in NSWPF was largely due to a peak in one quarter). There was also an increase in the average analyst hours per week allocated to the different intelligence activities involved in producing intelligence products, and an increase in the total hours spent by intelligence analysts working on cybercrime intelligence. In other words, the ACORN has contributed to an increase in overall time spent by analysts preparing cybercrime intelligence products.

However, in both cases, the increase in the total amount of time spent by intelligence analysts on cybercrime intelligence activities was not proportionate to the increase in the number of products, meaning that the estimated number of hours per intelligence product declined significantly—by around half. Specifically, the average hours per intelligence product generated by the ACC decreased from 208 hours to 121 hours, while the average hours per intelligence product generated by the NSWPF decreased from 47 hours to 24 hours.

Table 20 Time spent undertaking intelligence activities

	ACC		NSWPF	
	Pre-implementation	Post-implementation	Pre-implementation	Post-implementation
Intelligence activity				
Intelligence products per quarter	3	9	11	27
Average hours per intelligence activity				
Reviewing and analysing information	20	29	15	14
Grouping cybercrime reports	3	7	3	5
Preparing strategic intelligence	15	26	1	7
Preparing tactical intelligence	8	14	20	20
Disseminating intelligence	2	7	1	3
Analyst hours per week (total)	48	84	40	49
Efficiency of intelligence activity				
Average hours per intelligence product	208	121	47	24

Source: ACORN quarterly monitoring tool (intelligence), 1 July 2014—30 September 2015 [data file]

There is reportedly some scope to increase the capacity of police to interrogate and manage ACORN information, which impacts on both referral processes and intelligence activity. Some police who are responsible for dealing with the ACORN system commented that they did not receive training, and were unsure of how to operate the system and interrogate the ACORN data. It was recommended that police using the ACORN are provided training on how to use the system, including searching, grouping report sets and referral capabilities. Further, at the time of being interviewed, intelligence analysts had not had training in the searching and grouping functions of the ACORN.

Enforcement activity

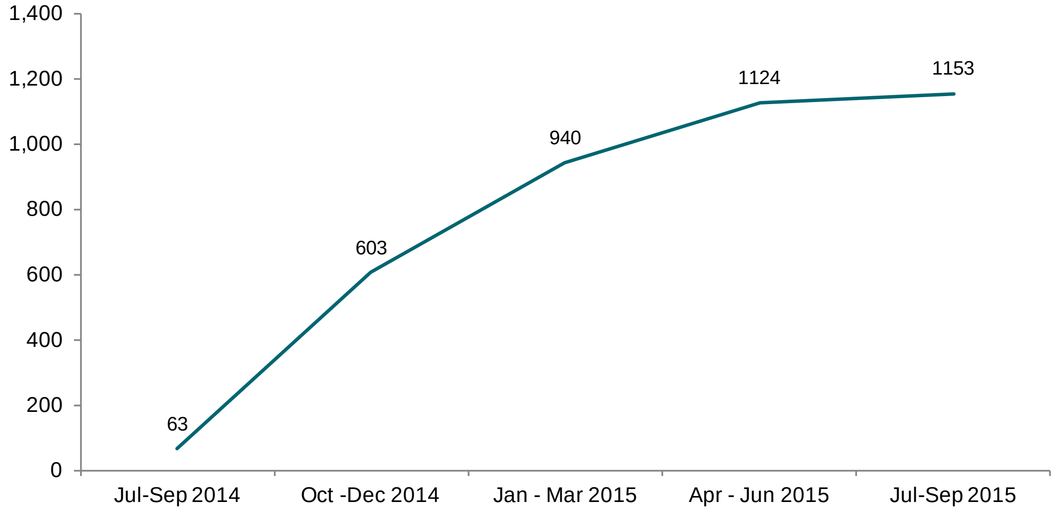
Information on cybercrime enforcement activity prior to the implementation of the ACORN was also collected for the July 2014—September 2015 period. Enforcement activity refers predominantly to investigations, and included measures of investigations commenced and finalised and investigation outcomes.

All three police agency partners involved in the evaluation have established specialist units responsible for the investigation of cybercrime offences. These units comprise a relatively small number of investigators and, with the exception of WAPOL, dedicated intelligence analysts. This reflects the very specialised nature of cybercrime investigations and the need for both investigators and intelligence analysts to have the technical capability and specialist knowledge of the area. However, police outside of these areas are also responsible for investigating cybercrime offences (including general duties police and detectives), particularly in Queensland and NSW where reports are referred to LACs for further investigation.

Different investigation models were described by the different agencies. In some cases, reports relating to cybercrime offences are received by the specialist unit, analysed to identify potential links with other offences or offenders, and then referred to the LAC for further investigation (on the basis that specialist knowledge is not required). Information on these offences may be recorded in the police information management system and this can be used by the specialist unit to monitor the progress of the investigation (as an accountability mechanism). In other cases, the specialist unit has elected to maintain greater control over the investigation of cybercrime offences, and therefore does not refer cases to LAC for further investigation.

The figures provided by each police partner agency reflect the model of operation that has been adopted in each jurisdiction, but also varies according to the parameters for the data set by each agency. NSWPF Fraud and Cybercrime Squad reported a significant, sustained increase in the number of investigations commenced following the implementation of the ACORN (Figure 19). This includes those investigations commenced by LACs based on reports submitted to the ACORN and subsequently referred by the Fraud and Cybercrime Squad. Some care needs to be taken in comparing these with the September 2014 quarter, prior to the implementation of the ACORN, as this was limited to investigations commenced by the Fraud and Cybercrime Squad. Nevertheless, the sustained upward trend, coupled with interview findings that suggest LACs investigated relatively few reported cybercrime offences, support the conclusion of a growing number of cybercrime investigations following the introduction of the ACORN.

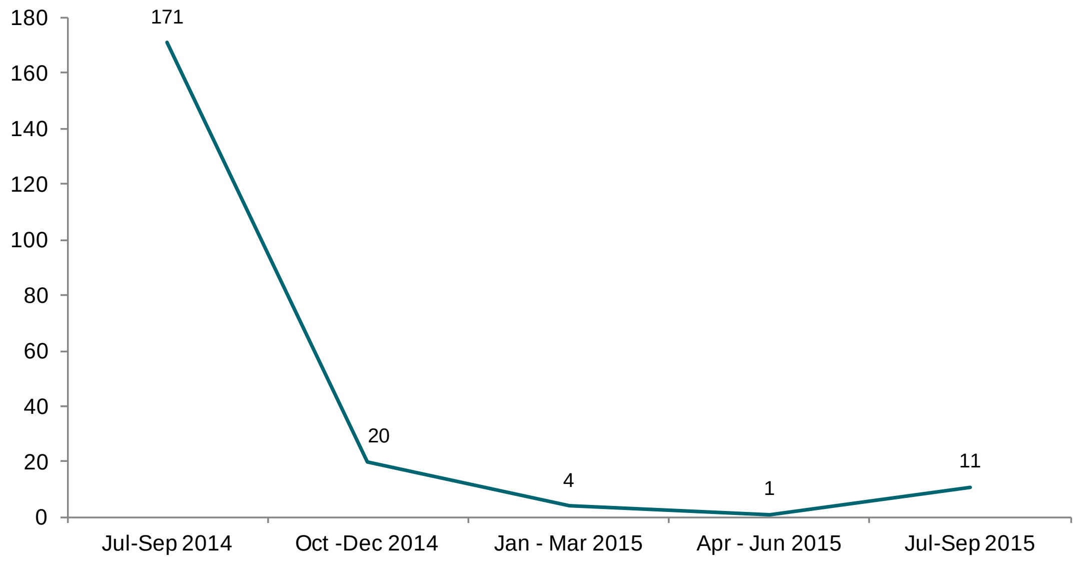
Figure 19 Number of cybercrime investigations commenced, NSWPF, by quarter



Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

Conversely, the QPS Cyber and Identity Crime Investigation Unit reported relatively few cybercrime investigations as having commenced following the introduction of the ACORN, particularly when compared with the September 2014 quarter (Figure 20). Unlike NSWFP, QPS reported on investigations commenced by the Unit, only. The number of investigations commenced during the observation period by this Unit reflects the referral model adopted by QPS to respond to ACORN reports, and the Unit's prioritisation of identifying high-risk reports received through the ACORN, Specifically, offences against children and domestic violence, which are referred to other QPS business areas for investigation.

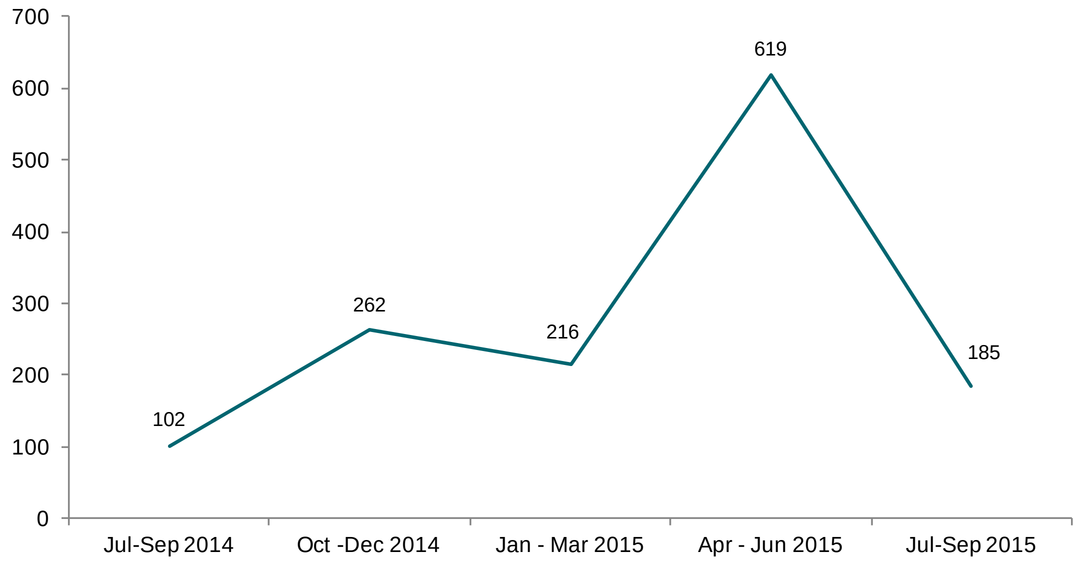
Figure 20 Number of cybercrime investigations commenced, QPS, by quarter



Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

Given the centralised model of investigations, data supplied by the WAPOL Technology Crime Investigation team arguably provide the most accurate picture of the impact of the ACORN on investigation activity. Based on a comparison of the average number of investigations commenced per quarter in the 12 months to September 2015 with the September 2014 quarter, there has been a three-fold increase in the number of investigations commenced (Figure 21). This ranged from a two-fold increase for attacks on computer systems, to a nine-fold increase in the number of investigations into online scams and fraud. Investigations were commenced into the vast majority of reports received and handled by the team.

Figure 21 Number of cybercrime investigations commenced, WAPOL, by quarter



Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

Senior police representatives reported several concerns regarding ACORN reports that impacted on investigations (as well as intelligence activity). An influx of reports results from the ACORN has placed a strain on the relatively small number of dedicated cybercrime intelligence analysts and investigators. As expected, resources have been further stretched by an increase in low-level reports that are unlikely to lead to resolutions, while this also acts as a disincentive for police in LACs. Low-level cybercrime is defined as the incidents that are small in monetary value, such as issues with buying and selling through online distribution websites like eBay and

Gumtree, but which can take up substantial investigation time and resources. The extent to which these low-level crimes are investigated, and thresholds for deciding whether to investigate, varied between agencies and business areas.

There was some acknowledgement that ACORN had assisted to link reports and identify offenders who were responsible for multiple low-level offences with a significant combined value. There were some notable examples of where this had aided with investigations, such as the GoPro case (see below). However, police also identified examples of where the ACORN had not assisted to link related reports, and where investigators who had commenced an investigation in one jurisdiction were not notified of reports having been grouped and referred to another police partner agency.

This was partly caused by the inconsistency of reports supplied by members of the public. There was also some concern about the quality and reliability of the information reported to ACORN, because reports are made directly by the general public. The information collected by ACORN is dependent on the general public's knowledge of cybercrime and technology in general. ACORN reports could also be exaggerated or malicious and not necessarily criminal, and may also be influenced by the broad definitions and understanding of cybercrime. Investigators may be required to seek additional information from the person making the report (assuming they don’t make an anonymous report) before a decision can be made regarding what action to take (eg further investigation). This impacts on the willingness of officers to commence investigations, but also the likelihood that expected benefits in terms of quicker enforcement action would be realised.

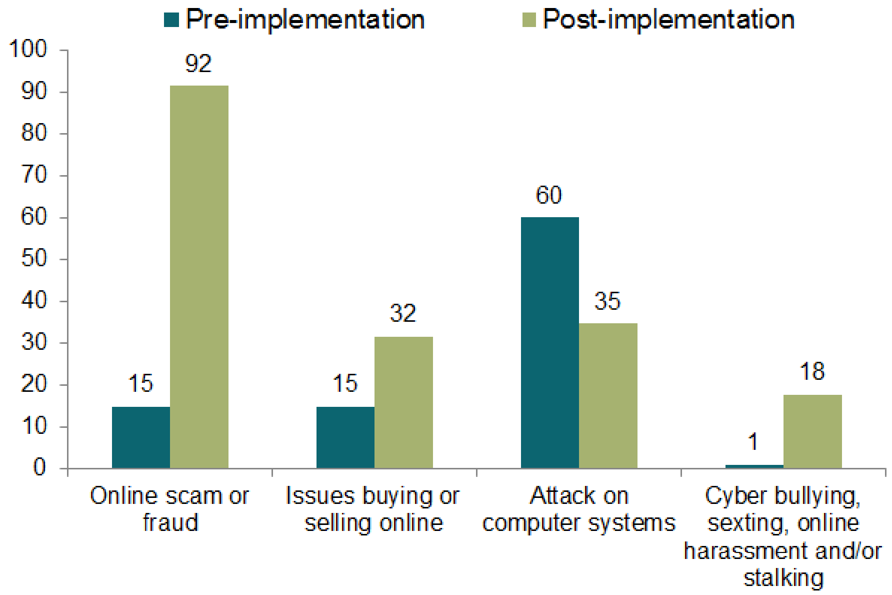
Resources allocated to cybercrime investigations

The improved accessibility of cybercrime data and the automated grouping and referral of reports was expected to have flow on benefits for investigators. Specifically, the ability to progress investigations more quickly due to the amount of information available from public reports made using the ACORN and the accessibility and automated referral of grouped reports. The degree to which this has occurred was difficult to properly assess, given the referral models adopted by NSWPF and QPS and the focus of the evaluation on specialist units.

What is apparent, however, is that the ACORN has resulted in a significant increase in resources being allocated to cybercrime investigations. Information on the number of cybercrime investigators and the average time spent per investigator per week within specialist units was supplied by NSWPF and WAPOL. Data were not available from QPS for the whole of the observation period. The pre-implementation period—the September 2014 quarter before the launch of the ACORN—was compared with the post-implementation period—the average of the four quarters up to September 2015. Importantly, this excludes the time spent by investigators outside of the centralised specialist units which, given the referral model in place in NSWPF, may be significant.

Results for the NSWPF Fraud and Cybercrime Squad are presented in Figure 22. While the average number of investigator hours per week appeared to decline for attacks on computer systems, there were significant increases for the remaining three cybercrime types. In particular, there was a six-fold increase in the amount of time spent investigating online scams and fraud, and investigators spent 18 hours per week investigating cyber bullying, sexting, online harassment and stalking, compared with just one hour prior to the implementation of the ACORN.

Figure 22 Average NSWPF Fraud and Cybercrime Squad investigator hours per week, by cybercrime type, pre- and post-implementation of the ACORN

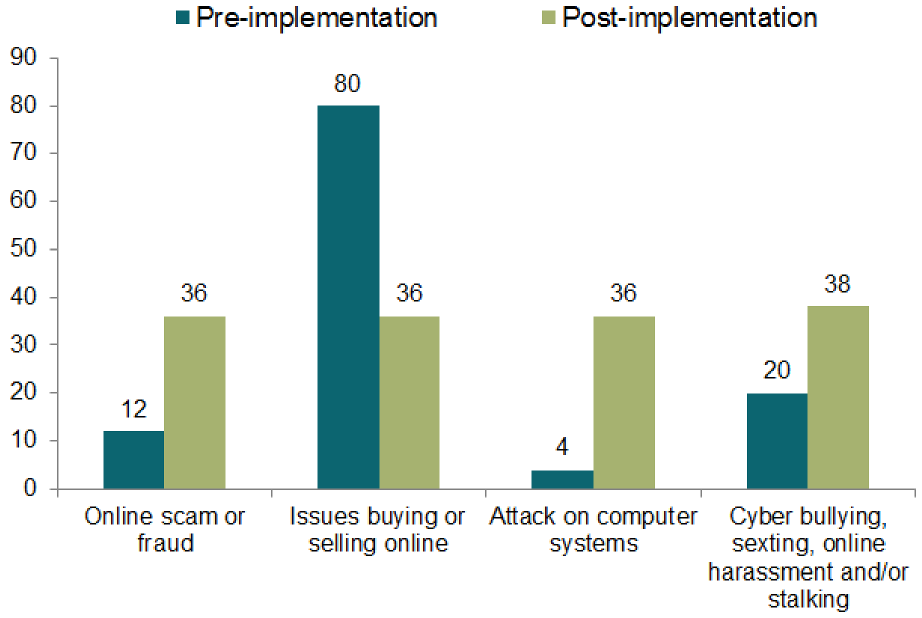


Pre-implementation period refers to July-September 2014. Post-implementation period represents average number of reports per quarter in 12 months to September 2015

Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

Results for the WAPOL Technology Crime Investigation team are presented in Figure 23. While the average number of investigator hours per week declined by around half for issues buying and selling online, there were significant increases for the remaining three cybercrime types. There was a three-fold increase in the number of hours spent investigating online scams and fraud, a nine-fold increase in the time spent investigating attacks on computer systems, and a doubling of the amount of time spent by investigators per week investigating cyber bullying, sexting, online harassment and stalking.

Figure 23 Average WAPOL Technology Crime Investigation team investigator hours per week, by cybercrime type, pre- and post-implementation of the ACORN



Pre-implementation period refers to July-September 2014. Post-implementation period represents average number of reports per quarter in 12 months to September 2015

Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

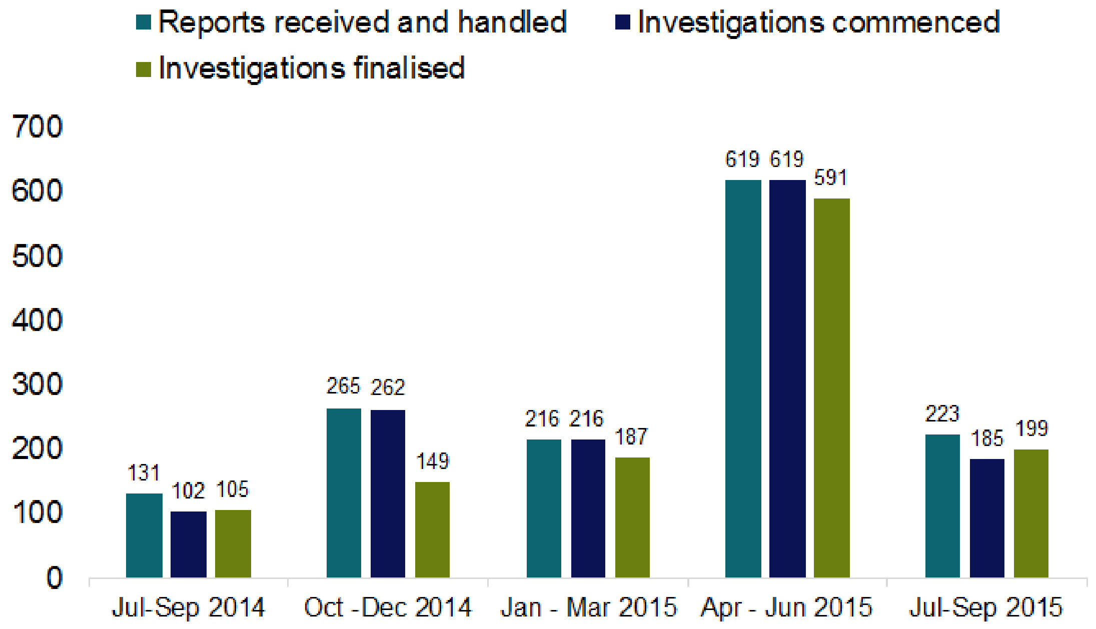
Together, these data suggested that the ACORN has contributed to increased resourcing for cybercrime investigations, at least within centralised specialist areas responsible for investigating cybercrime. Whether this reflects an increase in productivity is more difficult to assess, given not all investigations are conducted by these specialist areas. Nevertheless, a shift towards greater resourcing for cybercrime investigations is a positive outcome and, at least to some extent, something the ACORN set out to achieve. As has been described elsewhere, police reported still being significantly under resourced, primarily because of the sheer volume of reports they had received, and some of the administrative burden borne by investigators in handling these reports.

Investigation outcomes

Improved quality of information, coupled with the grouping and automated referral of reports, was expected to lead to quicker enforcement action and, as a result, action being taken against a greater number cybercrime targets. In the absence of a method for following individual investigations, particularly in light of the referral models operated by NSWPF and QPS, this is somewhat difficult to assess.

There have been examples of successful outcomes resulting from the grouping of reports to the ACORN and ability to identify patterns of offences. One of the more widely cited successes is the GoPro case, whereby dozens of consumers had been defrauded of the costs associated of a GoPro device bought online, but never received the item they had purchased. Individual financial losses were relatively small, but the collective loss was worth more than $20,000. By combining the information provided by individual complainants, the ACORN assisted police to identify, apprehend and successfully prosecute an offender.

Figure 24 Cybercrime reports received and investigations commenced and finalised, WAPOL Technology Crime Investigation



Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

In practice, however, the ACORN is able to assist investigators, but not overcome, the challenges associated with investigating cybercrime. Figure 24 presents the results from the analysis of data provided by WAPOL on investigations finalised, along with the number of reports received and handled and investigations commenced. As with before, WAPOL were able to provide the most accurate data on the finalisation and outcomes of investigations because they are largely managed by a central team. Noting that investigations commenced in one quarter could be finalised in another, there appears to be little attrition in terms of the number of investigations that are finalised.

However, further analysis of the outcomes of finalised investigations is presented in Table 21. This shows that, unlike in the September 2014 quarter prior to the implementation of the ACORN, several investigations had resulted in an offender being identified and, in some cases, apprehended. However, this represented less than one percent of all investigations. The proportion of investigations that were finalised and referred to another business area or agency had declined slightly, although (as previously reported) the average number of referrals per quarter had doubled. Most importantly, however, was that the proportion of investigations finalised where there was no further action because no offence had occurred had nearly doubled (64% c/f 37%), while there was a five-fold increase in the number of investigations per quarter with this outcome. Although the proportion of investigations that resulted in no further action due to insufficient evidence declined, the actual number of investigations per quarter with this outcome also increased by 1.5 times.

Table 21 Outcome of finalised investigations, WAPOL

	Pre-implementation		Post-implementation	
	n	%	n	%
Investigation finalised but no further action – no offence occurred	39	37	721	64
Investigation finalised but no further action – insufficient evidence	55	52	317	28
Investigation finalised and incident referred to another business area or agency for further investigation	11	10	83	7
Investigation finalised and offender identified but no arrest made	0	0	3	<1
Investigation finalised and resulted in the arrest of an offender	0	0	2	<1
Investigations finalised	105	100	1126	100

Source: ACORN quarterly monitoring tool (enforcement), 1 July 2014—30 September 2015 [data file]

These data on enforcement activity highlight the challenges of investigating cybercrime. Very few finalised investigations resulted in an offender being apprehended. A large proportion were subject to a preliminary assessment or investigation and found to have insufficient evidence to proceed any further, or an offender was identified but not arrested. None of the police agency partners identified having been involved in a joint investigation with another agency. However, a substantial number of investigations resulted in the matter being referred to another agency or jurisdiction for further investigation.

The reasons for this are varied, but reflect the barriers to conducting cybercrime investigations that have been identified in previous research. For example, interview participants regularly reported that a significant obstruction to developing an effective response to cybercrime was the lack of available resources. In comparison with other crime types, the cybercrime portfolios of all the agencies that participated in this evaluation were said to be small. There was also a perception that each law enforcement agency is different in its capacity to respond to cybercrime. Some jurisdictions reportedly have greater resources or technical skills and are better placed to address cybercrime than others.

According to the representatives from police partner agencies, a related barrier for effective enforcement is the lack of specialisation in policing. Rotation policies require individuals to exit a unit, including cybercrime units, for career progression after a few years of experience. Retraining new staff impacts on both the efficiency and effectiveness of the enforcement response. There are a number of officers who have spent considerable time within the cybercrime area (or have related experience, such as fraud), while others may spend a short period of time working in the area.

Jurisdictional issues were a recurring theme throughout the interviews. Cybercrime offending is not limited by borders as the offender does not require a physical proximity to victims. A large proportion of cybercrime offenders reside outside Australia, or in a different state to the victim. This presents a major challenge to investigators, and is something that is frequently encountered with investigations involving multiple jurisdictions. Often the victim has no idea where the offender originated from, meaning the agency to which the incident was reported must commence an investigation, often only to discover the offender was in fact based in another jurisdiction (in which case the matter must be referred to that jurisdiction). While there is a general policy for offences to be referred to the jurisdiction in which the offender resides, interview participants reported that acceptance of those referrals can still be decided by investigators or according to state based referral rules. The ACORN has greatly assisted with improving communication and collaboration between the business area in each police partner agency with responsibility for cybercrime; however, while it has assisted with directing reports, the ACORN has not on its own been able to remove the logistical barriers associated with cross-jurisdictional investigations.

Prevention and education

The fourth objective of the ACORN was to provide users with general and targeted educational advice. Providing this advice was expected to increase awareness of the strategies that can be taken to reduce the risk of cybercrime victimisation, increase the use of these strategies and, in-turn, reduce repeat victimisation among those individuals who report to the ACORN. While out of scope for the current evaluation, there was also a view that the ACORN may result in a more generalised reduction in cybercrime vulnerability as a result of members of the public taking preventative action in response to the general prevention advice.

This component of the evaluation assessed the extent to which ACORN users have accessed and read the general and targeted advice available through the ACORN, whether they have implemented any prevention strategies as a result, and perceived vulnerabilities to cybercrime. Repeat victimisation rates among victims of cybercrime who reported to the ACORN have also been assessed to help understand the impact of the ACORN's general and targeted educational advice.

General and targeted prevention advice

The ACORN provides users with access to two forms of prevention advice. General prevention advice is available to all users from the ACORN homepage, and includes a range of information for individuals on how to prevent and protect against cybercrime, including protecting children online, computer security, advice on online shopping, and advice on how to keep personal information protected and staying safe on social media. This includes links to external sources of information and, where appropriate, alternative methods of reporting. In addition, there is information on financial and emotional support available to victims of cybercrime incidents.

Around one in four users (27%) reported having accessed the general prevention advice at any time (Table 22). This was highest among victims of cyber bullying, sexting, online harassment and stalking (37%). Three quarters (74%) of the users who reporting having accessed the general prevention advice did so in the three months after submitting a report, around 14 percent had accessed the general prevention advice in the three months before submitting a report, and the remaining 12 percent had accessed it at some other time. These results suggest that the general prevention advice may offer greater potential as a mechanism to reduce repeat victimisation. It's worth noting, however, that these results do not include users who may have accessed the prevention advice but have not been a recent victim of cybercrime.

Table 22 Reading the ACORN's general prevention advice, by cybercrime type

	Online scams or fraud (n=940)		Issues buying and selling online (n=265)		Attacks on computer system (n=155)		Cyber bullying, sexting, online harassment and/or stalking (n=122)		All reports to the ACORN (n=1,482)	
	n	%	n	%	n	%	n	%	n	%
Reported visiting the ACORN to access general prevention advice at any time	250	24	66	25	42	27	45	37	403	27
When victims accessed general prevention advice[a]										
3 months before submitting report	25	11	8	13	6	15	12	29	51	14
3 months after submitting report	178	78	45	73	27	69	24	59	274	74
Some other time	25	11	9	15	6	15	5	12	45	12

a: Proportions are of those victims who accessed the general prevention advice, not total victims. Excludes cases with missing data, including respondents who had accessed general prevention advice but did not specify when

Percentages may not equal 100 due to rounding.

Source: ACORN Victim Survey [AIC data file]

Table 23 Feedback on the ACORN’s general prevention advice, by cybercrime type

	Online scams or fraud (n=250)[a]		Issues buying and selling online (n=66)[a]		Attacks on computer system (n=42)		Cyber bullying, sexting, online harassment and/or stalking (n=45)[a]		All reports to the ACORN (n=403)[a]	
	n	%	n	%	n	%	n	%	n	%
I understood the prevention advice provided by the ACORN	225	93	53	83	37	88	42	93	357	89
The prevention advice provided by the ACORN was relevant to my circumstances	164	68	36	58	20	49	23	51	243	57
The prevention advice provided by the ACORN was useful	193	79	40	63	30	71	29	64	292	69
I was satisfied with the prevention advice provided by the ACORN	178	74	37	60	24	57	24	56	263	62
I feel confident that the prevention strategies recommended by the ACORN will reduce my risk of becoming a victim of cybercrime	175	72	36	57	25	60	22	49	258	60
I would recommend the ACORN website to my friends or family for cybercrime prevention advice	191	79	44	70	31	74	30	67	296	73

a: Excludes cases with missing data

Proportions are of those victims who read the general prevention advice, not total victims.

Source: ACORN Victim Survey [AIC data file]

The majority of ACORN users (87%) reported that the general prevention advice was understandable, with little variation across offence types (Table 23). Fifty-seven percent of all ACORN users reported that the general prevention advice provided by the ACORN was relevant to their circumstances. Around two thirds of all ACORN users reported the general prevention advice as being useful (69%), while 60 percent of users reported feeling confident the recommended strategies could help reduce the risk of victimisation and 62 percent were satisfied with the advice. Overall, victims of online scams or fraud provided the highest ratings for the quality of general prevention advice. Victims of cyber bullying, sexting, online harassment or stalking were least likely to report being confident that the strategies recommended would reduce their risk of victimisation. Three quarters of all ACORN users (between 67 and 79 percent, depending on cybercrime type), would recommend the ACORN to family or friends for cybercrime advice.

ACORN users who report a cybercrime incident are also able to access targeted prevention advice, which relates specifically to the type of cybercrime reported by the user. This information is available once the report has been submitted, and aims to help the user reduce their risk of repeat victimisation.

Around three quarters of victims who reported to the ACORN, both in general and across all four offence types, read the targeted prevention advice at the time of submitting a report (Table 24). Among those who saw the advice but did not read it, the most common reason was that they did not think it would help (41%) (Table 25). Around one third reported that they did not have the time to read the advice (32%), while 21 percent did not think it was relevant. Once small numbers were taken into account, there was little difference between the categories of cybercrime.

Table 24 Reading the ACORN's targeted prevention advice, by cybercrime type

	Online scams or fraud (n=940)		Issues buying or selling online (n=265)		Attacks on computer system (n=155)		Cyber bullying, sexting, online harassment and/or stalking (n=122)		All reports to the ACORN (n=1,482)	
	n	%	n	%	n	%	n	%	n	%
Read the advice	689	74	199	76	166	76	88	70	1092	74
Saw but did not read the advice	73	8	23	9	6	4	10	8	112	8
Did not see the advice	165	18	41	16	30	20	27	22	263	18

Only includes numbers and percentages of respondents. Percentages may not equal 100 due to rounding. Excludes cases with missing data

Source: ACORN Victim Survey [AIC data file]

Table 25 Reasons for not reading the ACORN targeted prevention advice, by cybercrime type

	Online scams or fraud (n=73)[a]		Issues buying or selling online (n=23)		Attacks on computer system (n=6)		Cyber bullying, sexting, online harassment and/or stalking (n=10)		All reports to the ACORN (n=112)[a]	
	n	%	n	%	n	%	n	%	n	%
I was too busy or did not have time	25	36	7	30	2	33	1	10	35	32
Did not think it was relevant	15	21	3	13	1	17	4	40	23	21
Did not think it would help	27	39	11	48	3	50	4	40	45	41
It did not look interesting	3	4	2	9	0	0	1	10	6	6

a: Excludes cases with missing data.

Proportions are of those victims who saw the targeted prevention advice but did not read it, not total victims. Only one response could be specified. Percentages may not equal 100 due to rounding.

Source: ACORN Victim Survey [AIC data file]

Ratings of the quality of targeted prevention advice were similar to those for general prevention advice (Table 26). Nine in ten (91%) of users reported being able to understand the prevention advice, while 56 percent of users indicated that the advice was relevant to their circumstances. Almost two thirds of all users reported the targeted prevention advice was useful (62%) and that they were satisfied with the advice provided (61%). The proportion of users who reported feeling confident that the strategies recommended as part of the targeted prevention would help reduce their risk of becoming a victim of cybercrime was significantly lower than for the general prevention advice (48% c/f 61%). The lowest overall ratings were provided by victims of cyber bullying, sexting, online harassment and/or stalking, who were much less likely to report the targeted prevention advice as being relevant (38%), useful (48%), or that they were satisfied with the advice (47%). Around one third of victims of cyber bullying, sexting, online harassment and/or stalking who reported an incident to the ACORN and received targeted prevention advice felt confident that the strategies recommended would help reduce their risk of becoming a victim (or repeat victim) of cybercrime.

Table 26 Feedback on the ACORN's targeted prevention advice, by cybercrime type

	Online scams or fraud (n=689)		Issues buying or selling online (n=199)		Attacks on computer system (n=116)		Cyber bullying, sexting, online harassment and/or stalking (n=88)		All reports to the ACORN (n=1,092)	
	n	%	n	%	n	%	n	%	n	%
I understood the prevention advice provided by the ACORN	619	92	178	90	105	93	77	89	979	91
The prevention advice provided by the ACORN was relevant to my circumstances	427	64	114	58	68	62	33	38	642	56
The prevention advice provided by the ACORN was useful	460	69	117	59	80	73	41	48	698	62
I was satisfied with the prevention advice provided by the ACORN	465	69	124	63	74	65	40	47	703	61
I feel confident that the prevention strategies recommended by the ACORN will reduce my risk of becoming a victim of cybercrime	401	60	103	53	55	49	26	31	585	48

Proportions are of those victims who read the targeted prevention advice, not total victims.

Source: ACORN Victim Survey [AIC data file]

Given that little can be done in response to most cybercrimes, stakeholders argued that the ACORN's capacity to educate and promote prevention strategies should be increased. Currently, educational material on the ACORN website is not updated and does not include information on current scams and frauds. It was noted that this is important in order for the educational material provided by the ACORN to be useful. Police recommended that when a particular scam or fraud is identified the public should be advised on the ACORN website. Resources and parties responsible for collecting and updating the educational material on the ACORN website should also be identified in order to facilitate this.

Use of cybercrime prevention strategies

For the educational advice available on the ACORN to contribute to a reduction in repeat victimisation, victims who report to the ACORN must take action in response to the information provided. It is not enough for them to just read the information. Respondents to the survey of ACORN users were therefore also asked to identify whether they had started using the strategies recommended as part of the targeted prevention advice, or used these strategies more frequently, in the three months since submitting their report. The recommended strategies vary for each type of cybercrime, therefore respondents were asked about the prevention strategies recommended by the ACORN for the cybercrime type they reported.

The results for victims of online scams and fraud are presented in Table 27. Overall, 70 percent of victims of online scams or fraud reported having started using or using more frequently at least one prevention strategy since having submitted a report to the ACORN. The most common strategies used or used more frequently were choosing strong passwords (37%), exercising caution when clicking on unexpected or unfamiliar links (36%), only responding to emails from known individuals (34%), regularly changing passwords (33%), not replying to or forwarding certain messages (32%) and reviewing bank and card statements regularly (30%). All strategies except making use of biometric passwords (8%) were used or used more frequently by at least one in five victims.

Table 27 Victims of online scams and fraud who reported starting to use recommended prevention strategies since making the report, or using the strategies more frequently than before (n=689)

	n	%
Choose strong passwords	244	37
Exercise caution when clicking on unexpected or unfamiliar links	239	36
Only respond to e-mails from people I know personally	228	34
Change passwords regularly	217	33
Not replying to or forwarding suspicious or unsolicited messages	211	32
Review bank and credit card statements regularly	196	30
Seeking independent advice before sending money to an unknown person or organisation	191	29
Read terms and conditions carefully	182	28
Ensure device operating system is up to date	175	27
Spam filters	167	26
Protect my computer with anti-virus software	171	26
Disable remote access on computer	159	25
Use a firewall to block unauthorised access	155	24
Not sending money to people I do not know	154	23
Not providing my banking details to untrusted sites	154	23
Transaction limits on credit cards	146	22
Make use of biometric passwords (e.g. fingerprints or facial recognition)	53	8
At least one prevention strategy	454	70

Proportions are of those victims who read the targeted prevention advice, not total victims. Respondents could identify more than one option.

Source: ACORN Victim Survey [AIC data file]

Nearly two thirds of all victims of issues buying or selling online reported having started using or using more frequently at least one prevention strategy since having submitted a report to the ACORN (Table 28). The most common strategy used or used more frequently was relying on trusted and reliable online selling platforms (44%).This was followed by not sending money to people they didn’t know (38%), using a secure payment method (37%), and keeping personal details private and secure (34%). All strategies were used for the first time or used more frequently by at least one in five victims.

Table 28 Victims of issues buying and selling online who reported starting to use recommended prevention strategies since making the report, or using the strategies more frequently than before (n=199)

	n	%
Use trusted and reliable selling platforms	83	44
Not sending money to people I do not know	75	38
Use a secure payment method	71	37
Keep personal details private and secure	65	34
Not providing my banking details to untrusted sites	49	25
Review bank and credit card statements regularly	47	24
Only respond to e-mails from people I know personally	47	24
Transaction limits on credit cards	42	22
At least one prevention strategy	121	63

Proportions are of those victims who read the targeted prevention advice, not total victims. Respondents could identify more than one option.

Source: ACORN Victim Survey [AIC data file]

Table 29 Attacks on computer system victims who reported starting to use recommended prevention strategies since making the report, or using the strategies more frequently than before (n=116)

	n	%
Choose strong passwords	53	47
Exercise caution when clicking on unexpected or unfamiliar links	51	46
Change passwords regularly	36	34
Ensure device operating system is up to date	36	33
Keep software current with the latest patches and updates	34	30
Protect my computer with anti-virus software	30	27
Spam filters	29	27
Use reputable websites and mobile applications	30	27
Securing wireless networks and being careful when using pubic wireless networks	29	26
Use a firewall to monitor ingoing and outgoing information and block unauthorised access	27	25
Use a pop-up advertising blocker on internet browser	26	24
Make use of biometric passwords (e.g. fingerprints or facial recognition)	10	9
At least one prevention strategy	70	64

Proportions are of those victims who read the targeted prevention advice, not total victims. Respondents could identify more than one option.

Source: ACORN Victim Survey [AIC data file]

Sixty-four percent of victims of attacks on computer system started using, or increased the frequency with which they used, at least one prevention strategy in the three months since submitting their report (64%) (Table 29). Almost half reported using stronger passwords (47%) and exercising caution when clicking on certain links (46%). Around a third reported changing their passwords regularly (34%), and ensuring their operating system (33%) and software (30%) were updated. With the exception of biometric passwords (9%), the remaining strategies were used, or used more often, by around one quarter of victims.

Finally, victims of cyber bullying, sexting, online harassment and/or stalking were the least likely group to report having started using, or using more frequently, at least one prevention strategy (45%; Table 30). There were a limited number of specific strategies recommended as part of the targeted prevention advice; however, increasing security settings when using social media (37%) and blocking, removing or 'unfriending' users from social media (28%) were the strategies used most frequently.

Table 30 Cyberbullying, sexting, online harassment and/or stalking victims who reported starting to use recommended prevention strategies since making the report, or using the strategies more frequently than before (n=88)

	n	%
Increasing security settings when using social media	31	37
Blocking, removing or unfriending users from social media	23	28
Blocking senders from mobile phone	16	20
Installing filters, parental controls and safe searching modes	11	13
Changing mobile number	4	5
At least one prevention strategy	37	45

Proportions are of those victims who read the targeted prevention advice, not total victims. Respondents could identify more than one option.

Source: ACORN Victim Survey [AIC data file]

Risk of repeat victimisation

To assess levels of repeat victimisation, and to understand the impact of the ACORN on the risk of repeat victimisation, a number of questions about subsequent episodes of victimisation were included in the survey of ACORN users (Table 31). Overall, one in five victims who reported to the ACORN were a victim of a subsequent incident of the same cybercrime type in the three months following their report (19%). There was considerable variation between cybercrime types, with repeat victimisation rates ranging from four percent for online scams and fraud up to 47 percent for victims of cyber bullying, sexting, online harassment and/or stalking.

Respondents were also asked to indicate what action they had taken in response to this subsequent incident. Half (52%) of all victims who had a subsequent episode of victimisation indicated that they reported that incident to someone. Repeat victims of attacks on computer systems were the least likely to report the incident to another person or organisation (29%). Less than one third of ACORN users who experienced further investigation in the three months after making a report reported the latest incident to police, either by phone, in person or via the ACORN. Half of all repeat victims of cyber bullying, sexting, online harassment and/or stalking reported the most recent incident to police, while just 14 percent of victims of attacks on computer systems did the same.

Most importantly, overall rates of reporting repeat victimisation to the ACORN were relatively low, irrespective of the type of cybercrime experienced. One in six ACORN users who were a repeat victim in the three months after submitting the original report reported the subsequent and most recent incident to the ACORN. This was highest again among victims of cyber bullying, sexting, online harassment and/or stalking (27%). Fifty five percent of repeat victims who reported the most recent incident to police reported the incident through the ACORN.

Table 31 Repeat victimisation and reporting rates among ACORN users in the three months after reporting to ACORN

	Victim		Reported the most recent incident[a]		Reported the most recent incident to police[ab]		Reported the most recent incident to ACORN[a]	
	n	%	n	%	n	%	n	%
Online scams or fraud	37	4	21	57	10	27	5	14
Issues buying or selling online	15	5	9	60	3	20	2	13
Attacks on computer system	35	20	10	29	5	14	3	9
Cyber bullying, sexting, online harassment and/or stalking	66	47	41	62	33	50	18	27
Overall cybercrime	153	19	81	52	51	28	28	16

a: Proportions are of total victims, not total survey respondents.

b: Includes reporting to the ACORN, police by phone, in person, using a police website or via Crimestoppers.

Source: ACORN Victim Survey [AIC data file]

Finally, the repeat victimisation rates for those users who had read the general and targeted prevention advice were competed with those users who had neither seen nor read the advice to determine what impact, if any, the ACORN educational material has had on the risk of cybercrime victimisation. The results for general prevention advice are presented in Table 32. Repeat victimisation rates were higher among victims who had accessed the general prevention advice for victims of online scams or fraud (6% c/f 3%), issues buying and selling online (16% c/f 8%) and cyber bullying, sexting, online harassment and/or stalking (68% c/f 46%). Consistent with the findings presented earlier that most users accessed the general prevention advice after submitting their original report, these results suggest that many ACORN users access the general prevention advice in response to repeat victimisation.

Table 32 Repeat victimisation in the three months after reporting, by whether the user read the ACORN general prevention advice

	Read prevention advice		Did not read prevention advice[a]	
	n	%	n	%
Online scams or fraud[b]	14	6	21	3
Issues buying or selling online	10	16	15	8
Attacks on computer systems[b]	9	22	25	24
Cyberbullying, sexting, online harassment and/or stalking	30	68	36	46

a: Includes respondents who did not see the advice and those who saw the advice but did not read it.

b: Excludes cases with missing data

Proportions are of those victims who reported cybercrime victimisation subsequent to reporting to the ACORN, not total victims.

Source: ACORN Victim Survey [AIC data file]

With the exception of computer system attacks, where those who had read the targeted prevention advice were more likely to report having been a repeat victim (25% c/f 17%), there was little difference in the repeat victimisation rates for those ACORN users who had read the targeted prevention advice and those who did not (Table 33). Repeat victimisation rates for online scams and fraud (4% c/f 5%), issues buying and selling online (10% c/f 10%) and cyber bullying, sexting, online harassment and/or stalking (52% c/f 49%) were similar for both groups. These results suggest that the targeted prevention advice has had little impact on the rates of repeat victimisation among victims who report to the ACORN.

Table 33 Repeat victimisation in the three months after reporting, by whether the user read the ACORN targeted prevention advice

	Read prevention advice		Did not read prevention advice[a]	
	n	%	n	%
Online scams or fraud	25	4	12	5
Issues buying or selling online	19	10	6	10
Attacks on computer systems	28	25	6	17
Cyberbullying, sexting, online harassment and/or stalking[b]	45	52	18	49

a: Includes respondents who did not see the advice and those who saw the advice but did not read it.

b: Excludes cases with missing data

Proportions are of those victims who reported cybercrime victimisation subsequent to reporting to the ACORN, not total victims.

Source: ACORN Victim Survey [AIC data file]

Conclusion

The ACORN was launched by the Commonwealth government in November 2014 as a tool to assist members of the public to report certain types of cybercrime to law enforcement agencies. ACORN had four key objectives:

- to provide a centralised, national online facility that would receive reports from members of the public;
- to refer reports to the police and regulatory agencies for further consideration;
- to collect and aggregate data from reports to assist police, regulatory and other government agencies to develop improved strategic and tactical responses to cybercrime; and
- to provide ACORN users with general and targeted educational advice.

These largely process-oriented objectives were the subject of a detailed evaluation by the AIC, which employed a range of research methods to explore the extent to which the objectives were met.

On the whole, it is possible to conclude that the objectives have been met. A centralised, national online facility was established in November 2014 and over 65,000 reports had been received by the system by June 2016 (objective one). Sixty percent of victims who submitted a report to the ACORN were satisfied with the process of reporting. In addition, in 2015-16 nearly three quarters of reports made to the ACORN were automatically referred to police and regulatory agencies for further consideration, with the number of referred reports increasing over the period of the evaluation (objective two).

The introduction of the ACORN has, for the most part, resulted in an increase in the number of intelligence products generated by law enforcement agencies, as well as an increase in the number of investigations targeting cybercrime related issues (objective three). This has been achieved as a result of a significant increase in resources being directed towards cybercrime by law enforcement agencies. In this sense, the ACORN would appear to have been successful at leveraging additional law enforcement resources to focus on cybercrime. The ACORN has also provided both general and targeted educational advice, which has been well received by a significant proportion of those users who viewed the material (objective four).

While these objectives may have been achieved, the evaluation highlighted a number of issues of concern which (at least partly) stem from the separation of roles between receiving and acting on reports of cybercrime. While the Commonwealth has been responsible for developing and administering the ACORN as a reporting tool, it has largely been the responsibility of state and territory policing agencies to receive, handle and act upon the information received. Although the ACORN has been made available to the Australian public, it continues to have relatively low levels of awareness and there is evidence to suggest that publicity to raise the profile of the ACORN resulted in only a short-lived increase in reports. Most victims of cybercrime continue to find alternative means of reporting an incident, rather than through the ACORN. However, awareness of the ACORN does appear to improve the perception that the Commonwealth government is proactively addressing cybercrime.

This last finding is at odds with the finding that less than a third of those reporting to the ACORN are satisfied with the outcome of their report. This level of satisfaction varies according to the actual outcome of the report and, in particular, the level of contact ACORN users have with a law enforcement agency. Indeed, a quarter of those reporting to the ACORN believed they had not been notified that their report had been received, and only four percent of this group were satisfied with the outcome. In contrast, 71 percent of those that were notified that their report had been received, investigated and action taken were satisfied with the outcome. This serves to highlight the importance of two things. First, the need to manage the expectations of people reporting to the ACORN and second, the important role of communication with ACORN users following a report of a cybercrime.

The level of satisfaction with the outcome is also a function of the level of resources and activity of state and territory policing agencies. While resources have increased, these have in some cases been focused on administering reports from the ACORN, rather than on intelligence production or investigation. The sheer volume of reports that have been referred to some police agency partners means that they must handle many more reports than before. This has created backlogs and, as a result, delays before investigations can commence. While certain cases will attract more immediate attention because of the risk they pose to victims or the prospect of a positive investigation outcome, many victims have been left waiting without an obvious resolution to their case. As a result, there is a significant proportion of victims with heightened expectations that their case will be investigated who are ultimately disappointed by the outcome of engaging with the ACORN.

This evaluation has shown that, while the ACORN has met its objectives from a process perspective, there remain problems for both victims of cybercrime and law enforcement agencies that engage with the system. As a relatively new system, and innovative approach to encouraging victims to report crime to police, there is both an opportunity and imperative to address the challenges highlighted in this report so that they do not have a negative impact on the reputation of the system in future.

References

Action Fraud 2014. About us. http://www.actionfraud.police.uk/about-us

Alarid LF & Novak KJ 2008. Citizens' views on using alternate reporting methods in policing. Criminal Justice Policy Review 19:25-38

Attorney-General's Department 2009. Cyber security strategy. Canberra: Attorney-General's Department. http://www.ag.gov.au/RightsAndProtections/CyberSecurity/Documents/AG%20Cyber%20Security%20Strategy%20-%20for%20website.pdf

Attorney-General's Department 2013. National plan to combat cybercrime. Canberra: Attorney-General's Department. http://www.ag.gov.au/CrimeAndCorruption/Cybercrime/Documents/National%20Plan%20to%20Combat%20Cybercrime.pdf

Australian Bureau of Statistics 2012. Personal Fraud Survey 2010-2011. http://www.abs.gov.au/ausstats/abs@.nsf/PrimaryMainFeatures/4528.0

Australian Competition & Consumer Commission 2014. About SCAMwatch. http://www.scamwatch.gov.au/content/index.phtml/tag/scamAboutUs/

Broadhurst R 2006. Developments in the global law enforcement of cybercrime. Policing: An International. Journal of Police Strategies & Management 29(3): 408-433

Broadhurst R Grabosky P Alazab M & Chon S 2014. Organizations and cyber crime: An analysis of the nature of groups engaged in cyber crime. International Journal of Cyber Criminology 8(1): 1-20

Brown, R. and Evans, E. (2014) Determinants of complainant satisfaction with agency responses to anti-social behaviour. Crime Prevention and Community Safety Journal 16(2): 105–127

CERT Australia 2012. Cyber crime & security report 2012. CERT Australia

http://www.canberra.edu.au/cis/storage/Cyber%20Crime%20and%20Security%20Survey%20Report%202012.pdf

Ekblom P & Heal K 1982. The police response to calls from the public. Research and Planning Unit Paper no. 9. London: Home Office

FitzGerald, M., Hough, M., Joseph, I. and Qureshi, T. (2002) Policing for London. Collumpton, Devon: Willan Publishing.

Hunton P 2010. Cybercrime and security: A new model of law enforcement investigation. Policing 4(4): 385-394

Hunton P 2011a. A rigorous approach to formalising the technical investigation stages of cybercrime and criminality within a UK law enforcement evaluation. Digital investigation 7: 105-113

Hunton P 2011b. The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. Computer Law & Security Review 27:61-67

Hunton P 2012. Managing the technical resource capability of cybercrime investigation: a UK law enforcement perspective. Public Money & Management 32(3): 225-232

Iriberri A 2013. E-government services: design and evaluation of crime reporting alternatives. Electronic Government, an International Journal 10(2): 171-188

Johnson M 2013. Cybercrime: Treats and solutions. London: Ark Group

Kellermann T 2010. Building a foundation for global cybercrime law enforcement. Core Security Technologies. http://www.coresecurity.com/files/attachments/CFS_2010-05_May.pdf

Lasley JR 1995. When crime reporting goes high-tech: An experimental test of computerized citizen response to crime. Journal of Criminal Justice 23(6): 519-529

Levi M & Williams ML 2013. Multi-agency partnerships in cybercrime reduction. Information Management & Computer Security 21(5): 420-443

Skogen, W. (2005) Citizen Satisfaction with Police Encounters. Police Quarterly. Vol. 8, No. 3, pp. 298-321.

Standing Committee on Communications 2010. Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime. The report of the inquiry into Cyber Crime. The Parliament of the Commonwealth of Australia .http://www.aph.gov.au/parliamentary_business/committees/house_of_representatives_committees?url=coms/cybercrime/report/full_report.pdf

Symantec 2014. 2013 Norton Report. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013

The Internet Crime Complaint Center 2014. About us. http://www.ic3.gov/about

United Nations Office on Drugs and Crime 2013. Comprehensive study on cybercrime draft February 2013. Vienna: UNODC. http://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf

Urbas G 2012. Cybercrime, jurisdiction and extradition: The extended reach of cross-border law enforcement. Journal of Internet Law 16(1): 1,8-17