CRIMINOLOGY
RESEARCH GRANT

Responding to cybercrime: Perceptions and need of Australian police and the general community

Cassandra Cross
Thomas Holt
Anastasia Powell
Michael Wilson

Report to the Criminology Research Advisory Council Grant: CRG 23/16–17

August 2021

This project was supported by a Criminology Research Grant.

Published by the Australian Institute of Criminology
GPO Box 1936 Canberra ACT 2601
Tel: (02) 6268 7166
Email: front.desk@aic.gov.au
Website: www.aic.gov.au/crg

ISBN: 978 1 922478 21 4 (Online)

This research was supported by a Criminology Research Grant. The views expressed are those of the author and do not necessarily reflect the position of the Criminology Research Advisory Council or the Australian Government.

This report was reviewed through a double-blind peer review process.

Edited and typeset by the Australian Institute of Criminology.

Contents

d

Tables

Acknowledgements

The authors would like to acknowledge the support and assistance of the Queensland Police Service, New South Wales Police Force and Tasmania Police in undertaking this research.

They would also like to thank all cybersecurity/cybercrime professionals who participated in the research through the focus group. Without their collective support and belief in it, the project would not have come to fruition.

The authors would like to thank Jamie-Lee Emmanuel, Rosalie Gillett, Rebecca Layt, Megan Parker, Rahul Sinha Roy and Michael Wilson for their valuable assistance transcribing the focus group.

Cassandra Cross would like to thank all the staff at the Queensland University of Technology's School of Justice for their constant encouragement and mentorship. She extends greatest appreciation to Maxine Brown for her ongoing administrative support of this project.

Thomas Holt would like to thank his wonderful colleagues on this project, because it would not have been possible without their tireless efforts.

Anastasia Powell would like to thank colleagues and support staff in Criminology & Justice Studies at RMIT University and in the Centre for Social and Global Studies.

Michael Wilson would like to thank the academic and administrative staff across Queensland University of Technology's Faculty of Law for providing an environment welcoming to an early career researcher.

This research was funded through a Criminology Research Grant (CRG 23/16–17). The views expressed in this report are solely those of the authors and may not represent the views of the Criminology Research Advisory Council, the Australian Institute of Criminology, the Australian Government or relevant police agencies. Any errors of omission or commission are the responsibility of the authors.

Abbreviations and acronyms

ACCC	Australian Competition and Consumer Commission
ACORN	Australian Cybercrime Online Reporting Network
ACSC	Australian Cyber Security Centre
ICT	Information communications technologies
NSWPF	New South Wales Police Force
PC	Police constable
QPS	Queensland Police Service
QUT	Queensland University of Technology

Abstract

This research examines perceptions of cybercrime among police officers, community members and cybersecurity experts in Australia. It examines how these groups conceptualise the problem of cybercrime and where there is disagreement, as well as identifying opportunities for improvement to both officer capabilities and community awareness about cybercrime risk and prevention. The research draws from a survey of police officers based in Queensland, New South Wales and Tasmania; a survey of adult members of the general Australian community; and a focus group with cybersecurity experts.

The research suggests that police officers and community members are engaged in an ongoing negotiation about their responsibilities in cybercrime investigations and prevention programs. It affirms that an officer's preparedness to investigate cybercrime correlates with their levels of education, previous training, and degree of professional exposure to cybercrime investigations. It suggests that life experiences and sociodemographic characteristics influence perceptions of cybercrime among both police officers and community members, and notes disagreement between police officers and community members about the public's perception of risk related to cybercrime. Overall, the research advocates several recommendations for improving understandings of and responses to cybercrime in Australia.

Executive summary

The increasing importance of digital technologies within social, economic and political life is a source of both opportunity and vulnerability for Australian citizens. This makes cybercrime a strategic priority for government and law enforcement agencies. Previous criminological research suggests that police officers encounter multiple challenges when investigating cybercrime, that citizens have potentially unrealistic expectations about police investigative capabilities, and that victims experience frustration and stigmatisation when reporting a cybercrime incident to authorities. This research contributes to our understanding of the perception of cybercrime within an Australian context and assists decision-makers in developing innovative and effective policy responses.

This report examines perceptions of cybercrime among a diverse population of stakeholders, including police officers, community members and cybersecurity experts in Australia. Specifically, the study is guided by four key research questions. They seek to understand how these groups conceptualise the problem of cybercrime, to explore to what extent they agree and disagree, to identify opportunities for law enforcement agencies to equip officers with investigative capabilities, and to identify opportunities for improving community awareness about cybercrime risk and prevention. The research involves a mixed-method and multi-stage design, including a survey of police officers based in Queensland, New South Wales and Tasmania; a survey of adult members of the general Australian community; and a focus group with cybersecurity experts from government, law enforcement and industry. These results are analysed and triangulated to answer the research questions and develop associated, evidence-based recommendations.

Overall, this report suggests that police officers and community members are engaged in an ongoing negotiation about their responsibilities in cybercrime investigations and prevention programs. The study affirms how an officer's preparedness to investigate cybercrime correlates with their levels of education, previous training and degree of professional exposure to cybercrime investigations. Additionally, the research suggests that life experiences and sociodemographic characteristics structure perceptions of cybercrime among both police officers and community members. Indeed, sociodemographics influence judgements about the seriousness and frequency of cybercrime activity and about whether potential victims can effectively prevent cybercrime victimisation via cybersecurity-protective behaviours. Finally, the study observes that police officers and community members disagree about whether the public accurately appraise and understand the risks of cybercrime.

The knowledge generated through this research has led to the development of evidence-based recommendations for improving government, law enforcement and community responses to cybercrime and cybersecurity threats. These recommendations have been developed to enhance the cybercrime investigative capabilities and quality of victim service provision by law enforcement. They also identify the need to increase community awareness about incident reporting processes, the utility of cybersecurity-protective behaviours and the need to challenge victim-blaming attitudes. The study provides novel contributions to the criminological literature and practical recommendations for policy responses to the problem of cybercrime. It also identifies the potential for further research examining causal relationships and ways in which social interactions influence perceptions of cybercrime among police personnel, community members and cybersecurity experts.

Introduction

Cybercrime is a significant problem for all Australians. The Australian Competition and Consumer Commission (2020: 3) estimates that Australians lost $2.5b to technology-enabled scams between 2009 and 2019. Despite its magnitude, this figure is unlikely to reflect the full extent of harms resulting from cybercrime. Cybercrime has a notoriously low reporting rate. Research suggests that a sizable 'dark figure' of cybercrime eludes detection and measurement because of under-reporting by victims (Kemp, Miró-Llinares & Moneva 2020; Tcherni et al. 2016). Nor does the figure account for non-financial harms experienced by victims, including problems with physical and emotional health, depression and anxiety disorders, relationship breakdown, unemployment, homelessness, loss of reputation and the loss of time spent attempting to recover financial losses (Cross, Richards & Smith 2016; Australian Cyber Security Centre (ACSC) 2015). The consequences of cybercrime and cybersecurity incidents for businesses and governments are also significant and include financial losses, data breaches and reputational damage to organisations (ACSC 2015; Department of Home Affairs 2020).

The severity and diversity of these harms make cybercrime a strategic priority for state and federal governments. In 2013, the Australian Government launched the *National Plan to Combat Cybercrime*, which acknowledged the threat posed by cybercrime and the need to develop effective measures to minimise the 'social and personal risks associated with the use of computers and the internet and the protection of children online' (AGD 2013: 6). The plan defines cybercrime as:

> ...crimes directed at computers or other information communications technologies (ICTs) (such as hacking and denial of service attacks), and crimes where computers or ICTs are an integral part of an offence (such as online fraud, identity theft and the distribution of child exploitation material). (AGD 2013: 4)

This definition encompasses crimes that may only occur within an online environment (such as hacking) and also traditionally offline types of crime (such as fraud and identity theft) that have evolved along with advancements in information technologies.

Changes in the ways crime is committed through the use of technology present distinct challenges for law enforcement agencies (Brenner 2008; Hinduja 2007; Holt, Bossler & Fitzgerald 2010; McQuade 2006; National Institute of Justice 2008; Powell & Henry 2018; Stambaugh et al. 2001; Wall 2001). Further, a number of factors complicate the policing of cybercrime: its cross-jurisdictional nature, inconsistent legislative frameworks, a requirement for technical expertise and resources to investigate and prosecute offenders, and the comparatively low priority afforded to cybercrimes by police (Holt 2018: 143–144; Yar & Steinmetz 2019). There are also technical difficulties associated with investigating offenders who are able to mask their identities and real-world locations through the use of cryptographic technologies such as public key encryption, onion routing and cryptocurrencies (Holt, Bossler & Fitzgerald 2010; Weimann 2016). Finally, the decentralised nature of some forms of cybercrime (such as servers hosting pirated materials or the use of botnets to commit cyberattacks) make them highly resistant to being permanently shut down by law enforcement agencies (Dupont 2017: 101). This highlights the many difficulties encountered by police in effectively investigating cybercrimes.

Australia's cybercrime investigation capabilities

Australian law enforcement agencies are comparatively well equipped for investigating cybercrime. Each jurisdiction has specialised units constituted by officers with skillsets in digital forensics and cybersecurity. The Queensland Police Service (QPS), for example, houses the Financial and Cyber Crime Group (for investigating general cybercrime offences) and Taskforce Argos (for investigating online child exploitation and abuse). However, previous research suggests that the investigative capabilities of general duties officers remains limited, compared with these specialist units, despite the increasing role of digital technologies in the perpetration of traditionally offline crimes (ie computer-enabled crimes). Indeed, social and computer scientists have observed a lack of police training in digital crime scene investigations and associated strategies for preserving the integrity of electronic evidence (Casey 2019: 654; Dodge & Burrus 2019: 339). This shortage of skills among general duties officers is compounded by procedural difficulties with establishing cross-jurisdictional cooperation for the investigation of cybercrime (Willits & Nowacki 2016: 120). Finally, the investigative capabilities of law enforcement are also compounded by the 'problem of going dark', where the use of cryptographic technologies, such as public key encryption and onion routing, enable cybercriminals to mask their real-world identities and locations (Weimann 2016). Evidently, there are significant impediments to successful cybercrime investigations.

d

The Australian Government has attempted to expand the capabilities of law enforcement agencies to investigate cybercrime. Specifically, the launch of the Australian Cybercrime Online Reporting Network (ACORN) provided a central and online reporting mechanism for victims to report cybercrime incidents (ACORN 2014). Details of these reports were then sent to the appropriate Australian police jurisdiction for consideration. In some cases, the report initiated an investigation; in most cases, however, the report simply added to intelligence received by police. In 2019, ACORN was consolidated into the ACSC. The ACSC is part of the Australian Signals Directorate and similarly enables victims to report incidents via an online 'ReportCyber' portal (ACSC 2019). Australian federal and state law enforcement agencies refer victims of cybercrime to the ACSC, who then 'decide whether it should be referred to law enforcement agencies for possible investigation' (Australian Federal Police (AFP) 2019; QPS 2019: para 4).

The introduction of a centralised reporting mechanism potentially helps to improve police intelligence about the scope of cybercrime across the country. However, there is research suggesting that victims of cybercrime within Australia are generally dissatisfied with responses from law enforcement agencies, because of a lack of clarity about who is responsible for investigating reported incidents (Cross 2018b, 2019b: 5–7; Cross, Richards & Smith 2016). This is often an emergent problem of centralised reporting mechanisms. For example, the United Kingdom established ActionFraud in 2009 as a centralised reporting mechanism for all fraud complaints. In a recent review of this initiative, the Fraud Advisory Panel (2016: 2) observed that '[a]n unintended consequence of ActionFraud has been that too many local police forces no longer feel that fraud is their responsibility'. This problem may suggest a rethinking of the role that central reporting plays in cybercrime investigations. It therefore has significance for ongoing discussions about the policing of cybercrime in Australia.

Community attitudes to cybercrime investigations

There is a growing collection of research examining attitudes about cybercrime and associated police investigations, particularly the community's level of knowledge and awareness of cybercrime impacts, including an individual's initial risk of cybercrime victimisation, their willingness to report incidents to law enforcement, knowledge about retaining evidence for cybercrime investigations, and knowledge about which police agency or authority to contact after victimisation. This makes it important to recognise that the prevention of cybercrime is often a collaborative process between law enforcement agencies and members of the public (Wall 2007: 183). Such community attitudes are influenced by a variety of factors. Existing research suggests that popular views about cybercrime and the capabilities of law enforcement agencies to investigate incidents are shaped by cultural portrayals within media (Wall 2008a, 2008b). Specifically, there is a myth that cybercriminals possess complete mastery over information technologies; this is reflected in portrayals of computer hackers within cyberpunk media such as *The Matrix* and *Die Hard* (Wall 2008a: 863–865). These texts inform broader 'security mindsets' that influence expectations of cybercrime investigations and cybersecurity policymaking (Kremer 2014).

At a fundamental level, community attitudes about cybercrime are influenced by judgements about moral wrongdoing. For example, research examining victim decision-making processes suggests that they are motivated to report incidents to law enforcement by their internal sense of justice and an altruistic desire to protect others from similar harms (Cross 2018c: 550). Similarly, witnesses to a cybercrime, such as distribution of child exploitation material, report collating evidence for the purpose of passing it along to law enforcement agencies and organising 'cyber-vigilante' campaigns (Huey, Nhan & Broll 2013). These cyber-vigilantes similarly self-report that they are motivated by media representations of online crime (such as NBC's *To Catch a Predator*), their sense of justice and a desire to prevent further victimisation (Chang, Zhong & Grabosky 2018; Huey, Nhan & Broll 2013: 86). Consequently, members of the public generally differentiate between types of cybercrime according to their perceived severity, with some types of online crime (eg digital piracy) considered less serious than others (eg cyber-fraud and ransomware; see Holt & Bossler 2016 for a review).

Past experiences also influence public attitudes about cybercrime and associated police investigations. For example, previous victimisation positively correlates with heightened perceptions of cybersecurity risk and a greater likelihood of engaging in avoidance behaviours—such as avoiding online forms of banking and commerce (Randa 2013; Riek, Bohme & Moore 2016). The willingness of members of the public to report cybercrime incidents to law enforcement agencies—and therefore assist in their investigatory efforts—is also influenced by past experiences. For example, negative experiences of reporting online fraud, as when law enforcement agencies are not forthcoming with assistance, reduce self-reported levels of trust in the police (Cross, Richards & Smith 2016; Jang, Joo & Zhao 2010). Similarly, research examining the experiences of Australian victims of image-based sexual abuse reports that they believed that their complaints to law enforcement were not taken seriously (Henry, Flynn & Powell 2018: 569–574; Powell 2010). Individual law enforcement agencies that refuse to accept responsibility for investigations because of the cross-jurisdictional character of cybercrime complaints further compound this problem (Cross 2019b: 12). Finally, members of the public also report reduced levels of trust in law enforcement agencies where they consider investigatory priorities misguided, such as where police are perceived to spend excessive resources investigating digital piracy (Holt, Brewer & Goldsmith 2019: 1, 147, 152). Overall, the existing research suggests that there is a significant discrepancy between the community's expectations of the investigative capabilities of law enforcement agencies and the corresponding experiences of cybercrime victims.

d

Police attitudes to cybercrime investigations

There is a complementary collection of research examining attitudes among law enforcement officers about cybercrime and their perceived responsibilities as investigators. However, most of this research has examined attitudes of law enforcement officers based within the United States, United Kingdom and Canada, with comparatively little research examining Australian jurisdictions. Generally, this research indicates that police share some similar views about cybercrime to members of the public—but also that they feel ill equipped to conduct investigations. The research generally suggests that police officers support preventative cybercrime initiatives that equip citizens with the necessary knowledge about, and thus responsibility for, reducing their risk of online victimisation (Broll & Huey 2015: 167; Hinduja & Schafer 2009).

Like members of the public, law enforcement officers prioritise their work according to their judgements about the severity of different cybercrimes. Specifically, the concept of an 'ideal victim' is useful for understanding how police officers prioritise different types of investigations (Cross 2018a). The notion of the 'ideal' victim refers to heuristics used for distributing responsibility for criminal behaviours, with 'ideal victims' perceived as morally blameless and weak (Christie 1986: 19). For example, research based upon naturalistic observation of police control rooms within the United Kingdom suggests that the perceived 'blamelessness' of victims of cyber-harassment influences decisions about whether further investigation is warranted within a context of limited resources (Black, Lumsden & Hadlington 2019). Indeed, British police officers report frustrations with 'unhelpful victims' of cybercrime who fail to follow advice about preventing victimisation, such as by blocking offenders or avoiding social media platforms (Millman, Winder & Griffiths 2017: 93). In this sense, law enforcement officers view victims of cybercrime who do not take preventative measures as more blameworthy.

Similarly, studies based on US populations suggest that local law enforcement agencies are likely to place investigative priorities on one form of cybercrime—online child sexual exploitation (Hinduja 2004; Holt, Bossler & Fitzgerald 2010; Holt, Burruss & Bossler 2015). This probably reflects the seriousness of such offences, underpinned by the moral blamelessness and comparative powerlessness of victims. In contrast, law enforcement officers view other types of interpersonal cybercrime as less severe. For example, research examining the use of discretion among Canadian cybercrime investigators suggests that officers avoid opening formal investigations where child exploitation material is produced by adolescents engaging in 'sexting' behaviours (Dodge & Spencer 2018: 645). Here, the distinction between offender and victim is blurred, and the behaviour is viewed as inherently less harmful. Canadian law enforcement officers have reported that they do not view 'cyberbullying' as a form of 'criminal' behaviour, thus shifting responsibility for addressing such conduct to parents and educational institutions (Broll & Huey 2015: 163–165). Finally, research examining UK police suggests that officers have a limited understanding of what constitutes image-based sexual abuse as a criminal offence (Bond & Tyrell 2018: 11). Overall, the research suggests that law enforcement officers use similar moral heuristics when appraising the seriousness of cybercrime.

Police preparedness to investigate cybercrime

An expanding collection of research examines police assessments about their preparedness to investigate reports of cybercrime. Many researchers have argued the importance of general duties officers responding to cybercrime in the same way they would to a traditional report about criminal activity: securing the evidence, speaking with witnesses and gathering additional intelligence (Bossler & Holt 2012; Hinduja 2007; National Institute of Justice 2008; Stambaugh et al. 2001). Indeed, the quality of a first responder's scene management is known to have a dramatic impact on the likelihood of solving a real-world crime (Hinduja 2007). It is likely that the same or similar conditions would apply to solving cases of cybercrime. However, knowledge about the investigatory practices of officers and whether they have been adequately trained to appropriately investigate cybercrime remains limited (Hinduja 2007; Holt, Bossler & Fitzgerald 2010; Holt, Burruss & Bossler 2015).

Available information suggests that new police recruits in Australia receive limited instruction about cybercrime investigations, the handling of electronic evidence and basic digital forensics. For example, neither the AFP (2020) nor the New South Wales Police Force (NSWPF 2020) list cybercrime or computer training as part of their basic training curriculum. The QPS (2020: 29) Academy provides basic computer training to new recruits, although this training focuses primarily on how to navigate police information databases. Additionally, in Queensland, the analysis of electronic evidence is restricted to authorised officers who have been accredited by the Electronic Evidence Unit (QPS 2021: 70). Thus, while specialist officers are well equipped to investigate computer-dependent and enabled crimes, it is apparent that general duties officers lack basic training in cybercrime investigation. Clearly, significant training burdens are already placed upon police officers and recruits, but there is an evident gap in their investigatory capabilities in a context where cybercrime investigations are a strategic and funding priority of the federal government (Department of Home Affairs 2020).

A small body of research has examined how cybercrime investigations are perceived among administrators of local law enforcement agencies (Hinduja 2004; Holt, Bossler & Fitzgerald 2010; Marcum et al. 2010; Stambaugh et al. 2001). A smaller body of research examined the perceptions of general duties officers outside Australian jurisdictions (Bossler & Holt 2012, 2013; Holt & Bossler 2012a, 2012b, 2014; Senjo 2004). Research has examined the correlates of cybercrime investigatory capabilities, with technical expertise consistently identified as a relevant variable. Macro-level comparative studies of US law enforcement agencies suggest that larger police agencies are better equipped—in terms of expertise and infrastructure—to respond to cybercrime incidents (Willits & Nowacki 2016). Generally, the research suggests that the quality of investigations is impacted by inconsistent reporting practices, poor information-sharing arrangements, inadequate digital infrastructure and low levels of technical expertise among general duties officers (Nouh et al. 2019: 8–9). Indeed, police officers based within the United Kingdom report frustration about the contribution of the rapid advancement of information technologies to a lack of technical expertise among general duties officers, who are observed to be conceptually confused about what differentiates 'cybercrime' from 'ordinary' crime (Cross 2019a: 128; Hadlington et al. 2018: 4–7).

d

This suggests a lack of understanding about the distinction between 'cyber-enabled' and 'cyber-dependent' forms of crime (McGuire & Dowling 2013) and how technical expertise may be differentially important to respective forms of cybercrime investigation.

As a result, police administrators have argued for a need to improve the investigatory capabilities of local law enforcement agencies to respond to reports of cybercrime. Specifically, administrators have highlighted both the need for additional computer training for general duties officers (Brenner 2008; Collier & Spaul 1992; Hinduja 2007; Holt, Bossler & Fitzgerald 2010; McQuade 2006; Stambaugh et al. 2001; Wall 2007) and the utility of creating or improving specialised cybercrime investigation units (Hinduja 2007; Marcum et al. 2010; Stambaugh et al. 2001). Yet it is law enforcement management, rather than general duties officers, making most of these recommendations. As a result, management and officers may disagree about how first responders should respond to cybercrime incidents. For example, research suggests that general duties officers who lack experience responding to cybercrime reports would prefer that citizens change their online behaviours, not that police be required to receive additional training about effective investigations (Bossler & Holt 2012; Holt & Bossler 2012a). In contrast, officers who have been exposed to cybercrime or who already have computer skills express more enthusiasm about conducting cybercrime investigations (Holt & Bossler 2012b). Indeed, knowledge of digital forensics has been observed to enhance police understanding of the importance of intangible evidence (Brown 2015: 64–65), render officers more likely to view cybercrimes as comparatively serious offences (Holt & Bossler 2012a) and reduce the tendency to blame victims for failing to prevent online victimisation (Holt et al. 2019: 32). However, officers are still more likely to view the public as inadequately aware of cybersecurity risks (Lee et al. 2019).

Overall, the existing research suggests that the self-reported level of preparedness to investigate cybercrime is a function of both good organisational management and previous experience among well-trained police officers. For example, one recent survey-based study of British police officers suggests that self-reported levels of preparedness to investigate cybercrimes are dependent upon whether an organisation has clear policies and procedures about responses to cybercrime, the quality of investigation training programs, self-reported levels of technical expertise, and whether they already have experience in the area (eg Bossler et al. 2019; Holt, Burruss & Bossler 2019). Similar research suggests that general duties officers who have completed substantive face-to-face training on cybercrime investigations feel better equipped to respond effectively to incident reports than officers who completed online-based training programs (Cockcroft et al. 2018: 14–15). Finally, recent studies examining three (anonymous) cybercrime units across Australian policing jurisdictions suggest that investigators feel 'invisible' to police command, and therefore under-resourced and ill-equipped to deal with an increasing number of case referrals from the centralised reporting mechanism at the ACSC (Harkin & Whelan 2019: 5–13; Harkin, Whelan & Chang 2018; Whelan & Harkin 2019).

The need for Australian-focused research

Within the Australian context, the importance of understanding how police personnel comprehend and perceive their role in responding to cybercrime is further underscored by a set of guidelines, published by the Australia New Zealand Policing Advisory Agency (2019), that exist for all Australian police agencies. The guidelines refer to a minimum set of capabilities that officers have the skills and knowledge to perform, including the key competencies of frontline and first response officers in responding to technology-related crime. Research into policing cybercrime in the Australian context must therefore seek to gain the perspectives of general duties officers directly, in addition to the opinions of specialists, senior police and administrators. Finally, there is potential for a mismatch between community expectations of policing responses to cybercrime and the complexity of policing in this internet-enabled, and thus global, environment. International and emerging local research suggests that police agencies themselves face numerous barriers to updating their knowledge and capabilities in a constantly changing technical context, as well as resource and jurisdictional limitations (Button 2012; Cross & Blackshaw 2015).

To date, there is no Australian research examining the knowledge of general duties officers about cybercrime or documenting Australian community expectations and attitudes towards the policing of cybercrime. Therefore, it is critical that police respond in a way that meets the needs and expectations of the community, while also being realistic about their finite resources (Wall 2007: 185). Choo (2010: 68) asserts that, with the evolution of technology and cybercrime:

> ...law enforcement agencies need to reassess policing roles and techniques in order to better attune the delivery of community policing to the needs, wants and expectations of the community.

Without establishing the expectations of the community, it is difficult to ascertain whether police are meeting those expectations and, if not, where the gap lies in terms of improvement (in better education and community awareness or in improved training practices, for example). Without this knowledge, 'misinformation cannot be countered, misunderstandings are perpetuated and there is no firm platform to establish a responsive criminal justice policy' (Wall 2007: 185). These are major gaps in research that need to be addressed in order to meaningfully progress community understandings of, as well as Australian policy and policing responses to, cybercrime.

Methodology

This project used a three-stage, mixed-methods research design. It involved the collection and analysis of quantitative and qualitative data measuring perceptions among police officers and the general community of cybercrime investigations. This section provides details of the methods and data sources underpinning the current project. It outlines the research objectives and guiding questions, summarises the survey instruments and explains how this data was used to structure additional qualitative data collection via focus groups.

Research objectives and questions

The project focused on the understandings of, attitudes to and perceptions of cybercrime among general duties police officers and members of the general community in Australia. Given its significance as a strategic priority for the Australian Government, it is critical to understand how the issue of cybercrime is understood by first responders, such as law enforcement personnel. ReportCyber (via the ACSC) certainly acts as a central reporting portal for cybercrime victims, but previous research (Cross 2018b, 2018c) indicates that general duties officers remain the primary point of contact for many victims making an initial complaint. Accordingly, the study addressed four research questions:

- What are the understandings, perceptions and response expectations of internet-enabled crimes among the Australian adult community and by general duties police?
- To what extent, and in what ways, are the understandings, perceptions and response expectations of the Australian general community similar or different to those of general duties police?
- What opportunities are there for awareness raising, access to information and support in relation to online crimes for the general Australian community?
- What opportunities are there for improving police training, resources, capacity and confidence in responding to online crime?

To answer these four research questions, the project employed a three-stage, mixed-methods research design. Ethics approval was received from the Queensland University of Technology (QUT) Human Research Ethics Committee for all three stages of the research (#1700000292; #1700000504; #1700000923).

It is important to note that the research presented within this report was conducted under the previous processes for reporting cybercrime, established by ACORN. ACORN was decommissioned on 30 June 2019 and replaced with a new portal (cyber.gov.au). The research instruments were developed, and associated quantitative and qualitative data analyses conducted, with reference to the reporting practices recommended by ACORN.

At the time, ACORN (2014: para 1) defined cybercrime as:

> [C]rimes which are:
> – directed at computers or other devices (for example, hacking), and
> – where computers or other devices are integral to the offence (for example, online fraud, identity theft and the distribution of child exploitation material).
>
> Common types of cybercrime include hacking, online scams and fraud, identity theft, attacks on computer systems and illegal or prohibited online content.

This research project uses the term 'cybercrime' in a broader context than that above. ACORN's definition of cybercrime is primarily focused on 'cyber-dependent crimes', which target or require the use of computers or digital technologies. Instead, this project uses a broader definition of 'cybercrime' including also 'cyber-enabled crimes'—offences that involve the use of computers or digital technologies, yet are not dependent upon them (McGuire & Dowling 2013). For example, cybercrime offences such as cyberstalking, the non-consensual distribution of intimate images, online threats and criminal harassment are facilitated through the internet (Powell 2010; Powell & Henry 2018) but may not fall within the scope of ACORN's more restrictive definition.

Stage one: Police survey

We developed an online survey for dissemination to Australian police agencies, based on the previous work of Holt and colleagues. This established instrument measures respondent demographics, patterns of technology use, perceptions of cybercrime, confidence in responses to cybercrime and attitudes to technology in policing.

Participating police agencies

We invited all Australian police agencies to participate in the project by completing the online survey. The research team approached the research unit in each jurisdiction (where available) and submitted a research application.

The recruitment of police officers to participate in the project commenced in August 2017. Receiving approval from police agencies was time consuming and involved several delays. Because the intention of the project was to target the views of general duties officers, the survey targeted officers based within all state and territory law enforcement agencies. Overall, the QPS, NSWPF and Tasmania Police agreed to participate in the project. The Western Australia Police Force, South Australia Police and Victoria Police declined to participate. The Northern Territory Police and Australian Capital Territory Policing (through the AFP) did not respond to the initial request or any subsequent communications.

d

Survey dissemination

The survey instrument was disseminated to all policing staff in the participating agencies. The invitation included the following statement:

> We are inviting all general duties officers at the rank of Constable, Senior Constable, and Sergeant across the [police agency] as well as specialist staff (both sworn and unsworn) in a position related to cybercrime.

The QPS distributed the online survey link via email and organisation-wide notifications on six occasions between November 2017 and June 2018. This targeted approximately 5,000 sworn general duties officers at the rank of constable to sergeant across the state and 540 sworn specialist investigators within State Crime Command.

NSWPF distributed the survey through the Manager of Research Coordination. An email was sent to all NSWPF employees stating that the research was endorsed by the deputy commissioner. Additionally, the Investigations and Counter Terrorism group invited all employees to participate. An initial email was sent 13 March 2019, and a follow-up email was sent 4 April 2019. The emails were sent through the Nemesis system (used to send statewide emails to either all police or specific groups of NSWPF employees). Overall, the survey was disseminated to all NSWPF personnel, approximately 20,000 (NSWPF 2018: 79).

Tasmania Police distributed the survey in March 2019: to managers of investigative areas, for dissemination among staff; via email to staff within the Fraud and E-Crime unit; and posted on the agency's intranet. In total, the survey was disseminated to the agency's 1,859 employees (Tasmanian Government Department of Police, Fire, and Emergency Management 2019: 69).

Survey instrument and items

We adapted the survey instrument from a previous instrument used to examine attitudes about cybercrime among police officers based within the United States and United Kingdom (Bossler & Holt 2012, 2014; Holt & Bossler 2012a, 2012b). The survey was expected to take between 20 and 30 minutes to complete. It consisted of five distinct modules:

- technology use and general online experiences;
- perceptions of cybercrime;
- confidence in police responses;
- technology use and policing; and
- demographics.

Technology use and general online experiences

Respondents were asked specific questions about their use of technology across several distinct five- or six-point scales. For example, the survey instrument included items measuring: how often they access the internet (ranging from '3+ times a day' to 'less often than a few times a week'); how many hours they spend on the internet a day (ranging from 'less than 1 hour' to '6 or more hours'); how many specific types of devices they own (ranging from 0 to 5+); how comfortable they are using computers in their daily lives (ranging from 'very uncomfortable' to 'very comfortable'); and a self-assessment of their skill level with computers (ranging from not using computers 'unless I absolutely have to' to 'very knowledgeable').

Perceptions of cybercrime

Respondents were asked to rate how much they agreed with a series of 25 statements relating to the impact of technology on crime, policing and society. The items used a five-point scale ranging from 'strongly agree' to 'strongly disagree'. These survey items measured police attitudes to: the threat posed by cybercrime (as a whole); whether and how technology is changing police work; different strategies for responding to and investigating cybercrime; and who is primarily responsible for preventing cybercrime.

Additionally, respondents were asked to assess the seriousness and frequency of 27 types of online and offline criminal offences. The seriousness of different types of crimes was measured using a five-point scale ranging from 'not very serious' to 'very serious'. Similarly, the frequency of these offences was measured using a five-point scale ranging from 'never' to 'very frequently'. The survey items measured perceptions about the seriousness and frequency of several types of cybercrime offences, including fraud and identity cybercrime, interpersonal cybercrime, cyber-harassment and abuse, and cyber-enabled crimes.

Confidence in police responses

Respondents were asked to rate their confidence in police responses to cybercrime within their own jurisdiction and their specific agency. They were also asked to rate their own ability to respond to cybercrime as an individual. Several survey items specifically measured how confident the respondents were that their agency takes cybercrime seriously, adequately funds cybercrime investigations, supports victims of cybercrime, detects and charges offenders and effectively prevents cybercrime from occurring. These survey items were measured on five-point scales ranging from 'not at all confident' to 'very confident'. Respondents were also asked to rate and describe their perception of the importance of factors that could improve their preparedness to respond to cybercrime incidents, including: public education; digital forensics; increasing penalties for offenders; cooperating with businesses; investing in high-tech crime units; training general duties officers; additional legislation; and developing local, state or federal cybercrime investigative capabilities. These items were measured on a five-point scale ranging from 'not important' to 'very important'. Respondents were offered the option of providing additional, qualitative feedback.

d

Technology use and policing

Respondents were asked multiple questions related to their use of computer technology and the internet as part of their job. Survey items measured how often respondents access the internet as part of their policing duties (ranging from '3+ times a day' to 'less often than a few times a week') and how many hours they spend online for policing purposes on an average day (ranging from 'none' to '6 or more'). Other items described in the first module (technology use and general online experiences) were specified within the context of their work responsibilities.

The survey instrument also examined whether, and to what extent, respondents had received any training to investigate or respond to cybercrime. Where respondents indicated that they had received relevant training (yes/no), they completed an additional nine binary (yes/no) items measuring the type of training received. These included items measuring whether they were instructed to: refer victims to ACORN, take initial reports of cybercrimes, collect or preserve digital evidence, and collect and use open source intelligence. They also asked whether respondents were trained in digital investigation techniques or about relevant state or federal legislation.

Additionally, a series of questions canvassed the average amount of work hours respondents spend each week dealing with specific types of cybercrime and in various aspects of investigations. These items were measured on a six-point scale ranging from 'none', 'less than 1 hour', '1–4 hours' and increasing four-hour increments up until 'over 16 hours'. Relevant items included whether respondents spent time: assessing reports from ACORN, writing cybercrime-related reports or completing paperwork, seizing devices, triaging seized devices, and interpreting the results of a digital forensic analysis report.

Demographics

Respondents were asked to provide a range of descriptive details related to their occupation and personal demography. These items recorded respondents' gender, age, highest level of education, rank, policing region, Indigenous status and country of birth and asked whether they were general duties officers or cybercrime specialists (hereafter 'specialists').

This demographic module was initially placed at the end of the survey instrument (administered to officers based within the QPS). There was an observably high rate of participant drop-off among these respondents. Therefore, when the survey was disseminated to NSWPF and to Tasmania Police, the demographics module was shifted to the beginning of the instrument. All other modules and questions remained the same.

Response rate

Overall, there were 686 responses to the survey, although there was a substantial number of incomplete responses to individual questions. These inconsistencies permeate the data, even for basic descriptive information. To that end, the respondent population does not necessarily reflect the views of the overall police agencies from which they were drawn. For example, there were 148 total respondents from QPS, with 79 indicating that they served as general duties officers, 61 as specialists, and eight as unsworn respondents. Measured against the targeted recruitment sample, 11 percent of all specialists contacted replied, while only two percent of those general duties police participated.

All members of NSWPF were invited to participate, so the response rate is particularly low. Only two percent of the force responded. Of those, 65 were general duties officers, 177 were specialists and 97 were unsworn. Because we do not have a specific breakdown of generalists versus specialist police from NSWPF as a whole, we can only determine an overall response rate for the entire police force.

Tasmania Police respondents included 14 general duties officers, 15 specialists and two unsworn members. This represents a total of 31 respondents from a population of 1,859 employees. Again, because we do not have a specific breakdown of generalists versus specialists within the police from Tasmania, we can only determine that the survey had an overall response rate of two percent. Finally, it should be noted that one individual self-identified as a member of Victoria Police. It is unclear whether this was entered in error, or how an individual could have engaged in the survey despite the non-participation of their agency.

Although the original intention was to target general duties police rather than specialist officers, the sample clearly over-represents the views of specialists employed across the three agencies. This is important in interpreting the results of the survey. However, low response rates are typical of online police survey research and are not inherently problematic (Nix et al. 2019: 533–34). Previous research has documented frequent high non-response rates to police surveys, attributed to officers' distrust of external investigators (Skogan 2015). In the case of Australian police agencies, these difficulties are compounded by bureaucratic processes that limit access and by the possibility of survey fatigue among respondents (Nix et al. 2019: 534).

d

Data analysis

Researchers analysed the data using SPSS Statistics software (IBM SPSS V.26) and consolidated the raw data associated with the dependent variables across modules 2 (perceptions of cybercrime) and 3 (confidence in police response) into three-point scales, in order to increase the sensitivity of contingency tables to statistical analyses. For example, items within the perceptions of cybercrime module were consolidated from a five-point scale ('strongly agree' to 'strongly disagree') to a three-point scale ('agree' to 'disagree'). We compared descriptive statistics for responses on each of the survey items. Contingency tables were analysed to examine the influence of sociodemographic (module 5) and technology-related variables (modules 1 and 4) on patterns of responses to survey items across modules 2 to 3, using Pearson's chi-square test for independence where independent variables are nominal (eg respondent gender, experiences of cybercrime training and expressed comfort with technology). The results of these tests are interpreted together with patterns observed within contingency tables, which indicate the direction of any significant relationships. Finally, where the independent variable is ordinal (eg age), Pearson's correlation coefficient is used to assess the strength of relationships.

Stage two: Community survey

The second stage of the research design involved conducting a national survey to examine attitudes and experiences of cybercrime within a general (non-representative) sample of the Australian community. This enabled the collection of comparative survey data, because the survey instrument and specific items were designed to complement those outlined above.

Participant recruitment

The research sample included Australian adults aged 18 to 69 years. This age range was selected because it represents the majority of mobile and internet technology users (ACMA 2011, 2015). A social research panel provider (Qualtrics Panels) recruited respondents and invited them to take part in the survey. This was a non-probability sample with quota sampling across gender and age to approximate the demographics representative of the Australian population (as per the Australian Bureau of Statistics Census data). Qualtrics Panels informed all respondents that the purpose of the study was to examine attitudes and experiences of cybercrime and online harm.

Survey instrument and items

We developed the survey instrument used in the second stage of the research to obtain comparative data about community attitudes to cybercrime. Researchers again adapted the survey from the work of Holt and Bossler (2012) and estimated that it would take between 20 and 30 minutes to complete. It contained six distinct modules:

- technology use and general online experiences;
- perceptions of cybercrime;
- cybercrime risk and resilience behaviours;
- cyber victimisation, reporting and experience of police response;
- overall confidence in police response to cybercrime; and
- demographics.

Technology use and general online experiences

Respondents were asked nine specific questions:

1. frequency of internet use;
2. daily active time spent online;
3. number and type of devices used;
4. most frequent device used;
5. comfort with computer use;
6. skill level in solving computer problems;
7. frequency of use of digital communications (including social media);
8. weekly hours spent online for various tasks; and
9. relationship to various people regularly connected with online.

The items listed above are comparable to technology-related modules within the police survey (1 and 4). With the exceptions of questions 4 and 9, items were rated by participants on a five-point scale. Responses of 1 indicated lower levels of engagement or confidence with technology use, and responses of 5 indicated higher engagement or confidence. Participant responses to questions 1, 2, 3, 7 and 8 were aggregated to create an overall 'engagement with technology use' score (with higher mean scores indicating greater frequency, hours and types of online engagement). Responses to questions 5 and 6 were aggregated to create an overall confidence with technology use score (with higher mean scores indicating greater comfort and confidence in using computer technologies).

d

Perceptions of cybercrime

Community respondents were asked to rate their agreement with 25 statements about perceptions of cybercrime. We measured responses using a five-point scale ranging from 'strongly agree' to 'strongly disagree'. The survey items were the same used within module two (perceptions of cybercrime) within the police survey, with only minor changes in phrasing.

Respondents were then asked to rate three sets of statements regarding their fear of different types of crime. These items are comparable with the survey items measuring perceived seriousness of cybercrime offences within module two of the police survey. We again measured responses using a five-point scale ranging from 'not afraid at all' to 'very afraid'. The first set of 15 questions measured levels of fear of traditional crimes (eg 'having someone break into your home while you are there' and 'being raped or sexually assaulted'). The second set of 10 questions measured levels of fear of identity and fraud-related cybercrimes (eg 'having your personal information exposed to the public by another organisation without your knowledge/consent' and 'having someone hack into one of your (online) accounts'). The third set of 16 questions measured levels of fear of interpersonal cybercrime, cyber-abuse and image-based abuse (eg 'having someone threaten they will send a nude or sexual photo/video of you onto others or post it online' and 'having someone make online threats to sexually harm you, rape or sexually assault you').

Finally, respondents were asked to rate the same three sets of statements regarding their perceived likelihood of crime victimisation. We measured responses using a five-point scale ranging from 'not at all likely' to 'very likely'. The measures are comparable with the survey items about officer perceptions of frequency within module two of the police survey.

Cybercrime risk and resilience behaviours

This module posed a series of questions concerning cybercrime risk and associated protective behaviours, including an item measuring self-assessed confidence to protect against cybercrime on a five-point scale ranging from 'not at all confident' to 'very confident'. Subsequently, respondents indicated the frequency with which they engaged in 16 types of protective behaviours on a five-point scale ranging from 'none of the time' to 'all of the time'. For example, survey items measured how often respondents 'use and update antivirus software on your devices', 'change the passwords for your online accounts' and 'avoid updating your real-time location online'.

Cyber victimisation, reporting and experience of police response

This module asked respondents about their experience of a range of cybercrime victimisation types, including identity crime and online fraud, interpersonal harassment, and cyberbullying and abuse. These items are comparable to the measures of police experiences of investigating or responding to cybercrimes within module four of the police survey. For each cybercrime subtype, respondents were asked to indicate whether they had experienced multiple examples of crime victimisation. For example, to gauge whether respondents had ever experienced an incident of interpersonal harassment, they were asked whether they had ever 'received insulting or threatening comments by strangers online' or 'had a friend or acquaintance post offensive content pretending to be you online'. Where respondents indicated that they had experienced any example of a subtype of cybercrime victimisation, they were prompted to answer additional questions that measured: whether they reported the incident to police (yes/ no); how they reported it to police (via ACORN, in person, via phone or other); how helpful they found the police response (on a five-point scale ranging from 'very helpful' to 'not at all helpful'); whether they sought other forms of assistance (eg from a friend, family member, lawyer or health professional); and how helpful they found this form of assistance (also on a five-point scale ranging from 'very helpful' to 'not at all helpful'). They were then prompted to provide additional qualitative information about their experiences of victimisation and the support offered by police or other services.

Overall confidence in police response to cybercrime

Independent of any personal experiences of cybercrime victimisation, all respondents were asked to rate their confidence in the police within their jurisdiction to respond to cybercrime incidents. These measures are comparable to measures within module three of the police survey. Overall levels of confidence were measured on a five-point scale ranging from 'not at all confident' to 'very confident'. Using the same scale, respondents were asked to specifically rate their confidence on four specific items about whether police: take cybercrime as seriously as face-to-face crimes, are adequately funded and resourced to address cybercrimes, are effective in supporting victims of cybercrime, and are effective in detecting and charging perpetrators of cybercrime.

Survey items included within this module are also comparable to measures within module four of the police survey (technology use and policing). Respondents were directly asked about any recent contact with police concerning cybercrime. This included items that measured the most recent time they contacted police concerning a cybercrime incident, the most recent time a neighbour or loved one had contacted the police regarding a cybercrime incident, and the most recent time they had discussed a cybercrime incident with a neighbour or loved one. These items were measured on a six-point scale with increasing time frames: 'within the last week', 'within the last several weeks', 'within the last several months', 'within the last year', 'over a year ago', and 'never'. Finally, respondents were prompted to provide any additional qualitative information about their confidence in police responses to cybercrime, including whether they had any thoughts about how these responses could be improved in the future.

d

Demographics

Finally, respondents were asked to provide a range of demographic information. This included nominal and ordinal data about their gender, sexuality, whether they identified as Aboriginal or Torres Strait Islander, age, country of birth, details about household occupants, details about any ongoing disabilities, highest level of education, employment status, current occupation and annual income.

Response rate

Overall, Qualtrics Panels sent 5,736 invitations to prospective participants. Excluding responses with missing demographic datapoints, 2,037 surveys were completed. This represented a response rate of 36 percent—a good result for comparable social science survey research (Crow et al. 2017: 597; Davis & Dossetor 2010: 2).

Data analysis

Researchers used IBM SPSS (V.26) to analyse the data and generate descriptive statistics about the independent variables. These included sociodemographic data (module six) and measures of technology use and general online experiences (module one). Descriptive statistics were also generated and reported for the dependent measures across modules two to five (perceptions of cybercrime; risk and resilience behaviours; cyber victimisation, reporting and experience of police responses; and confidence in police response to cybercrime). We analysed the relationships between gender (binary male or female) and age (re-coded as categorical variable) on the dependent measures (eg mean levels of fear of different types of crime; binary measures of crime victimisation, yes or no) using one-way ANOVA and chi-square tests of independence respectively.

The data collected during stage one (police survey) and stage two (community survey) of the research have also been comparatively analysed where there are identical or similar measures. To conduct these comparative analyses, the five-point scales were consolidated into three-point scales across modules two, three and four (eg by consolidating ‘strongly agree’ and ‘agree’ into a single response). This enables chi-square analyses to compare response patterns between the police and community samples. Police measures of crime seriousness (ie stage one, module two) are compared with community measures of fear of crime (ie stage two, module two). In this manner, police and community perceptions of cybercrime, cybercrime prevention strategies and protective behaviours, and confidence in police responses to cybercrime incidents are all comparatively analysed.

Stage three: Focus group with cybercrime and cybersecurity professionals

The third stage involved a large-scale focus group discussion with a diverse group of cybercrime and cybersecurity professionals. The aim was to analyse and calibrate the survey results and to provide additional insights.

Recruitment of participants

Chief Investigator (CI) Cross facilitated the recruitment of a purposive sample of focus group participants through several channels. Firstly, invitations were extended across existing professional networks. This included potential participants from police, government and industry with whom CI Cross has previously worked in the areas of fraud and cybersecurity. Secondly, specific agencies and individuals were selected, based on their known expertise in cybercrime or cybersecurity, and invited to participate. Thirdly, a snowball sampling technique enabled us to access additional attendees from the broader networks of participants.

To be eligible for participation in the workshop, individuals met the following requirements:

- aged 18 years or over;
- able to give informed consent; and
- expertise in either cybercrime or cybersecurity.

Participants were invited from across Australia to attend a day-long focus group at the QUT Gardens Point campus in Brisbane, Australia. Participants based outside of Brisbane were offered return flights to attend the workshop, and the event was scheduled to enable participating individuals to fly in and out the same day. An exception was made for attendees from Perth and Hobart, who were offered one night's accommodation. Participants from Brisbane, the Sunshine Coast and the Gold Coast were offered free parking at QUT for the day.

The demographics of focus groups invariably affect the characteristics of qualitative data. On the day, 28 participants attended. Almost all (n=26) completed a short demographic form. Of these 26 participants, the majority (n=21) were male. The average age of participants was 45 years; the youngest was 27 and the oldest 64. Ten participants (39%) were from law enforcement, seven (27%) were from government, six (23%) were from industry or the private sector, and the remaining three (12%) were from other sectors, including tertiary education and the not-for-profit sector. Although there was an over-representation of Brisbane-based participants, participants also came from other states and territories. They had a range of experience working broadly in cybercrime, some with limited experience and others with detailed experience. The average was 11 years of experience, and the highest was 30 years. Overall, the focus group offered a diverse range of views across law enforcement, government and the private sector.

d

Format of the focus group

CIs Cross and Holt facilitated the focus group. Participants sat randomly at one of six tables in the room. Members of the research team made several presentations. After members of the research team and participants had introduced themselves to the broader group, CI Cross provided an overview of the research project, including a brief summary of the results of both the community and police surveys. CI Holt then provided an overview of the existing research examining police perceptions of cybercrime within the United States and United Kingdom. These presentations gave the participants an understanding of the context and purpose of the focus group component of the project. They also prompted discussion about the preliminary results.

The following discussion focused on key questions spread across six modules throughout the day. These questions, discussed at the individual tables and then with the whole group, provided the basis for collaborative brainstorming and robust debate. The six modules of group discussions throughout the day were:

- current approaches to policing cybercrime;
- reflections on police survey results;
- reflections on comparative police and community survey results;
- public education about cybercrime;
- cybercrime, specialisation and general duties policing; and
- final thoughts and additional comments.

Current approaches to policing cybercrime

These discussions focused on broad questions about police responses to cybercrime incidents. Discussion questions included:

- What do you think are the strengths of current approaches to the policing of cybercrime across police, government and industry?
- What do you think are the weaknesses of current approaches to the policing of cybercrime across police, government and industry?

Reflections on police survey results

These questions related to the summarised results of the police survey. These results were visible on screen and within handouts temporarily provided to participants. The corresponding discussion questions included:

- What are your initial thoughts about the police results?
- What are some possible explanations for any of the results?
- Are there any results that are surprising to you or that you disagree with?
- Is there anything you think is left out/missing from the data?

Reflections on comparative police and community survey results

The police results were discussed in isolation. Participants were then asked their thoughts about different patterns of responses within the police and community survey results. These results again appeared on a screen and within handouts temporarily provided to participants. The corresponding discussion questions included:

- Do you agree with this data? If so, why?
- Do you disagree with any of these questions? If so, why?
- What surprises you with this data?
- Do you have any context for these answers, and any similarities/differences?
- Why do you think some of these differences exist?
- Are there any similarities that are surprising?
- Based on results, do you think your agency could play a role, and what could that be?
- Are there any current practices from your agency that you think are relevant and could be applied in this context?

Public education about cybercrime

The discussion about comparative perceptions of police officers and community members flowed directly into a discussion about the merits of cybercrime-related public education campaigns. The corresponding discussion questions included:

- What current approaches do you know of that seek to educate the public?
- Do you think these are effective or ineffective?
- Who do you think has the responsibility to educate the public?
- Based on the gaps, how might we go about better educating the public on the risks of cybercrime victimisation?

Cybercrime, specialisation and general duties policing

Pivoting back to police responses to cybercrime incidents, participants were next asked their thoughts about whether cybercrime investigations should be a specialist or generalist policing area. To facilitate a discussion, each table was allocated an initial position to argue (either the 'specialist' or 'generalist' perspective). They then shifted into a broader discussion about the issue. The corresponding discussion questions included:

- Please put down all the reasons why you think this should be a generalist police area.
- Please put down all the reasons why you think this should be a specialist police area.

d

Final thoughts and additional comments

Finally, CIs asked the focus group for any final thoughts about anything discussed (or not yet discussed) throughout the day. The corresponding discussion questions included:

- Are there other questions that we have not touched upon?
- Are there any other areas that you think are important that have not been covered today?

Data collection

To facilitate data collection, a research assistant sat at each of the six tables and acted as a scribe. Their primary purpose was to record all conversations at the table and their table's contribution to group discussions. Each scribe recorded a combination of verbatim quotes and a summation of the discussions at their table. The focus group was conducted under Chatham House rules, which enable participants to freely discuss ideas across the day without any specific individual or associated organisation being identified. The scribe placed at each table did not record any personally identifiable information about participants or their specific organisations. Building this assurance of confidentiality into the research design enabled more robust and honest discussions, unconstrained by fear of disclosure.

Data analysis

The notes and transcripts generated by scribes (a combination of the verbatim and summary points) were uploaded into NVivo 12 (qualitative computer assisted software tool) for data analysis. A member of the research team coded this textual data according to various themes inductively derived from repeated and prolonged analysis of the data. Three distinct themes were identified across the discussion modules outlined above: police responsibilities, community expectations, and public education. Each of these themes was constituted and contested by multiple categories and subcategories. For example, discussions about police responsibilities can be categorised and subcategorised into different views about specialist and generalist police responsibilities or competing views about cybercrime training requirements. Overall, the qualitative analysis of the focus group discussions triangulates and extends the results of the comparative analysis of police and community surveys measuring perceptions of cybercrime.

Results: Police survey

This section provides an overview of the results from the police survey, disseminated across the Queensland, New South Wales and Tasmania police agencies. The single Victorian respondent's answers have been excluded here.

It is important to note that not all respondents completed every module included within the survey. Partial responses have been used where relevant. For each question, the number of responses to the question (*n*) is provided. Additionally, tests for significance were conducted, when possible, to explore any demographic variations present in the expressed views and opinions of respondents. Significant relationships are noted, along with their attendant statistical results.

Demographics of survey respondents

A majority (61%) of survey respondents were male (*n*=321); 37 percent were female (*n*=208). The mean age of those who provided the information (*n*=529) was 42 years. Most respondents had either a university undergraduate degree (*n*=199, 39%) or a tertiary diploma (*n*=167, 33%). Most respondents in the sample were from NSWPF (*n*=347, 66%) and reported serving in a specialist role (*n*=253, 49%), although many indicated that they were serving in general duties roles (*n*=158, 30%). The largest proportion of respondents were constables (*n*=271, 40%), with an average of 16 years of service as a police officer. The overwhelming majority of respondents were born in Australia (*n*=428, 84%). Only seven percent of the sample indicated that they were of Aboriginal or Torres Strait Islander origin. A large majority of the sample (87%) indicated that they only spoke English at home.

d

Technology use and general online experiences

The majority of respondents indicated that they accessed the internet three or more times per day (*n*=543, 86%). The modal time spent online was 1–2 hours per day (*n*=284, 45%). Most owned one smartphone (*n*=561, 89%), a laptop (*n*=443, 71%) or a tablet (*n*=361, 58%). The majority used a mobile device or smartphone to access the internet (*n*=437, 70%).

When asked how comfortable they were with using computers, respondents offered an unexpected range of responses. Most reported being either very comfortable (*n*=247, 39%) or comfortable (*n*=176, 28%) with computers, although 26 percent were very uncomfortable. Similarly, a significant number of respondents (*n*=251, 40%) reported that they could use a variety of software and fix some computer problems.

Technology use and policing

The majority of respondents (*n*=297, 60%) indicated that they used the internet more than three times a day as part of their policing duties. Asked how many hours they spent online for policing purposes, on average, most respondents indicated that they spent less than one hour (*n*=189, 38%) or one to two total hours (*n*=177, 36%) online. The overwhelming majority of respondents used a desktop computer to access the internet while at work (*n*=408, 81%). Respondents also reported being comfortable with computers while at work (*n*=219, 44%). Few respondents indicated that they had received any sort of training associated with internet use or cybercrime (*n*=39, 8%).

Despite the lack of training, a significant number had responded to a cybercrime incident within the preceding six weeks (*n*=160, 36%) or knew of a fellow officer who had responded to a cybercrime in the preceding week (*n*=177, 40%). Half the respondents reported discussing an online cybercrime case with a colleague within the preceding six weeks (*n*=222, 50%). Similarly, many respondents had discussed an online or cybercrime case with a member of the public within the preceding six weeks (*n*=164, *n*=32%). A significant number of respondents also reported never having witnessed cybercrime being discussed during departmental meetings (*n*=197, 44%).

Perceptions of cybercrime

The respondents were asked to indicate their views about different types of cybercriminal behaviour by indicating how much they agreed with a series of statements. Respondents commonly disagreed with the notion that most types of online incidents are minor annoyances (*n*=226, 42%). A majority disagreed with the statement that online harassment is less serious than face-to-face harassment (*n*=364, 68%). Many disagreed that cybercrime occurs more frequently in businesses rather than among home users (*n*=258, 48%), although 41 percent indicated that they neither agreed nor disagreed with that statement. A similar pattern was observed with respect to the statement: 'the majority of cybercrimes are perpetrated by younger individuals in their teens and twenties'; nearly half disagreed with this statement (*n*=260, 49%), although 41 percent neither agreed nor disagreed. Many respondents neither agreed nor disagreed (*n*=195, 37%) with the statement: 'cybercriminals are often individuals living in foreign countries rather than here in Australia'.

There were statistically significant positive relationships between age and the likelihood that an officer viewed: most online incidents as minor annoyances (r=0.17, p<0.01); online harassment as less serious than face-to-face harassment (r=0.09, p<0. 05); and most online experiences as not requiring a police response (r=0.102, p<0.05). There was also a positive relationship between age and believing that most cybercrimes are committed by younger people (r=0.107, p<0. 05) and that cybercrimes more frequently affect businesses rather than home users (r=0.103, p<0.05). It is important to note that these relationships have small effect sizes; although there was an observable relationship, age only accounts for a small amount of the variance in responses.

Gender also influenced perceptions of cybercrime. Female respondents were more likely to disagree with the statements that online harassment is less serious than face-to-face harassment ($\chi^2(8)=42.65$, p<0.01) or that most types of online incidents are minor annoyances ($\chi^2(8)=21.26$, p<0.01). Male respondents were more likely to agree with the statements that cybercrimes do not require a police response ($\chi^2(8)=19.02$, p<0.05) and that offenders are often based overseas ($\chi^2(8)=15.597$, p<0.05).

Most respondents agreed with the statements that cybercrime is a serious problem in society today (*n*=462, 87%), that the internet has dramatically changed police work (*n*=487, 91%) and that the internet has caused more problems for law enforcement than it has helped (*n*=246, 46%). Over three-quarters of respondents disagreed with the statement that the public understand the risks of being online (*n*=414, 78%). Respondents also disagreed with the statement that cybercrime is not taken seriously by law enforcement (*n*=247, 46%).

d

Age and gender had an observable impact upon patterns of responses. Male respondents were more likely to agree that online bullying and harassment can be avoided by changing phone numbers or email addresses ($\chi^2(8)=19.58$, $p<0.05$), that victims of fraud lose money because they are not paying attention to what they read ($\chi^2(8)=22.67$, $p<0.01$), and that an individual who sends a nude image to someone else is partly responsible if it ends up on the internet ($\chi^2(8)=16.39$, $p<0.05$). Interestingly, there was a negative relationship between age and the belief that a victim is responsible if they send a nude image ($r=–0.18$, $p<0.01$), that people should know better than to take nude selfies in the first place ($r=–0.2$, $p<0.01$), and that victims of domestic violence should stop using social media, email and online sites ($r=–0.08$, $p<0.05$). This suggests that younger officers are more prone to ascribing responsibility to victims of cybercrime.

Whether an officer had a tertiary education and whether they reported feeling comfortable using technology influenced their perceptions about cybercrime. Tertiary-educated respondents were more likely to assess the public as not recognising the threat posed by cybercrime ($\chi^2(4)=10.63$, $p<0.05$), as were those who were more comfortable using technology ($\chi^2(8)=27.53$, $p<0.01$). These two groups also recognised more frequently the overlap between cybercrime and traditional crimes. Respondents with a tertiary education were more likely to believe that digital evidence can be a feature of all crime types ($\chi^2(4)=16.86$, $p<0.01$), as were those who reported being comfortable using technology within their work ($\chi^2(8)=16.7$, $p<0.05$). Similarly, respondents with a tertiary education agreed that crimes that used to be offline now have increasingly online elements ($\chi^2(4)=15.82$, $p<0.01$), as did officers who reported being comfortable using technology ($\chi^2(8)=18.02$, $p<0.05$).

Tertiary-educated respondents were also more likely to disagree with statements that apportioned blame to victims: that online bullying can be avoided by changing numbers or email addresses ($\chi^2(4)=13.3$, $p<0.01$), that victims of image-based abuse are partly responsible ($\chi^2(4)=9.51$, $p<0.05$), and that people should know better than to send nude selfies ($\chi^2(4)=19.25$, $p<0.01$). Additionally, those with a tertiary degree were more likely to disagree strongly with the statement that rape threats over Facebook should not be taken seriously ($\chi^2(4)=12.08$, $p<0.05$). Finally, officers who had received training in cybercrime investigations were also more likely to disagree with the statement that online bullying can be avoided by changing mobile phone numbers or email addresses ($\chi^2(4)=10.31$, $p<0.05$).

Support for a high-tech crime unit was influenced by gender and education. Male respondents were more likely to agree with the statement that most cybercrimes should be investigated by a high-tech crime unit ($\chi^2(8)=19.52$, $p<0.05$). However, respondents with a tertiary education were more likely to agree with the statement that ‘responding to initial reports of cybercrime from victims is increasingly part of general duties police work’ ($\chi^2(4)=11.98$, $p<0.05$), while those without a tertiary degree were more likely to agree that most cybercrimes should be investigated by a specialised high-tech crime unit ($\chi^2(4)=10.02$, $p<0.05$).

Respondents were asked to express their perception of the level of seriousness across several offence categories by rating them from not very serious (1) to very serious (5). Table 1 shows the mean score for each offence type in ranked order from most to least serious.

Table 1: Ranking offence seriousness (*n*=534)

Survey item	Mean score
Physical terrorist attack (bombings, hijackings)	4.98
Child abuse material and sexual solicitation of children	4.94
Selling hard drugs such as heroin, cocaine or methamphetamine	4.61
Cyberterrorism (ie the use of computers or the internet to harm an electronic resource (website, database) for an ideological, political or social cause)	4.55
Threats made online to sexually harm or rape someone	4.31
Posting nude photos or videos of another person online without their permission (revenge pornography)	4.27
Stalking or threatening an ex-intimate partner online, such as via social media	4.25
Identity theft (using someone else's identity to steal money or gain other benefits)	4.25
Hitting someone without any reason	4.24
Electronic theft of money from accounts	4.18
Stalking or threatening a stranger online, such as via social media, dating apps or web	4.12
Threats made online to harm someone with physical violence	4.07
Viruses and malicious software infection	3.99
Deceiving someone into sending money over the internet	3.97
Breaking into a vehicle or building to steal something	3.95
Hacking into someone else's email or social media account	3.72
Harassment over the internet	3.64
Viewing someone else's electronic data without permission	3.62
Romance fraud (establishing a false online relationship so as to ask for money)	3.58
Purposely damaging or destroying property that does not belong to you	3.58
Advance fee fraud (emails asking for money with the promise of reward)	3.48
Phishing (emails asking for personal details)	3.45
Stealing something worth more than $50	3.11
Unauthorised copying of software	2.98
Using someone else's wireless connection without permission	2.82
Unauthorised copying of media (such as music)	2.67
Stealing an item worth less than $5	2.02

Note: Rank orders for the seriousness of cybercrime offences by police respondents

d

Respondents were then asked to rank the perceived frequency of this same list of offences, with responses ranging from never (1) to very frequently (5). The table below shows the mean score for each offence type.

Table 2: Ranking offence frequency (*n*=534)

Survey item	Mean score
Unauthorised copying of media (such as music and software)	4.76
Harassment over the internet	4.66
Selling hard drugs such as heroin, cocaine or methamphetamine	4.58
Phishing (emails asking for personal details)	4.57
Breaking into a vehicle or building to steal something	4.53
Child abuse material and sexual solicitation of children	4.42
Unauthorised copying of software	4.38
Electronic theft of money from accounts	4.37
Stealing something worth more than $50	4.37
Viruses and malicious software infection	4.35
Advance fee fraud (emails asking for money with the promise of reward)	4.34
Stealing an item worth less than $5	4.31
Deceiving someone into sending money over the internet	4.30
Threats made online to harm someone with physical violence	4.29
Stalking or threatening an ex-intimate partner online, such as via social media	4.24
Romance fraud (establishing a false online relationship so as to ask for money)	4.23
Hacking into someone else's email or social media account	4.14
Purposely damaging or destroying property that does not belong to you	4.08
Posting nude photos or videos of another person online without their permission (revenge pornography)	4.07
Stalking or threatening a stranger online, such as via social media, dating apps or web	4.07
Identity theft (using someone else's identity to steal money or gain other benefits)	4.02
Threats made online to sexually harm or rape someone	4.02
Using someone else's wireless connection without permission	3.86
Hitting someone without any reason	3.86
Viewing someone else's electronic data without permission	3.84
Cyberterrorism (ie the use of computers or the internet to harm an electronic resource (website, database) for an ideological, political or social cause)	3.77
Physical terrorist attack (bombings, hijackings)	2.77

Note: Rank orders for the frequency of cybercrime offences by police respondents

Tables 1 and 2 examine how police respondents ranked the seriousness and frequency of cybercrime offences. Table 3 presents a comparison of respondents' rankings of the seriousness and the estimated frequency of these offence categories.

Table 3: Comparison of rank orders for the seriousness and frequency of offences

Offence type	Seriousness rank (Mean)	Frequency rank (Mean)
Physical terrorist attack (bombings, hijackings)	1 (4.98)	27 (2.77)
Child abuse material and sexual solicitation of children	2 (4.94)	6 (4.42)
Selling hard drugs such as heroin, cocaine or methamphetamine	3 (4.61)	3 (4.58)
Cyberterrorism (ie the use of computers or the internet to harm an electronic resource (website, database) for an ideological, political, or social cause)	4 (4.55)	26 (3.77)
Threats made online to sexually harm or rape someone	5 (4.31)	22 (4.02)
Posting nude photos or videos of another person online without their permission (revenge pornography)	6 (4.27)	19 (4.07)
Stalking or threatening an ex-intimate partner online such as via social media	7 (4.25)	15 (4.24)
Identity theft (using someone else's identity to steal money or gain other benefits)	7 (4.25)	21 (4.02)
Hitting someone without any reason	9 (4.24)	24 (3.86)
Electronic theft of money from accounts	10 (4.18)	8 (4.37)
Stalking or threatening a stranger online such as via social media, dating apps or web	11 (4.12)	20 (4.07)
Threats made online to harm someone with physical violence	12 (4.07)	14 (4.29)
Viruses and malicious software infection	13 (3.99)	10 (4.35)
Deceiving someone into sending money over the internet	14 (3.97)	13 (4.30)
Breaking into a vehicle or building to steal something	15 (3.95)	5 (4.53)
Hacking into someone else's email or social media account	16 (3.72)	17 (4.14)
Harassment over the internet	17 (3.64)	2 (4.66)
Viewing someone else's electronic data without permission	18 (3.62)	25 (3.84)
Romance fraud (establishing a false online relationship so as to ask for money)	19 (3.58)	16 (4.23)
Purposely damaging or destroying property that does not belong to you	19 (3.58)	18 (4.08)
Advance fee fraud (emails asking for money with the promise of reward)	21 (3.48)	11 (4.34)
Phishing (emails asking for personal details)	22 (3.45)	4 (4.57)
Stealing something worth more than $50	23 (3.11)	9 (4.37)
Unauthorised copying of software	24 (2.98)	7 (4.38)
Using someone else's wireless connection without permission	25 (2.82)	23 (3.86)
Unauthorised copying of media (such as music)	26 (2.67)	1 (4.76)
Stealing an item worth less than $5	27 (2.02)	12 (4.31)

Note: Comparison of rank orders for the seriousness and frequency of cybercrime offences by police respondents

d

Correlates of police perceptions of cybercrime

These perceptions of the seriousness of offences were also analysed according to sociodemographic subgroups of respondents (ie by age, gender, Indigenous status and education), self-reported measures of 'comfort with using technology at work', and whether an officer had undergone any type of cybercrime investigation training. A summary of the statistical relationship between age and perceptions of crime severity can be found in Table 4.

Table 4: Age and perceptions of crime seriousness (*n*=468)

Offence type	Pearson's *r*
Stealing an item worth less than $5	0.215*
Purposely damaging or destroying property that does not belong to you	0.121*
Breaking into a vehicle or building to steal something	0.065
Stealing something worth more than $50	0.200*
Hitting someone without any reason	0.155*
Selling hard drugs such as heroin, cocaine or methamphetamine	0.205*
Viewing someone else's electronic data without permission	0.112*
Child abuse material and sexual solicitation of children	0.066
Unauthorised copying of software	0.205*
Unauthorised copying of media (such as music)	0.218*
Electronic theft of money from accounts	0.219*
Harassment over the internet	0.213*
Viruses and malicious software infection	0.337*
Deceiving someone into sending money over the internet	0.175*
Cyberterrorism (the use of computers or the internet to harm an electronic resource (website, database) for an ideological, political or social cause)	0.061
Physical terrorist attack (bombings, hijackings)	0.008
Hacking into someone else's email or social media account	0.230*
Using someone else's wireless connection without permission	0.264*
Posting nude photos or videos of another person online without their permission ('revenge pornography')	0.150*
Stalking or threatening a stranger online, such as via social media, dating apps or web	0.146*
Stalking of threatening an ex-intimate partner online, such as via social media	0.148*
Phishing (emails asking for personal details)	0.226*
Advanced fee fraud (emails asking for money with the promise of reward)	0.215*
Romance fraud (establishing a false online relationship so as to ask for money)	0.209*
Identity theft (using someone else's identity to steal money or gain other benefits)	0.200*
Threats made online to harm someone with physical violence	0.217*
Threats made online to sexually harm or rape someone	0.209*

*statistically significant at $p<0.01$

Note: Relationship between age and judgements about the seriousness of cybercrime offences by police respondents

Evidently, there is a consistent yet weak positive correlation between age and perceptions of the seriousness of criminal offences, with older officers generally judging offences as more serious than younger officers. Similarly, older officers view online harassment (r=–0.09, p<0.05), online threats (r=–0.11, p<0.01), phishing (r=–0.09, p<0.05) and petty theft (r=–0.17, p<0.01) as less common than do younger officers. Older officers are more likely than younger officers to view cyberterrorism (r=–0.14, p<0.01) and physical terrorism (r=0.08, p<0.05) as common.

Additionally, there is evidence of a relationship between gender and perceptions about the severity and frequency of offences. Female respondents consistently ranked offences as more serious than male officers did. Female respondents also tend to view some cybercrime as more serious, including online harassment ($\chi^2(8)=41.31$, p<0.01); online stalking by a stranger ($\chi^2(8)=28.58$, p<0.01); online stalking by an ex-partner ($\chi^2(8)=22.44$, p<0.01); and image-based abuse ($\chi^2(8)=25.96$, p<0.01). Female respondents also viewed ransomware ($\chi^2(8)=18.18$, p<0.05), cyber-fraud ($\chi^2(8)=19.53$, p<0.05), hacking into another's social media account ($\chi^2(8)=17.08$, p<0.05), posting nude photographs without permission ($\chi^2(8)=25.96$, p<0.01), romance fraud ($\chi^2(8)=18.83$, p<0.05), identity theft ($\chi^2(8)=18.92$, p<0.01), online threats of physical violence ($\chi^2(8)=23.62$, p<0.01) and online rape threats ($\chi^2(8)=16.26$, p<0.05) as more serious than their male colleagues. Finally, female respondents view online harassment as more common than male officers do ($\chi^2(4)=9.64$, p<0.05).

Finally, respondents with cybercrime training ranked hacking ($\chi^2(4)=9.48$, p<0.05) and identity theft ($\chi^2(3)=8.31$, p<0.05) as more frequent, compared with officers without cybercrime training.

Confidence in police responses

Respondents were asked to rate how confident they were in the current police response to cybercrime in their own jurisdiction, from not at all confident (1) to very confident (5). The mean was 2.37 (n=505), which is not confident. The modal category was somewhat confident (34%), followed by not confident (31%). Finally, 23 percent of respondents were not at all confident in the current response.

Respondents who had a tertiary qualification were less confident than those without a tertiary qualification ($\chi^2(4)=13.65$, p<0.01). Male officers were more likely to have low levels of confidence in the police response to cybercrime ($\chi^2(8)=17.21$, p<0.05).

d

Respondents were then asked to scale their response to factors associated with the specific response in their state (*n*=505). Responses range from not at all confident (1) to very confident (5), and the mean score is presented in Table 5.

Table 5: Factors associated with police response (*n*=505)

Survey item	Mean score
Taking cybercrime as seriously as face-to-face crime	2.64
Effective in supporting victims of cybercrime	2.27
Effective in charging perpetrators of cybercrime	2.16
Effective in detecting perpetrators of cybercrime	2.14
Effective in disrupting cybercrime	2.03
Effective in preventing cybercrime	1.94
Adequately funded and resourced to address cybercrimes	1.89

Note: Rank order of factors associated with police agency responses to cybercrime by police respondents

Older respondents were slightly more likely to consider law enforcement as not effective at preventing (r=–0.08, p<0.05) or disrupting (r=–0.1, p<0.05) cybercrime. Female respondents were more likely to have some confidence in the ability of police to effectively charge perpetrators of cybercrime ($\chi^2(8)=22.1$, p<0.01).

Respondents with a tertiary degree were less confident that police take cybercrime as seriously as face-to-face crimes ($\chi^2(4)=11.64$, p<0.05). However, respondents who self-reported as comfortable using technology at work were more confident that police take cybercrime as seriously as face-to-face crimes ($\chi^2(8)=21.99$, p<0.01).

Respondents were then asked to assess their own ability to respond to cybercrime effectively, in contrast to their organisation's ability. The average for this question was 2.62 (*n*=505), which is higher than for their organisations, but still not very confident. Most respondents indicated that they were either not confident (36%) or somewhat confident (35%) in their own ability.

Respondents who were likely to rate their own abilities higher included those with tertiary degrees ($\chi^2(4)=21.59$, p<0.01) and those who reported being comfortable with technology ($\chi^2(4)=33.65$, p<0.01).

Respondents were then asked to rate what was most important to improving their own individual capacities to respond to cybercrime, with responses ranging from not important (1) to very important (5) (n=505) against identified factors. Table 6 presents a summary of these factors and mean scores for each.

Table 6: Factors to increase personal ability to respond to cybercrime (n=505)

Survey item	Mean score
Taking cybercrime as seriously as face-to-face crime	2.64
Effective in supporting victims of cybercrime	2.27
Effective in charging perpetrators of cybercrime	2.16
Effective in detecting perpetrators of cybercrime	2.14
Effective in disrupting cybercrime	2.03
Effective in preventing cybercrime	1.94
Adequately funded and resourced to address cybercrimes	1.89

Note: Rank order of factors to increase personal ability to respond to cybercrime by police respondents

The only relevant sociodemographic or technology-related variable was age. There were statistically significant positive relationships between age and support for some responses to cybercrime: better education (r=0.118, p<0.01), cooperation with businesses (r=0.116, p<0.01), developing national capabilities (r=0.08, p<0.05), and developing state capabilities (r=0.08, p<0.05). However, the strength of these observed relationships is generally weak.

Results: Community survey

Demographics of survey respondents

The second stage of the project involved a community survey of 2,021 adult respondents. Forty-nine percent (*n*=993) identified as female, 51 percent (*n*=1,028) as male. A further 16 respondents identified as transgender or non-binary; these were excluded from the analyses presented here because they do not meet the threshold for statistical reliability. Nonetheless, we acknowledge the importance of including gender diversity in future cybercrime studies, particularly because some research suggests that online abuse is disproportionately experienced by transgender and non-binary people (see Powell, Scott & Henry 2018). Consistent with the Australian population, most respondents identified as heterosexual (82%, *n*=1,652) rather than gay, lesbian, bisexual or diverse sexuality more broadly. The mean age of respondents was 41 years (*SD*=14.64). A minority of respondents identified as Aboriginal (4%, *n*=70), Torres Strait Islander (1%, *n*=22) or both Aboriginal and Torres Strait Islander (1%, *n*=24). Most respondents spoke only English at home (87%, *n*=1,749).

Approximately 15 percent of respondents reported experiencing long-term difficulty with hearing, seeing, communicating, walking, climbing stairs, bending, learning or doing any similar activities (a measure for disability, *n*=307); 78 percent (*n*=1,568) reported no long-term difficulties. The majority of respondents were tertiary educated (diploma/certificate: 23%, *n*=463; undergraduate degree: 28%, *n*=552; postgraduate degree: 12%, *n*=238), as opposed to the smaller numbers with a primary (3%, *n*=55) or secondary (34%, *n*=680) level of highest education. Approximately half of respondents were currently employed (52%, *n*=1,050).

Technology use and general online experiences

The majority of community respondents indicated that they accessed the internet three or more times a day (83%, *n*=1,682). A third spent three to four hours actively online each day (33%, *n*=660), followed by those who spent five to six hours (22%, *n*=447) and one to two hours (22%, *n*=444). Respondents most commonly had one smartphone or mobile device (73%, *n*=1,470), one desktop (41%, *n*=822), one laptop (60%, *n*=1,201), one tablet (46%, *n*=923). Gaming consoles were less common; many did not own one (47%, *n*=949) or owned only one (28%, *n*=557). The device used most often was a smartphone or mobile (53%, *n*=1,079), followed by a laptop (20%, *n*=412).

Most respondents reported being very comfortable (44%, *n*=888) or comfortable (30%, *n*=614) using a computer. Many reported a mid-level of general computer skills, indicating that they can use a variety of software and fix some computer problems (32%, *n*=647). Others can use the internet and common software but cannot fix computer problems that arise (28%, *n*=559).

Email and text messaging were the most common forms of digital communications used, with 87 percent (*n*=1,753) using email once a day or more, and 74 percent (*n*=1,492) using text messaging once a day or more. Most community respondents also used Facebook once a day or more (68%, *n*=1,371), with somewhat fewer using other social media platforms such as Instagram (39%, *n*=784) once a day or more. Among the most common activities respondents reported engaging in most often on a daily basis online were: communication (3+ times daily: 42%, *n*=847); general web browsing (3+ times daily: 40%, *n*=793); research/information (3+ times daily: 28%, *n*=564); and entertainment/amusement (3+ times daily: 25%, *n*=513). Shopping, banking/finance, blogs/online communities and dating sites were more likely to be engaged in a few times a week or less often.

Community respondents were most likely to report regularly connecting online with family members (79%, *n*=1,597), friends they knew face to face (69%, *n*=1,397), work colleagues (33%, *n*=667), friends they knew online only (31%, *n*=69), and acquaintances (28%, *n*=564). Less common were regular connections online with a current intimate or de facto partner (22%, *n*=43), strangers (11%, *n*=220) or current, past or potential sexual partners (10%, *n*=210).

Perceptions of cybercrime

Community respondents were asked to indicate their position on several statements about general perceptions of cybercrime, under the general topics of ‘Fear of crime’ and ‘Perceived risk’. Results are presented below, in comparison with police data on the same items.

d

Fear of crime

Community participants were asked three sets of questions about their fear of crime. Firstly, they were asked about their fear of traditional crimes. They then responded to an adapted fear of cybercrimes measure (comprising items on identity fraud and financial theft) and to an adapted fear of online abuse and/or interpersonal cybercrimes measure (comprising items on harassment and abuse by strangers, friends or acquaintances, and intimate or ex-intimate partners).

On their fear of traditional crimes, male respondents reported feeling most afraid of:

- their home being broken into (48%);
- being attacked by someone with a weapon (40%);
- being mugged on the street (40%);
- being murdered (38%); or
- having their property damaged (38%).

Female respondents reported feeling more afraid of:

- their home being broken into (70%);
- being attacked by someone with a weapon (63%);
- being mugged on the street (60%);
- being raped (68%);
- being murdered (61%); or
- being harassed, stalked or threatened by stranger (64%).

Consistent with findings in the international literature regarding fear of crime (Callanan & Teasdale 2009; May, Rader & Goodrum 2010), females were overall more fearful than males across all crime types. Females were particularly fearful of violent interpersonal crimes (Table 7). Furthermore, males' mean scores for fear of traditional crime indicated relatively low feelings of fear (averaging between unafraid (2) and neutral (3) points in the scale), while females' mean scores indicated an average rank between neutral (3) and afraid (4). This association between gender and fear of crime was very strong (η^2=0.10) and is also evident in the almost 10 points of difference in the overall mean scores for fear of traditional crimes.

Table 7: Fear of traditional crimes among community respondents, by gender			
Survey item	**Males afraid (%)**	**Females afraid (%)**	**Total afraid (%)**
Being approached on the street by a beggar asking for money	17.7	20.5	19.1
Being cheated, conned or swindled out of your money	35.7	50.4	42.9
Being harassed, stalked or threatened by an intimate partner or ex-partner	26.3	47.9	36.9
Having someone break into your home while you are away	47.9	62.0	54.8
Having someone break into your home while you are there	45.4	70.3	57.6
Being raped or sexually assaulted	31.6	67.5	49.2
Being murdered	38.4	61.0	49.5
Being harassed, stalked or threatened by a stranger	33.4	63.9	48.4
Being physically assaulted by a current or former intimate partner	26.1	47.5	36.6
Being attacked by someone with a weapon	40.8	62.6	51.5
Having your car stolen	35.6	48.2	41.8
Being robbed or mugged on the street	40.3	59.7	49.8
Being sexually harassed by strangers in the street, such as from unwanted whistles, comments and/or looks	23.7	44.5	33.9
Having your property damaged by vandals	38.1	48.1	43.0
Being physically injured in a terrorist attack	33.3	53.5	43.2
Overall fear of traditional crimes, score out of 75, *M (SD)*	43.30 (15.32)	52.94* (14.28)	48.04 (15.58)

*denotes statistically significant difference between males and females mean scores ($F(1, 2019)=214.026$, $p<0.001$, $\eta^2=0.10$). For ANOVA, eta-squared (η^2) of 0.01 indicates a small/weak effect, 0.06 indicates a medium effect, and 0.14 or greater indicates a large effect size

We further analysed mean fear of traditional crime by age groups. Younger adults (18 to 29 years) had higher overall fear of traditional crime scores ($M=50.45$, $SD=14.75$) than older adults (60 to 69 years, $M=45.06$, $SD=16.04$), and the difference by age was statistically significant ($F(4, 2{,}016)=11.201$, $p<0.001$). However, the effect of association by age was small ($\eta^2=0.02$), which is further evident in small (eg one point) changes in mean scores for each age range examined (Table 8).

Table 8: Fear of crime and cybercrime among community respondents, by age					
Aggregate measure	**18–29**	**30–39**	**40–49**	**50–59**	**60–69**
Fear of traditional crimes, *M (SD)*	50.45 (14.75)	49.53 (15.20)	47.92 (15.68)	44.74 (16.00)	45.06 (16.04)
Fear of cybercrimes, *M (SD)*	32.43 (9.83)	32.77 (9.94)	32.61 (10.00)	30.84 (10.36)	31.71 (10.23)
Fear of abuse/interpersonal cybercrimes, *M (SD)*	51.47 (18.25)	48.22 (18.59)	46.47 (19.84)	40.38 (19.97)	39.11 (21.12)

d

When asked about fear of 'conventional cybercrimes' (eg identity and financial computer crimes), respondents were most fearful of having their accounts hacked or having their personal or banking information used for fraudulent transactions (Table 9). Consistent with fear of traditional crimes, females were more likely to rate themselves as afraid or very afraid across all crime subtypes and were overall statistically more likely be afraid of each cybercrime subtype than male participants. However, interestingly, this association for fear of identity/financial cybercrimes by gender was relatively weak, which is further evident in just a few points of difference in overall mean scores. There was no significant difference in mean fear of cybercrime scores by age.

Table 9: Fear of cybercrimes among community respondents, by gender

Survey item	Males afraid (%)	Females afraid (%)	Total afraid (%)
Sending money in response to an email request that you have received	24.7	29.3	27.0
Sending money for an online purchase, but not receiving the goods as expected	34.2	44.5	39.3
Sending money in response to a request from someone you have initiated an online relationship with	25.9	31.4	28.6
Being asked to send money in response to a business/ employment opportunity that was promoted online	27.3	32.1	29.7
Sending personal information (such as username, password or banking details) to an organisation in response to an email request	36.5	43.6	40.0
Having your personal information exposed to the public by another organisation without your consent/knowledge	48.3	62.4	55.3
Having someone use your personal information without your permission to make purchases, create new accounts or pretend to be you	50.0	66.3	58.0
Having someone use your credit card or bank accounts without your permission to make financial transactions	49.4	67.2	58.1
Having someone hack into one of your accounts	51.2	68.9	59.9
Having a virus on your computer or other device	44.1	60.3	52.1
Overall fear of cybercrimes, score out of 50; *M (SD)*	30.49 (9.97)	33.89* (9.83)	32.16 (10.04)

*denotes statistically significant difference between males and females mean scores ($F(1, 2{,}019)=59.618$, $p<0.001$, $\eta^2=0.03$)

Finally, we examined fear of interpersonal cybercrimes (such as sexual harassment, image-based abuse and intimate partner abuse) and online harassment and abuse, whether received from strangers or friends and acquaintances. Community participants rated themselves as most afraid of a stranger accessing their online accounts and/or posting offensive content while pretending to be them (Table 10). However, there was a clear overall pattern of variance between genders. Females were more likely to self-rate as being afraid or very afraid of interpersonal crimes generally, as well as of specific subtypes, such as sexually violent threats, image-based abuse and sexual harassment behaviours. This difference between male and female respondents was statistically significant for overall mean fear of crime scores, with a medium effect size ($\eta^2=0.06$), which is further reflected in an approximately 10-point difference in mean scores by gender.

Table 10: Fear of online abuse/interpersonal cybercrimes among community respondents, by gender

Survey item	Males afraid (%)	Females afraid (%)	Total afraid (%)
Having someone take a photo or video of you, when you were nude or semi-nude, without your permission	25.7	46.9	36.1
Having someone send your nude or sexual photos/videos on to others or post them online without your permission	29.7	48.0	38.7
Having someone threaten that they will send a nude or sexual photo/video of you on to others or post them online	28.8	45.5	37.0
Receiving insulting or threatening comments by strangers online, such as via social media, dating apps or web forums	25.8	43.9	34.7
Having a stranger spread rumours or lies about you online	28.2	42.7	35.3
Having a stranger access your online accounts without your permission and/or post offensive content pretending to be you online	38.7	56.1	47.3
Receiving insulting or threatening comments by friends or acquaintances online, such as via social media, dating apps or web forums	26.0	41.4	33.5
Having a friend or acquaintance spread rumours or lies about you online	26.8	41.8	34.1
Having a friend or acquaintance access your online accounts without your permission and/or post offensive content pretending to be you online	29.7	45.0	37.2
Having someone make online threats to sexually harm you, rape or sexually assault you	26.8	50.3	38.3
Being sent unwanted requests for sex, or sexual comments, by someone online	25.2	44.7	34.8
Receive nude or sexual images (photos or videos) from a person when you did not want or request them	25.9	44.5	35.0
Having an intimate partner or ex-partner make threats to physically hurt you, via phone calls, text messages, social media or online posts	23.7	44.6	34.0
Having an intimate partner or ex-partner repeatedly ask where you are or what you are doing through phone calls, text messages, social media or online posts	23.6	40.7	32.0
Having an intimate partner or ex-partner access your online accounts without your permission, eg email, social media, banking or phone data	29.6	41.7	35.5
Having an intimate partner or ex-partner send insulting or derogatory messages to you, such as via text message, email, social media or online posts	23.9	41.5	32.6
Overall fear of online abuse/interpersonal cybercrimes, score out of 80; *M (SD)*	41.46 (18.83)	51.09* (19.76)	46.19 (19.88)

*denotes statistically significant difference between males and females mean scores ($F(1, 2019)=125.765$, $p<0.001$, $\eta^2=0.06$)

d

We further analysed mean fear of online abuse and interpersonal cybercrimes by age groups. Younger adults (18 to 29 years: *M*=51.47, *SD*=18.25; and 30 to 39 years: *M*=48.22, *SD*=18.59) had higher overall fear of traditional crime scores than older adults (50 to 59 years: 40.38, *SD*=19.97; and 60 to 69 years: *M*=39.11, *SD*=21.12), and the difference by age was statistically significant (*F(*4, 2,016)=29.337, *p*<0.001). Further, the effect of association by age was medium (η^2=0.06), which is further evident in an approximately 12-point difference in mean scores between the youngest and oldest age range.

Perceived risk

Community respondents were asked to rate their perceived risk of crime victimisation by responding to a set of statements and indicating how likely they thought it was that they would experience this crime in the next 12 months. Overall, a majority of community respondents indicated that they were not likely to become a victim of the traditional crimes surveyed. The crime types that were perceived as most likely to be experienced in the next 12 months were: being approached on the street for money, having someone break into their home while they are away, and having property damaged by vandals. There were no significant differences between males and females in overall mean perceived risk of traditional crimes scores (Table 11). There were, however, significant (although small) differences by age (see Table 14): younger adults (18 to 29 years, *M*=34.22, *SD*=14.39) were more likely than older adults (60 to 69 years, *M*=29.70, *SD*=11.45) to self-rate as likely or very likely to experience these traditional crimes in the next 12 months (*F*(4, 2,016)=6.977, *p*<0.001, η^2=0.01).

Table 11: Perceived risk of traditional crimes among community respondents, by gender			
Survey item	**Males likely (%)**	**Females likely (%)**	**Total likely (%)**
Being approached on the street by a beggar asking for money	41.2	38.2	39.7
Being cheated, conned or swindled out of your money	14.5	9.2	11.9
Being harassed, stalked or threatened by an intimate partner or ex-partner	14.1	10.9	12.5
Having someone break into your home while you are away	17.2	15.6	16.4
Having someone break into your home while you are there	14.8	14.0	14.4
Being raped or sexually assaulted	13.7	10.7	12.2
Being murdered	14.3	9.4	11.9
Being harassed, stalked or threatened by a stranger	14.8	12.0	13.4
Being physically assaulted by a current or former intimate partner	12.7	10.2	11.5
Being attacked by someone with a weapon	15.1	10.6	12.9
Having your car stolen	15.9	12.9	14.4
Being robbed or mugged on the street	14.5	12.4	13.5
Being sexually harassed by strangers in the street, such as from unwanted whistles, comments and/or looks	11.9	17.3	14.5
Having your property damaged by vandals	17.2	15.2	16.2
Being physically injured in a terrorist attack	13.3	9.8	11.6
Overall perceived risk of traditional crimes, score out of 75; *M (SD)*	33.29 (14.69)	32.67 (12.78)	32.99 (13.78)

The majority of respondents rated themselves as unlikely to experience identity and financial cybercrimes in the next 12 months. Among those crime types most likely to be perceived as a risk were: having a computer virus (20% agreed that it was likely or very likely); having an account hacked (16% agreed that it was likely or very likely); having personal information exposed publicly (15% agreed that it was likely or very likely); and having someone fraudulently use their credit card or banking information to make purchases (14% agreed it was likely or very likely). Table 12 shows the gender breakdown. There was a significant (although small) statistical difference between males and females in overall mean perceived risk of identity/financial cybercrimes scores ($F(1, 2{,}019)=12.115$, $p<0.01$, $\eta^2=0.006$). There were also significant (although again small) differences by age (see Table 14), such that younger adults (18 to 29 years, $M=21.48$, $SD=9.80$), were more likely than older adults (60 to 69 years, $M=19.07$, $SD=7.92$) to self-rate as likely or very likely to experience these cybercrimes in the next 12 months ($F(4, 2{,}016)=6.715$, $p<0.001$, $\eta^2=0.013$).

d

Table 12: Perceived risk of cybercrimes among community respondents, by gender

Survey item	Males likely (%)	Females likely (%)	Total likely (%)
Sending money in response to an email request that you have received	9.1	4.6	6.9
Sending money for an online purchase, but not receiving the goods as expected	13.9	12.6	13.3
Sending money in response to a request from someone you have initiated an online relationship with	11.3	6.3	8.9
Being asked to send money in response to a business/ employment opportunity that was promoted online	13.4	8.8	11.1
Sending personal information (such as username, password or banking details) to an organisation in response to an email request	12.2	9.9	11.0
Having your personal information exposed to the public by another organisation without your consent/knowledge	16.1	13.7	14.9
Having someone use your personal information without your permission to make purchases, create new accounts or pretend to be you	16.0	10.1	13.1
Having someone use your credit card or bank accounts without your permission to make financial transactions	15.9	13.0	14.4
Having someone hack into one of your accounts	17.2	14.2	15.7
Having a virus on your computer or other device	20.0	19.0	19.5
Overall perceived risk of cybercrimes, score out of 50; *M (SD)*	21.50* (9.72)	20.06 (8.78)	20.79 (9.30)

*denotes statistically significant difference between males and females mean scores ($F(1, 2019)=12.115$, $p<0.01$, $\eta^2=0.006$)

Finally, we asked community survey participants to rate their perceived risk of experiencing a range of online abuse and/or interpersonal cybercrimes in the next 12 months. Receiving unwanted sexual requests (14%) and unsolicited nude or sexual images (14%) were rated among the most likely to be experienced. There was a significant, although very weak, difference in overall mean scores by gender, such that males were more likely to self-rate themselves as likely or very likely to experience these crimes in the next 12 months (Table 13).

Table 13: Perceived risk of online abuse or interpersonal cybercrimes among community respondents, by gender

Survey item	Males likely (%)	Females likely (%)	Total likely (%)
Having someone take a photo or video of you, when you were nude or semi-nude, without your permission	10.3	5.9	8.2
Having someone send your nude or sexual photos/videos on to others or post them online without your permission	12.9	6.6	9.8
Having someone threaten that they will send a nude or sexual photo/video of you on to others or post them online	12.8	7.5	10.2
Receiving insulting or threatening comments by strangers online, such as via social media, dating apps or web forums	14.0	11.8	12.9
Having a stranger spread rumours or lies about you online	14.6	9.5	12.1
Having a stranger access your online accounts without your permission and/or post offensive content pretending to be you online	12.1	8.6	10.3
Receiving insulting or threatening comments by friends or acquaintances online, such as via social media, dating apps or web forums	12.5	8.1	10.3
Having a friend or acquaintance spread rumours or lies about you online	14.0	9.8	11.9
Having a friend or acquaintance access your online accounts without your permission and/or post offensive content pretending to be you online	11.9	7.6	9.7
Having someone make online threats to sexually harm you, rape or sexually assault you	12.2	8.7	10.4
Being sent unwanted requests for sex, or sexual comments, by someone online	15.2	13.5	14.3
Receive nude or sexual images (photos or videos) from a person when you did not want or request them	14.4	13.2	13.8
Having an intimate partner or ex-partner make threats to physically hurt you, via phone calls, text messages, social media or online posts	12.4	8.5	10.4
Having an intimate partner or ex-partner repeatedly ask where you are or what you are doing through phone calls, text messages, social media or online posts	11.9	8.7	10.3
Having an intimate partner or ex-partner access your online accounts without your permission, eg email, social media, banking or phone data	11.8	8.4	10.1
Having an intimate partner or ex-partner send insulting or derogatory messages to you, such as via text message, email, social media or online posts	10.1	8.8	9.5
Overall perceived risk of online abuse/interpersonal cybercrimes, score out of 80; *M (SD)*	31.45* (16.77)	29.05 (14.90)	30.27 (15.92)

*denotes statistically significant difference between males and females overall mean scores ($F(1, 2019)=11.517$, $p<0.01$, $\eta^2=0.006$)

d

There was also a significant (although again small) difference in perceived risk of online abuse and/or interpersonal cybercrimes by age (Table 14). Younger adults (18 to 29 years, *M*=34.09, *SD*=16.45) reported an overall higher self-rating of perceived victimisation risk than older adults (60 to 69 years, *M*=23.70, *SD*=11.65), with a medium effect size ($F(4, 2{,}016)=28.194$, $p<0.001$, $\eta^2=0.053$).

Table 14: Perceived risk of crime and cybercrime among community respondents, by age

Aggregate measure	18–29	30–39	40–49	50–59	60–69
Traditional crimes, score out of 75; *M (SD)*	34.22 (14.39)	34.53 (14.88)	32.72 (13.74)	31.88 (12.56)	29.80 (11.45)
Cybercrimes, score out of 50; *M (SD)*	21.48 (9.80)	21.99 (9.78)	20.82 (9.40)	19.52 (8.39)	19.07 (7.92)
Abuse/interpersonal cybercrimes, score out of 80; *M (SD)*	34.09 (16.45)	32.63 (16.96)	29.72 (15.96)	26.90 (14.20)	23.70 (11.65)

Cybercrime risk and resilience

Community respondents also self-rated their confidence in their knowledge and skills to protect themselves from potential cybercrimes. Overall, most respondents were either very or somewhat confident (47%, *n*=955) or neither confident nor unconfident (35%, *n*=712). Male participants were significantly more likely to self-rate as more confident in their knowledge and skills (51%, *n*=519) than female participants (44%, *n*=436, $F(1, 2{,}019)=6.693$, $p<0.05$), although the association by gender was very weak ($\eta^2=0.003$). Similarly, there was a statistically significant, although weak, difference by age: younger adults (18 to 29 years, *M*=3.51, *SD*=1.20) were more likely to self-rate as more confident in their knowledge and skills to protect themselves from cybercrime than older adults (60 to 69 years, *M*=3.20, *SD*=1.06, $F(4, 2{,}016)=4.371$, $p<0.01$, $\eta^2=0.009$).

The most common strategies for protecting themselves from cybercrimes included: avoiding opening email attachments from unknown senders, conducting online purchases only with trusted companies, deleting emails from unknown senders, avoiding clicking on pop-ups when web browsing, and blocking users they did not want to communicate with. Among the least common actions taken were: using a password manager, regularly changing passwords, using two-step authentication on online accounts, obscuring online identity information, and updating their operating system. Interestingly, female participants (*M*=58.90, *SD*=12.57) were significantly more likely to report regularly engaging in self-protection behaviours from cybercrime than males (*M*=57.51, *SD*=13.56, $F(1, 2{,}019)=5.8$, $p<0.05$), although the association was again very weak ($\eta^2=0.003$). There was again a significant (although very weak) association by age, whereby younger adults (18 to 29 years, *M*=55.47, *SD*=13.79) were less likely to report regularly taking action to protect themselves from cybercrimes than older adults (60 to 69 years, *M*=61.00, *SD*=11.90, $F(4, 2{,}016)=12.198$, $p<0.001$, $\eta^2=0.024$).

Cybercrime victimisation, reporting and police responses

Community respondents were asked about their experience of a range of cybercrime victimisation types and whether they reported their experience to police. If so, they were asked to rate the police response. Cybercrime victimisation types included identity crimes, financial crimes, sexual harassment, image-based abuse, intimate partner abuse and general online harassment or abuse, whether from strangers, friends or acquaintances.

Overall, 82 percent (*n*=1,648) of our community respondents had experienced at least one of the listed forms of cybercrime victimisation. In order of the most commonly experienced, they were:

- identity crimes (63%, *n*=1,272);
- stranger harassment or abuse (52%, *n*=1,052);
- financial crimes (51%, *n*=1,028);
- acquaintance or friend harassment or abuse (44%, *n*=884);
- online sexual harassment (39%, *n*=788);
- online intimate partner abuse (35%, *n*=709); and
- image-based abuse (28%, *n*=558).

The following sections examine these victimisation rates and reporting experiences (where applicable) in further detail.

Identity and financial cybercrimes

Among experiences of identity cybercrimes, the most common were having a computer virus, or having bank account or credit card information fraudulently accessed (Table 15). Identity cybercrime victimisation differed somewhat by gender, with overall rates of victimisation higher for males than females, although effect sizes were very small (approaching zero) and indicated little strength of association between gender and victimisation for identity crimes. For overall victimisation of any identity cybercrimes, younger adults (18 to 29 years, 67%) were more likely than older adults (60 to 69 years, 58%) to disclose victimisation experience.

d

Table 15: Identity cybercrime victimisation among community respondents, by gender

Survey item	Males (%)	Females (%)	Total (%)
You've sent personal information (such as username, password, banking details) to an organisation in response to an email request	12.3	8.4	10.3
Having your personal information exposed to the public by another organisation without your consent/knowledge	13.4	9.4	11.4
Having someone use your personal information without your permission to make purchases, create new accounts or pretend to be you	9.7	7.8	8.8
Having someone use your credit card or bank accounts without your permission to make financial transactions	15.5	15.6	15.5
Having someone hack into one of your accounts	10.1	13.6	11.8
Having a virus on your computer or other device	29.2	27.1	28.2
Any identity cybercrime victimisation	66.9*	58.8	62.9

*denotes statistically significant difference between males and females for any victimisation ($\chi^2(1, N=2,021)=14.26$, $p<0.001$, $\phi=0.08$). For chi-square analyses (χ^2), a phi (ϕ) of 0.1 or less indicates a small/weak effect size, 0.3 indicates a medium effect, and 0.5 or greater indicates a large effect size

Asked whether they had reported their most recent identity cybercrime experience to police, fewer than one in five (17%, *n*=216) said that they had. Most reported either in person or by phone to their local police station, followed by online (such as via the ACORN website). Of those who reported to police, a large majority (71%, *n*=146) said that they found it helpful or very helpful.

For financially based cybercrimes, more respondents reported experiencing failed or fraudulent online purchases, followed by online requests for money for a 'business opportunity' (Table 16). As with identity crimes, there was a significant difference by gender, with males again reporting higher victimisation rates; once again, tests of effect size indicate little strength in the association between gender and financial cybercrime victimisation. Almost twice as many younger adults (18 to 29 years, 62%) reported experiencing at least one type of financial cybercrime, compared with older adults (60 to 69 years, 32%).

Table 16: Financial cybercrime victimisation among community respondents, by gender

Survey item	Males (%)	Females (%)	Total (%)
Sending money in response to an email request that you have received	12.1	6.1	9.2
Sending money for an online purchase, but not receiving the goods as expected	19.8	26.0	22.9
Sending money in response to a request from someone you have initiated an online relationship with	9.1	4.8	7.0
Being asked to send money in response to a business/ employment opportunity that was promoted online	19.3	16.4	17.9
Any financial cybercrime victimisation	53.3*	48.3	50.9

*denotes statistically significant difference between males and females for any victimisation ($\chi^2(1, N=2,021)=4.99$, $p<0.05$, $\phi=0.05$)

Participants were again asked whether they had reported their most recent experience to police. Of those who responded, again, fewer than one in five (17%, *n*=176) said that they reported their most recent experience to police, most commonly to their local station or online (such as via ACORN). Again, of those who did report to police, a majority found it helpful or very helpful (68%, *n*=116).

Interpersonal cybercrime

Respondents were asked about three categories or subtypes of interpersonal cybercrimes: online sexual harassment, image-based abuse and abuse from an intimate or former intimate partner, spouse or date. For sexual harassment, respondents were most likely to report having received a nude or sexual image from a person (which they had neither wanted nor requested, 17%, *n*=352), followed closely by receiving unwanted requests for sex or sexual comments (16%, *n*=324). Male and female participants were equally likely to have experienced at least one of the listed sexually harassing behaviours. Females were significantly more likely to experience three of the four behaviours (Table 17), although the associations by gender were again weak. For overall victimisation by any online sexual harassment, younger adults (18 to 29 years, 59%) were much more likely than older adults (60 to 69 years, 16%) to disclose victimisation experience, which is reflective of broader patterns of in-person sexual harassment in Australia (Australian Human Rights Commission 2018: 21).

Table 17: Online sexual harassment victimisation among community respondents, by gender

Survey item	Males (%)	Females (%)	Total (%)
Someone made online threats to sexually harm you, rape or sexually assault you	9.0	8.2	8.6
Someone online sent unwanted requests for sex, or sexual comments (not including 'spam' email or advertisements)	14.0	18.1#	16.0
You've received nude or sexual images (photos or videos) from a person when you did not want or request them	14.1	20.8^	17.4
Someone online has made sexual comments or sent sexual messages to you, when you did not want or request them (not including 'spam' email or advertisements)	11.3	18.1*	14.6
Any online sexual harassment	40.0	38.0	39.0

#denotes statistically significant difference between males and females ($\chi^2(1, N=2,021)=6.37$, $p<0.01$, $\phi=0.06$)
^denotes statistically significant difference between males and females ($\chi^2(1, N=2,021)=15.96$, $p<0.001$, $\phi=0.09$)
*denotes statistically significant difference between males and females ($\chi^2(1, N=2,021)=18.92$, $p<0.001$, $\phi=0.1$)

Almost one in five respondents (19%, *n*=150) said that they reported their most recent experience to police, with most reporting either to their local police station or online (such as via the ACORN website). Of those who reported to police, a large majority (73%, *n*=108) said that they found police responses to their complaint helpful or very helpful.

d

Overall, approximately one in three men and almost one in four women reported ever having experienced any image-based abuse—although the strength of association of gender was again weak. Most commonly, participants reported having experienced the non-consensual distribution or posting online of a nude or sexual image (Table 18). Consistent with previous Australian-based research (see Henry, Flynn & Powell 2017), younger adults (18 to 29 years, 46%) were much more likely to report victimisation from image-based abuse than older adults (60 to 69 years, 5%).

Table 18: Image-based abuse victimisation among community respondents, by gender

Survey item	Males (%)	Females (%)	Total (%)
Someone has taken a photo or video of you, when you were nude or semi-nude, without your permission	10.7	7.7	9.2
Someone sent your nude or sexual photos/videos on to others or post them online without your permission	13.3	11.0	12.2
Someone threatened that they will send a nude or sexual photo/video of you on to others or post it online	10.1	9.7	9.9
Any image-based abuse	32.0*	23.1	27.6

*denotes statistically significant difference between males and females for any victimisation ($\chi^2(1, N=2,021)=20.21$, $p<0.001$, $\phi=0.1$)

Note: Measures of victimisation for image-based abuse adapted from Powell & Henry (2017)

We asked those respondents who disclosed an experience of image-based abuse victimisation whether they had reported their most recent experience to police, and how helpful it was. Overall, 28 percent (*n*=156) said that they reported their most recent experience to police (notably higher than for the preceding cybercrime types), most commonly at their local police station, and most (76%) found reporting to police to be helpful or very helpful.

Overall, approximately one in three community respondents (35%, *n*=709) reported having ever experienced at least one of the intimate partner abuse behaviours surveyed. Male and female participants were similarly likely to have experienced at least one of the listed intimate partner behaviours, but females were significantly more likely to experience three of the five behaviours (Table 19), including stalking behaviours and insulting or derogatory messages—although the associations by gender were weak. Again, consistent with an overall trend for age, we found that younger adults (18 to 29 years, 52%; and 30 to 39 years, 43%) were more likely than older adults (50 to 59 years, 23%; and 60 to 60 years, 9%) to report experiencing intimate partner abuse.

Table 19: Intimate partner abuse victimisation among community respondents, by gender			
Survey item	**Males (%)**	**Females (%)**	**Total (%)**
A current or former partner made threats to physically hurt you, via phone calls, text messages, social media or online posts	10.8	12.9	11.8
A current or former partner repeatedly asked where you are or what you are doing, through phone calls, text messages, social media or online posts	12.5	17.4#	14.9
A current or former partner accessed your online accounts without your permission, eg email, social media, banking or phone data	6.9	10.1^	8.5
A current or former partner sent insulting or derogatory messages to you, such as via text message, email, social media or online posts	6.9	15.1*	10.9
A current or former partner tracked your location using a positioning device or mobile phone application ('app')	6.5	6.8	6.7
Any online intimate partner abuse	35.7	34.4	35.1

#denotes statistically significant difference between males and females (χ^2{1, N=2,021]=9.44, p<0.01, ϕ=0.07)
^denotes statistically significant difference between males and females (χ^2(1, N=2,021)=6.53, p<0.01, ϕ=0.06)
*denotes statistically significant difference between males and females (χ^2(1, N=2,021)=34.86, p<0.001, ϕ=0.13)

Of the respondents disclosing experiences of intimate partner abuse, approximately one in four (24%, *n*=171) said that they reported their most recent experience to police. As with the other cybercrimes reported here, this was most often to their local police station (either in person or by phone) or online (such as via ACORN). Again, most respondents found reporting to police to be either very helpful or helpful (75%, *n*=112).

General online harassment and abuse

The last two cybercrime types we asked about in our community survey concerned more general experiences of online harassment and abuse, whether from strangers or from friends and acquaintances. Approximately one in two community respondents (52%, *n*=1,052) reported ever having experienced online harassment or abuse from strangers. The most common was receiving insulting or threatening comments, with more than one in four (29%, *n*=577) respondents reporting such an experience. Overall, men were statistically more likely to report at least one experience of stranger online harassment or abuse (Table 20). For overall victimisation of online harassment or abuse from strangers, younger adults (18 to 29 years, 74%) were much more likely than older adults (60 to 69 years, 23%) to disclose any victimisation experience.

d

Table 20: Stranger online harassment/abuse victimisation among community respondents, by gender

Survey item	Males (%)	Females (%)	Total (%)
Received insulting/threatening comments by strangers online	29.3	27.8	28.6
Had a stranger spread rumours or lies about you online	17.6	15.7	16.7
Had a stranger access your online accounts without your permission	16.5	14.1	15.3
Had a stranger post offensive content pretending to be you online	6.1	6.3	6.2
Any stranger online harassment/abuse	56.4*	47.5	52.1

*denotes statistically significant difference between males and females for any victimisation ($\chi^2(1, N=2,021)=15.99$, $p<0.001$, $\phi=0.09$)

Approximately one in four (23%, *n*=241) respondents said that they reported their most recent experience of cybercrime victimisation to police. A majority, although notably fewer than for other cybercrimes, said that reporting to police had been either helpful or very helpful (67%, *n*=158).

Finally, 44 percent (*n*=884) of community respondents reported at least one experience of online harassment or abuse from friends or acquaintances. Most common was receiving insulting or threatening comments and having rumours or lies spread about them (Table 21). Males were significantly more likely to report ever having at least one harassment or abuse experience from friends or acquaintances, although the small effect size again suggests a weak association. Consistent with the overall trend of response variance according to age, younger adults (18 to 29 years, 64%) were more likely than older adults (60 to 69 years, 17%) to disclose experiencing online harassment or abuse from friends or acquaintances (Table 22).

Table 21: Friend/acquaintance online harassment/abuse victimisation among community respondents, by gender

Survey item	Males (%)	Females (%)	Total (%)
Received insulting or threatening comments by friends or acquaintances online	18.7	21.2	19.9
Had friends or acquaintances spread rumours or lies about you online	19.4	20.1	19.7
Had friends or acquaintances access your online accounts without your permission	9.1	8.0	8.6
Had friends or acquaintances post offensive content pretending to be you online	7.1	6.0	6.6
Any friend/acquaintance online harassment/abuse	46.1*	41.3	43.7

*denotes statistically significant difference between males and females for any victimisation ($\chi^2(1, N=2,021)=4.77$, $p<0.05$, $\phi=0.05$)

Approximately one in four respondents (23%, *n*=197) said that they reported their most recent experience of online harassment or abuse from friends or acquaintances to police. A majority (71%, *n*=137) said that reporting to police had been either helpful or very helpful.

Table 22: Overall cybercrime victimisation among community respondents, by age

Victimisation category	18–29[a] (%)	30–39[b] (%)	40–49[c] (%)	50–59[d] (%)	60–69[e] (%)
Any identity cybercrimes	67.1	66.6	62.6	56.1	57.8
Any financial cybercrimes	62.4	54.5	51.9	41.3	32.3
Any online sexual harassment	58.8	43.9	35.8	22.5	15.6
Any image-based abuse	46.3	31.6	22.7	15.1	5.3
Any online intimate partner abuse	51.6	42.8	32.1	22.8	8.5
Any stranger online harassment/abuse	73.8	58.6	48.7	35.0	23.0
Any friend/acquaintance online harassment/abuse	64.0	50.3	40.4	27.4	17.0
Any cybercrime victimisation*	89.3[c,d,e]	85.8[d,e]	80.7[a,d,e]	74.9[a,b]	68.4[a,b,c]

*denotes statistically significant difference by age range for any overall cybercrime victimisation ($\chi^2(4, N=2,021)=70.63$, $p<0.001$, $\phi=0.19$). Letters denote which age ranges differ from each other

Results: Comparison between the police and community survey

One of the issues identified within the existing research was a potential disconnect between police and community expectations about responses to cybercrime. Specifically, criminological research has revealed how members of the public often have unrealistic expectations about responses to cybercrime (eg Wall 2008a, 2008b); how police and the community assess the seriousness of cybercrime offences and ascribe responsibility according to the criteria of 'ideal' victimisation (eg Black, Lumsden & Hadlington 2019; Holt & Bossler 2016); how victims of cybercrime are often not satisfied with police responses (eg Cross, Richards & Smith 2016; Jang, Joo & Zhao 2010); and how police feel ill equipped to respond to cybercrime and cybersecurity threats (eg Hadlington et al. 2018; Nouh et al. 2019). This section presents a comparative analysis of the police and community survey results, examining these issues in greater detail and within an Australian context.

The data analyses presented in this section are based on a sub-sample of the data discussed in the two preceding sections. The results of the survey are based upon a sample of police officers (*n*=422) and members of the public (*n*=754) from the states of Queensland and New South Wales. This sub-sample has been used to ensure that the samples are sufficiently matched and therefore enable robust comparative analysis (see Gorard 2017: 101). Data collected from the Policing Cybercrime in Australia survey (stage one) and Cybercrime and Online Harm survey (stage two) are presented in contingency tables that compare police and community attitudes on various survey items. Additionally, these data were analysed using chi-square tests for independence between the sample groups (police and community). The results are presented across four identified themes:

- seriousness of cybercrime offences;
- knowledge of cybercrime offences;
- perceived distribution of responsibility; and
- confidence in police responses to cybercrime.

Broadly, the analyses reveal that police officers rank cybercrime as more serious, that the groups have different understandings about cybercrime and its impact on policing, that the community ascribes comparatively greater responsibility to individuals for preventing cybercrime victimisation, and that the community reports comparatively more confidence in law enforcement to effectively respond to cybercrime and cybersecurity threats.

Seriousness of cybercrime

The first set of comparative analyses concerns the extent to which police and community respondents hold different views about the seriousness of cybercrime offences. The results of cross-tabulation and chi-square analyses comparing such attitudes across three response levels (agree, neutral, disagree) are presented in Table 23.

Table 23: Attitudes to seriousness of cybercrime among police and community respondents

Sample group	Police (%)			Community (%)		
Survey item/response	Agree	Neutral	Disagree	Agree	Neutral	Disagree
Cybercrime is a serious problem in society today***	86.2	3.7	10.1	80.0	12.6	7.4
Most types of online incidents are minor annoyances***	31.4	24.1	44.5	43.9	32.0	24.1
Harassment online is less serious than face-to-face harassment***	21.1	8.9	70.0	21.1	17.5	61.4
Stealing $100 from a person's bank account electronically is equivalent to someone pickpocketing $100***	77.8	3.9	18.3	77.6	12.1	10.3
Cybercrime is not taken seriously by law enforcement**	33.5	19.5	47.0	29.4	28.6	41.9
Most negative online experiences do not require a police response**	47.0	29.6	23.4	37.1	37.4	25.5

**indicates χ^2 with $p<0.01$, ***indicates χ^2 with $p<0.001$

The six items listed within Table 23 highlight significant differences in the response patterns of police officers and community members in Queensland and New South Wales. Across all categories, members of the community were more likely to provide 'neutral' responses to survey items. Specifically, members of the community were more likely to remain 'neutral' about whether 'cybercrime is a serious problem in society today' and whether 'cybercrime is not taken seriously by law enforcement', with otherwise comparatively similar proportions of participants either agreeing or disagreeing with the statements. This observed pattern is probably a result of respective levels of expertise and self-confidence in providing meaningful responses to survey items.

Generally, police officers were more likely to assess cybercrimes as serious. For example, police were comparatively more likely to disagree with the statements: 'most types of online incidents are minor annoyances' and 'harassment online is less serious than face-to-face harassment'. Although more police officers disagreed with the statement that 'stealing $100 from a person's bank account is equivalent to someone pickpocketing $100', this difference was apparently due to fewer 'neutral' responses.

d

Similarly, police officers were more likely to agree with the statement that 'most negative online experiences do not require a police response', whereas community members were more likely to offer a neutral response. These different patterns of responses reflect the differences in how the groups perceive the seriousness of cybercrime, including differences in their perception of how serious law enforcement agencies consider the issue.

Knowledge of cybercrime

The second set of analyses examined the comparative knowledge of cybercrime among police and community respondents. Table 24 presents the results of cross-tabulation and chi-square analyses comparing attitudes across three response levels (agree, neutral, disagree).

Table 24: Knowledge of cybercrime among police and community respondents

Sample group	Police (%)			Community (%)		
Survey item/response	Agree	Neutral	Disagree	Agree	Neutral	Disagree
The public understand the risks of being online***	11.9	11.2	76.8	37.7	25.3	37.0
The local community does not recognise the threat posed by cybercrime***	76.6	14.0	9.4	54.5	29.6	15.9
The internet has dramatically changed police work***	92.4	6.2	1.4	75.2	18.7	6.1
The internet has caused more problems for law enforcement than it has helped*	46.3	32.1	21.6	46.3	37.4	16.3
Cybercrime occurs more frequently in businesses, rather than among home users***	10.1	42.7	47.2	27.2	37.5	35.3
The majority of cybercrimes are perpetrated by younger individuals in their teens and twenties***	11.0	41.3	47.7	34.2	35.0	30.8
Cybercriminals are often individuals living in foreign countries rather than here in Australia	36.2	37.2	26.6	34.5	35.3	30.2
Cybercrime is mostly traditional crimes using a computer***	29.6	21.3	49.1	35.0	28.9	36.1
Crimes that used to be offline now increasingly have online elements***	81.4	17.0	1.6	72.4	23.9	3.7
Digital evidence can be a feature of all types of crime	77.3	17.4	5.3	71.5	22.7	5.8
Most cybercrime incidents or crimes should be responded to by a specialised high-tech crime unit***	65.6	17.9	16.5	62.1	30.6	7.3

*indicates χ^2 with $p<0.05$, ***indicates χ^2 with $p<0.001$

Note: Selected cross-tabulations for police and community knowledge of cybercrime offences

The 11 items listed in Table 24 highlight the greater variation between the response pattern of police officers and community members on measures about knowledge of cybercrime. In particular, the groups have significantly different response patterns on measures about public understanding of the risks and threat of cybercrime. Police are more likely to disagree with the statement that 'the public understand the risks of being online' and agree with the statement that 'the local community does not recognise the threat posed by cybercrime'. Additionally, there were observable differences between the groups in measures of how technology has impacted policing. Police officers were more likely to agree with the statement that 'the internet has dramatically changed police work'. Police officers were also more likely to disagree with the statement that 'the internet has caused more problems for law enforcement than it has helped', but this resulted from fewer neutral responses than came from community members. Finally, police were also more likely to disagree with, rather than remain neutral on, the statement that 'most cybercrime incidents or crimes should be responded to by a specialised high-tech crime unit'.

The groups showed significant differences on the relationship between cybercrime and traditional crimes. For example, police were more likely to disagree with the statement that 'cybercrime is mostly traditional crimes using a computer' and agree with the statement that 'crimes that used to be offline now increasingly have online elements'. This suggests that police appreciate the importance of conceptually differentiating cybercrime from offline crimes (ie cyber-dependent crimes), yet are aware of how technology is also used to facilitate traditional forms of crime (ie cyber-enabled crimes). It is also important to note that these patterns are potentially explained by more 'neutral' responses to the survey items by community respondents, which may suggest that members of the public are simply uncertain or indifferent. Still, it is interesting to observe no significant differences in responses to the statement that 'digital evidence can be a feature of all types of crime'.

Finally, there were some notable differences in perceptions of cybercriminals and their targets. Community respondents were more likely to agree with the statements: 'cybercrime occurs more frequently in businesses rather than among home users' and 'the majority of cybercrimes are perpetrated by younger individuals in their teens and twenties'. However, there were no differences between groups in attitudes to whether 'cybercriminals are often individuals living in foreign countries rather than here in Australia'. Interestingly, these survey items measuring knowledge of the sociodemographic characteristics of cybercrime offenders and victims were the only items where police reported more 'neutral' responses than community members. Community members seemed more confident in their assessment of victim and offender profiles, while being comparatively more likely to believe that cybercriminals are young people who target businesses rather than individuals.

d

Distribution of responsibility

The third set of comparative analyses examined measures of how police officers and community members distributed responsibility for cybercrime offences. Table 25 presents the results of cross-tabulation and chi-square analyses comparing such attitudes across three response levels (agree, neutral, disagree).

Table 25: Distribution of responsibility for cybercrime among police and community respondents

Sample group	Police (%)			Community (%)		
Survey item/response	Agree	Neutral	Disagree	Agree	Neutral	Disagree
Online bullying and harassment can be avoided by victims changing mobile phone numbers or email addresses*	32.3	22.7	45.0	30.8	29.8	39.4
Online fraud victims lose money because they do not pay attention to what they read***	34.4	25.7	39.9	43.9	30.9	25.2
If a person sends a nude or sexual image to someone else, then they are at least partly responsible if the image ends up online**	55.5	16.7	27.8	60.3	19.8	19.9
People should know better than to take nude selfies in the first place, even if they never send them to anyone***	50.5	21.1	28.4	60.2	22.3	17.5
If a threat to rape a person is made on Facebook, it probably shouldn't be taken too seriously***	4.4	7.1	88.5	14.7	12.9	72.4
For safety reasons, victims of domestic violence should stop using social media, email and online sites***	20.6	27.5	51.8	33.7	32.0	34.4

*indicates χ^2 with $p<0.05$, **indicates χ^2 with $p<0.01$, ***indicates χ^2 with $p<0.001$
Note: Percentages may not total 100 due to rounding

The six items listed in Table 25 demonstrate that members of the community generally ascribed more responsibility to victims of cybercrime for their own victimisation. Overall, there was less between-group variance in the number of participants who provided 'neutral' responses to these survey items, although the comparatively higher number of police officers who disagreed that online bullying could be avoided (by victims) was due to fewer neutral responses. Otherwise, community members were more likely to agree with each listed item, reflecting greater acceptance that online fraud victims do not pay attention to what they read; that victims of image-based abuse are partly responsible and should know better than to send another person naked images; that rape threats on Facebook should not be taken too seriously; and that victims of domestic violence should stop using social media, email and other online sites.

Confidence in police responses

The fourth and final set of comparative analyses examined measures of police officers' and community members' confidence in the capabilities of law enforcement to investigate cybercrime. Table 26 presents the results of cross-tabulation and chi-square analyses comparing such attitudes across three response levels (agree, neutral, disagree).

Table 26: Confidence in police responses to cybercrime among police and community respondents

Sample group	Police (%)			Community (%)		
Survey item/response	Confident	Neutral	Not confident	Confident	Neutral	Not confident
How confident are you that the current police response to cybercrime in your state is effective?***	12.1	34.8	53.1	31.3	39.1	29.6
How confident are you that police in your state take cybercrime as seriously as face-to-face crimes?***	21.8	33.9	44.3	39.3	32.6	28.1
How confident are you that police in your state are adequately funded and resourced to address cybercrimes?***	5.0	18.2	76.8	23.5	35.5	41.0
How confident are you that police in your state are effective in supporting victims of cybercrime?***	9.5	28.9	61.6	31.7	34.2	34.1
How confident are you that police in your state are effective in detecting and charging perpetrators?***	8.5	24.9	66.6	29.8	35.7	34.5

***indicates χ^2 with $p<0.001$

The five items listed in Table 26 highlight the fact that police officers consistently reported lower levels of confidence in law enforcement's capacity to respond to or investigate cybercrime. Indeed, community members were significantly more likely to report confidence 'that the current police response to cybercrime is effective' and 'that police take cybercrime as seriously as face-to-face crimes'. Across both groups of participants, about one-third reported that their confidence in law enforcement on these items was 'neutral'. Additionally, community members were more likely either to express 'confidence' or remain neutral concerning whether 'police are adequately funded and resourced to address cybercrimes', 'police are effective in supporting victims of cybercrime' and 'police are effective in detecting and charging perpetrators'. Overall, these patterns reflect the greater optimism of the community about the capabilities of law enforcement to effectively respond to and investigate cybercrimes; police officers lack similar levels of confidence.

Results: Focus group

A focus group with cybercrime and cybersecurity professionals enabled the collection of deeper insights into both survey samples. It also allowed for a more nuanced understanding of the issues faced by police and other agencies in attempting to respond effectively to cybercrime. This section provides a thematic analysis of the issues raised and discussed by focus group participants. To reiterate: the focus group discussion was recorded by scribes situated at each of the six tables. Each scribe produced a transcript for their respective table, containing a mixture of direct participant quotes and discussion summaries. All transcripts were combined for analysis, and this section quotes relevant extracts to illustrate and support the arguments. Each quote is attributed to an individual scribe or a participant.

Overall, the focus group discussion did not generate any insights that are necessarily new or unique to the policing of cybercrime or protection of cybersecurity. Indeed, the sample was made up of cybercrime specialists and cybersecurity experts, influencing the nature of the information discussed and data collected. Therefore, many of the points raised and debated throughout the day mirror previous arguments on policing more broadly. They include a desire for more money and resources, the need for improved training and for a better understanding of cybercrime as a category of behaviour, the adequacy of current legislation, and the need for increased collaboration (eg Holt, Burruss & Bossler 2015; Stambaugh et al. 2001). Although the focus group does not necessarily add to what is already known about the challenges of responding to cybercrime, it is important to acknowledge these insights, as disclosed by professionals working within the field, and to consider the need (and, more importantly, the desire) for change.

The focus group was structured around a set of questions posed to participants across the day. Topics included the results of the police survey, the comparative results of police and community respondents, strategies for policing cybercrime (including specialist versus generalist approaches) and the need for additional education or training focused on policing cybercrime. Consequently, not all the themes explored emerged unprompted; they were the result of deliberate questioning and discussion throughout the day.

Police responsibilities

A large part of the day's discussion revolved around the role and responsibilities of the police in responding to cybercrime. Comments related to their performance and to external factors that influence the way police do their job. There was some discussion about the definition of cybercrime and what it included or excluded. This is evident in the following extracts:

> What is the definition of cybercrime? Everyone is going to have their own definition. Some would include child exploitation material, some wouldn't. (Participant, Table 3)
>
> A weakness is that we are actually hung up on the definition. (Participant, Table 3)
>
> We do not have uniform clear channels of communication for cybercrime—it isn't a different city in the same country…We have issues with inconsistent priorities and even definitions of crime. (Participant, Table 2)

The lack of clarity and consistency around definitions of cybercrime was cited as highly problematic in effectively responding to offences in a similar fashion across the country. Some points of discussion focused on the lack of direction that, it was argued, exists in the area of cybercrime and on a desire for greater leadership across all agencies:

> Some of it seems like 'someone should do something' mentality, but a lack of understanding of what should be done and who should be doing it. Police seem to recognise that there is a problem, but need help with what to do about it so they can meaningfully respond (want more training). (Participant, Table 2)
>
> Who is going to do something with it, there is no one to do it…We had all this data and we did all these products but there was no one to take the lead. No one is organising it nationally. (Participant, Table 3)
>
> We are having a lot of national discussions. Who have the responsibility?…We are slowly pulling it together…It is about five years too late. (Participant, Table 3)
>
> [There is a] disconnect of which department and who is responsible for the policing of cyber. Needs to be a certainty of who is responsible for the management of victims. (Scribe, Table 6)

Participants therefore asserted the need for a central vision in responding to cybercrime, which would act as a framework for all agencies.

The issues associated with the prosecution of cybercrime were noted across several tables:

> We have the legislation and the general intent but very little vision on how it should be in practice. (Participant, Table 1)
>
> While laws still cover offences committed outside jurisdiction, the issue becomes how to investigate and enforce the law. The legislation is ready but processes can be confusing and unclear to police officers. (Participant, Table 2)
>
> [There are] barriers to investigation, such as the transnational aspect of cybercrime, jurisdictional issues, how to obtain evidence—Who has it? Who is responsible for it? Who do we tell/report to? (Scribe, Table 2)

d

There was some contentious discussion about adequate legislation regarding cybercrime, as illustrated in the following two comments:

> It pisses me off that people say that we need more legislation. We have enough. (Participant, Table 3)
>
> Outdated legislation is a problem as well. We have a law on the books and leave it for 100 years and there is no reform. (Participant, Table 5)

Some comments expressed a desire to learn from those who had been able to prosecute successfully in this area:

> It would be interesting to know—were any of the police officers successful in terms of policing cybercrimes? As opposed to just knowing that they have discussed/come into contact with cybercrime. (Participant, Table 2)

This specific quote also highlighted a desire among police to learn from other agencies when there has been successful action and/or a prosecution.

Some participants focused on the lack of understanding of cybercrime by those in senior positions across police and other organisations. Some also noted a lack of political will to provide the required amount of resources across finance, personnel and training:

> If we don't have results, how can we get resources? How do we collaborate with other industries? There's a lack of resources. There are plenty of resources for drugs et cetera. There's a lack of understanding around cybercrime. Lack of funding and potential support from the hierarchy. (Participant, Table 1)
>
> It is more difficult to argue for prioritisation when the public do not understand the risks. (Participant, Table 2)
>
> The rate of solving a cybercrime…there isn't a quick fix. Everything is against it. If I was a PC [police constable], and I saw something about an IP address…I'd just chuck it. You want to deal with the rapes and assaults. That is what will help your career. If you tell your boss…they're gonna say 'get a car, get a gun, and get out there and do something actually important'. (Participant, Table 5)
>
> I think our capabilities and resources have significant shortcomings. But that isn't what politicians are talking about…they're already talking about more powers. (Participant, Table 5)

The inability of management to understand the importance of and need for a better response to cybercrime incidents was a common concern across all tables.

Some participants acknowledged that the reporting of cybercrime is problematic, with implications for an agency's ability to obtain resources or produce an accurate understanding of the reality of cybercrime—for example:

> We need you to report it to get more funding and more resources. I know that only one out of 100 clients reports attacks. (Participant, Table 1)

This is only one of the many identified challenges relating to the online environment. There was also recognition of the different nature of the virtual environment and the challenges that creates for traditional policing models:

> Policing is still on a traditional crime level. (Participant, Table 3)
>
> For your average copper at the station if they get something and they don't know how to deal with it, there could be a disparity. It's not that they don't think it's [cybercrime] important, it's just that it's too hard. (Participant, Table 3)
>
> [There are] jurisdictional issues largely (made reference to how policing is connected to the terrestrial nature of policing cyber and legal constraints of governance under legislation). (Scribe, Table 6)

These issues are, unfortunately, not new. They were coupled with a recognition that society operates differently in this space:

> Simultaneously seems like police are more supportive of changes to their own capabilities and agencies, rather than expecting online platforms to police themselves—speculation that perhaps this is based on pessimism about the idea of expecting a company like Google to actually do something to police themselves. (Participant, Table 2)
>
> We need to be able to rely on most people to do the right thing, but it isn't the case in cybercrime. With offline issues, there are certain community values and standards that we understand and tacitly enforce, 'if someone stepped out of line, it was obvious, but we don't have that online'. Community values do not exist in the same way to meaningfully police people's behaviour online, we need to create this. (Participant, Table 2)

Discussion also focused on the way in which agencies respond to victims of cybercrime.

> Reporting is good but issue arises in 'what happens after that?' (Participant, Table 2)
>
> Negatives were largely based on the lack of interconnected management of victims between organisations, lack of transparency or information for victims to know where to go for help or information. (Scribe, Table 6)

The difficulties associated with responding to victims of cybercrime are well documented and largely align with the sentiment expressed by participants.

d

Training requirements

As part of their discussion of the role and responsibilities of police in responding to cybercrime, participants addressed in some depth the utility of additional police training. Generally, all six tables noted the need for better training. One example was the recognition of the need for training officers in specific skills related to cybercrime:

> For me, I see the cybercrime discussion is slowly filtering in at all levels. We now have a cybercrime focus—not just funding and resources, but also training. (Participant, Table 2)
>
> The biggest strength I see…every police officer I've trained accepts the fact that they need more training in it. (Participant, Table 1)
>
> There are limits to officers' capabilities to be equipped to deal with these things. If you have more tools at your disposal to commit cybercrime…how can a local officer know what you can and can't do? It might be an unrealistic expectation. (Participant, Table 5)

Participants recognised that the skills needed to investigate cybercrime were somewhat different, not always captured in generic training:

> We need specific tools to police cybercrime. An investigator needs different skills for cybercrime. It's different to homicide training, for instance…Training needs to start from when police are students. (Participant, Table 1)

Relatedly, participants observed that officers need to be provided with training in a straightforward and jargon-free manner:

> Discussed that many police officers are struggling with 'analysis paralysis', whereby they are bombarded with too much technical information regarding cyber offences. (Scribe, Table 6)
>
> They [police] need clear information that demystifies the process and the tech behind it… they need the information to be less tech based. (Participant, Table 6)

Participants discussed the effect of generational influences on cybercrime training. Given that newer officers are likely to be more technically skilled and internet savvy than older members of the force, how would this influence the need for officer training on these topics?

> Interested in junior recruits to see if they are more savvy. Follow up with recruits who have done training in this area, to see now do they feel comfortable. (Scribe, Table 3)

However, discussion about the utility of training officers in digital forensics to identify evidence at crime scenes (across both online and offline contexts) was limited. The need for further training in this area was highlighted by a series of comments during a discussion at one table:

> How can any police disagree…how can you have any crime with no chance of any digital evidence?
>
> I think with law enforcement, you need to look for digital evidence no matter which department you are in.
>
> Quite scary, that is a high number. One in 20 cops think that digital evidence isn't a part of all crimes.
>
> It doesn't matter what it is, all crimes can have digital evidence and it is disturbing that 5 percent don't think there is. (Participants, Table 3)

This suggests a need to better educate police officers about what constitutes digital evidence and how this can be identified and collected, regardless of offence type, when investigating a crime.

Similar subcategories were identified by participants while considering the utility of training officers in a broader sense. One participant raised the potential drawbacks for the police service of upskilling officers if it makes them more attractive for other potential employers:

> There are tensions among the police as to how to offer training, and if they do, will the employees leave for other jobs? (Participant, Table 4)

Evidently, the differences in workplace risk and higher salaries could directly affect an officer's decision to leave the police. There was also continued discussion around the issues of resources and political will from senior management that impacted the training available and delivered to police:

> [One participant] expressed surprise at the information that police were not given any training. [Another participant] responded by saying that [they] got [their] specialised training on [their] own (degrees, certificates etc). (Scribe, Table 4)
>
> Yeah, it shows how officers are not equipped to deal with it…The higher ups don't have a f***ing idea what a computer is. A judge wouldn't know what an IP address is. And getting the information needed to investigate…they just waste weeks and weeks of time (Participant, Table 5).
>
> Law enforcement need more support more than ever. There is a lot of pointing the finger but not a lot of support. (Participant, Table 6)

Despite these concerns, there was some degree of optimism expressed by a participant about the way this discussion was headed:

> For me, I see the cybercrime discussion is slowly filtering in at all levels. We now have a cybercrime focus—not just funding and resources, but also training. It's moving in the right way. (Participant, Table 1)

Overall, these discussions illustrate the degree of improvement that is arguably needed to better equip police to respond more effectively to various types of cybercrime.

d

Specialist versus generalist duties

Another issue identified within the broader theme of police responsibilities was whether cybercrime investigations should be a specialist field of policing or a necessary part of the skillset for general duties officers. Overall, there were persuasive arguments made in favour of both perspectives: that cybercrime investigations should be a specialist area of policing because of their comparative complexity, and that cybercrime investigations are inevitably becoming part of the necessary skillset for generalist police officers. These arguments are discussed below.

Specialist policing

The main arguments in favour of having the policing of cybercrime as a specialist area were founded on the notion that these offences have a level of technological complexity that requires a set of skills beyond that of the general duties police officer. This is evident in these quotes:

> Digital chain of custody—requires more specialisation to secure accountability. (Scribe, Table 2)
>
> Because it is highly technical and you need a specialist to deal with it. (Participant, Table 3)
>
> It has to be a threshold at some point. If technology impacts the crime, you do need technical skills. (Participant, Table 5)
>
> In addition to technical knowledge, a specialist would need other skills around counselling. (Participant, Table 6)

An analogy was drawn between cybercrime and other specialist areas currently within the police service. The following excerpts highlight this:

> Specialist police could be more about supporting investigators, eg scenes of crime, fingerprint experts, handwriting experts. (Participant, Table 2)
>
> For the specialist response we likened it to a homicide investigation. You will call in other resources. There will be teams. (Participant, Table 3)

Lastly, the argument focused on the logistics of being able to effectively train a large organisation:

> It is easier to train 20-odd police persons (specialist) than training a whole general unit of police. (Participant, Table 4)
>
> When you talk about giving it to generalist police, you might need to bring them up a bit. But there is a limit how far you can bring up [thousands of] officers. You cannot train them all to be specialist. (Participant, Table 5)
>
> With the specialist, it would be easier to keep them abreast of the changes [to cybercrime]. (Participant, Table 6)

Generalist policing

Several arguments supported the perspective that cybercrime investigations must become part of the skillset of generalist police officers: increasing numbers of cybercrime offences, an inability to clearly or unambiguously distinguish between online and offline elements of a criminal offence, and the role of police as first responders to crime generally. Firstly, participants acknowledged the number of cybercrime offences occurring on a regular basis. As a result, they considered it desirable to ensure that general duties police are equipped to respond to such problems:

> Whether we like it or not, cyber-enabled crime is on a massive rise. So, the point being, that is where crime is going whether we want it to or not. So, there is a much larger pool of general police. Upskill them to deal with it. (Participant, Table 5)

> With a generalist, anyone can do it. Potentially a smaller uplift of knowledge. Improves the skills set of police over all. (Participant, Table 6)

Secondly, participants described the difficulties of investigating crime without some degree of technical expertise, because the boundary between online and offline criminal activity is increasingly ambiguous. Indeed, many crimes have both an online and offline element. Some participants therefore expressed a view that all crime should be treated simply as a criminal offence, regardless of the medium:

> A crime could be occurring both online and offline and to pull them apart would be difficult and unnecessary. (Scribe, Table 2)

> I think that is where we get lost, is that it's just a crime. (Participant, Table 3)

It was also noted that general duties police are likely to be the first responders to all cybercrime offences. On that basis, it was argued that they require an ability to respond in an effective manner.

> I think every police officer should be trained to respond. (Participant, Table 3)

> There is always going to be a first responder. (Participant, Table 3)

Finally, some participants argued that agencies do not encourage officers to specialise in a particular area. There was a belief that doing so would be detrimental to one's potential for promotion. Participants at one table agreed:

> If you look at policing, as a whole, it is a detriment to your career to specialise. So, you need to take a step back and address things generally. (Participant, Table 5)

> Yeah, the service, as a whole, wants to abandon specialisation and wants to push generalising approaches. (Participant, Table 5)

Whether or not there is merit in this argument is worthy of further exploration, because the politics of police agencies may have an influence on officers' decision to accept certain responsibilities.

d

Overall, the focus group participants were evidently capable of reasonably justifying both the specialist and generalist perspectives in an abstract sense. In making sense of the debate on a practical level, it is useful to conceptualise the policing of cybercrime along a spectrum, with generalist skills at one end and specialist skills at the other. All police require some degree of skill to be able to investigate certain forms of cybercrime effectively, manage digital evidence appropriately, and properly pass these investigations onto specialist police where the complexity of the case requires a higher level of expertise and skills. This was evident in the summary of one table's discussion:

> Consensus for this question was that there should be somewhat of a sliding scale where police are empowered to deal with 'lower-tech' cybercrime, but there is a more specialised department for more complex, 'high-tech' issues for which it would be unrealistic to train all police officers. (Scribe, Table 2)

What the baseline skills should be for all police officers, and how this expands to a specialist role, is debatable and ultimately remains to be determined. However, it is likely that complex technical skills such as computer programming and digital forensics are associated with the investigation of cyber-dependent offences (such as computer hacking or malware) rather than those that occur across both online and offline mediums (such as fraud and harassment). It is possible, then, that a clearer distinction between 'cyber-enabled' and 'cyber-dependent' criminal offences, as well as the degree to which offenders are using cryptographic techniques to evade surveillance, might help to clarify the respective responsibilities of generalist and specialist officers.

Community expectations

The second theme identified through an analysis of the focus group data concerned whether the community had a realistic understanding of the risks associated with cybercrime and of law enforcement's investigative capabilities. These categories were identified in response to results of the comparative analysis of police and community surveys. All six tables noted these issues in a variety of contexts.

The first point to note was a disagreement about whether the community accurately understands the risks posed by cybercrime for individuals. Generally, focus group participants were critical of the community respondents' self-assessments:

> The community has a perception that the problem is quite large, but they don't recognise the threat. They're starting to suspect, but they just don't know really. (Participant, Table 1)
>
> 'Public understand the risks' jumps out to me. It's something from my experience that I don't think the public are aware of the risks. This includes the elderly et cetera. (Participant, Table 1)
>
> The general population is ignorant to the potential dangers of cybercrime…[and] ignorant to their own vulnerability. (Scribe, Table 2)
>
> Everyone agreed that community thinks that they understand the risks, but the police knows the truth that they do not. (Scribe, Table 4)
>
> Look at the community results—they don't recognise the threat of cybercrime. The community don't think they don't know. They don't recognise their own lack of education. (Participant, Table 5)
>
> I think there is a general feel that the public think they know cybercrime is bad and understand the risks involved. But they don't really. (Participant, Table 5)

All these comments suggest an incongruity between community members' perception and the risks posed by cybercrime. Building upon this subcategory, a related point concerned the relationship between knowledge and protective behaviours for preventing cybercrime victimisation:

> There's also a perception that people's identity information is already out there, so people might think that if it's already out there, oh well, I can't do anything about it now. (Participant, Table 1)
>
> People seem completely comfortable with advertising their geographical locations and putting photos of their bank cards and plane tickets online, with no thoughts to the potential danger (this was brought up by all participants in different ways). (Scribe, Table 2)
>
> Our data suggest that awareness doesn't translate into action. (Participant, Table 6)
>
> Group discussed the increasing built in safety of devices but not the 'community knowledge or awareness'—Consumers not using the safety features of devices, specifically noting that many people 'don't even change their wifi passwords from the default'. (Scribe, Table 6)

These comments illustrate that the professionals in the room understood how the ability of the community to successfully prevent their own victimisation is linked to their having a realistic understanding of the risks associated with cybercrime and cybersecurity.

d

There was also discussion about the relationship between community and police. In particular, focus group participants were critical of the community's understanding of the investigative capabilities of law enforcement agencies in responding to cybercrime. Indeed, the points raised speak to a discrepancy between public expectations of a police response and the reality of what can genuinely be achieved:

> People expect police to be able to fix it all, so they don't really take any responsibility for themselves staying safe online. But, of course, police often can't really do anywhere near as much as people expect them to do. (Participant, Table 2)
>
> I do think that it is interesting about the attitudes about changing police work. The community lacks understanding of what police work involves. It comes back to how victims have expectations about what policing involves. (Participant, Table 5)
>
> A lot of [the] time, the community just want their money back. They don't necessarily want a police response. They don't care about the investigation. They are just after getting their money back. Police aren't going to do that. They don't necessarily understand that police can't solve that problem. They can report to us, but we can't make that problem go away. They are after some kind of restitution, rather than a 'police response' as we understand it today. (Participant, Table 4)

These comments indicate the ways in which the public desire a particular response from police in the aftermath of an incident. They may, however, be unlikely to receive such an outcome.

Overall, the discussion revolved around areas for improvement, including an accurate understanding of cybercrime and the threat it posed, a better alignment of one's actions to prevent cybercrime where possible, and a more accurate understanding of the reality of what can be expected from a police response to an incident. The identification of these areas of concern is important, because it can lead to a focused exploration of how to improve these areas.

Public education

The final theme discussed in detail across the day centred on public education. This is a contested issue, articulated using various categories and expressed views about what is being done well, what is currently missing, and what might be improved. Some of the main points discussed included the need to consider the audience when crafting a message, the contents of the message, who is responsible for delivering the message, the challenges of delivering an effective message, and what might be learned from existing public education campaigns.

There were a few elements identified that speak to the need to consider the audience when creating public education campaigns about cybercrime. Participants identified a conflict between the technical and non-technical elements of cybercrime and called for the human factor of cybercrime to be at the forefront in delivering education and training:

> One of the major things I see is you've got IT [professionals] trying to educate. There's no social proof for IT. When IT are asked to educate, they're focusing on tech, not on human element. This is problematic because IT professionals can't highlight how this impacts people. (Participant, Table 1)
>
> The ease of the technology and its pervasiveness is not reconciled with an individual's behaviour. They're bored, come midnight, what are they going to do? Go on the internet and go shopping. This is a personal problem. Not an IT issue. It's a human issue. (Participant, Table 1)
>
> Highlighted that engagement with personal stories of victimisation helped to engage the public in awareness campaigns. (Scribe, Table 6)

There was also discussion about the targeting of education campaigns to appropriate levels of public knowledge and understanding. Much of this concerned the manner in which messages are delivered:

> Putting messages online are less likely to reach vulnerable populations because they engage with the internet significantly less anyway. We need to meet people where they are. What do they consume? Maybe commercial TV? Radio? Mediums that these people actually consume. (Participant, Table 2)
>
> However, it is also important that ads are put in during the news on radio and TV to cater to varying demography. Targeted advertising using different formats (like 30-seconds short films) is important as same advertisements do not work for all demography. (Participant, Table 4)
>
> But the most basics aren't understood. Even in information security. The big thing I have been saying…is we need to have a personal conversation. I need to talk about your family. If we can have that sort of conversation it can work. We can't be using statistics and percentages to talk to individuals. There is no impact. (Participant, Table 4)
>
> We are pretty good at awareness raising but the response needs to be tailored…It's difficult to get the right information to the right people. (Participant, Table 6)

d

This also encompassed the contents of the message, particularly around consistency:

> There is so much information out there, but the obvious goal would just be to get people to read these things in the first place, (Participant, Table 2)
>
> As a group of police, academics and security professionals…we don't have a unified message. (Participant, Table 4)
>
> It is also important to keep disseminating same message again and again, as telling and disseminating information constantly is important for awareness creation. (Participant, Table 4)
>
> For better or worse…identifying a particular agency or organisation…everyone has to agree that 'thing' is our lead, our voice. And we need to all feed into that. I understand that is politically and socially difficult to achieve. But it is the only solution. (Participant, Table 5)

Relatedly, several participants observed that individuals did not currently have the necessary level of knowledge to understand how their own actions might make them vulnerable to victimisation:

> People know to lock their doors but have no idea how to keep themselves safe online. (Participant, Table 2)
>
> 'Base-level cyber hygiene' is awful, even in government—people don't know why not to click on links in emails, what is and is not appropriate to put online. (Participant, Table 2)

This discussion also captured the 'who' of cybercrime education campaigns. There was an expressed desire to collaborate (and coordinate) on the delivery of education across multiple organisations. Importantly, it was not seen to be solely the responsibility of police, but rather of police, government and other relevant public and private organisations:

> It comes down to the way that people treat the information. It's a collaborative effort, not just up to one person. (Scribe, Table 1)
>
> Law enforcement has a role in education, but I don't think they have the primary role for education, they have too many things to do. It has to be part of education. (Participant, Table 4)

The specific challenges of educating against fraud were clearly articulated as well:

> My question to everybody—have we managed to educate our way out of general fraud? No. (Participant, Table 3)
>
> There is a barrier to educating people because they just don't want to know. They just don't want anyone getting between them and Facebook. There is sometimes a resistance to education campaigns. (Participant, Table 5)

The discussion also included an acknowledgement that public education campaigns are not a silver bullet to combat cybercrime:

> One thing we did talk about is that education is not a magical pill. This can leak into a victim-blaming thing, we just need to educate people more. People still buy bridges, they still sign up for dodgy time shares. Education is fine but how are you going to measure the impact, for example with phishing campaigns it works for a little bit but then it drops off. I think we tend to throw education around like it's a magical solution but it's actually really hard to implement. (Participant, Table 3)

> I'm not against education, I'm in favour. Part of the problem is that we use education as a pill to do something harder than education. (Participant, Table 3)

Participants drew several analogies with education campaigns in other areas, such as drink driving and skin cancer, arguing that there are lessons to be learned from areas such as public health:

> Anti-drink driving messages were simple and effective after 10–20 years. (Scribe, Table 2)

> Need to make it somewhat of a public health style problem. (Scribe, Table 2)

> Why can't we do an ad campaign? Repetitive ones like drunk driving or speeding are important. (Participant, Table 4)

> Things are occurring, but it isn't being pushed far enough. If it was pushed as a real risk, like drink driving or skin cancer. It just isn't put down our throats. You need to go out and find it. (Participant, Table 5)

Overall, the extracts above highlight the complexity of discussions that focus on public education campaigns about cybercrime. It is relatively easy to identify the current weaknesses and gaps that exist, but identifying solutions and ways to overcome these challenges is more difficult. This discussion has captured the difficulty of seeking to achieve this effectively.

Discussion and implications

This project set out to answer four key research questions examining perceptions of cybercrime among police officers and members of the general Australian community and to generate ideas to help improve responses to cybercrime and cybersecurity threats. Specifically, the research was prompted by the need for more robust knowledge and analysis of whether, and to what extent, these populations perceive the policing of cybercrime differently. The project has, therefore, expanded our knowledge about the discrepancies between police and public perceptions of cybercrime within the Australian context (ie Cross 2018c). This section examines how the above analyses provide answers to, and raise additional questions concerning, each of the four key research questions. It is important to note that this section examines prevalent or significant patterns that emerged across all three stages of the research project, rather than merely reproducing all results discussed above. Overall, the section highlights how the project has contributed to our understanding of comparative perceptions of cybercrime within Australia.

Research Question 1: What are the understandings, perceptions and response expectations of internet-enabled crimes among the Australian adult community and among general duties police?

The first research question concerned how the general community and police perceive cybercrime and their associated expectations about law enforcement's investigative capabilities. Specifically, this question explored how Australian samples (both police and community) share similarities or demonstrate differences in perceptions about cybercrime investigations, enabling comparisons with existing international research. Indeed, the results from the community survey build upon an expanding international literature examining perceptions of cybercrime, with the majority of community respondents (82%) having experienced at least one form of cybercrime victimisation. The most common experiences of victimisation included identity crimes (63%), stranger harassment or abuse (52%), financial crimes (51%), acquaintance or friend harassment or abuse (44%), online sexual harassment (39%), online intimate partner abuse (35%), and image-based abuse (28%). The findings thus suggest that, alongside the 'conventional' offences of identity and financial crime, the community may appreciate further information about what to do in response to online forms of harassment and abuse, given how similarly common these experiences are.

For this report, we examined community respondents' self-reported victimisation of these cybercrime subtypes across the key demographics of gender and age (which have been identified in the international literature as potentially significant). Although the present findings are consistent with the international research (eg Bossler et al. 2019; Holt & Bossler 2012b), the strength of the observed differences between demographic groups was comparatively weak. There were observable gender differences in community respondents' levels of fear of cybercrime, with women more likely than men to self-report being afraid or very afraid of most crime types. However, although we found statistically significant differences in overall victimisation rates by gender for most crime types, the effect sizes were small. They thus may reflect an artefact of sample size rather than any meaningfully large difference. There was a very clear trend in cybercrime victimisation by age, such that younger adults (18 to 29 and 30 to 39) were more likely to experience victimisation than older adults (50 to 59 and 60 to 69), although this was less the case for identity cybercrimes than for interpersonal cybercrimes and online harassment or abuse. There were further interesting trends by age: younger adults were more likely than older adults to rate themselves as afraid of cybercrimes, to perceive themselves as at risk of cybercrimes and to have experienced cybercrime victimisation personally.

For all cybercrime types, only a minority of our respondents had reported their most recent experience of victimisation to police. Interestingly, victims of image-based abuse (28%), intimate partner abuse (24%) and online harassment or abuse by a stranger (23%) were more likely to have reported their most recent experience of these crimes to police. This, unsurprisingly, suggests that these crimes are perceived and experienced by respondents as more serious and therefore worthy of reporting. It may also suggest that participants lacked confidence in police ability to achieve an outcome for other types of cybercrime, such as identity (17%) and financial crimes (17%). The research does suggest that community respondents are unlikely to report, but most of those who reported did so to their local police station, either in person or by phone. This reaffirms the fact that general duties officers remain the first point of contact for most cybercrime victims.

Across all cybercrime subtypes, where participants did report their most recent experience to police, the vast majority found the experience to be helpful or very helpful. Interestingly, these results are inconsistent with some of the existing international research suggesting that victims of cybercrime generally have negative experiences when reporting their victimisation (eg Cross, Richards & Smith 2016; Jang, Joo & Zhao 2010). Importantly, given the low initial reporting rates, this finding should not be cause for complacency about the effectiveness of police responses to cybercrime. Additionally, community respondents were generally confident in their ability to protect themselves from potential cybercrime victimisation, with almost half indicating that they were either 'confident' or 'very confident' (47%). However, although men and young adults were more likely to be confident in their ability to prevent victimisation, women and older adults were significantly more likely to engage in self-protective behaviours. This is further complicated by the observation that, although women are also more likely to experience victimisation, older adults are less likely to be victims of cybercrime. This suggests a complicated interaction between perceptions of cybercrime victimisation, the performance of protective behaviours and sociodemographic characteristics such as age and gender. These effects should be explored in further detail in future research projects.

d

The results from the police survey similarly suggest that officers' life experiences influence their perceptions of cybercrime. For example, there were gendered patterns of perception among Australian police officers. Female officers are more likely to perceive cybercrimes as serious, particularly those involving interpersonal harassment (person-based crimes). This suggests that gendered life experiences influence perceptions of cybercrime severity. This pattern has been observed in other policing jurisdictions; for example, a survey of UK constables found that male officers perceived online harassment as less serious than their female colleagues did (Holt et al. 2019: 34). This further adds to an expanding literature highlighting how perceptions of and responses to cybercrime are highly gendered (Powell & Henry 2018).

The present results suggest that there has been little (if any) evolution in the preparedness of police to investigate cybercrime over the past 15 years. Indeed, the results of this research replicate those found in previous studies (Bossler & Holt 2012; Senjo 2004). However, it is also clear that exposure to cybercrime during professional practice influences attitudes about cybercrime severity. Officers who had undergone training involving cybercrime-related materials were more likely to assess cybercrime as being comparably serious to offline crimes. This replicates the results found in the UK data, where it was similarly observed that officers whose training included cybercrime-related materials self-reported greater preparedness to respond to online crime incidents (Bossler et al. 2019: 11). Interestingly, officers who had a tertiary education were less likely to have confidence in the ability of law enforcement agencies to effectively respond to and investigate cybercrime incidents, but were also more likely to have greater levels of self-confidence in responding to cybercrime incidents.

There is tension between the increasing importance of technology for policing (as expressed within focus groups) and the fact that only a small minority of police officers (8%) had undergone any formal training in the area of cybercrime. It is also clear that how police officers distribute responsibility for cybercrime prevention varies according to sociodemographic factors, again suggesting that life experiences influence perceptions of cybercrime. Officers who had a tertiary education or who had more contact with investigating cybercrime incidents were more likely to believe that general duties officers should receive additional training. They were also less likely to agree that citizens can effectively prevent their own victimisation by engaging in self-protective behaviours, whereas police officers who were younger or male were more likely to agree with such views, acknowledging the importance of victims' avoiding social media platforms or changing their mobile phone number. Finally, an officer's familiarity with technology correlates with a more nuanced understanding of how criminal offences increasingly involve both online and offline components. Overall, these results confirm two different features of the international literature in the Australian context: that different subgroups of police respondents (according to their sociodemographic characteristics) variously ascribe moral responsibility to victims of cybercrime; and that education, training and workplace exposure influence the attribution of responsibility for cybercrime victimisation.

Research Question 2: To what extent, and in what ways, are the understandings, perceptions and response expectations of the Australian general community similar or different to those of general duties police?

The second research question concerned whether, and to what extent, there are significant differences in how members of the public and police officers perceive cybercrime and the associated investigative capabilities of law enforcement agencies. This question was prompted by an observation drawn from the existing literature—that the general community tends to have high expectations of responses to cybercrime incidents, yet also to experience the process of reporting their victimisation as unsatisfying (Cross, Richards & Smith 2016; Kremer 2014). Additionally, previous international research from a policing perspective suggests that general duties officers mostly believe that they lack the necessary training to effectively investigate cybercrime, experience frustrations about the rapid pace of technological development and tend to have muddled understanding of the conceptual distinctions (if any) between 'cyber' and 'ordinary' crimes (Cross 2019a; Hadlington et al. 2018; Nouh et al. 2019). Consistent with the existing literature, the present study has observed several notable differences between police and the community.

At a base level, it is clear from both the quantitative and qualitative data that police respondents hold different views from community respondents about the community's understanding of cybercrime and cybersecurity. Whereas police respondents assessed the community's understanding of cybercrime as quite low, community respondents reported greater confidence in their ability to understand the risks associated with the use of technology. This was also supported by focus group data indicating that experts within the law enforcement, government and non-government sectors expressed significant scepticism about the public's self-perception as accurately assessing cybersecurity risks. This difference might be attributed to a tendency for non-experts to misjudge the prevalence and severity of cybersecurity threats.

Potentially contributing to this pattern, police respondents were overwhelmingly more likely to provide definitive answers to survey questions. They were more likely to indicate that they either agreed or disagreed with a statement, whereas community respondents were more likely to indicate a 'neutral' response. This pattern can possibly be explained by different levels of confidence and experience with criminal offences and investigations, both broadly and within a cybercrime context specifically. The police respondents were also more likely to rank cybercrime as being as serious as traditional (or offline) forms of crime. This contrasted with community respondents, who were more likely to express agreement with the statement that online forms of harassment are less serious than face-to-face forms of interpersonal harassment. Indeed, there was a tendency for the community to be less sympathetic to victims of cybercrime, consistent with existing research observing the prevalence of victim-blaming attitudes associated with cybercrime (Black, Lumsden & Hadlington 2019; Holt & Bossler 2016).

d

There were significant differences in the expectations of police and community respondents about the investigative capabilities of law enforcement agencies. Specifically, community respondents were more likely to express confidence in the investigative capabilities of law enforcement agencies, whereas police officers were less confident. This suggests that community respondents were both more likely to assess their risk of victimisation as low and more likely to believe that police are well equipped to respond to instances of cyber victimisation. This appears to be consistent with current understandings of the mediated perception of cybercrime investigations by law enforcement (Kremer 2014). We noted above that, although a significant majority of community respondents indicated that they had experienced at least one incident of cybercrime victimisation, only a minority reported the incident to the police (by any method). Such discrepancy between confidence in law enforcement and the low prevalence of reporting among cybercrime victims again supports a view that exposure to, or experiences with, incidents and investigations have an impact on community and police perceptions of cybercrime.

The comparative element of the research also suggested that community respondents were more likely to ascribe responsibility to the victims of cybercrime and to believe in the utility of protective behaviours as a means of cybercrime prevention. This is surprising, given our finding that community respondents have faith in the investigative capabilities of law enforcement to respond to cybercrime. For example, police respondents were observed to be less likely to agree that victims of image-based sexual abuse are partially culpable for their victimisation under circumstances where they have taken naked images or sent them to another party. Similarly, police respondents were less likely than community respondents to believe that citizens can prevent online harassment by avoiding social media or changing phone numbers. These results indicate that police respondents tend to be more understanding than the average community respondent who participated within our survey, despite previous research showing that police officers tend to lack detailed insights into the lived experiences of specific cybercrime victims (eg Cross 2018b, 2018c; Powell & Henry 2018).

Finally, the themes identified within the focus group stage of research allow for detailed interpretation of the comparative police–community survey results. The contested roles and responsibilities of law enforcement agencies (and general duties officers specifically) were evidently linked with participant concerns about unrealistic community expectations. Specifically, the focus group session highlighted discrepancies in the expectations of police and community respondents, evidence for the necessity and utility of cybersecurity-oriented public education campaigns. These campaigns are thus positioned as mechanisms for rectifying the discrepancy between attitudes of experts (including law enforcement) and members of the general Australian community, to ensure that the latter have an appropriate baseline of digital literacy. This triangulation of the quantitative and qualitative data provides evidence of an ongoing negotiation between police and community respondents about the respective roles and responsibilities of both law enforcement agencies and the general Australian community for cybercrime prevention.

Research Question 3: What opportunities are there for awareness raising, access to information and support in relation to online crimes for the general Australian community?

The third key research question shifted focus and considered any opportunities for improving the awareness of the general Australian community about cybercrime and cybersecurity issues. Consequently, this question seeks to provide greater clarity about the role and responsibilities of citizens within cybercrime prevention programs. The opportunities identified below were derived deductively, from both the community and police survey results, and inductively, from the qualitative data collected via a focus group. Overall, we identified several features about the content and form of public education campaigns that contribute to knowledge about future opportunities for Australian citizens to participate effectively to cybercrime prevention programs.

One of the most significant overarching issues identified across all stages of the research presented in this report was the discrepancy between police and community expectations about the investigative capabilities of law enforcement agencies. This finding is concerning, because previous research has suggested that the discrepancy between police and public expectations of responses to cybercrime is a significant factor contributing to under-reporting (Cross 2019a). This highlights the importance of developing policy initiatives that reduce such discrepancies. Indeed, data collected during the focus group stage of research suggest that opportunities exist to educate members of the public about the scope and limitations of cybercrime investigations. This may help to challenge the distorting effects that popular culture representations may be having on community perceptions of cybercrime (ie Kremer 2014; Wall 2008a). Dispelling or weakening myths surrounding cybercrime investigations could ensure that citizens understand more accurately what law enforcement officers can do in response to a complaint, thus potentially decreasing the disparity between police and community expectations of investigative capabilities.

One of the most important findings from the community survey was the discrepancy between the number of respondents who had experienced a cybercrime incident (82%) and the number who reported this incident to law enforcement (17%). It was also evident that most of these respondents reported firstly to a general duties officer, either in person or by telephone, rather than through the centralised online portal (then ACORN). Consequently, there is another opportunity (and arguably a clear need) to develop the contents of public awareness campaigns to include information about how to report cybercrime incidents. Such a program may help to reduce the under-reporting of cybercrime (ie Kemp, Miró-Llinares & Moneva 2020; Tcherni et al. 2016) and ensure that those who do report incidents are aware of existing processes.

d

There were also some interesting patterns of responses about the utility of protective behaviours and the attribution of responsibility for cybercrime prevention programs. Specifically, we found that community respondents are more likely to ascribe blame to victims of cybercrime, while also being confident in their own ability to prevent themselves from being victimised. This suggests an opportunity to ensure that members of the general community are cognisant of both the utility of protective behaviours and the potential harms of personally ascribing blame to cybercrime victims. For example, the contents of public education programs might be structured to redress public overconfidence in their cybersecurity practices, encourage effective protective behaviours (eg the use of password managers) and challenge beliefs that victims are morally responsible for the circumstances leading to their victimisation (eg that victims of image-based sexual abuse are responsible if they have voluntarily shared nude selfies). There are, therefore, opportunities for improving community awareness about an appropriate role for citizens in cybercrime prevention initiatives, while also avoiding victim-blaming narratives.

Finally, focus group data identified several ideas relating to both the target audience and the method of delivery for public education campaigns. Other government departments, such as the Commonwealth Attorney-General's Department and Home Affairs, have an opportunity to produce educational and training materials for public consumption. Additionally, given the increasing importance of digital technologies in social and economic life, participants noted that information about cybersecurity practices could be integrated into secondary and tertiary education curricula to target young populations effectively. Indeed, significant opportunities exist to develop, implement and evaluate cybercrime training awareness programs for these populations, together with campaigns that target the broader Australian community. Such programs have the potential to avoid placing excessive responsibility on law enforcement agencies to act as the sole conduit between citizens and officials on cybersecurity issues.

Research Question 4: What opportunities are there for improving police training, resources, capacity and confidence in responding to online crime?

The fourth research question concerned the associated opportunities for improving police responses to cybercrime within Australia. This question seeks to provide greater clarity about the roles and responsibilities of law enforcement agencies in both cybercrime investigations and prevention programs. Additionally, the research question complements the discussion about the role of citizens in cybercrime prevention. Several of the identified opportunities derived from both the surveys and the focus group data related to revising police training programs, including suggestions for possible improvements to service delivery by both general duties and specialist officers.

The focus group data reveal some observable disagreement about whether cybercrime investigations should be the remit of general duties or specialist police officers. We noted earlier that a nuanced analysis of this issue highlights how both these groups must necessarily—albeit differently—be equipped for effective agency-wide responses to cybercrime. It is evident that some cyber-dependent criminal offences will involve technical expertise outside the reasonable domain of investigation by general duties police officers. This situation offers some opportunities for ensuring that agencies are adequately equipped with specialists. There may be value, for example, in direct government subsidies of digital forensics training for interested and capable officers. Indeed, we note that the Australian Government has committed $26.5m for upskilling a range of professionals in cybersecurity (Department of Home Affairs 2020: 33). Another potential avenue for collaboration could be to create collaborative policing models, as used within the United States (eg InfraGard or the Electronic Crimes Task Force), where the public and private sectors work together. This would also be consistent with the funding priorities outlined in Australia's Cyber Security Strategy (Department of Home Affairs 2020: 33).

It is equally important that general duties officers be sufficiently equipped to act as first responders to cybercrime incidents, regardless of their technical complexity. Survey respondents and focus group participants generally accepted the desirability of additional cybercrime-related police education and training. Opportunities are also identified for improving both the capacity and the confidence of general duties officers, enabling them to meaningfully investigate cyber-enabled criminal offences. The contents of these more generalist programs should focus on improving digital evidence recognition and preservation for specialists, where appropriate (eg Casey 2019; Dodge & Burruss 2019). However, it is also important to note that many surveyed officers expressed resistance to additional training in operational requirements. This may partly be a reaction of officers enmeshed in a police culture that is resistant to change (eg Schafer & Varano 2017). It is also clear that expanding existing training requirements for general duties officers will involve associated financial and resource investment. However, the survey results do suggest that previous exposure to cybercrime incidents positively correlates with increased investigative confidence; the introduction of cybercrime-focused programs at the police academy phase of training may produce associated outcomes that warrant such an investment. A cybercrime module could be developed and delivered with the direct assistance of cybercrime and cybersecurity specialist units already existing within the agency.

d

Police perceptions of cybercrime in Australia were observed to vary according to sociodemographic characteristics such as age, gender and education, although these differences were modest in comparison to those found in previous international research (eg Bossler et al. 2019; Holt & Bossler 2012b). This suggests that, as with members of the general community, the life experiences of a police officer structure their views about cybercrime, investigations and victimisation. It was observed that younger and male officers were less likely to consider interpersonal cybercrimes (eg threats of sexual abuse made online) as serious criminal offences warranting their attention. In line with the results discussed above, there are opportunities for targeted training programs to ensure that all officers are adequately equipped to deal with cybercrime victims who report an incident to police. To further improve the quality of victim responses, there is potential value in ensuring that education and training programs specifically encourage young male officers to empathise with the gendered nature of much interpersonal cybercrime victimisation. For example, training programs might be developed to mirror existing training for dealing with victims of intimate partner violence, to effectively minimise the stigmatisation and attribution of responsibility to the victims themselves. In addition to the opportunities for increasing community awareness, the police have an opportunity to continue improving service delivery, to reduce the under-reporting of cybercrime offences.

Finally, it was clear that most police respondents who participated in the survey had not been present during a staff meeting where cybercrime or cybersecurity issues were discussed. Therefore, building upon this identified relationship between incident exposure and the investigative capabilities of Australian police officers, there are potential opportunities to ensure that cybercrime is being more regularly discussed by police management across all levels. Regular staff meetings can (without additional costs) include items about cybersecurity issues, such as the importance of online fraud and theft awareness during holiday shopping periods. There is inherent and instrumental value in cultivating workplace environments that explicitly recognise the seriousness of both cyber-dependent and cyber-enabled criminal offences. This can contribute to the development of an officer's self-confidence and investigative capabilities.

Conclusion

Cybercrime is recognised by the Australian Government as a strategic priority for law enforcement. Indeed, the increasing role of digital technology in Australian social, economic and political life has created new and exciting opportunities for citizens; it has also rendered them vulnerable to associated cybersecurity threats. It is therefore important for governments, law enforcement, citizens and other actors to understand the nature of the cybercrime problem and to work collaboratively to develop innovative and effective solutions. This report has examined perceptions of cybercrime among members of the general community, police officers and cybersecurity experts, with the aim of contributing to our understanding of cybercrime and developing potential policy responses.

This project was guided by four key research questions, based upon existing criminological literature. Previous studies have revealed how police officers based within the United States and United Kingdom encounter personal and organisational challenges in the investigation and prevention of cybercrime, including a lack of self-confidence, insufficient cybersecurity expertise, poor reporting practices and the evolving character of cybersecurity threats (eg Hadlington et al. 2018; Nouh et al. 2019). International research also suggests that inter-agency variance in the quality of service provision is partially explained by whether officers are adequately resourced, trained and regularly exposed to cybercrime investigations (eg Bossler et al. 2019; Holt, Brewer & Goldsmith 2019). Finally, research has indicated that many victims of cybercrime experience frustration when reporting incidents to law enforcement (Cross 2018b, 2018c; Powell & Henry 2018). Indeed, studies examining both police and community populations suggest that cybercrime victims experience stigmatisation and routinely encounter victim-blaming attitudes, because cybercrime is viewed as comparatively less serious than offline types of criminal behaviour (eg Black, Lumsden & Hadlington 2019; Holt & Bossler 2016).

Despite the advances in the field, the existing body of criminological literature had not directly examined comparative perceptions of cybercrime among different populations, police data applicable within an Australian context, or substantive, solution-oriented research that assists in the development of potential policy responses. The present study addressed these gaps by conducting a mixed-method and multi-stage investigation examining the perceptions of cybercrime among and between a more diverse sample of police officers, community members and cybersecurity experts.

d

The results detailed and discussed in this report highlight the importance of education, training and practical exposure for equipping officers with the necessary confidence and capabilities to investigate cybercrime; the impact of life experiences on both police and community perceptions of cybercrime; and several perceptual discrepancies between these populations about cybercrime investigations. Our research suggests that these differences are indicative of an ongoing negotiation between police officers and community members about their respective roles and responsibilities in cybercrime investigations and prevention programs. Consequently, we have developed multiple evidence-based recommendations to assist government and law enforcement agencies.

Although the original research contributions of this report are significant, it is also important to reiterate the limited scope of the present findings. Identifying and acknowledging these limitations also provides guidance for further research to refine knowledge about cybercrime investigations. Firstly, the current research project focused on macro-level issues associated with the policing of cybercrime as a broad category of offences, rather than exploring more detailed insights into different investigative strategies associated with specific offences. The findings presented here should therefore be further developed in future studies that adopt a narrower scope. Secondly, it is also likely that the over-representation of cybercrime specialists within the police sample affected the observed patterns of responses. Although general duties officers still outnumbered specialists, the skewed character of the sample has probably led to an overestimation of measures of police knowledge of cybercrime, the seriousness of cybercrime and the patterns of attribution of moral responsibility. It is important to keep this in mind when interpreting the results. Thirdly, many of the statistically significant differences between sub-sample groups (ie police and community, gender, age) are generally weak, even where scale categories have been consolidated to increase the sensitivity of cross-tabulations. While the findings remain broadly consistent with comparable studies from the United States and United Kingdom (Bossler et al. 2019; Holt & Bossler 2012b), the scope of differences between these sub-sample groups is smaller. This suggests that there may be important socio-legal differences between these jurisdictions.

Overall, the present study has contributed novel insights into the perception of cybercrime within Australia among and between diverse populations of stakeholders. Based upon these new contributions to criminological knowledge, and acknowledging the methodological limitations of the present study, it is also clear that this report highlights several avenues for further research. Firstly, it is important to reiterate that the low response rate among police officers and the over-representation of specialists within the data may affect the patterns of observed results; it is important to conduct follow-up surveys that systematically test the observed relationship between officers' level of education, previous cybercrime-focused training and professional exposure to cybercrime investigations against their levels of self-confidence and investigative capabilities. For example, there are opportunities and potential value in exploring these relationships through a piloted case-control study testing some or all of the proposed initiatives included within the recommendations. Secondly, there are additional opportunities for examining the social negotiation between police officers and community members concerning their respective responsibilities in cybercrime investigation and prevention programs. For example, it would be useful to examine the extent to which public education campaigns reduce perceptual discrepancies between these population groups.

Recommendations

The research detailed throughout this report has examined perceptions of cybercrime among police officers, community members and cybersecurity experts, using these insights to identify opportunities for improving public awareness and investigative capabilities. No single initiative or program is going to completely solve the challenges presented by cybercrime; however, there is a clear need to expand the investigative capabilities of Australia law enforcement agencies and to address the discrepancy between police and public perceptions. Indeed, these recommendations flow directly from the results of both the quantitative and qualitative analyses, which highlighted the discrepancy between police and community attitudes as an impediment to the investigation of cybercrime. The recommendations are pragmatic proposals that affect both sides of the policy equation: police investigative capabilities and community knowledge.

Recommendation 1: Integrate and expand cybercrime training for general duties officers

Australian law enforcement agencies should recognise and address the need for general duties police officers to be equipped as first responders to cybercrime incidents. General duties officers should be trained in the appropriate handling of devices, to ensure that the chain of custody is preserved, and given basic awareness about cryptographic technologies.

In the short term, general duties officers should receive additional training that expands the following skillsets (arising out of the present findings):

- understanding of the conceptual and practical overlap between online and offline criminal activity;
- understanding of the distinction between cyber-dependent and cyber-enabled criminal offences;
- understanding of cybercrime reporting procedures and capacity to advise victims correctly;
- understanding of their responsibilities (as first responders) to recognise and preserve digital evidence; and
- sensitivity to the serious and gendered nature of online harms.

d

As a long-term policy initiative, Australian law enforcement agencies should develop and embed cybercrime modules within cadet training requirements. Such modules would go beyond existing training requirements in computer skills (such as the use of a police database) to familiarise cadets with the basics of digital forensics and their responsibilities as first responders in electronic evidence preservation. Revisions to academy curricula should be developed on the basis of the needs of specialist units and with input from external experts from industry and academia. To ensure that cadets receive practical instruction on how to receive, and respond to, instances of cybercrime, academy curricula should also introduce a rotation working with cybercrime specialist units.

Recommendation 2: Subsidise digital forensics training for cybercrime specialist officers

In recognition of the practical limitations associated with upskilling general duties officers, it is also imperative that governments redress the under-resourcing of existing cybercrime specialist units (apparent from both the quantitative and qualitative data).

Australian law enforcement agencies require more officers with specific knowledge of digital crime scene investigation procedures, electronic evidence management and digital forensic analysis while preserving the chain of custody. Additionally, the 'problem of going dark' highlights the need for specialist officers with an understanding of cryptography (ie the viability of cryptanalysis for accessing data at rest) and user reidentification (ie techniques used for traffic analysis of data in transit). These skillsets can be acquired by hiring officers with pre-existing skills in computer science and cybersecurity or by subsidising digital forensics training for existing officers seeking to specialise. Such a funding arrangement would be consistent with the strategic and funding priorities of Australia's Cyber Security Strategy (Department of Home Affairs 2020: 33).

Recommendation 3: Address cultural and operational impediments to cybercrime specialisation

Australian law enforcement agencies should also address workplace practices that act as a disincentive to specialisation in cybercrime investigations, as the qualitative data arising out of a focus group with cybercrime specialists and cybersecurity experts documented. This may require agencies to review promotion processes and to ensure that specialisation does not unfairly disadvantage career advancement. This will need to be part of a broader cultural change addressing any distinct and arbitrary impediments to career progression within specific agencies. For example, the importance of cybercrime as a strategic priority should be regularly and emphatically communicated to both general duties and specialist officers through police administration, command and line supervisors.

Additionally, police agencies should explore the potential benefits of expanding collaboration with technology companies and cybersecurity experts in the private sector. Indeed, our focus group data suggest that officers recognise the utility of building these public–private partnerships, to enable the expansion of internal cybercrime investigation skills. Any eventuating arrangements should be developed in accordance with the Australian Privacy Principles and with respect for the human rights implications of data-sharing arrangements.

Recommendation 4: Develop short- and long-term cybersecurity education initiatives

To complement any expansion in the cybercrime investigatory capabilities of Australian law enforcement agencies, it is also important to reduce the discrepancy in expectations between police and the broader community. This should involve both a short-term public education campaign and a longer-term initiative to implement cybersecurity practices into secondary education curricula.

As a short-term policy initiative, the Australian Government should consider developing and disseminating a general audience public education campaign that seeks to address some of the discrepancies currently observed between police and members of the public. This could include information about the risks posed by cybercrime, how to report a cybercrime, the investigative capabilities and limits of law enforcement, the utility of pre-emptive cybersecurity practices, and messages that challenge victim-blaming narratives.

As a longer-term cybercrime prevention initiative, Australian governments should consider integrating standardised cybersecurity training into secondary education curricula. While such a program might advance the same key points as an education campaign, the effects would be bolstered through classroom instruction. Curricula should be developed with the input of cybersecurity experts from both technological and social science disciplines. Such a program could be piloted and refined in a limited number of school districts prior to a national rollout.

References

URLs correct as at April 2021

ACSC—see Australian Cyber Security Centre

ACORN—see Australian Cybercrime Online Reporting Network

AFP—see Australian Federal Police

AGD—see Attorney-General's Department

Attorney-General's Department 2013. *National plan to combat cybercrime*. Now available from the Department of Home Affairs: https://www.homeaffairs.gov.au/about-us/our-portfolios/criminal-justice/cybercrime-identity-security

Australia New Zealand Policing Advisory Agency 2019. Australia and New Zealand police principles. https://www.anzpaa.org.au/publications/general#police_principles

Australian Communications and Media Authority (ACMA) 2015. *Communications report 2014–15*. Canberra: ACMA

Australian Communications and Media Authority (ACMA) 2011. *Communications report 2010–11*. Canberra: ACMA

Australian Competition and Consumer Commission (ACCC) 2020. *Targeting scams 2019: A review of scam activity since 2009*. Canberra: ACCC. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-2019-a-review-of-scam-activity-since-2009

Australian Cyber Security Centre (ACSC) 2019. Welcome to ReportCyber. https://www.cyber.gov.au/report

Australian Cyber Security Centre (ACSC) 2015. *2015 threat report*. Canberra: ACSC. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-threat-report-2015

Australian Cybercrime Online Reporting Network (ACORN) 2014. What is cybercrime? https://web.archive.org/web/20190101212736/https://www.acorn.gov.au/learn-about-cybercrime

Australian Federal Police 2020. Recruit training. https://www.afp.gov.au/careers/recruit-training

Australian Federal Police 2019. Cyber crime. https://www.afp.gov.au/what-we-do/crime-types/cyber-crime#What-to-do

Australian Human Rights Commission 2018. *Everyone's business: Fourth national survey on sexual harassment in Australian workplaces*. https://www.humanrights.gov.au/our-work/sex-discrimination/publications/everyones-business-fourth-national-survey-sexual

Black A, Lumsden K & Hadlington L 2019. 'Why don't you block them?' Police officers' constructions of the ideal victim when responding to reports of interpersonal cybercrime. In K Lumsden & E Harmer (eds), *Online othering: Exploring digital violence and discrimination on the web*. Cham, Switzerland: Palgrave Macmillan: 355–378. DOI: 10.1007/978-3-030-12633-9_15

Bond E & Tyrrell K 2018. Understanding revenge pornography: A national survey of police officers and staff in England and Wales. *Journal of Interpersonal Violence*. DOI: 10.1177/0886260518760011

Bossler AM & Holt TJ 2014. Further examining officer perceptions and support for online community policing. In CD Marcum & GE Higgins (eds), *Social networking as a criminal enterprise*. Boca Raton, FL: CRC Press: 167–196

Bossler AM & Holt TJ 2013. Assessing officer perceptions and support for online community policing. *Security Journal* 26(4): 349–366. DOI: 10.1057/sj.2013.23

Bossler AM & Holt TJ 2012. Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management* 35(1): 165–181. DOI: 10.1108/13639511211215504

Bossler AM, Holt TJ, Cross C & Burruss GW 2019. Policing fraud in England and Wales: Examining constables' and sergeants' online fraud preparedness. *Security Journal*. DOI: 10.1057/s41284-019-00187-5

Brenner SW 2008. *Cyberthreats: The emerging fault lines of the nation state*. New York: Oxford University Press

Broll R & Huey L 2015. 'Just being mean to somebody isn't a police matter': Police perspectives on policing cyberbullying. *Journal of School Violence* 14(2): 155–76. DOI: 10.1080/15388220.2013.879367

Brown CSD 2015. Investigating and prosecuting cyber crime: Forensic dependencies and barriers to justice. *International Journal of Cyber Criminology* 9(1): 55–119. DOI: 10.5281/ZENODO.22387

Button M 2012. Cross-border fraud and the case for an 'interfraud'. *Policing: An International Journal of Police Strategies and Management* 35(2): 285–303. DOI: 10.1108/13639511211230057

Callanan VJ & Teasdale B 2009. An exploration of gender differences in measurement of fear of crime. *Feminist Criminology* 4(4): 359–76. DOI: 10.1177/1557085109345462

Casey E 2019. The chequered past and risky future of digital forensics. *Australian Journal of Forensic Sciences* 51(6): 649–64. DOI: 10.1080/00450618.2018.1554090

Chang LYC, Zhong LY & Grabosky PN 2018. Citizen co-production of cyber security: Self-help, vigilantes, and cybercrime. *Regulation & Governance* 12(1): 101–14. DOI: 10.1111/rego.12125

Choo KR 2010. Harnessing information and communications technologies in community policing. In J Putt (ed), *Community policing in Australia*. Research and public policy series no. 111. Canberra: Australian Institute of Criminology: 67–75. https://www.aic.gov.au/publications/rpp/rpp111

Christie N 1986. The ideal victim. In E Fattah (ed), *From crime policy to victim policy: Reorienting the justice system*. Basingstoke, UK: Palgrave Macmillan: 17–30. DOI: 10.1007/978-1-349-08305-3

Cockcroft T, Shan-A-Khuda M, Schreuders ZC & Trevorrow P 2018. Police cybercrime training: Perceptions, pedagogy, and policy. *Policing: A Journal of Policy and Practice*. DOI: 10.1093/police/pay078

Collier PA & Spaul BJ 1992. A forensic methodology for countering computer crime. *Artificial Intelligence Review* 6(2): 203–15. DOI: 10.1007/BF00150234

Cross C 2019a. Is online fraud just fraud? Examining the efficacy of the digital divide. *Journal of Criminological Research, Policy and Practice* 5(2): 120–31. DOI: 10.1108/JCRPP-01-2019-0008

Cross C 2019b. 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. *Criminology & Criminal Justice*. DOI: 10.1177/1748895819835910

Cross C 2018a. Denying victim status to online fraud victims: The challenges of being a 'non-ideal victim'. In M Duggan (ed), *Revisiting the ideal victim concept: Developments in critical victimology*. Bristol, UK: Policy Press: 243–62

Cross C 2018b. Expectations vs reality: Responding to online fraud across the fraud justice network. *International Journal of Law, Crime and Justice* 55: 1–12. DOI: 10.1016/j.ijlcj.2018.08.001

Cross C 2018c. Victims' motivations for reporting to the 'fraud justice network.' *Police Practice and Research* 19(6): 550–564. DOI: 10.1080/15614263.2018.1507891

Cross C & Blackshaw D 2015. Improving the police response to online fraud. *Policing: A Journal of Police and Practice* 9(2): 119–28. DOI: 10.1093/police/pau044

Cross C, Richards K & Smith RG 2016. The reporting experiences and support needs of victims of online fraud. *Trends & issues in crime and criminal justice* no. 518. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi518

Crow MS, Snyder JA, Crichlow VJ & Smykla JO 2017. Community perceptions of police body worn cameras: The impact of views on fairness, fear, performance, and privacy. *Criminal Justice and Behavior* 44(4): 589–610. DOI: 10.1177/0093854816688037

Davis B & Dossetor K 2010. (Mis)perceptions of crime in Australia. *Trends & issues in crime and criminal justice* no. 396. Canberra: Australian Institute of Criminology. https://aic.gov.au/publications/tandi/tandi396

Department of Home Affairs 2020. *Australia's cyber security strategy 2020*. Canberra: Department of Home Affairs. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy

Dodge A & Spencer DC 2018. Online sexual violence, child pornography or something else entirely? Police responses to non-consensual intimate image sharing among youth. *Social & Legal Studies* 27(5): 636–657. DOI: 10.1177/0964663917724866

Dodge C & Burruss G 2019. Policing cybercrime: Responding to the growing problem and considering future solutions. In R Leukfeldt & TJ Holt (eds), *The human factor of cybercrime*. London: Routledge: 339–58

Dupont B 2017. Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change* 67(1): 97–116. DOI: 10.1007/s10611-016-9649-z

Fraud Advisory Panel 2016. *The fraud review: 10 years on*. https://www.fraudadvisorypanel.org/wp-content/uploads/2016/06/The-Fraud-Review-Ten-Years-On-WEB.pdf

Gorard S 2017. *Research design: Creating robust approaches for the social sciences*. London: Sage

Hadlington L, Lumsden K, Black A & Ferra F 2018. A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime. *Policing: A Journal of Policy and Practice*. DOI: 10.1093/police/pay090

Harkin D & Whelan C 2019. Exploring the implications of 'low visibility' specialist cyber-crime units. *Australian & New Zealand Journal of Criminology* 52(4): 578–94. DOI: 10.1177/0004865819853321

Harkin D, Whelan C & Chang L 2018. The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research* 19(6): 519–36. DOI: 10.1080/15614263.2018.1507889

Henry N, Flynn A & Powell A 2018. Policing image-based sexual abuse: Stakeholder perspectives. *Police Practice and Research* 19(6): 565–81. DOI: 10.1080/15614263.2018.1507892

Hinduja S 2007. Computer crime investigations in the United States: Leveraging knowledge from the past to address the future. *International Journal of Cyber Criminology* 1(1): 1–26. DOI: 10.5281/zenodo.18275

Hinduja S 2004. Perceptions of local and state local law enforcement concerning the role of computer crime investigative teams. *Policing: An International Journal of Police Strategies and Management* 27(3): 341–357. DOI: 10.1108/13639510410553103

Hinduja S & Schafer JA 2009. US cybercrime units on the world wide web. *Policing: An International Journal of Police Strategies & Management* 32(2): 278–96. DOI: 10.1108/13639510910958181

Holt TJ 2018. Regulating cybercrime through law enforcement and industry mechanisms. *The Annals of the American Academy of Political and Social Science* 679(1): 140–57. DOI: 10.1177/0002716218783679

Holt TJ & Bossler AM 2016. *Cybercrime in progress: Theory and prevention of technology-enabled offenses*. London: Routledge

Holt TJ & Bossler AM 2014. An assessment of the current state of cybercrime scholarship. *Deviant Behavior* 35(1): 20–40. DOI: 10.1080/01639625.2013.822209

Holt TJ & Bossler AM 2012a. Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. *American Journal of Criminal Justice* 37(3): 396–412. DOI: 10.1007/s12103-011-9131-5

Holt TJ & Bossler AM 2012b. Predictors of patrol officer interest in cybercrime training and investigation in selected United States Police departments. *Cyberpsychology, Behavior, and Social Networking* 15(9): 464–72. DOI: 10.1089/cyber.2011.0625

Holt TJ, Bossler AM & Fitzgerald S 2010. Examining state and local law enforcement perceptions of computer crime. In TJ Holt (ed), *Crime on-line: Correlates, causes, and context*. Raleigh, NC: Carolina Academic Press: 221–46

Holt TJ, Brewer R & Goldsmith A 2019. Digital drift and the 'sense of injustice': Counter-productive policing of youth cybercrime. *Deviant Behavior* 40(9): 1, 144, 156. DOI: 10.1080/01639625.2018.1472927

Holt TJ, Burruss GW & Bossler AM 2019. An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents. *Policing and Society* 29(8): 906–21. DOI: 10.1080/10439463.2018.1450409

Holt TJ, Burruss GW & Bossler AM 2015. *Policing cybercrime and cyberterror*. Durham, NC: Carolina Academic Press

Holt TJ, Lee JR, Liggett R, Holt KM & Bossler AM 2019. Examining perceptions of online harassment among constables in England and Wales. *International Journal of Cybersecurity Intelligence and Cybercrime* 2(1): 24–39. https://vc.bridgew.edu/ijcic/vol2/iss1/3

Huey L, Nhan J & Broll R 2013. 'Uppity civilians' and 'cyber-vigilantes': The role of the general public in policing cyber-crime. *Criminology & Criminal Justice* 13(1): 81–97. DOI: 10.1177/1748895812448086

Jang H, Joo HJ & Zhao J 2010. Determinants of public confidence in police: An international perspective. *Journal of Criminal Justice* 38(1): 57–68. DOI: 10.1016/j.jcrimjus.2009.11.008

Kemp S, Miró-Llinares F & Moneva A 2020. The dark figure and cyber fraud rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research*. https://doi.org/10.1007/s10610-020-09439-2

Kremer J 2014. Policing cybercrime or militarizing cybersecurity? Security mindsets and the regulation of threats from cyberspace. *Information & Communications Technology Law* 23(3): 220–37. DOI: 10.1080/13600834.2014.970432

Lee JR, Holt TJ, Burruss GW & Bossler AM 2019. Examining English and Welsh detectives' views of online crime. *International Criminal Justice Review*. DOI: 10.1177/1057567719846224

Marcum C, Higgins GE, Freiburger TL & Ricketts ML 2010. Policing possession of child pornography online: Investigating the training and resources dedicated to the investigation of cybercrime. *International Journal of Police Science and Management* 12(4): 516–25. DOI: 10.1350/ijps.2010.12.4.201

May DC, Rader NE & Goodrum S 2010. A gendered assessment of the 'threat of victimization'. *Criminal Justice Review* 35(2): 159–82. DOI: 10.1177/0734016809349166

McGuire M & Dowling S 2013. *Cybercrime: A review of the evidence—Summary of key findings and implications*. Home Office Research Report no. 75. https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

McQuade S 2006. Technology-enabled crime, policing and security. *Journal of Technology Studies* 32: 32–42. https://eric.ed.gov/?id=EJ847568

Millman CM, Winder B & Griffiths MD 2017. UK-based police officers' perceptions of, and role in investigating, cyber-harassment as a crime. *International Journal of Technoethics* 8(1): 87–102. DOI: 10.4018/IJT.2017010107

National Institute of Justice 2008. *Electronic crime scene investigations: A guide for first responders*, 2nd ed. Washington, DC: US Department of Justice, National Institute of Justice. https://www.ncjrs.gov/pdffiles1/nij/219941.pdf

New South Wales Police Force 2020. The training. https://www.police.nsw.gov.au/recruitment/the_training

New South Wales Police Force 2018. *Annual report 2017–2018*. Sydney: New South Wales Police Force. https://www.police.nsw.gov.au/about_us/publications

Nix J, Pickett JT, Baek H & Alpert GP 2019. Police research, officer surveys, and response rates. *Policing and Society* 29(5): 530–550. DOI: 10.1080/10439463.2017.1394300

Nouh M, Nurse JRC, Webb H & Goldsmith M 2019. *Cybercrime investigators are users too! Understanding the socio-technical challenges faced by law enforcement*. Paper to 2019 Workshop on Usable Security, 24 February 2019, San Diego, CA. DOI: 10.14722/usec.2019.23032

NSWPF—see New South Wales Police Force

Powell A 2010. Configuring consent: Emerging technologies, unauthorized sexual images and sexual assault. *Australian & New Zealand Journal of Criminology* 43(1): 76–90. DOI: 10.1375/acri.43.1.76

Powell A & Henry N 2018. Policing technology-facilitated sexual violence against adult victims: Police and service sector perspectives. *Policing and Society* 28(3): 291–307. DOI: 10.1080/10439463.2016.1154964

Powell A & Henry N 2017. *Sexual violence in a digital age*. London: Springer

Powell A, Scott AJ & Henry N 2018. Digital harassment and abuse: Experiences of sexuality and gender minority adults. *European Journal of Criminology*. DOI:1477370818788006

QPS—see Queensland Police Service

Queensland Police Service 2021. *Operational procedures manual*, issue 81 (public edition). Chapter 2: Investigative process. https://www.police.qld.gov.au/qps-corporate-documents/operational-policies/operational-procedures-manual

Queensland Police Service 2020. *Recruit handbook: Queensland Police Service Academy: Oxley Campus*. https://www.police.qld.gov.au/recruit-intake-documents

Queensland Police Service 2019. Reporting cybercrime. https://www.police.qld.gov.au/reporting/reporting-cybercrime

Randa R 2013. The influence of the cyber-social environment on fear of victimization: Cyberbullying and school. *Security Journal* 26(4): 331–48. DOI: 10.1057/sj.2013.22

Riek M, Bohme R & Moore T 2016. Measuring the influence of perceived cybercrime risk on online service avoidance. *IEEE Transactions on Dependable and Secure Computing* 13(2): 261–273. DOI: 10.1109/TDSC.2015.2410795

Schafer JA & Varano SP 2017. Changes in police organizations: Perceptions, experiences, and the failure to launch. *Journal of Contemporary Criminal Justice*, 33(4), 392–410. DOI: 10.1177/1043986217724532

Senjo SR 2004. An analysis of computer-related crime: Comparing police officer perceptions with empirical data. *Security Journal* 17(2): 55–71. DOI: 10.1057/palgrave.sj.8340168

Skogan WG 2015. Surveying police officers. In MD Maltz & SK Rice (eds), *Envisioning criminology: Researchers on research as a process of discovery*. New York, NY: Springer: 109–15

Stambaugh H et al. 2001. *Electronic crime needs assessment for state and local law enforcement*. Washington, DC: US Department of Justice, National Institute of Justice. http://www.ncjrs.gov/pdffiles1/nij/186276.pdf

Tasmanian Government Department of Police, Fire and Emergency Management 2019. *Annual report 2018–19*. https://www.police.tas.gov.au/about-us/corporate-documents/annual-report/

Tcherni M, Davies A, Lopes G & Lizotte Z 2016. The dark figure of online property crime: Is cyberspace hiding a crime wave? *Justice Quarterly* 33(5): 890–911. DOI: 10.1080/07418825.2014.994658

Wall DS 2008a. Cybercrime and the culture of fear: Social science fiction(s) and the production of knowledge about cybercrime. *Information, Communication & Society* 11(6): 861–84. DOI: 10.1080/13691180802007788

Wall DS 2008b. Cybercrime, media and insecurity: The shaping of public perceptions of cybercrime. *International Review of Law, Computers & Technology* 22(1–2): 45–63. DOI: 10.1080/13600860801924907

Wall DS 2007. Policing cybercrimes: Situating the public police in networks of security within cyberspace. *Police Practice and Research* 8(2): 183–205. DOI: 10.1080/15614260701377729

Wall DS 2001. Cybercrimes and the internet. In DS Wall (ed), *Crime and the internet*. New York: Routledge: 1–17

Weimann G 2016. Going dark: Terrorism on the dark web. *Studies in Conflict and Terrorism* 39(3): 195–206. DOI: 10.1080/1057610X.2015.1119546

Whelan C & Harkin D 2019. Civilianising specialist units: Reflections on the policing of cyber-crime. *Criminology & Criminal Justice*. Advance online publication. DOI: 10.1177/1748895819874866

Willits D & Nowacki J 2016. The use of specialized cybercrime policing units: An organizational analysis. *Criminal Justice Studies* 29(2): 105–24. DOI: 10.1080/1478601X.2016.1170282

Yar M & Steinmetz K 2019. *Cybercrime and society*, 3rd ed. London: Sage

CRG reports
CRG 23/16–17

Dr Cassandra Cross is an Associate Professor in the School of Justice at the Queensland University of Technology.

Dr Thomas Holt is a Professor in the School of Criminal Justice at Michigan State University.

Dr Anastasia Powell is an Associate Professor in Criminology & Justice Studies at RMIT University.

Dr Michael Wilson is a Lecturer in Criminology in the School of Law at Murdoch University.

www.aic.gov.au/crg