Australian Government

Australian Institute of Criminology

Submission

Parliamentary Joint Committee on Law Enforcement: Inquiry into the capability of law enforcement to respond to cybercrime

Prepared by the Australian Institute of Criminology

Contents

Introduction

The Australian Institute of Criminology (AIC) is Australia's national research and knowledge centre on crime and justice. The AIC informs crime and justice policy and practice in Australia by undertaking, funding and disseminating policy-relevant research of national significance.

The AIC has prepared this submission in response to an invitation from the Parliamentary Joint Committee on Law Enforcement (PJCLE) as part of its inquiry into the capability of law enforcement to respond to cybercrime.

The AIC welcomes the opportunity to contribute to the PJCLE review. Cybercrime is a major focus of the AIC's research program. The information presented in this submission is based on the AIC's recent Cybercrime in Australia 2023 report, other AIC research and the wider Australian and international evidence base. Unless otherwise stated, statistics in this submission are drawn from the Cybercrime in Australia report (Voce & Morgan 2023a), with key sections summarised for the purpose of this submission.

Our submission covers a wide range of cyber-enabled and cyber-dependent crimes. While we recognise the importance of improving law enforcement capability to respond to the online sexual exploitation of children (OSEC), this crime is not a specific focus of this submission. A detailed overview on the OSEC problem and evidence-based responses was provided by the AIC to the PCJLE inquiry into law enforcement capabilities in relation to child exploitation.

Cybercrime Research Program

The AIC is undertaking a significant body of research into cybercrime to enhance the Commonwealth's capability with respect to understanding new and emerging cybercrime threats. Our goal is to draw on our specialist research expertise and a crime science approach to better understand and disrupt cybercrime, including the development of innovative methods and analytical tools to understand cybercrime victimisation. Our focus is on the human factor in cybercrime—the victims who are vulnerable to exploitation and who are impacted by cybercrime, the offenders who exploit digital technology to commit offences, and the institutional responses to cybercrime (Leukfeldt & Holt 2020).

Current focus areas

High quality evidence is central to the development of effective responses to cybercrime. This research needs to advance our understanding of the patterns and causes of cybercrime, but also the impact of prevention, disruption and enforcement. We are focused on several areas, including:

- Cybercrime in Australia, our annual report on the state of cybercrime victimisation, help-seeking and harms;
- repeat cybercrime victimisation;
- building cybercrime prevention capability;
- cybercrime help-seeking and the response to victims;
- vulnerability to ransomware victimisation among individuals and small businesses.

We will continue to work with our partners across the Commonwealth government to ensure this research is focused on government priorities and reflects the evolving nature of cybercrime.

Australian Cybercrime Survey

A major component of the cybercrime research program is the Australian Cybercrime Survey. This survey was developed as an annual survey and collects a wide range of data on Australian computer users' experiences of cybercrime victimisation. The survey examines a range of cyber-dependant and cyber-enabled crimes, including online abuse and harassment, malware, identity crime and misuse and online scams and fraud. The core survey, which is completed by a minimum of 10,000 respondents, collects information on recent and lifetime victimisation, help-seeking behaviour and the financial losses and other harms from victimisation, along with a range of information about online behaviour that can help inform the development of prevention strategies.

Cybercrime in Australia

Cybercrime is a common but varied crime type

Cybercrime is a common occurrence among Australian computer users. Two-thirds of respondents to the Australian Cybercrime Survey said they had been a victim of at least one type of cybercrime measured by the survey during their lifetime. Forty-seven percent of respondents had been a victim of cybercrime in the 12 months prior to the survey.

While there is no equivalent measure in Australia, data from the Crime Survey for England and Wales shows that fraud—much of which will be cyber-enabled—and computer misuse accounts for nearly half of all self-reported crime incidents (Office for National Statistics 2023).

It is important to recognise that cybercrime is not just one type of crime. Cybercrime comprises an extremely broad range of crime types, each with different targets, risk factors, offender motivations and modus operandi, harms to victims and response requirements. It spans both property and personal offences and intersects with other offline crime types. This calls for more of a problem-solving approach (Dodge & Burruss 2020) than is currently used. This involves detailed assessment of specific problems and the development and testing of tailored solutions. This approach is likely to be more effective than trying to develop responses to cybercrime that do not distinguish between different types of incidents.

Online abuse and harassment

According to the 2023 survey, online abuse and harassment was the most common type of cybercrime experienced by computer users. In the 12 months prior to the survey, more than one in four (27.0%) respondents had been a victim of online abuse and harassment. The most common form was being sent unsolicited sexually explicit messages, images or videos (9.8%); someone hacking into their social media or network account (4.9%); and someone sending or posting messages via electronic communication that made them feel hurt, embarrassed or unsafe (3.7%).

Unlike other forms of cybercrime, online abuse and harassment often involves people known to the victim. While at least half of all victims said it involved a stranger online (48.6%), friends, former friends, partners, former partners, and family members accounted for around a quarter of offenders in the most recent incident (24.4%). This may reflect a wider pattern of behaviour that also involves offline offending.

Malware

Twenty-two percent of respondents had been a victim of malware in the 12 months prior to the 2023 survey. Ransomware is one type of malware that has attracted concern. While the focus is frequently on ransomware attacks against larger organisations, ransomware can also impact individuals and smaller businesses. Overall, 4.8 percent of respondents received a ransom message on their device demanding payment in the 12 months prior to the survey. This was higher than the estimated 2.1 percent of respondents in a 2021 survey who received a ransom message on their device (Voce & Morgan 2021). When limited to incidents involving signs of a malware attack as well as a ransom message—what we might call pure ransomware—2.4 percent of respondents said they had been a victim.

Identity crime and misuse

One in five respondents (20.1%) had been a victim of identity crime and misuse in the 12 months prior to the survey. The most common incidents of identity crime and misuse that respondents experienced in the past year were suspicious transactions appearing in their bank statements or accounts, credit card or credit report (9.3%); receiving calls from debt collectors asking about unpaid bills they did not recognise (5.7%); and someone using their details to purchase or order something or receiving unfamiliar bills, invoices or receipts (3.0%). Together, these accounted for over two-thirds of the most recent incidents of identity crime and misuse.

Online fraud and scams

Eight percent of respondents had been a victim of fraud and scams in which they paid money or provided sensitive information. Online shopping scams were the most common type of online fraud or scam reported in the 12 months prior to the survey (2.2% of respondents) and accounted for more than one-quarter of the most recent incidents reported by victims. This was followed by providing sensitive information to a scammer pretending to be a known service institution or company, such as a bank, internet provider or post office—a common form of phishing scam (1.2%). Remote access scams were the next most common (0.7%), while 0.5 percent of respondents had fallen victim to a romance scam. Overall, 1.1 percent of respondents had fallen victim to an investment scam in the 12 months prior to the survey. While less common than other cybercrime types, online fraud and scam victims lost more money than other victims and also experienced more negative outcomes, especially practical, social and financial harms.

Large-scale data breaches increase the risk of cybercrime

The observation period for the Australian Cybercrime Survey included the period in which the customer databases of Optus and Medibank were breached. One in three respondents (33.6%) had their financial or personal information exposed in a data breach in the 12 months prior to the survey. The Latitude Financial data breach was reported in the days after the completion of data collection, and it is unlikely that respondents would have been aware of it when they completed the survey, meaning this is almost certainly an underestimate.

An earlier survey of 14,994 respondents, conducted in mid-2021, found only 9.3 percent of respondents had been *notified* of a data breach (Morgan & Voce 2022). In the Australian Cybercrime Survey, 26.7 percent of respondents had been notified of a data breach—a threefold increase on the previous survey.

Data breaches increase the risk of cybercrime. According to McAlister et al. (2023), one in seven (14.4%) identity crime and misuse victims said that, in the most recent incident, their information was obtained during a data breach. Data breaches have been shown to significantly increase the likelihood of identity theft, online scams and fraud and ransomware (Morgan & Voce 2022). This highlights importance of proactive prevention strategies for people impacted by data breaches.

Contextual factors and emerging technologies provide new opportunities for malicious actors

Cybercrime is constantly evolving. While the major threats to individuals, business and government are relatively constant, the modus operandi of perpetrators is constantly evolving. This 'arms race' occurs in response to both emerging opportunities and action taken by governments and law enforcement to disrupt prominent forms of cybercrime. We can categorise these emerging opportunities into two main groups—the opportunities created by situational factors, and the opportunities created by advancement in new technologies that can be used by malicious actors.

An excellent example of the opportunities created by contextual factors is how malicious actors have exploited major disaster events (Smith & Levi 2021). During the COVID-19 pandemic, phishing scams shifted their focus, exploiting people's fear of illness, and need to access health products and financial supports—messages that would have been unlikely to work in other contexts. Offenders have also attempted to capitalise on natural disasters, including bushfires and floods, such as with charity fundraising scams. We know the risk of cybercrime victimisation increases when someone's life circumstances make them vulnerable to manipulation, coercion and exploitation (Voce & Morgan 2023b), which may be especially true when communities are affected by natural disasters.

A range of new technologies have and will continue to create new opportunities for cybercrime. The last decade has seen the uptake of artificial intelligence (AI), end-to-end encryption, the darknet, cloud data storage platforms, cryptocurrency, and various new social media and messaging apps. Cybercriminals are quick to adopt emerging technologies for criminal purposes. For example, AI is already being leveraged by criminal actors to upscale and enhance criminal activities, exploit human-centric vulnerabilities and lower the barriers and costs to engaging in criminal activities (EUROPOL 2020). Artificial intelligence has the potential to facilitate better targeted, more frequent and widespread criminal attacks, and is already being used for password guessing, CAPTCHA-breaking and voice cloning (EURPOL 2020). Large language models like ChatGPT have the potential to improve the success rates of phishing and fraud attempts, where emails and messages can be created faster, be tailored to prey on specific vulnerabilities, appear more legitimate and be deployed at a significantly increased scale (EUROPOL 2023).

We need better data on these emerging technologies. The AIC is developing a module to be included as part of the Australian Cybercrime Survey to capture better data on the impact of emerging technologies. This will provide valuable data on awareness, use and consequences of these technologies. In 2024, the focus of the emerging technology module will be on the use of AI.

Cybercrime disproportionately impacts certain groups in our community

Not everybody has the same risk of falling victim to cybercrime. It disproportionately affects certain groups in our community. According to the Australian Cybercrime Survey:

- Younger respondents, First Nations respondents, respondents with a restrictive health condition were each more likely to have been a victim of all four types of cybercrime.
- Men were more likely than women to be the victim of fraud and scams and online abuse and harassment.
- Respondents who identified as LGB+ (lesbian, gay, bisexual or other non-heterosexual orientation) were significantly more likely than heterosexual respondents to have been a victim of online abuse and harassment and malware.
- Respondents who mainly spoke a language other than English at home were more likely to have been a victim of malware, identity crime and misuse, and scams and fraud.
- Respondents currently in a relationship were less likely than respondents not in a relationship to be a victim of online abuse and harassment.
- Respondents with children living at home were more likely to have been a victim of identity crime and misuse than respondents without children.
- Respondents with higher incomes were also more likely to be the victim of online abuse and harassment, identity crime and misuse, and fraud and scams.

While some of this may be due to differences in online behaviour and technology use, it is also possible that some of these groups are more vulnerable to exploitation. It highlights the need to consider tailored responses that meet the needs of different sections of our community.

Cybercrime is most frequently a high volume, low yield crime, but with big financial losses to some victims

Individual losses associated with cybercrime victimisation vary widely. Most victims report losing no money from the most recent incident. Among those victims who do lose money and who could report how much, the majority lost less than $1,000. A small group of victims did lose substantial amounts of money. Seven percent of fraud and scam victims, 5.5 percent of online abuse and harassment victims, 2.5 percent of malware victims and 4.1 percent of identity crime victims lost more than $10,000 in the most recent incident. 1.4 percent of online abuse and harassment victims and 1.7 percent of fraud and scam victims lost more than $100,000 in the most recent incident. The impact of these losses is potentially catastrophic and can have long-term effects on victims. These incidents are more likely to be reported to authorities and tend to be reflected in estimated losses based on recorded data.

Cybercrime targeting individual computer users is most frequently a high volume, low yield crime. The high rate of victimisation means that, even with the relatively small median losses per victim, the overall cost to Australian individuals is likely to be enormous. Previous AIC research into the cost of pure cybercrime showed that the amount lost per victim was relatively small, but the total estimated cost to Australian computer users exceeded $3 billion (Teunissen, Voce & Smith 2021). Similar patterns in terms of individual losses have been observed in other countries (Office for National Statistics 2022).

With such a high rate of victimisation, even with modest returns, the cybercrime targeting Australian computer users is extremely lucrative for cybercriminals.

Cybercrime impacts extend well beyond financial losses

Given the profit-motivated nature of many types of cybercrime, the emphasis is often on financial losses. However, the impact of cybercrime can extend well beyond these financial losses (Cross, Richards & Smith 2016). According to the Australian Cybercrime Survey, 53.1 percent of cybercrime victims were negatively impacted by cybercrime in the 12 months prior to the survey. Taking into account the prevalence of victimisation, this means an estimated 24.7 percent of all respondents to the survey were negatively impacted by cybercrime. Practical impacts, such as the loss of confidence in using the internet, impact on a person’s ability to communicate with others, or problems accessing accounts or resources were most common (40.9% of victims). This was followed by social impacts, such as the loss of trust, increased isolation, and relationship breakdown (17.9%). Health impacts included mental or emotional distress, trouble sleeping and deteriorating health (15.9 percent). Around one in six victims reported financial problems, meaning not everyone who lost money were impacted financially. While financial support is important, support for cybercrime victims must address these non-financial harms.

Intervention and support efforts can also be targeted at types of cybercrime that cause the highest harm to victims. The type and extent of harm varied according to which cybercrime victims experienced, with fraud and scam victims the most likely to experience practical and social impacts, and online abuse and harassment victims most likely to experienced health-related impacts. The AIC is currently developing a harm index for individual victims of cybercrime that provides validated measures of the relative harm from different types of cybercrime (Voce & Morgan forthcoming).

Victims who experience multiple forms of cybercrime account for a disproportionate level of harm

The 2023 Australian Cybercrime Survey found that nearly half of all cybercrime victims (43%) reported having experienced multiple types of cybercrime in the 12 months prior to the survey. Those who did experienced much greater levels of harm as a result.

Despite this, there has been relatively limited research how repeat victimisation occurs for cybercrime victims and offences. In traditional crime, research demonstrates that an individual's risk of becoming a repeat victim is heightened during the period immediately following a victimisation incident, and that the risk of repeat victimisation increases with each subsequent incident (Grove & Farrell 2012). Most recorded crime constitutes repeat victimisation of the same targets, with a small group of victims experiencing a disproportionate amount of repeat victimisation (O, Martinez, Lee & Eck 2017).

Forthcoming AIC research measures the concentration of harm from cybercrime among victims. It shows that a relatively small group of victims who experience multiple forms of cybercrime account for a disproportionate level of harm. Repeat victims who experienced multiple types of cybercrime are disproportionately impacted and should be prioritised for intervention.

Small to medium businesses are especially vulnerable to cybercrime

Small to medium businesses account for more than 99 percent of all Australian businesses (ASBFEO 2023). Small to medium business owners, operators and managers experience significantly higher rates of all types of cybercrime. When they fell victim, small to medium business owners and operators were more likely to have lost money or spent money on consequences and, when they did, they lost larger amounts of money than other victims. Two in five respondents who were small business owners and operators said their business was impacted as a result of cybercrime.

Small to medium businesses may be large enough to have the infrastructure, data holdings (or access to networks of larger organisations) and profits to be attractive targets for cybercrime, but not the resources, expertise and capability of larger organisations to prevent cybercrimes. Despite losing larger amounts of money than other victims, there was little difference in reporting, suggesting that small business owners and operators may be reluctant to seek help from law enforcement. The effect of cybercrime on small businesses may have flow-on implications, such as for customers who are secondary victims of data breaches, or for larger organisations, if offenders use these smaller businesses in the supply chain to gain access to other systems and networks.

This highlights the importance of building the capability of small to medium business operators to prevent cybercrime and ensuring that support for victims is both available and accessible. The recent announcement of funding to provide cyber resilience training for small businesses as part of the new Cyber-Security Strategy will help to address this vulnerability. Further work is needed to understand what types of prevention activities are most effective in preventing cybercrime against small businesses (Kemp 2023).

Law enforcement response to cybercrime

Under-reporting and the effects on official data sources

The 2023 Australian Cybercrime Survey showed that most cybercrime victimisation went unreported to police or to ReportCyber (the main online reporting platform for reporting cybercrime to police). Data on whether victims reported the most recent incident to police or ReportCyber can be used to estimate multipliers, which can be applied to the number of recorded cybercrime incidents to estimate the total number of incidents impacting Australian computer users:

- 14.8 percent of online abuse and harassment victims sought help, advice or support from police or the ACSC. The true number of online abuse and harassment incidents involving unique victims will be *at least* 6.8 times the number recorded by ReportCyber.
- 7.9 percent of malware victims sought help, advice or support from police or the ACSC. The true number of malware incidents involving unique victims will be *at least* 12.7 times the number recorded by ReportCyber.
- 13.9 percent of identity crime victims sought help, advice or support from police or the ACSC. The true number of identity crime incidents involving unique victims will be *at least* 7.2 times the number recorded by ReportCyber.
- 22.1 percent of fraud and scam victims sought help, advice or support from police or the ACSC. The true number of fraud and scam incidents involving unique victims will be *at least* 4.5 times the number recorded by ReportCyber.

While these are broad categories of cybercrime, these multipliers illustrate the large number of incidents not captured by ReportCyber—which recorded nearly 94,000 reports in 2022–23, equivalent to one report every six minutes (ASD 2023).

There is a disconnect between the expectations of victims and what can be delivered by law enforcement

Most victims sought help from police or ReportCyber in order to prevent the crime happening to them again or to someone else; however, one in three victims of identity crime and misuse and two in five fraud and scam victims who sought help did so because they wanted to get their money back or be compensated for loss or damage. Many police agencies are clear that they are unable to assist with the recovery of funds when a victim makes a report.

Data from the Australian Cybercrime Survey shows that many victims of identity crime and misuse are able to recover at least some of their losses and, on average, recover 90 percent of their financial losses. That is not the case for other types of cybercrime. Less than one third (29.5%) of fraud and scam victims who lose money were able to recover any of their losses. This was even less common among malware (25.1%) and online abuse and harassment (12.9%) victims.

Seeking help from police or ReportCyber doesn’t always result in an investigation or outcome (see ‘Barriers to policing cybercrime can impact clearance rates’). We know from the evaluation of the Australian Cybercrime Online Reporting Network (ACORN) that when victims’ expectations about what will happen when they report to police are not met, they are much less likely to be satisfied with the outcome of the report (Morgan et al. 2016).

There are positive signs with victim satisfaction with reporting to police, but still room for improvement

Victims who reported the most recent incident to police or to ReportCyber were usually more likely to be satisfied than dissatisfied with the outcome of their report. Up to 43.1 percent of victims who sought help were satisfied with the outcome and up to 36.1 percent were dissatisfied with the outcome.

Since the introduction of the ACORN—the predecessor to ReportCyber—the platform has been improved and steps taken to improve the information sharing with law enforcement and the capability of police to respond to cybercrime reports. While there are still significant challenges, it is possible that these changes have led to some improvements in the reporting experiences of victims.

As part of an evaluation of ACORN, cybercrime victims who had reported to ACORN were surveyed about the outcome of their report and their satisfaction with that outcome (Morgan et al. 2016).

Despite some methodological differences, this allows for some crude comparisons of satisfaction rates between victims who reported to ACORN in mid-2015 and victims who sought help, advice or support from police or ReportCyber in 2022:

- 21 percent of victims of cyberbullying, sexting, online harassment or stalking who reported to ACORN were satisfied with the outcome, compared with 36 percent of online abuse and harassment victims who sought help, advice or support from the police or ReportCyber;
- 32 percent of victims of computer system attacks who reported to ACORN were satisfied with the outcome, compared with 39 percent of malware victims who sought help, advice or support from the police or ReportCyber; and
- 30 percent of victims of online scams and fraud who reported to ACORN were satisfied with the outcome, compared with 43 percent of victims who sought help, advice or support from the police or ReportCyber.

The consistent upward trend in satisfaction rates suggests that responses to cybercrime victims have improved. Nevertheless, there is scope to ensure that victims receive the necessary support, especially given the range of harmful impacts they may experience.

Barriers to policing cybercrime can impact clearance rates

Among those who sought help from police or ReportCyber, between 40.9 and 49.5 percent either heard nothing, did not know what had happened, or were told nothing could be done. Overall, 6.1 percent of online abuse and harassment victims, 5.8 percent of malware victims, 5.4 percent of identity crime victims and 2.5 percent of fraud or scam victims were told by the police that someone had been arrested, charged or prosecuted.

This reflects the many barriers encountered by law enforcement in trying to respond to cybercrime. Several factors can influence whether a cybercrime reported to police (including via ReportCyber) is investigated and, if so, whether the offender will be apprehended. Some of these factors are not unique to cybercrime. Not every incident reported to police or ReportCyber will meet the threshold for a criminal offence. In other cases, there will be a low prospect of arrest, particularly where there is insufficient evidence to proceed with an investigation.

Previous research has highlighted some of the challenges associated with investigating cybercrime. Limited specialist capability and training impacts the ability and confidence of police to respond (Wilson et al. 2022). These capability gaps are amplified by increasingly complex and technologically sophisticated offenders and offences, which also undermine police surveillance and evidence-gathering efforts (Cross et al. 2021). Further, jurisdictional boundaries and the borderless nature of cybercrimes also hinder investigation and offender identification (Morgan et al. 2016). Many cybercrimes are committed by offenders located in geographical jurisdictions different from their victims, which creates distinct issues with establishing jurisdiction to investigate and prosecute offenses (Cross 2019).

The need to raise awareness of reporting options

The most common reasons that victims gave for not reporting to police or ReportCyber were that they felt they could deal with the incident by themselves or they did not regard the incident as a serious offence. This is consistent with reporting to police among victims of crime more generally—the harm associated with crime incidents, as measured by the degree of bodily injury, economic loss, emotional damage, potential for harm, and perceived wrongfulness, is the strongest correlate of victim reporting (see Xie & Baumer 2019 for a review). This relationship extends to cybercrime, with a study conducted in the Netherlands finding that the seriousness and type of offence were the best predictors of cybercrime reporting (Van de Weijer, Leukfeldt & van der Zee 2021).

While many people didn't report because they felt they could deal with the problem themselves or because it wasn't serious enough, a large proportion didn't know where or how to report. They did not know reporting to the police or ReportCyber was an option, did not think the police or the ACSC would be able to do anything, or did not know how or where to report the matter.

As has already been made clear, police are already responding to cybercrimes which, on average, are more harmful and results in higher financial losses. Further, there is already a large volume of reports submitted to ReportCyber—one every six minutes (ASD 2023)—which far outweighs the capacity of law enforcement to respond. Efforts to increase reporting need to be balanced against the potential implications of exceeding law enforcement's capacity to respond.

Cybercrime prevention

Certain platforms expose online Australians to increased risk of cybercrime

Frequent use—defined as daily or weekly use—of certain platforms is associated with a much higher likelihood of online abuse and harassment and profit-motivated cybercrime. Using subscription-based sexually explicit interactive adult platforms; making donations or payments over gaming, streaming or fundraising platforms; being active on dating or romance websites and apps; and purchasing items from online marketplaces is associated with much higher rates of victimisation. In the case of profit-motivated cybercrimes, this is true even after other factors have been considered (Voce & Morgan 2023b). These platforms may be attractive for malicious actors to exploit, as they often involve communication between strangers, registration processes, and payments between parties and the platform.

While we can encourage people using these platforms to take steps to protect their safety online, some responsibility must fall to the operators of these platforms to ensure the safety of their users. This kind of 'passive' approach to crime prevention is generally more effective than approaches that rely of active engagement by users (Brown 2013).

People use online safety measures, but not as frequently as they could

We know that many people use online safety measures to protect themselves from cybercrime. However, many other people do not. For example, half or fewer than half of all respondents to the Australian Cybercrime Survey said they used online safety measures that are widely promoted as ways to stay safe online. This includes using a different password for secure online accounts, especially for banking or financial transactions (51.8% of respondents), using voice, fingerprint, facial or iris recognition technology to access devices such as their mobile phone (46.8%), installing or using antivirus software or firewalls on their devices (42.3%), checking their privacy settings on social media accounts (40.5%), and regularly updating the security software on their device when prompted by their device's security system (39.9%).

This also extends to measures to protect the safety of children online. Among respondents who had children living at home, around one in five (19.1%) said they had set, or had already installed, parental controls on devices and browsers to restrict access to certain content.

Relatively few people had recently participated in cybercrime education and awareness raising. Only one in eight respondents said they had recently participated in training to stay safe online or to protect their information (12.6%).

Respondents who used various online safety measures had a higher prevalence of cybercrime victimisation. This may be because respondents who had fallen victim to cybercrime were more likely to implement safety measures to prevent repeat victimisation. Further analysis by McAlister et al. (2023) showed that many victims of identity crime and misuse implemented simple online safety measures after they have fallen victims—being more careful when using or sharing person information (55.6% of victims), changing passwords (42.2%), implementing two-factor authentication (32.5%), being more cautious about adding people on social media (27.7%) and reviewing financial statements more carefully (26.9%).

Certain higher risk online activities have been shown to increase the likelihood of victimisation (Voce & Morgan 2023b). These activities included using freely available Wi-fi in a public location to conduct a financial transaction, opening emails from people or organisations they did not know, accepting friend requests from people they had not met in person, and sharing a password or a code for an account with someone else. Importantly, around one in 10 respondents or fewer have engaged in these behaviours in the 12 months prior to the survey, suggesting most people understand the risks.

This information should be used to help shape the development of more targeted prevention efforts. Especially for people who have already fallen victim and who might be at risk of becoming repeat victims.

Prevention programs must be based on rigorous evidence, which is currently lacking

There is mixed evidence about the role cybercrime prevention and awareness campaigns can play in reducing victimisation by educating individuals and organisations about potential threats and preventive measures. School educational campaigns are often cited as a cost-effective means for addressing prevention and criminal justice issues with youth, particularly regarding cyberbullying and raising young people's awareness of emerging risks (CCPCJ 2010). Some cyberbullying prevention and internet safety initiatives which are employed in school environments are evidence-based and have produced positive outcomes. These include iSAFE in the United States, KiVa in Finland, ConRed in Spain, No Trap in Italy, and ViSC in Austria (See ICPC 2018, Brewer et al 2019). However, empirical studies testing the impact of school campaigns have shown mixed results with regards to participants' intentions to take protective actions online (Dooley et al 2011) and no impact with regards to changes in risky online behaviour (Mishna et al 2009).

Kemp (2023) recently analysed whether two UK government schemes aimed at encouraging and helping businesses to adopt cybersecurity controls and policies ('Cyber Essentials' and '10 Steps to Cyber Security') were associated with safer organisational behaviour and whether adopting the recommended measures was related to lower levels of cybercrime victimisation and its impacts. They showed that awareness of the Government schemes was associated with more cyber secure practices; however, it is possible that more cautious businesses may be more likely to hear of the scheme. Moreover, there was no evidence that implementing the recommended measures was associated with a lower likelihood of victimisation or negative consequences.

Further, van Steen and colleagues (2020) recently analysed 17 government-sponsored cybersecurity campaign materials aimed at improving citizens' cybersecurity hygiene, awareness and skills. They found that that security campaigns are often focused on education and increasing awareness, under the assumption that if citizens are made aware of risks and how to improve their security behaviour, they will change their behaviour. They identified a lack of published studies investigating the direct effects of governmental cybersecurity campaigns, and noted that merely increasing awareness does not necessarily lead to behavioural change.

Importantly, research has repeatedly demonstrated that the effectiveness of messages is greatly influenced by how they are designed. For example, messages are more likely to influence decision-making when they attract attention, are clear and concise, are believable, come from a credible source, and impart explicit information about specific hazards, potential harms, and what to do to avoid harm (Haddad et al. 2020; Prichard et al. 2022). According to Bada, Sasse and Nurse (2014), effective influencing requires more than simply informing people about what they should and should not do. In the context of cyber security awareness campaigns, the way a person carries out a campaign's recommendations depends on both their appraisal of threat and their self-efficacy (Bada, Sasse & Nurse 2014). The attempt to change a certain behaviour is much more difficult when a person is overwhelmed by a large number of messages about certain issues. One way of increasing behavioral compliance may be to break down complex goals into smaller 'calls to action' which are specific, easy and achievable (Neimand et al 2020).

Giving clear and simple instructions is associated with behaviour change and compliance. The Behavioural Economics Team at the Department of Prime Minister and Cabinet (2020) recently published a paper examining the use of behavioural insights to boost the impact of cyber security alerts. They found that a salient call to action (ie. having a banner encouraging email recipients to share the email with their contact list) more than doubled the rates at which participants engaged in that desired action.

Building on these findings, the AIC has partnered with the Australian Federal Police Joint Policing Cybercrime Coordination Centre (JPC3) and eSafety to test the effects of targeted prevention messages with clear calls for action. We are undertaking a randomised control trial to test whether delivering targeted messages to computer users can reduce the prevalence of online abuse and harassment and profit-motivated cybercrime. A subsample of 3,500 respondents have been recruited from the 2023 Australian Cybercrime Survey and been randomly allocated to one of three groups: An online abuse and harassment intervention group (1,250 participants) who will receive monthly prevention messages from eSafety for six months; a profit-motivated cybercrime intervention group (1,250 participants) who will receive monthly prevention messages from the AFP JPC3 for six months; and a control group (1,000 participants) who will not receive any messages. They will all be surveyed as part of the 2024 Survey. This will allow us to measure whether the deployment of targeted prevention messages has any impact on awareness of online safety, use of higher risk or protective online behaviours, cybercrime victimisation, repeat cybercrime victimisation and help-seeking behaviour. This is an important step in building an Australian evidence base.

Summary

Main findings

We end our submission by summarising our main findings:

- Cybercrime is a common but highly varied crime problem affecting a large proportion of online Australians. The harms extend well beyond financial losses.
- The risk of cybercrime is not evenly distributed. Certain groups within the community are more likely to be a victim.
- The frequent use of certain platforms, and some higher risk online behaviours, are associated with a higher likelihood of falling victim to cybercrime.
- Many victims experience multiple types of cybercrime and, as a result, are more negatively impacted across a range of measures. They account for a disproportionate level of harm.
- Most incidents of cybercrime are not reported to police or to ReportCyber. Official statistics significantly underestimate the scale of the problem. Reported cybercrime is more serious and involves greater financial losses.
- Many victims of cybercrime do not seek help from police or ReportCyber because they do not know where or how to report cybercrime incidents.
- Very few incidents of cybercrime reported to police result in an offender being arrested and convicted. This reflects the many barriers encountered by law enforcement in trying to respond to cybercrime.

- Expectations of the law enforcement response to cybercrime vary, and a significant proportion of victims report to police or ReportCyber in the hope their lost funds will be recovered. Whether these expectations are met has a significant bearing over whether victims are satisfied with police.
- Research into cybercrime, especially the human factor of cybercrime, is not as well developed as other crime types. There are significant gaps in our knowledge of how certain cybercrimes are committed, what makes certain individuals and businesses more vulnerable, the response to cybercrime by victims, why individuals become involved in cybercrime, and the efficacy of prevention, disruption and enforcement efforts.

Implications

The implications of these findings are as follows:

- Adopt a problem-solving approach that allows for a detailed assessment of specific cybercrime problems and the development and testing of tailored solutions.
- Ensure that responses are tailored to the needs of different sections of our community, particularly those who are a higher risk of victimisation.
- Target intervention and support efforts at types of cybercrime that cause the highest harm to victims.
- Prioritise repeat victims who experience multiple types of cybercrime and are disproportionately impacted.
- Build the capability of small to medium business operators to prevent cybercrime and ensuring that support for small to medium business victims is both available and accessible.
- Raise awareness of reporting options for victims and address any confusion about the different options that are available. Balance this against the potential implications of exceeding law enforcement's capacity to respond.
- Build the capability of specialist and frontline police to respond to cybercrime victims.
- Ensure that operators of those platforms which are associated with higher rates of cybercrime take their own steps to ensure the safety of their users.
- Use information on people's online behaviour to shape the development of more targeted prevention efforts, especially for people who have already fallen victim and who might be at risk of becoming repeat victims, and measure the impact of prevention programs using rigorous methods.
- Increase the research capability within government that can capitalise on the vast amount of data collected on cybercrime and provide high quality evidence to guide decision making. This is particularly true of research into what works in prevention, disruption and enforcement.

AIC references

Brown R 2013. Regulating crime prevention design into consumer products: Learning the lessons from electronic vehicle immobilisation. Trends & issues in crime and criminal justice no. 453. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi453

Cross et al 2021. Responding to cybercrime: Perceptions and need of Australian police and the general community. Report to the Criminology Research Advisory Council Grant: CRG 23/16–17. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2021-08/CRG_Responding to cybercrime_0.pdf

Levi M & Smith R 2021. Fraud and its relationship to pandemics and economic crises: From Spanish flu to COVID-19. Research Report no. 19. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/rr78115

McAlister M et al. 2023. Identity crime and misuse in Australia 2023. Statistical Bulletin no. 42. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb77048

Morgan A & Voce I 2022. Data breaches and cybercrime victimisation. Statistical Bulletin no. 40. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78832

Morgan et al 2016. Evaluation of the Australian Cybercrime Online Reporting Network. Australian Institute of Criminology: Canberra. https://www.aic.gov.au/sites/default/files/2020-06/acorn_evaluation_report_.pdf

Teunissen C, Voce I & Smith R 2021. Estimating the cost of pure cybercrime to Australian individuals. Statistical Bulletin no. 34. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78269

Voce I & Morgan A 2021. Ransomware victimisation among Australian computer users. Statistical Bulletin no. 35. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78382

Voce I & Morgan A 2022. Help-seeking among Australian ransomware victims. Statistical Bulletin no. 38. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sb78504

Voce I & Morgan A 2023a. Cybercrime in Australia 2023. Statistical Report no. 43. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/sr77031

Voce I & Morgan A 2023b. Online behaviour, life stressors and profit-motivated cybercrime victimisation. Trends & issues in crime and criminal justice no. 675. Canberra: Australian Institute of Criminology. https://doi.org/10.52922/ti77062

Voce I & Morgan A forthcoming. Developing a harm index for individual cybercrime victims. Trends & issues in crime and criminal justice.

Other references

Australian Signals Directorate (ASD) 2023. ASD Cyber Threat Report 2022-2023. Canberra: Australian Signals Directorate. https://www.cyber.gov.au/sites/default/files/2023-11/asd-cyber-threat-report-2023.pdf

Australian Small Business and Family Enterprise Ombudsman (ASBFEO) 2023. Number of small businesses in Australia. ASBFEO Website. https://www.asbfeo.gov.au/sites/default/files/2023-10/Number of small businesses in Australia_Aug 2023_0.pdf

Bada M, Sasse A & Nurse JRC 2014. Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. ArXiv, abs/1901.02672. https://doi.org/10.48550/arXiv.1901.02672

Brewer R et al 2019. Cybercrime Prevention. Cham, Switzerland: Palgrave Pivot

Nations Congress on Crime Prevention and Criminal Justice (CCPCJ) 2010. Report of the Twelfth United Nations Congress on Crime Prevention and Criminal Justice. Salvador: United Nations Congress on Crime Prevention and Criminal Justice. https://www.unodc.org/documents/crime-congress/12th-Crime-Congress/Documents/A_CONF.213_18/V1053828e.pdf

Cross C 2019. 'Oh we can't actually do anything about that': The problematic nature of jurisdiction for online fraud victims. Criminology & Criminal Justice 2020, 20(3): 358–375. https://doi.org/10.1177/1748895819835910

Department of Prime Minister and Cabinet 2020. On the alert: Using behavioural insights to boost the impact of cyber security alerts. Canberra: Department of Prime Minister and Cabinet. https://behaviouraleconomics.pmc.gov.au/projects/alert-using-behavioural-insights-boost-impact-cyber-security-alerts

Dodge C & Burruss G 2020. Policing cybercrime: Responding to the growing problem and considering future solutions. In Leukfeldt R & Holt TJ (eds) The Human Factor of Cybercrime. London: Routledge: 339-358

Dooley J et al 2011. Educational evaluation of Cybersmart Detectives: final report: presented to the Australian Communications and Media Authority (ACMA). Perth, Australia: Child Health Promotion Centre, Edith Cowan University. https://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1861&context=ecuworks2011

EUROPOL 2023. ChatGPT: The impact of Large Language Models on Law Enforcement. https://www.europol.europa.eu/cms/sites/default/files/documents/Tech Watch Flash -The Impact of Large Language Models on Law Enforcement.pdf

EURPOL 2020. Malicious Uses and Abuses of Artificial Intelligence. https://www.europol.europa.eu/cms/sites/default/files/documents/malicious_uses_and_abuses_of_artificial_intelligence_europol.pdf

Grove L & Farrell G 2012. Once bitten, twice shy: Repeat victimisation and its prevention, in Farrington DP & Welsh BC (eds) The Oxford handbook of crime prevention. New York: Oxford University Press: 404–422

Haddad A et al 2020. Gaming tasks as a method for studying the impact of warning messages on information behaviour. Library Trends, 68(4): 576–598. https://doi.org/10.1353/lib.2020.0012

International Centre for the Prevention of Crime (ICPC) 2018. 6th International Report: Crime prevention and community safety: Preventing cybercrime. Montréal: ICPC

Kemp S 2023. Exploring public cybercrime prevention campaigns and victimization of businesses: A Bayesian model averaging approach. Computers & Security: 127. https://doi.org/10.1016/j.cose.2022.103089

Leukfeldt R & Holt TJ 2020. The Human Factor of Cybercrime. London: Routledge

Mishna F et al 2009. Interventions for Children, Youth, and Parents to Prevent and Reduce Cyber Abuse. Campbell Systematic Review, 5(1). https://doi.org/10.4073/csr.2009.2

Neimand A et al 2020. How to build better calls to action. Stanford Social Innovation Review, 6 January 2020. https://ssir.org/articles/entry/how_to_build_better_calls_to_action#

O S, Martinez NN, Lee Y & Eck JE 2017. How concentrated is crime among victims: A systematic review from 1977 to 2014. Crime Science, 6(9): 1–16. https://doi.org/10.1186/s40163-017-0071-3

Office for National Statistics 2022. Nature of fraud and computer misuse in England and Wales: year ending March 2022. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2022

Office for National Statistics 2023. Crime in England and Wales: year ending March 2023. https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingjune2023

https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingmarch2023

Prichard J et al 2022. Effects of automated messages on internet users attempting to access "barely legal" pornography. Sexual Abuse 34(1): 106–124. https://doi.org/10.1177/10790632211013809

Van de Weijer SGA, Leukfeldt R & Van der Zee S 2021. Cybercrime Reporting Behaviors Among Small- and Medium-Sized Enterprises in the Netherlands. In Weulen Kranenbarg, M., & Leukfeldt, R. (Eds.). (2021). Cybercrime in Context: Crime and Justice in Digital Society.

Van Steen T et al 2020. What (if any) behavior change techniques do government-led cybersecurity awareness campaigns use? Journal of Cybersecurity, 1-8. https://doi.org/10.1093/cybsec/tyaa019

Wilson et al 2022. Police preparedness to respond to cybercrime in Australia: An analysis of individual and organizational capabilities. Journal of Criminology, 55(4). https://doi.org/10.1177/26338076221123080

Xie M & Baumer EP 2019. Crime victims' decisions to call the police: Past research and new directions. Annual Review of Criminology, 2(1): 217–240. https://doi.org/10.1146/annurev-criminol-011518-024748