CRIME AND JUSTICE STATISTICS

BUREAU BRIEF

Trends in and characteristics of cybercrime in NSW

Ilya Klauzner and Amy Pisani

AIM

To examine the trends in, major characteristics of, and the police response to cybercrime in NSW.

METHOD

We extracted data from the ReportCyber Application Platform (RCAP), a national cybercrime reporting system operated by the Australian Cyber Security Centre. Data was analysed over a three-year period from 1 July 2019 to 30 June 2022 and was restricted to incidents where the victim resided in NSW. We separate cybercrime into five offence categories: cyber-enabled fraud, identity theft, cyber-enabled abuse, online image abuse (OIA), and device. We conducted a descriptive analysis on the victim, suspected perpetrator, and report characteristics to report on trends and characteristics of reported cybercrime. We estimated an ordinary least squares regression model to identify factors correlated with a referral to police of reported cybercrime.

RESULTS

Over the three years to June 2022, there were 39,494 reports of cybercrime where the victim resided in NSW, and more than $404 million reported lost. Cybercrime reports increased by 42%, with all cyber offence categories increasing except cyber abuse. Increases in cyber enabled fraud and identity crime, spurred a corresponding increase in reported cybercrime-related financial losses by individuals. Most victims were individuals (89%), male (53%) and over 25 years of age (87%); however, differences in victim type were observed within offence categories. While a high proportion of victims have evidence about the incident (94%), the majority did not know their perpetrator and therefore few reports included suspect details (28%). The majority (71%) of reports were closed by police in RCAP with no further investigation undertaken. Reports were however more likely to be referred to police when the incident involved a victim aged 17 years or younger, the suspect was known to the victim, money was lost, or an OIA offence was indicated.

CONCLUSION

Our results show that cybercrime in NSW largely follows the same increasing trend that has been observed in national cybercrime studies. However, the statistics we report here only offer a partial view of reported cybercrime in NSW as we do not capture data reported directly to police or other national reporting systems. There are clear benefits in ongoing public reporting of cybercrime trends both at the national level and separately for individual states and territories, which could be enabled by integrating reporting systems and enhancing police data.

KEYWORDS Cybercrime | Victims | Policing

Suggested citation: Klauzner, I. & Pisani, A. (2023). *Trends in and characteristics of cybercrime in NSW* (Bureau Brief No. 165). Sydney: NSW Bureau of Crime Statistics and Research.

INTRODUCTION

Cybercrime covers a wide range of criminal behaviours. It includes traditional offences that are enabled by technology (e.g., cyberstalking, identity theft and online fraud) as well as offences generated solely using computers (e.g., hacking and malware attacks) (O'Shea et al., 2022). Cybercrime can be directed towards personal computers and devices but can also target large business and government data systems. The breadth of cybercrime means that its impact on individuals, businesses and government and the associated financial, social, emotional, psychological, reputational and operational costs are substantial (Australian Cyber Security Centre [ACSC], 2022; Saleem et al., 2022).

Cybercrime is a matter of increasing public concern in Australia. The ACSC (2022) reported that in the 2021-22 financial year cybercrime increased by 13% compared to the previous year. The Australian Competition and Consumer Commission (ACCC, 2022) also found a 33% increase in reports of cyber-enabled fraud in 2021 compared to 2020, while the Australian e-Safety Commissioner reported a 55% increase in image-based abuse (also referred to as online image abuse or OIA) over the same period (eSafety Commissioner, 2022). The COVID-19 pandemic is suspected to be a major contributor to this upward trend due to increased opportunities for cybercrime from most daily activities moving online. Kemp et al. (2021) examined cyber-enabled fraud and device crime, including hacking and malware in the United Kingdom (UK). They found an increase (above usual seasonal trends) in these types of crime during the COVID-19 pandemic for individuals but not for organisations. Similarly, Levi and Smith (2021) examined fraud in Australia and the UK and found a rise in online fraud during the pandemic. Recognising this, in March 2022, the Australian Government created a new Joint Policing Cybercrime Coordination Centre to respond to the growing threat of cybercrime in Australia (How, 2022).

Martin and Whelan (2022) argue that cybercriminals, especially those that conduct data theft, are becoming ever more specialised and sophisticated, therefore many more breaches can be expected in the future. In October 2022, seven high-profile Australian companies, including Optus, Medibank and Energy Australia, had their systems hacked and protected customer data subsequently compromised (and in a number of cases publicly released). The Optus and Medibank data thefts alone were estimated to have impacted up to 20 million customers, or 75% of the Australian population (Wall, 2022). Scams targeting households are also becoming more sophisticated. The "hi mum" mobile phone scam, where cybercriminals pose as children in distress, scammed $7.2 million from 11,100 Australian parents (McElroy, 2022). Further, "ID spoofing" allows cybercriminals to impersonate official telephone numbers, including numbers associated with banks, to scam money out of consumers (Anonymous, 2023).

In terms of financial costs, Scamwatch estimates that in 2021 there were more than $2 billion in cybercrime-related financial losses reported to federal government agencies and financial institutions (ACCC, 2022). This is likely to be an underestimate as a significant proportion of scams are not reported to authorities. It is difficult to quantify the non-financial impacts of cybercrime given the breadth of cyber-enabled abuse and OIA, but these are also likely to be significant. For example, a survey on the impact of cyber abuse on adults in the United States (U.S.) found that the majority (88%) of victims reported negative impacts of the crime, including mental health (24%), emotional (16%), social (15%) and financial/education/employment related (2.9%) issues (Vakhitova et al., 2021).

Currently there are no reliable estimates of cybercrime in Australia, including in NSW. National crime prevalence studies (Australian Bureau of Statistics [ABS], 2017; ABS, 2022a) and officially reported crime statistics largely do not distinguish between cyber-enabled and other types of crime.[1] Instead, cybercrime is typically classified within 'traditional' crimes, such as fraud, or in many cases is not recorded. To fill this void, several Australian researchers have conducted surveys to estimate the prevalence of particular types of cybercrime. Voce and Morgan (2021) surveyed a representative sample of the Australian population and found that 2% of respondents had been a victim of a ransomware attack in the 12 months

1 An exception is for certain categories of fraud where the Australian Bureau of Statistics (2022b) does ask whether certain types of fraud (e.g., card fraud, and scams) were committed online.

prior to the survey. Wolbers et al. (2022) surveyed dating application users in Australia regarding their experience of cyber abuse and OIA. They found that 45% of respondents had been subjected to abusive and threatening language, 19% had been subjected to OIA, and 28% had been stalked online.

The increasing prevalence of cybercrime and the absence of police recording of cyber-specific incidents has resulted in the development of several potentially overlapping national reporting systems for cybercrime, complicating researchers' ability to report on the total number of reported cybercrimes. Currently, scams can be reported to Scamwatch, cyber abuse can be reported to the eSafety Commissioner, online child abuse to the Australian Centre to Counter Child Exploitation and data breaches to the Office of the Australian Information Commissioner. Additionally, all cybercrimes can be reported to the ReportCyber Application Platform (RCAP). RCAP is the only platform used to triage reports to state and federal police agencies.

The current study

This bureau brief analyses cybercrime in NSW using a data extract from RCAP. RCAP was created in July 2019 as a national reporting system for cybercrime. It is an online system that enables the Australian public to securely report most common types of cybercrime. These reports are then triaged[2] to law enforcement agencies, who may choose to investigate further or, if there isn't sufficient evidence to proceed, use the report for intelligence.[3] Police can also choose to re-refer the report to another jurisdiction (e.g., another state) if a new suspect living in that jurisdiction is identified. RCAP also acts as a resource for cybercrime prevention and mitigation, by providing various agencies including police agencies, with summary information reports.

In this report we aim to:

a) describe recent trends in reported cybercrime and its component offences in NSW;

b) quantify the financial impact of reported cybercrimes in NSW;

c) describe the characteristics of victims, including the extent to which they can identify a suspect; and

d) examine the proportion of matters that are referred to the police, the timeliness of such referrals, and the factors associated with a police referral.

2 Reports are triaged based on the state the suspect resides in, or if the suspect is unknown or lives outside Australia, the victim's state. Once reports are triaged to the relevant police jurisdiction, the police agency (e.g., NSW police) will decide whether to further investigate the offence (in this brief, we define this as a police referral) or take no further action. We examine the factors that lead to report being referred to the police in the results section.

3 If the police choose to investigate a report on RCAP they would close a report and refer the report to the relevant department in their police agency. Therefore, when closing a case on RCAP, police choose either to refer the case to local police for investigation or conduct no further investigation. Victims may still report cybercrime directly to police agencies. If a victim does this, police also encourage them to make a report on RCAP.

METHOD

We extracted reports made to RCAP over a three-year period starting from 1 July 2019 (the beginning of RCAP) to 30 June 2022. This period included a pre and post COVID-19 lockdown period allowing us to observe any changes associated with increased online activity (Kemp et al., 2021). We restrict our sample to reports where the victim was residing in NSW. We also remove any duplicate reports.[4] This leaves us with a rich dataset of 39,494 reports.

We examine the following demographic characteristics for victims:

- Victim type: coded as an individual or organisation. Further demographic variables are missing for organisations.
- Age: coded as 0 –17, 18 – 24, 25 – 34, 35 – 44, 45 – 54, and 55 and above. Calculated at the date the report was created from an individual's self-reported date of birth.
- Gender: coded as female, male and other.
- Aboriginal and Torres Strait Islander: self-reported and coded as yes or no.
- Special requirements/needs: A free-text field that allows victims to indicate if they have any needs. Responses range from a self-identified disability, mental illness, or health problem to a need for an interpreter. However, some "needs" are simply recorded as wanting to get money back.

We also examine any details that victims reported regarding the suspected perpetrator of the crime:

- Suspect details included: True if a victim included in their report one of the following: the suspect's name, alias, address, postcode, relationship to victim, their country, or date of birth.[5]
- Suspect personally known to the victim: True if the victim has reported a relationship to the suspect (e.g. mother, ex-partner). This variable is missing if the victim did not include suspect details.
- International suspect: True if the victim reported an address with a country other than Australia. This variable is missing if the victim did not include suspect details.
- Unknown country: True if the victim reported an unknown country for the suspect's address. This variable is missing if the victim did not include suspect details.

The following characteristics included in the report are also examined in the analysis:

- Report made to police: This variable is true if the victim made an independent report to police (e.g. by going to a police station) as well as their report on RCAP.
- Report includes evidence: True if the victim has indicated they have some form of evidence for their complaint (e.g., text records, bank statements). However, a victim is not able to attach any evidence to the initial report.
- Threat to life: True if a victim's description of the cybercrime indicates a threat to life. This is determined by whether the description includes any words in a word list that has been determined by the ACSC and police to indicate a threat to life.
- Money loss: True if victim reports money lost in cybercrime.
- Amount lost: The amount of money reportedly lost by the victim. The responding police may change this value if they find it to be inaccurate.

4 In RCAP, reports are characterised as either primary, secondary, for information, or not referred. Secondary and for information reports are duplicates of primary reports that can be sent to other jurisdictions. This may occur if a report concerns multiple jurisdictions. To avoid any overcounting we restrict our analysis to 'primary' and 'not referred' reports.

5 Not all offence categories allow the reporter to report suspect details, and some offence categories only allow the reporter to report certain suspect characteristics. However, the categories that do not accept suspect characteristics are categories where it is highly unlikely for the victim to know any suspect characteristics, such as, malware attacks and data loss.

- Date report closed: The date the report is closed on the RCAP system.
- Reason report closed: The reason the report has been closed. Most commonly this is either because the report has been referred to local police for further investigation (outside of RCAP), or that no further action is to be taken and the report is used for intelligence/ statistics.

We undertook descriptive analyses of this data to report on trends and characteristics of reported cybercrime. To identify factors correlated with a police referral of reported cybercrime, we estimated an ordinary least squares regression model.[6]

In this report, we consider cybercrime to encompass a wide range of criminal behaviours involving technology, networks, and computers to conduct sophisticated attacks on individuals, organisations or governments (O'Shea et al., 2022). For our analyses, we separate cybercrime into the following five offence categories (ACCC, 2021; ACSC, 2022; eSafety Commissioner, n.d.): [7]

- *Cyber-enabled fraud* refers to the use of online services or computers to commit fraud or to deceive victims into sending money or goods to someone online. It may be conducted in many different ways (for a full list see ACCC, 2021) including:
  - *Dating and romance scams* where scammers enter an online relationship with a victim to steal money from them;
  - *Investment scams* involve scammers offering different "investment opportunities" to victims, including cryptocurrencies, stocks, and superannuation typically resulting in victims losing much of their money; and
  - *Penalty scams* involve impersonating a government agency or trusted organisation to threaten a victim with a penalty (e.g., fine, arrest) if a victim does not pay immediately.
- *Identity theft* is when a cybercriminal gains access to personal information through means such as hacking, phishing, remote access scams, malware/ransomware, and fake online profiles. The stolen identities may then be used to steal money or gain other benefits.
- *Cyber-enabled abuse* is where someone is being bullied, threatened, harassed, or stalked online, with the intent to intimidate, scare, or harm them socially, psychologically, or even physically.
- *Online Image Abuse (OIA)* is where an intimate image or video is threatened to be shared or is shared without the consent of the person pictured. This includes images that are digitally altered. Image based abuse is sometimes called 'revenge porn', 'online image abuse' or 'sextortion'.
- *Device* refers to malware and ransomware attacks. Malware refers to the use of code or programs for malicious purposes (e.g., obtaining confidential information). They often come in the form of ransomware attacks where computers or files are blocked, or access is limited until a ransom is paid.

6 The regression allows us to estimate the independent impact of a characteristic on police referral, once controlling for all other characteristics in our model. For more information on ordinary least squares regression see Wooldridge (2015).

7 All these agencies have similar definitions of cyber-offences. We primarily use the ACSC's definitions, but the ACSC references both the ACCC and the eSafety commissioner in their definitions of cyber-enabled fraud and cyber abuse respectively.

RESULTS

Trends in cyber offences

Table 1 shows yearly incidents of cybercrime from July 2019 to June 2022. There were 39,494 reported incidents of cybercrime concerning victims residing in NSW over these three years. Of these incidents, 79% were for fraud and identity crime. Of the remaining reports, cyber abuse was the most common (14% of all reported cybercrime) followed by device (3%) and OIA (3%) offences.

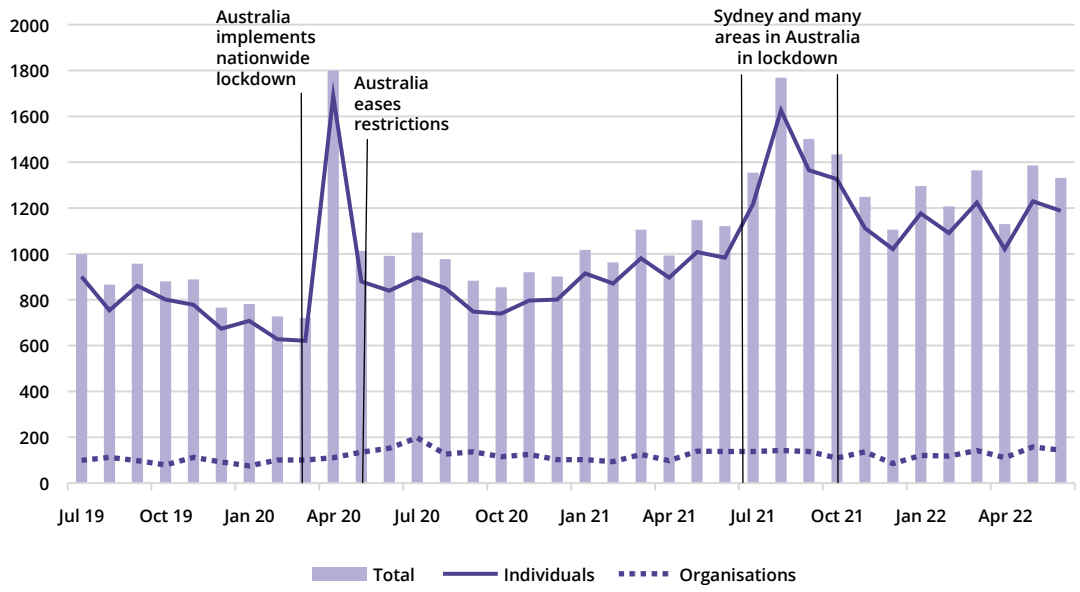
Reported cybercrime in NSW increased by 42% over the three years examined, from 11,389 reports between July 2019 and June 2020 to 16,130 reports between July 2021 and June 2022. The bulk of this increase occurred between July 2021 to June 2022. Fraud and identity crime contributed most to the upward trend. Over the three years these two categories accounted for 5,295 additional incidents of cybercrime. Fraud increased by 95% or 3,917 incidents and identity crime increased by 35% or 1,378 incidents. Device and OIA increased by similar proportions (up 117% or 329 incidents and 70% or 228 incidents respectively), however the volume of these offences was much lower than other categories. The only category of cybercrime which fell over the period examined was cyber abuse, which decreased by 41% or 1,111 incidents.

Table 1. Number of cybercrime incidents reported in NSW by year and offence type, July 2019 - June 2022

	Jul 19 - Jun 20		Jul 20 - Jun 21		Jul 21 - Jun 22		Total (N)		Change from year 1 to year 3	
	(N)	(%)	(N)	(%)	(N)	(%)	(N)	(%)	(N)	(%)
Cyber abuse	2,708	24%	1,258	11%	1,597	10%	5,563	14%	-1,111	-41%
Device	281	2%	415	3%	610	4%	1,306	3%	329	117%
Fraud	4,142	36%	5,611	47%	8,059	50%	17,812	45%	3,917	95%
Identity	3,934	35%	4,254	36%	5,312	33%	13,500	34%	1,378	35%
OIA	324	3%	437	4%	552	3%	1,313	3%	228	70%
Total	11,389		11,975		16,130		39,494		4,741	42%

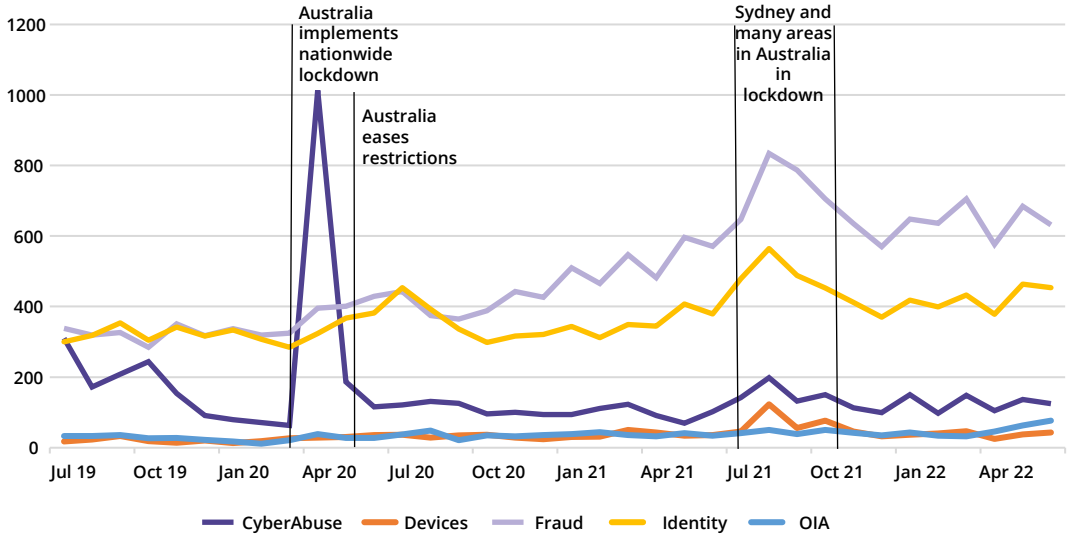
Figure 1 plots the total monthly number of reported cybercrime incidents in NSW and the number reported by individuals and organisations. Aside from a brief decline from late 2019 to early 2020, cybercrime has trended upward over the time series. The bulk of the reports and the increase was attributed to individuals. RCAP reports for organisations may however be less reliable as organisations may be reluctant to report if they are covered by insurance, and there are also more reporting options for organisations, including the option of reporting directly to the ACSC, instead of RCAP (ACSC, n.d.). Two notable peaks occurred for individuals, both coinciding with national and state COVID-related restrictions and lockdowns. During this period there was a greater reliance on online digital services for work, social and everyday life activities (Commonwealth of Australia, 2021; Deloitte, n.d.). As such, online activities reached unprecedented levels, creating more opportunities for cybercrime.

Figure 1. Monthly number of cybercrime incidents reported in NSW, July 2019 - June 2022



We further examine these trends by the type of offence. Figure 2 plots the monthly number of incidents by offence type over the same period. The first peak observed in April 2020 largely appears to be caused by an increase in cyber abuse which reached 1,013 incidents against the individual. According to the ACSC (2020), this peak relates to an Australia wide (non-Covid related) bulk extortion campaign (BEC) (a sub-category of cyber abuse). In this BEC, one or more adversaries emailed thousands of Australians threatening to release sensitive information to the recipient's friends and family unless a specified amount of money was paid in cryptocurrency. ACSC issued an alert on this campaign through their website (cyber.gov.au), the StaySmartOnline service, social media channels and the ReportCyber portal. The widespread alert may have increased awareness of the BEC contributing to increased reporting (ACSC, 2020). A second peak in cybercrime in NSW occurred in August 2021. This appears to be due to gradual increase in both fraud and identity crime. However, after December 2021, the volume of cybercrime returned to pre-lockdown levels with a slow incline observed thereafter.

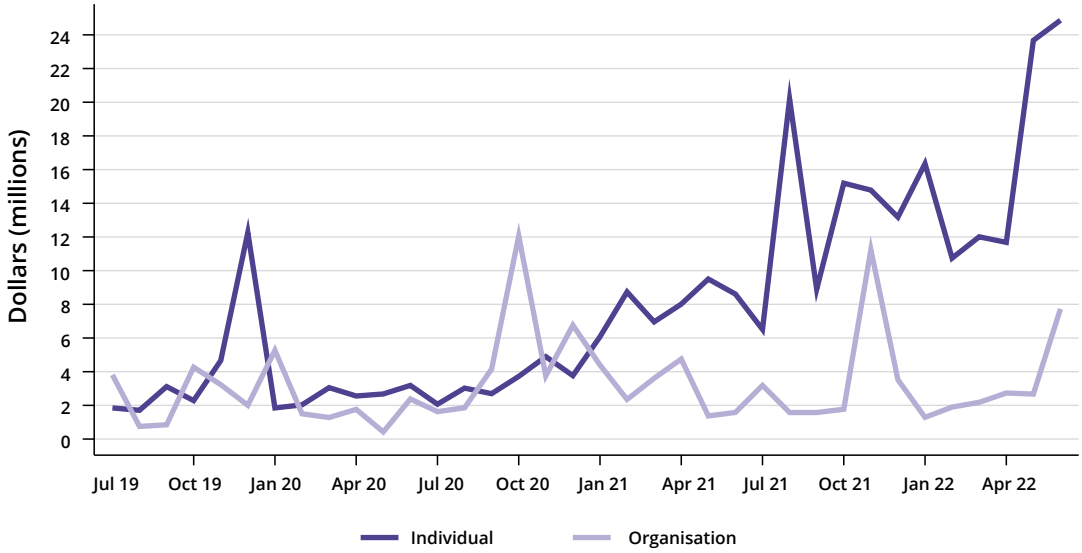
Figure 2. Monthly number of cybercrime incidents in NSW, by offence category, July 2019 - June 2022



Financial impact of cybercrime

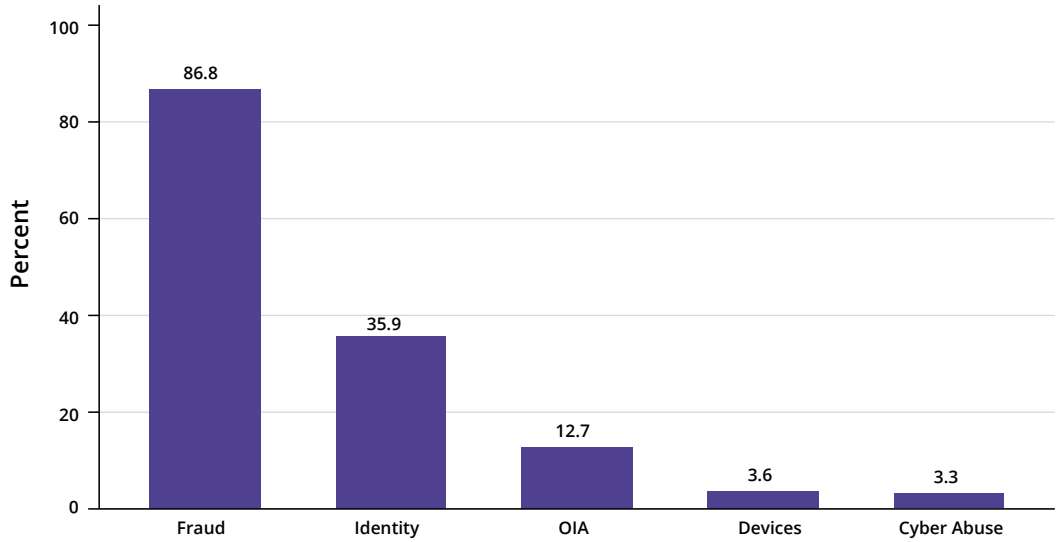
This section examines the reported financial impact of cybercrime. Figure 3 plots the monthly total amount of money lost to all cybercrime types, as reported in RCAP. The dark purple line plots this outcome for individuals while the light purple line plots the outcome for organisations. Figure 3 shows that cybercrime has a substantial and increasing financial impact on individuals over time. In June 2022, individuals reported losing $24,866,537 to cybercrime while organisations reported losing $7,732,204. The financial loss for individuals has been steadily increasing since July 2019, rising from $1,848,237 to $24,866.537. In contrast, aside from several peaks, the financial loss for organisations remained stable between 2019 and 2022. The cumulative reported amount lost was $287,379,904 for individuals and $117,215,656 for organisations between July 2019 and June 2020.

Figure 3. Monthly dollar amount lost by individuals and organisations from cybercrime in NSW, July 2019 - June 2022



Not all cybercrimes are equally susceptible to financial loss. Figure 4 presents the proportion of reports in each cybercrime category where it was indicated that the victim lost money. Unsurprisingly, the vast majority of fraud reports (86.8%) involved money loss, while 39.5% of identity theft reports involved money loss. A small minority of victims of cyber abuse (3.3%) and online image abuse (12.7%) reported losing money as a result of the crime. Finally, although some device offences have the potential for money loss (such as ransomware attacks), barely any (3.6%) device reports involved money loss.

Figure 4. Proportion of cybercrime reports where the victim has reported losing money, by offence category, NSW, July 2019-June 2022



Victims of cybercrime

Table 2 and Figure 5 (a and b) show the characteristics of victims of reported cybercrimes in NSW. Most of the victims who reported cybercrime were individuals (89%), male (53%) and over 25 years of age (87%). A small proportion of victims indicated that they had a special requirement or need (5%) or were of Aboriginal and or Torres Strait Islander descent (2%).

The gender and age profile of victims differed across offence categories. Figure 5(a) shows that most victims of fraud (54%), identity crime (54%) and OIA (58%) were men, while women made up the majority of victims of cyber abuse (55%) and device (53%) offences. Examining age, the highest proportion of reports for cyber abuse (25%), device (30%) and fraud (24%) offences were made by individuals aged 55 and over, while individuals aged 35 to 44 made up the largest proportion of victims of identity crime (26%). Individuals aged between 18 and 24 (37%) reported OIA more often than any other age group. Special requirements or needs information could be entered as a free text field in RCAP, with 5% of victims opting to complete this field. However, we could not reliably examine what type of needs these were.

Table 2. Characteristics of victims of cybercrime in NSW, by offence category, July 2019 - June 2022

	Cyber Abuse		Device		Fraud		Identity		OIA		Total	
Victim type												
Individual	5,177	93%	1,005	77%	15,651	88%	12,078	89%	1,298	99%	35,209	89%
Organisation	386	7%	301	23%	2,161	12%	1,422	11%	15	1%	4,285	11%
Total	5,563	100%	1,306	100%	17,812	100%	13,500	100%	1,313	100%	39,494	100%
Age												
0 - 17	121	3%	11	1%	211	1%	77	1%	80	7%	500	1%
18 - 24	495	10%	61	7%	1,828	12%	1,020	9%	441	37%	3,845	11%
25 - 34	1,000	21%	173	19%	3,525	23%	2,896	25%	355	30%	7,949	24%
35 - 44	1,082	22%	234	25%	3,381	22%	3,078	26%	151	13%	7,926	23%
45-54	914	19%	173	19%	2,501	17%	2,143	18%	83	7%	5,814	17%
55+	1,212	25%	282	30%	3,611	24%	2,538	22%	74	6%	7,717	23%
Total	4,824	100%	934	100%	15,057	100%	11,752	100%	1,184	100%	33,751	100%
Gender												
Female	2,666	55%	493	53%	6,905	46%	5,378	46%	493	42%	15,935	47%
Male	2,141	44%	439	47%	8,164	54%	6,381	54%	693	58%	17,818	53%
Other	33	1%	6	1%	37	0%	27	0%	1	0%	104	0%
Total	4,840	100%	938	100%	15,106	100%	11,786	100%	1,187	100%	33,857	100%
Aboriginal and/or Torres Strait Islander												
No	5,057	98%	982	98%	15,323	98%	11,810	98%	1,253	97%	34,425	98%
Yes	120	2%	23	2%	328	2%	268	2%	45	3%	784	2%
Total	5,177	100%	1,005	100%	15,651	100%	12,078	100%	1,298	100%	35,209	100%
Special requirements/ needs												
No	5,201	93%	1,205	92%	16,905	95%	12,935	96%	1,178	90%	37,424	95%
Yes	362	7%	101	8%	907	5%	565	4%	135	10%	2,070	5%
Total	5,563	100%	1,306	100%	17,812	100%	13,500	100%	1,313	100%	39,494	100%

Figure 5. Gender and age of cybercrime victims in NSW, by offence category, July 2019 - June 2022

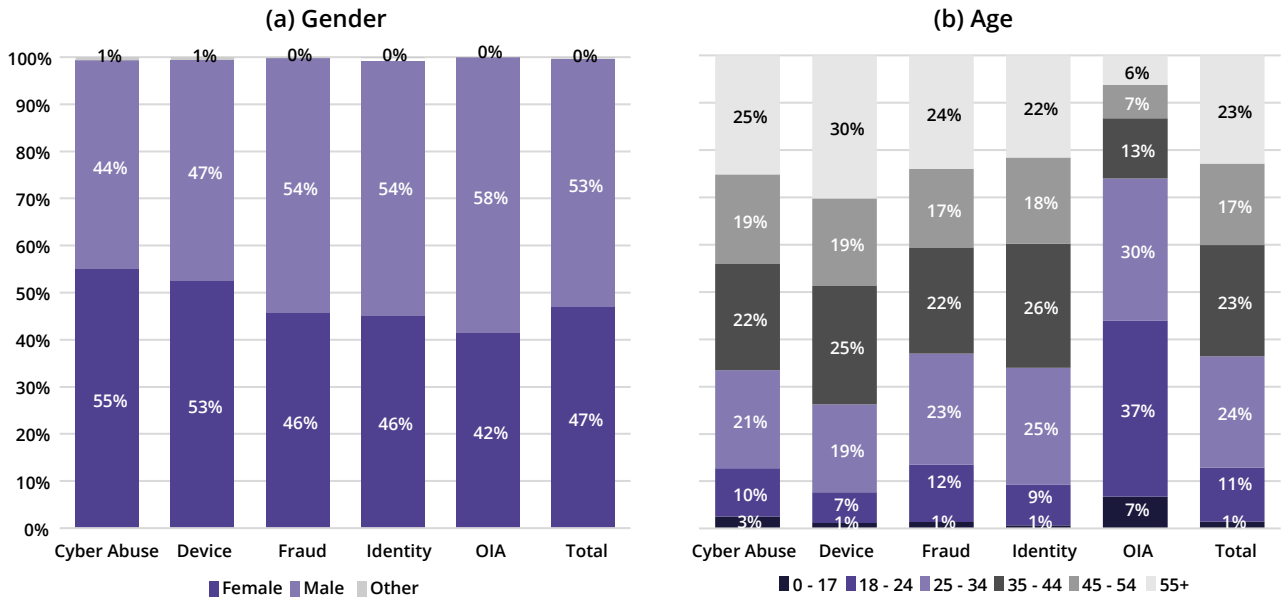


Table 3 presents further characteristics of the incident from the cybercrime report. It shows that less than one fifth (21%) of incidents were reported to police at a police station as well as being reported on RCAP. The proportion of incidents reported to police ranged from 28% for both identity crime and OIA to 12% for both cyber abuse and device offences. In most reports (94%) the victim indicated that they had evidence of the incident (although this could not be uploaded when entering the report). While cyber offences are typically non-violent, a small portion of reports (4%) included language in the incident narrative[8] which might indicate a threat to the victim's life. Unsurprisingly, such language was more frequently used in narratives within cyber abuse (13%) and OIA (12%) reports.

Table 3. Report characteristics of cybercrime in NSW, by offence category, July 2019 - June 2022

	Cyber Abuse		Device		Fraud		Identity		OIA		Total	
Report also made to police												
No	4,880	88%	1,154	88%	14,627	82%	9,694	72%	948	72%	31,303	79%
Yes	683	12%	152	12%	3,185	18%	3,806	28%	365	28%	8,191	21%
Total	5,563	100%	1,306	100%	17,812	100%	13,500	100%	1,313	100%	39,494	100%
Reporter has evidence												
No	213	4%	97	8%	435	3%	1,403	11%	80	6%	2,228	6%
Yes	4,540	96%	1,102	92%	15,760	97%	11,952	89%	1,233	94%	34,587	94%
Total	4,753	100%	1,199	100%	16,195	100%	13,355	100%	1,313	100%	36,815	100%
Threat to life												
No	4,864	87%	1,247	95%	17,411	98%	13,288	98%	1,149	88%	37,959	96%
Yes	699	13%	59	5%	401	2%	212	2%	164	12%	1,535	4%
Total	5,563	100%	1,306	100%	17,812	100%	13,500	100%	1,313	100%	39,494	100%

Table 4 examines suspect characteristics. The vast majority of victims of cybercrime in NSW did not know their offender, and therefore few reports included any details regarding the perpetrator (28%). Suspect details were more commonly included in reports of fraud (48%), OIA (40%) and cyber abuse (22%). In 11% of cyber abuse and 7% of OIA reports, which included suspect details, the victim reported that they knew the suspect personally. Of reports which included suspect details, 18% involved an international suspect. This varied from 1% of identity crime reports to 41% of OIA reports. The perpetrator's country of origin was not known in just over a fifth (22%) of reports where suspect details were recorded.

8 The incident narrative is a free text field which allows respondents to describe the incident.

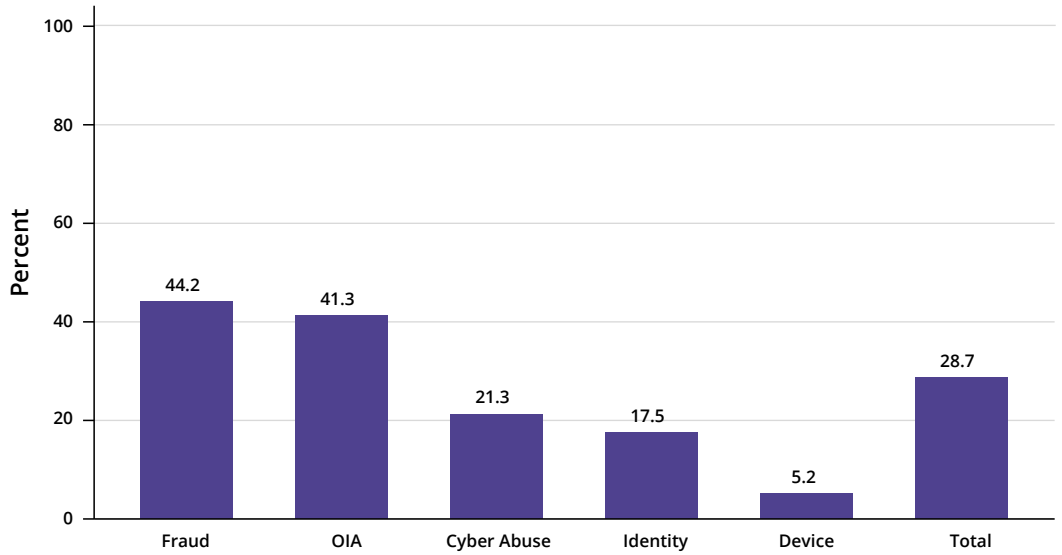
Table 4. Suspect characteristics for cybercrime incidents in NSW, by offence category, July 2019 - June 2022

	Cyber Abuse		Device		Fraud		Identity		OIA		Total	
Report includes suspect details												
No	4,324	78%	1,302	100%	9,188	52%	12,920	96%	789	60%	28,523	72%
Yes	1,239	22%	4	0%	8,624	48%	580	4%	524	40%	10,971	28%
Total	5,563	100%	1,306	100%	17,812	100%	13,500	100%	1,313	100%	39,494	100%
Suspect personally known to victim												
No	1,104	89%	4	100%	8,624	100%	580	100%	486	93%	10,798	98%
Yes	135	11%	0	0%	0	0%	0	0%	38	7%	173	2%
Total	1,239	100%	4	100%	8,624	100%	580	100%	524	100%	10,971	100%
International suspect												
No	1,054	85%	3	75%	7,031	82%	576	99%	311	59%	8,975	82%
Yes	185	15%	1	25%	1,593	18%	4	1%	213	41%	1,996	18%
Total	1,239	100%	4	100%	8,624	100%	580	100%	524	100%	10,971	100%
Suspect country unknown												
No	945	76%	2	50%	6,682	77%	553	95%	385	73%	8,567	78%
Yes	294	24%	2	50%	1,942	23%	27	5%	139	27%	2,404	22%
Total	1,239	100%	4	100%	8,624	100%	580	100%	524	100%	10,971	100%

Police response

One of RCAP's main functions is to triage reports to the relevant police jurisdiction.[9] Police agencies can then decide whether to refer reports to relevant officers for further investigation and prosecution. We consider that a police referral occurred when a report is closed on RCAP on the grounds of being referred to local police to investigate.

Figure 6. Proportion of closed cybercrime reports referred to local police[10] for further investigation, NSW, July 2019 - June 2022



9 RCAP can triage reports to all police agencies in Australia including state police (such as NSW police, Victoria police, and Queensland police), and the Australian Federal Police.

10 Although our sample is restricted to victims that reside in New South Wales, the investigating police agency is usually where the suspect resides. This means that reports could be referred to any police agency.

Figure 6 examines the proportion of closed reports that were referred to police for further investigation. Less than half of all reports to RCAP resulted in a referral to police. The most likely crime type to be referred was fraud (44.2% of reports referred to police), closely followed by online image abuse (41.3%). Only 21.3% of cyber abuse reports were referred to police. Reports regarding identity crime or device offences were unlikely to be referred to police with just 17.5% and 5.2% of reports referred, respectively. In total, 28.7% of all cases closed on RCAP were referred to local police.

Table 5 examines statistics regarding time to police referral and the number of jurisdictions that were allocated the report. Reports of OIA and cyber abuse are reported to police the quickest, with half of all reports from both categories being referred to the police within a day of the victim reporting on RCAP. The majority of OIA reports (84%) and cyber abuse reports (80%) were referred to police within 7 days. Other cybercrime types take longer to be referred. The median time for referral for device, fraud and identity reports is 8, 9 and 18 days, respectively. Less than half of the reports for device (47%), fraud (48%) and identity (42%) offences were referred to police within 7 days. However, as shown in the 90th percentile row in Table 5, some reports can take substantially longer to be referred to police. For example, 10% of fraud cases take more than 171 days to be referred. Nine in 10 cybercrime reports were referred to just one jurisdiction. The crime category with the greatest cross-jurisdictional involvement was fraud, where 15% of reports were assigned to more than one jurisdiction.

Table 5. Time to case closure and number of jurisdictions involved for police referred reports of cybercrime, NSW, July 2019 - June 2022

	Cyber abuse	Device	Fraud	Identity	OIA	Total
N referred	1,118	60	5,099	1,999	541	8,817
Median days to referral	1	8	9	18	1	6
90th percentile of days to referral	48	130	171	160	32	151
Referred within 7 days (%)	80%	47%	48%	42%	84%	53%
Mean number of jurisdictions	1.03	1	1.16	1.05	1.01	1.11
More than one jurisdiction (%)	3%	0%	15%	5%	1%	10%

Note: a small number of closed dates are missing, impacting the first four measures. The sample size for these measures is 1,077 (cyber abuse), 57 (device), 4,994 (fraud), 1,953 (identity), and 535 (OIA).

Table 6 examines the factors associated with a cybercrime report being referred to police. We run separate regression models for individuals and organisations. The table shows the output from both models. Each coefficient, when multiplied by 100, indicates the percentage point change in the likelihood of police referral associated with that factor. Stars next to coefficients indicate that this change is statistically significant.

We find that for individuals:

- a report by a **victim aged under 18 is 28 percentage points (p.p.) more likely** to be referred to police than a report by a victim aged 55 or above;
- **a report with information about the suspect** who committed the offence **is 19.8 p.p. more likely** to referred to police;
- **a report indicating money loss is 8.4 p.p. more likely** to be reported to police;
- **a report of OIA is 15.7 p.p. more likely** to be referred to police compared to cyber abuse reports (the base category). All other offence categories are less likely to be referred to police than cyber abuse reports;

Table 6. Factors associated with a cybercrime report being referred to police, NSW, July 2019 - June 2022

	(1) Individuals Police Referral	(2) Organisations Police Referral
Age		
0 - 17	0.280***	
	(0.0179)	
18 - 24	-0.0146	
	(0.00802)	
25 - 34	0.0114	
	(0.00641)	
35 - 44	0.00409	
	(0.00638)	
45 - 54	0.0106	
	(0.00694)	
Gender		
Female	-0.00583	
	(0.00435)	
Other	0.000814	
	(0.0397)	
Aboriginal	-0.0189	
	(0.0143)	
Has suspect	0.198***	0.154***
	(0.00994)	(0.0249)
Has evidence	-0.0783***	-0.102*
	(0.00898)	(0.0425)
Offence category		
Device	-0.123***	-0.132***
	(0.0145)	(0.0351)
Fraud	-0.119***	-0.0183
	(0.00859)	(0.0291)
Identity	-0.0846***	-0.0748**
	(0.00738)	(0.0267)
OIA	0.157***	0.200
	(0.0130)	(0.112)
Suspect country		
International	0.0279*	-0.141**
	(0.0108)	(0.0529)
Unknown	-0.0125	0.100***
	(0.0107)	(0.0280)
Money loss	0.0836***	0.230***
	(0.00581)	(0.0176)
No investigation	-0.107***	-0.124***
	(0.00662)	(0.0229)
Constant	0.277***	0.200***
	(0.0157)	(0.0550)
R squared	0.10	0.13
Observations	31,531	3,826

Note: Standard errors in parentheses. * p<0.05 ** p<0.01 *** p<0.001

- **a report involving international suspects is slightly more likely (2.8 p.p.)** to be referred to police than a report involving Australian suspects;
- **a report with evidence is 7.8 p.p. less likely** to be referred to police, which is likely a reflection of the very high proportion of reports claiming to have evidence (94%, see table 3);
- a report **that requests no further investigation is 10.7 p.p. less likely** to be referred to police.[11]

Similar factors are associated with police referrals for reports of cybercrime directed at organisations as was found for individuals. The exceptions are money loss and the involvement of suspects not residing in Australia. Money loss is associated with a 23 p.p. increase in the likelihood of a police referral for organisations compared to 8.4 p.p. for individuals. For organisations, reports involving international suspects were 14.1 p.p. less likely to be referred to police, compared to a 2.8 p.p. increase for individuals.

DISCUSSION

This brief presents the first overview of cybercrime in NSW. We measured cybercrime by examining reports to RCAP, a national cybercrime reporting system operated by the Australian Cyber Security Centre. Over the three years to June 2022, there were 39,494 reports of cybercrime with the victim residing in NSW, and more than $404 million reported lost. We found that cybercrime reports increased rapidly (by 42%) over the same period, particularly for crimes against individuals. Reports in every cybercrime category except cyber abuse increased over our sample period, with device offences demonstrating the largest increase of 117%, followed by cyber-enabled fraud at 95%. This has spurred a corresponding increase in reported cybercrime-related financial losses by individuals, which grew exponentially in the three years to June 2022 but remained stable for organisations. Cyber-enabled fraud and identity crime made up most cybercrime reports and comprised the vast majority of reports where money was reportedly lost.

The profile of cybercrime victims differed by the type of offence. While fraud and identity crime victims were often older and male, device and cyber abuse victims were more often older and female. In fact, the largest proportion of victims of cyber abuse, device, and fraud offences were aged 55 or over. Yet, most victims of online image abuse (OIA) were young (37% between 18 and 24) and male (58%). Most victims of cybercrime (72%) did not know who the suspected perpetrator was, and of those who did, 18% reported that the suspect resided outside of Australia and 22% of those that had a suspect, reported that the suspect resided in a country that was unknown to the victim.

Regarding the police response, the majority (71%) of reports were closed by police in RCAP with no further investigation undertaken. Fraud and OIA were the most likely offence categories to be referred to police for further investigation (at above 40%). Device offences were the least likely to be referred to police at 5%. Reports were more likely to be referred to police when the incident involved a victim aged 17 years or younger, the suspect was known to the victim, money was lost, or an OIA offence was indicated. Most OIA reports (84%) were referred to police within 7 days compared to just 42% of identity crime reports. In the vast majority of cases, victims do not know any details about the offender and many of those who do, report that the suspected perpetrator resides overseas. This makes it near impossible for local and federal police agencies to prosecute offenders and undermines the deterrent value of any criminal sanctions prescribed for these offences.

Our results show that cybercrime in NSW largely follows the same increasing trend that has been observed in national cybercrime studies (ACCC, 2022; ACSC, 2022; eSafety Commissioner, 2022). The especially large increase in device offences (117% from 2019 to 2022) is consistent with Martin and Whelan's (2022) observation that ransomware attackers are becoming much more specialised and

11 However, some reports are still referred to police even if they indicate they want no further investigation.

sophisticated. Similarly, the 95% increase in cyber enabled fraud found in our study may reflect the proliferation of new types of mobile phone scams (such as the "hi mum" scam (McElroy, 2022)) that can target large segments of the Australian population at little cost to the cybercriminal. Like Kemp et al. (2021), we also find significant increases in cybercrime reports during the periods that NSW was in lockdown and most people were relying on the internet to undertake work, household and social activities (Commonwealth of Australia, 2021; Deloitte, n.d.).

The statistics we report here only offer a partial view of reported cybercrime in NSW. This is because our study does not capture cybercrime that is reported directly to NSW police (unless a report was also made through RCAP). In particular, we were unable to capture cyber abuse or OIA incidents where the suspect was a partner or an ex-partner, as RCAP requires victims of these types of crime to report the abuse directly to the local police. Our data also does not capture reports of cybercrime that were made to other national reporting systems. Currently, in addition to RCAP, cyber fraud can be reported to Scamwatch, cyber abuse may be reported to the eSafety Commissioner, online child abuse to the Australian Centre to Counter Child Exploitation, and data breaches to the Office of the Australian Information Commissioner. Organisations also have the option of reporting directly to the ACSC, instead of RCAP (ACSC, n.d.). Integration of these different national reporting systems or greater sharing of information between agencies hosting these platforms would allow a more comprehensive picture of cybercrime to be produced. A consolidated approach to national reporting platforms may also help reduce confusion of victims and potentially enable agencies to better serve victims' needs.

Perhaps a more important limitation of the analysis presented in this paper is that many incidents of cybercrime are not reported to officials. Therefore, we do not know the extent to which the trends and patterns observed in cybercrime reports accurately reflect the incidence of these criminal behaviours. Organisations may be reluctant to report if they are covered by insurance, and if the cybercrime may cause reputational damage. For individuals, underreporting of cybercrime is partly due to embarrassment, including as a result of community members often blaming victims for not taking enough precautions to protect themselves from many types of cybercrime (Anonymous, 2023; Cross et al., 2021). Regular public reporting of cybercrime statistics, drawing attention to the high volume of victims and breadth of offences, may assist with dispelling some of these negative stereotypes and help to boost reporting rates. Promoting greater awareness of RCAP among the general population, including highlighting the fact that RCAP is the only platform that refers reports directly to police, could further encourage cybercrime reporting. However, dissatisfaction with the police response to cybercrime might also be a contributor to underreporting (Cross et al., 2021). Ensuring that reports of cybercrime made to RCAP or other national reporting platforms are referred to police in a timely manner could encourage more reporting. While we found that 53% of reports were referred to police within 7 days, one in ten reports took longer than 151 days to be referred. Long delays in action being taken could discourage victims from reporting other cyber offences in the future.

There are clear benefits in ongoing public reporting of cybercrime trends both at the national level and separately for individual states and territories. In addition to promoting victim awareness of the importance, and best method, of reporting, regular publishing of cybercrime statistics would draw attention to this emerging crime area and assist policy makers to develop strategies, policies and programs to respond to it. Integrated national reporting systems will be a critical step in achieving this. However, there are also enhancements that could be made to police recorded crime data systems to improve our ability to monitor trends in cybercrime at the state level. For example, currently in NSW the crime category stalking and intimidation includes both cyber abuse and in-person intimidation (Ramsey et al., 2022) but we are unable to determine how much each of these sub-categories contribute to the total volume of incidents. NSW Police could address this data gap by recording whether crimes that are reported to them are cyber-enabled.[12]

12 i.e. whether it is a traditional crime that is facilitated by technology.

ACKNOWLEDGEMENTS

We would like to thank the Australian Cyber Security Centre for sharing their data with us, and especially Sarah Yap for assisting in the drafting of the MOU, and the approvals process. We thank Therese Honess from NSW Police for taking the time to answer our questions about RCAP and the police referral process. We thank Annaliese Stuart for her literature search of relevant papers and preliminary data work. We thank Suzanne Poynton and Sara Rahman for their helpful feedback on numerous drafts of this report, Adam Teperski for proofreading this report, and Florence Sin for desktop publishing this report.

REFERENCES

Anonymous. (2023). I believed the SMS was from my bank – and fell victim to a $22,000 scam. *The Guardian.* https://www.theguardian.com/commentisfree/2023/jan/24/i-believed-the-sms-was-from-my-bank-and-fell-victim-to-a-22000-scam

Australian Bureau of Statistics. (2017). *Personal Safety, Australia.* ABS. Retrieved 11 Jan. 2023 from https://www.abs.gov.au/statistics/people/crime-and-justice/personal-safety-australia/2016

Australian Bureau of Statistics. (2022a). *Crime Victimisation, Australia*. ABS. Retrieved 6 Dec. 2022 from https://www.abs.gov.au/statistics/people/crime-and-justice/crime-victimisation-australia/2020-21

Australian Bureau of Statistics. (2022b). *Personal Fraud*. ABS. Retrieved 11 Jan. 2023 from https://www.abs.gov.au/statistics/people/crime-and-justice/personal-fraud/2020-21

Australian Competition and Consumer Commission. (2021). *The Little Black Book of Scams*. https://www.accc.gov.au/system/files/Little%20Black%20Book%20of%20Scams%202021.pdf

Australian Competition and Consumer Commission. (2022). *Targeting scams: Report of the ACCC on scams activity 2021*. https://www.scamwatch.gov.au/system/files/Targeting%20scams%20-%20report%20of%20the%20ACCC%20on%20scams%20activity%202021.pdf

Australian Cyber Security Centre. (2020). *Annual Cyber Threat Report—July 2019 to June 2020*. https://www.cyber.gov.au/sites/default/files/2020-09/ACSC-Annual-Cyber-Threat-Report-2019-20.pdf

Australian Cyber Security Centre. (2022). *Annual Cyber Threat Report*. https://www.cyber.gov.au/sites/default/files/2022-11/ACSC-Annual-Cyber-Threat-Report-2022.pdf

Australian Cyber Security Centre. (n.d.). *ReportCyber: Report a cybercrime, incident or vulnerability.* Retrieved 25 Jan. 2023 from https://www.cyber.gov.au/acsc/report

Commonwealth of Australia. (2021). COVID-19, *criminal activity and law enforcement*. Retrieved from https://parlinfo.aph.gov.au/parlInfo/download/committees/reportjnt/024564/toc_pdf/COVID-19,criminalactivityandlawenforcement.pdf;fileType=application%2Fpdf

Cross, C., Holt, T., Powell, A., & Wilson, M. (2021). *Responding to cybercrime: Results of a comparison between community members and police personnel.* (Trends and issues in crime and criminal justice no. 635). Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2021-08/ti635_responding_to_cybercrime.pdf

Deloitte. (n.d.). *Cyber crime – the risks of working from home*. Retrieved 25 Jan. 2023 from https://www2.deloitte.com/ch/en/pages/risk/articles/covid-19-cyber-crime-working-from-home.html

eSafety Commissioner. (2022). *Young men bear the brunt of sexual extortion as reports rise.* https://www.esafety.gov.au/newsroom/media-releases/young-men-bear-brunt-sexual-extortion-reports-rise

eSafety Commissioner. (n.d.). *Key issues.* Retrieved 28 Nov. 2022 from https://www.esafety.gov.au/key-issues

How, B. (2022). New $89 million cybercrime centre to be based in NSW. *InnovationAus.com.* https://www.innovationaus.com/new-89-million-cybercrime-centre-to-be-based-in-nsw/

Kemp, S., Buil-Gil, D., Moneva, A., Miró-Llinares, F., & Díaz-Castaño, N. (2021). Empty Streets, Busy Internet: A Time-Series Analysis of Cybercrime and Fraud Trends During COVID-19. *Journal of Contemporary Criminal Justice, 37*(4), 480-501. https://doi.org/10.1177/10439862211027986

Levi, M., & Smith, R. G. (2021). Fraud and pandemics. *Journal of Financial Crime, 29*(2), 413-432. https://doi.org/10.1108/jfc-06-2021-0137

Martin, J., & Whelan, C. (2022). Why are there so many data breaches? A growing industry of criminals is brokering in stolen data. *The Conversation*. https://theconversation.com/why-are-there-so-many-data-breaches-a-growing-industry-of-criminals-is-brokering-in-stolen-data-193015

McElroy, N. (2022). Australians have lost at least $7.2 million to the 'Hi Mum' scam. How does it work and why is it so lucrative for cybercriminals? *ABC news*. https://www.abc.net.au/news/2022-12-12/inside-the-hi-mum-text-scam-how-it-works-whos-behind-it/101726762

O'Shea, B., Asquith, N. L., & Prichard, J. (2022). Mapping Cyber-Enabled Crime: Understanding Police Investigations and Prosecutions of Cyberstalking. *International Journal for Crime, Justice and Social Democracy, 11*(4), 25-39.

Ramsey, S., Kim, M.-T., & Fitzgerald, J. (2022). *Trends in domestic violence-related stalking and intimidation offences in the criminal justice system: 2012 to 2021* (Bureau Brief No. 159). NSW Bureau of Crime Statistics and Research. https://www.bocsar.nsw.gov.au/Publications/BB/BB159-2022-Report-DV-related-stalking.pdf

Saleem, S., Khan, N. F., Zafar, S., & Raza, N. (2022). Systematic literature reviews in cyberbullying/cyber harassment: A tertiary study. *Technology in Society, 70.* https://doi.org/https://doi.org/10.1016/j.techsoc.2022.102055

Vakhitova, Z. I., Alston-Knox, C. L., Reeves, E., & Mawby, R. I. (2021). Explaining victim impact from cyber abuse: An exploratory mixed methods analysis. *Deviant Behavior, 43*(10), 1153-1172. https://doi.org/https://doi.org/10.1080/01639625.2021.1921558

Voce, I., & Morgan, A. (2021). *Ransomware victimisation among Australian computer users* (Statistical Bulletin No. 35). Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2021-10/sb35_ransomware_victimisation_among_australian_computer_users.pdf

Wall, D. (2022). Cybercrime and the Transformation of Criminology in the 2020s: Ransomware evolutions. 2022 ANZSOC Conference: Transforming Criminology for the 2020s and Beyond, Darwin.

Wolbers, H., Boxall, H., Long, C., & Gunnoo, A. (2022). *Sexual harassment, aggression and violence victimisation among mobile dating app and website users in Australia* (Research Report No. 25). Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2022-10/rr25_sexual_harassment_aggression_and_violence_victimisation.pdf

Wooldridge, J. M. (2015). *Introductory econometrics: A modern approach*. Cengage learning.

NSW BUREAU OF CRIME STATISTICS AND RESEARCH - 6 PARRAMATTA SQUARE, 10 DARCY STREET, PARRAMATTA NSW 2150
bcsr@justice.nsw.gov.au • www.bocsar.nsw.gov.au • Ph: (02) 8688 9800 • ISBN 978-1-922576-35-4