Australian Government
Australian Institute of Criminology

Statistical Bulletin 38

March 2022

Abstract | This study examines the help-seeking behaviour of 321 Australian ransomware victims who participated in a national survey of computer users in June 2021.

Nearly three-quarters of ransomware victims sought help, advice or support from at least one person or organisation, and nearly 60 percent sought help from at least one formal source (ie they told someone other than a family or friend).

Nineteen percent of victims sought help, advice or support from the police or the Australian Cyber Security Centre (ACSC). The main reasons for not seeking help were that victims felt they could deal with the ransomware attack themselves, they did not think there was anything the police or ACSC could do, they did not regard the incident as a serious offence or they did not know that reporting to the police or ACSC was an option.

The results confirm that official reports of ransomware significantly underestimate the levels experienced in the community. They also highlight the importance of consistent and accurate messaging about sources of advice and support.

Serious & Organised Crime
Research Laboratory

Help-seeking among Australian ransomware victims

Isabella Voce and Anthony Morgan

Ransomware is malicious software (also known as malware) used to deny a person or organisation access to their IT systems and devices and/or to threaten the release of private data unless a ransom is paid (Australian Cyber Security Centre (ACSC) 2020b). ReportCyber is a national online tool run by the Australian Cyber Security Centre which receives cybercrime reports from members of the public, provides information to Australian law enforcement agencies and provides crime prevention advice to the public. The ACSC has observed an increase in the number of ransomware incidents against Australian organisations in recent years (ACSC 2020b) and states that ransomware has become one of the most significant threats facing Australia given the potential impact on the operations of businesses and governments (ACSC 2020a).

It is likely that ransomware reports to law enforcement, such as the police or ACSC, underestimate the true prevalence of victimisation in the community. Law enforcement data is limited to offences reported to or detected by police, and cybercrime activity in general is often difficult to detect even by victims (Cobb 2015). Businesses can be reluctant to divulge information on cyber attacks, partly due to fear of reputational damage and possible legal proceedings (Pereira 2016), while individuals may also be reluctant to report due to shame and embarrassment, confusion about which agency to contact, and uncertainty about whether they have actually been the victim of a crime (Morgan et al. 2016). Cybercrimes, including crimes targeting computer systems, are among those least reported to police (van de Weijer, Leukfeldt & Bernasco 2019). The seriousness of the incident, and perceptions of police, are also important factors in whether a victim will report a cybercrime incident to law enforcement (Graham, Kulig & Cullen 2020; van de Weijer, Leukfeldt & Van der Zee 2020).

Ransomware victimisation in the Australian community was recently examined in the Australian Cybercrime Survey (Voce & Morgan 2021). This was a large-scale survey of 15,000 members of the public which provides information on the prevalence of and trends in ransomware victimisation, independent of victim reporting behaviour and police recording practices. Nearly five percent of respondents had ever experienced ransomware, and two percent had experienced it in the past year. Small to medium business owners were twice as likely as other respondents to have been the victim of a ransomware attack in the past year and were more likely to have paid the ransom. In line with advice given by the ACSC (2020b), most respondents did not pay the ransom.

The advice given to ransomware victims was consistently identified as the most common reason for a respondent's decision about whether or not to pay the ransom, particularly in the case of small to medium business owners. This highlights the crucial role of the advice provided to ransomware victims in shaping their behaviour and underscores the need to understand where victims go for help, advice and support.

The current study aimed to measure the help-seeking behaviour of ransomware victims among a sample of adult Australian computer users in the Australian Cybercrime Survey (Voce & Morgan 2021). This paper examines the informal and formal sources of advice and support, the reasons for seeking help, and the satisfaction with the help provided. A focus of this paper is the prevalence, experience and outcome of reporting to law enforcement, including directly to police or to the ACSC.

Method

A large-scale survey of 15,000 members of the public was conducted in June 2021 (Voce & Morgan 2021). The survey was conducted in partnership with JWS Research. An invitation to complete the survey was sent out to 171,537 individuals who were members of the data collection agency Online Research Unit, with a total completion rate of nine percent (which is consistent with online panels generally; see Pennay et al. 2018). Importantly, not all recipients of an invitation will read it or access the survey—77 percent of respondents who accessed the survey and read the information sheet went on to complete the survey. The survey took an average of approximately 17 minutes to complete. The survey measured a range of experiences related to cybercrime victimisation, help-seeking behaviour, risk factors for victimisation and harms resulting from victimisation. A range of sociodemographic information was also collected.

To ensure the final sample was representative of the spread of the Australian adult population, post-stratification weights based on jurisdiction, age and gender were applied to male and female respondents using Australian demographic data from December 2020 (Australian Bureau of Statistics 2021). Weights were not applied to non-binary respondents (*n*=47), for whom population-level data are not available, or to respondents who did not provide their gender (*n*=19), who accounted for less than 0.5 percent of all respondents. Of the 15,000 respondents, six respondents were removed from the sample for providing illogical responses to sets of questions which implied they were answering the survey randomly, resulting in a final survey sample of 14,994 respondents.

Respondents were identified as ransomware victims if they had received instructions on their device for paying a ransom. In the last 12 months, 321 respondents (2.1%) had been the victim of ransomware. Victims of other forms of malware were identified if they had experienced any of the following issues or incidents:

- pop-up ads started appearing everywhere;
- people they knew told them they had been sending them suspicious messages and links over social media or email;
- their device was working excessively while no programs were running;
- their device slowed down and acted strangely;
- their browser kept getting redirected when they tried to search for a familiar site;
- their devices kept crashing for some reason;
- their programs were opening and closing automatically;
- their files had gone missing or been replaced with odd file extensions and the icons for the files were blank;
- there was a lack of storage space that they could not explain; and
- previously accessible system tools (such as personalised or security settings) were disabled.

While ransomware victimisation was determined based on whether respondents had received a ransom demand, some of these other symptoms of malware may be a feature of ransomware. For all these incidents, respondents were asked whether they had ever been a victim and, if so, whether it had occurred within the last year. Respondents who had experienced ransomware in the 12 months prior to the survey were asked whether they had sought help, advice or support from a range of sources, their satisfaction with the help received and, for respondents who sought help from police or the ACSC, their reasons for seeking help and their satisfaction with the outcome. Ransomware victims who did not seek help were asked their reasons for not seeking help.

The limitations of the methodology used in this study are outlined in Voce and Morgan (2021). There are advantages to using online panels as they allow for the rapid collection of data from large samples, but there are limitations in relation to generalising results from a non-probability sample to the general population. There are also limitations specific to the measurement of help-seeking in the survey. First, respondents were asked about sources of help, advice and support for incidents of malware they had experienced in the previous 12 months. While we report on help-seeking among ransomware victims, we cannot be certain which sources of help were sought for ransomware versus other types of malware they had experienced (where they experienced multiple incidents,

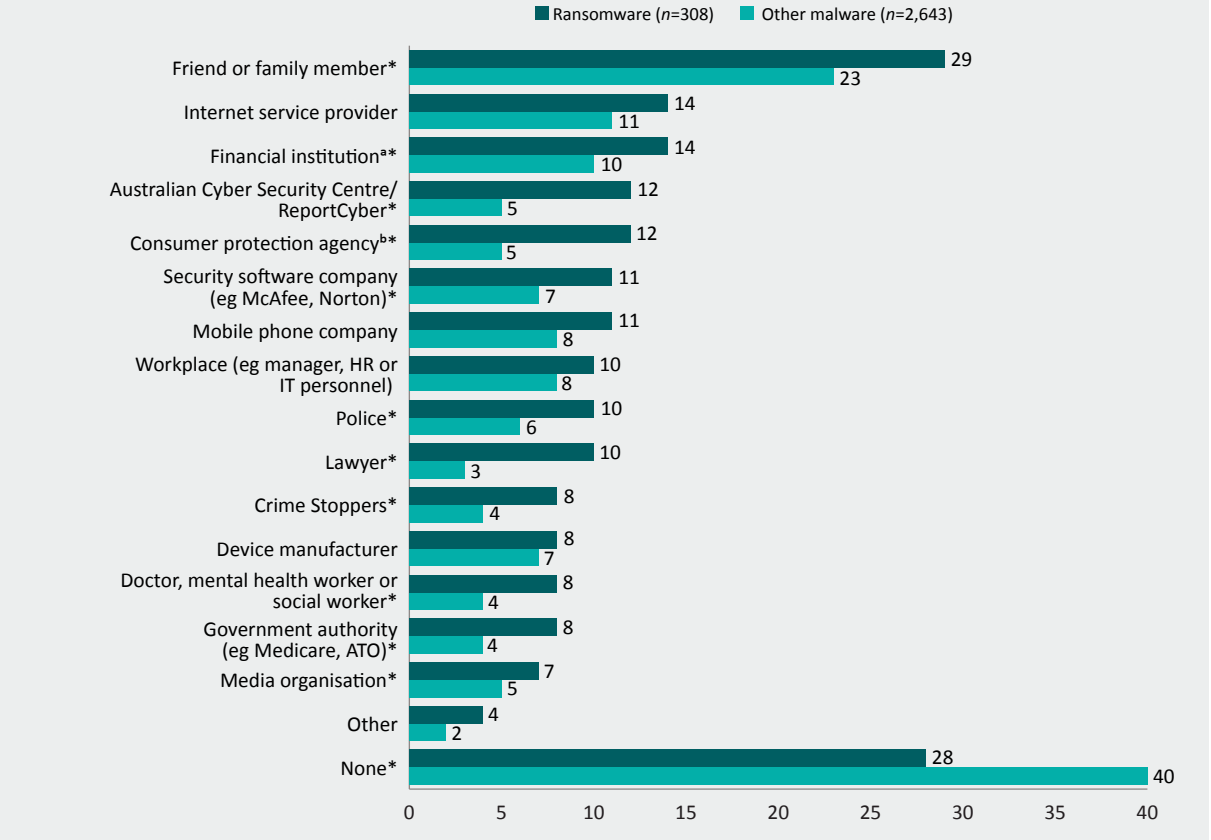
many of which may also be related to ransomware attacks). Second, we asked whether respondents had sought help, advice or support, but do not define the nature of the help sought or received. While respondents who sought help from police were subsequently asked questions about the reasons for and experience of reporting to police, we cannot be certain that they ever submitted an official report.

Results

Sources of advice and support

Victims could seek help, advice or support from multiple people or organisations, including formal and informal sources (Figure 1).

Figure 1: People and organisations reported to by ransomware and other malware victims (%)



a: Such as a bank or credit union, a credit/debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)

b: Includes Scamwatch, Consumer Affairs, Office of Fair Trading

Note: Excludes 13 ransomware victims and 145 other malware victims who did not indicate whether they had sought help, advice or support from anyone or from whom. Categories are not mutually exclusive. Statistically significant differences are marked by an asterisk (*). Results from corrected Pearson chi-square tests are as follows: told a friend or family member: F=5.04, p<0.05; told a doctor, mental health worker or social worker: F=10.29, p<0.05; told a lawyer: F=32.12, p<0.001; told the police: F=8.80, p<0.05; told Crime Stoppers: F=8.45, p<0.05; told the Australian Cyber Security Centre: F=21.21, p<0.001; told a consumer protection agency: F=23.45, p<0.001; told a financial institution: F=4.42, p<0.05; told a government authority: F=9.38, p<0.05; told the company that runs their security software: F=5.27, p<0.05; told a media organisation: F=4.04, p<0.05; and did not tell anyone: F=15.93, p<0.001. Percentages may not total 100 due to rounding. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

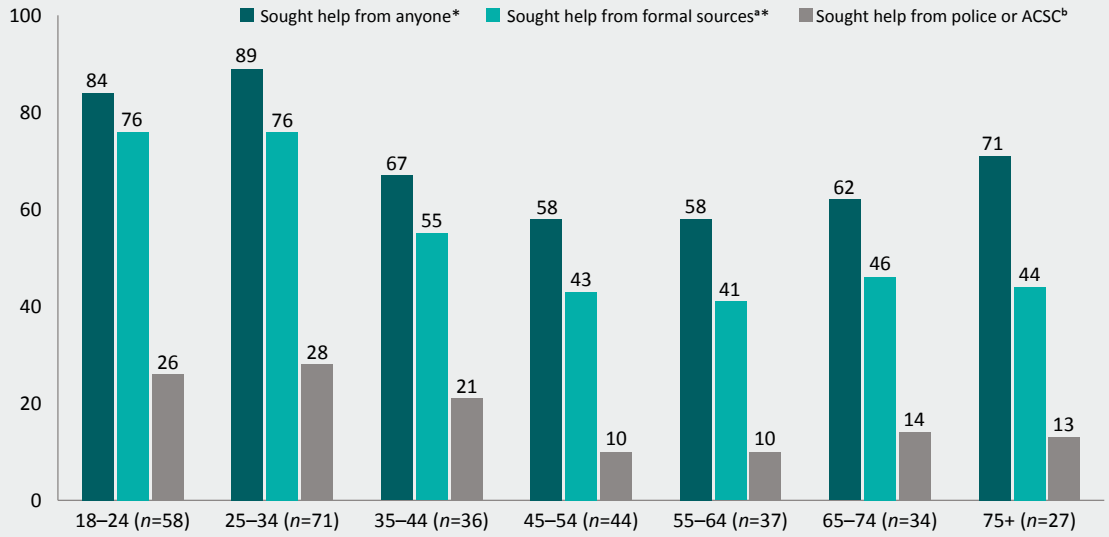
Source: AIC Cybercrime Survey [weighted data]

Overall, nearly three-quarters of ransomware victims sought help, advice or support from at least one source (*n*=223, 72%). Most of these victims—58 percent of all ransomware victims—sought help, advice or support from at least one formal source (ie they told someone other than a family or friend, *n*=180). Ransomware victims most commonly told a family member or friend (*n*=88, 29%), their internet service provider (*n*=43, 14%), or a financial institution—a bank or credit union, a credit/debit card company (eg Visa or MasterCard) or an e-commerce provider such as PayPal (*n*=43, 14%). Other organisations reported to include the Australian Cyber Security Centre, through its ReportCyber portal (https://www.cyber.gov.au/acsc/report; *n*=37, 12%), and consumer protection agencies such as Scamwatch, Consumer Affairs or the Office of Fair Trading (*n*=37, 12%). Ten percent of victims sought help, advice or support from the police (*n*=31). Overall, 19 percent of victims sought help, advice or support from either the police or the ACSC (*n*=58).

Ransomware victims were significantly more likely than other malware victims to have sought help, advice or support from a range of sources (see Figure 1, significant differences marked with an asterisk). Ransomware victims were significantly more likely to seek help, advice or support from police (*n*=31, 10% vs *n*=155, 6%) and the ACSC (*n*=37, 12% vs *n*=137, 5%), but also consumer protection agencies (including Scamwatch, *n*=37, 12% vs *n*=127, 5%), Crime Stoppers (*n*=24, 8% vs *n*=106, 4%) and legal representatives (*n*=29, 10% vs *n*=78, 3%). Ransomware victims were also more likely to seek help, advice or support from friends and family (*n*=88, 29% vs *n*=603, 23%); the company that runs their security software (*n*=33, 11% vs *n*=184, 7%); a financial institution (*n*=43, 14% vs *n*=259, 10%); a doctor, mental health worker or social worker (8% vs 4%); a government authority (*n*=23, 8% vs *n*=93, 4%); or a media organisation (*n*=22, 7% vs *n*=120, 5%). The proportion of respondents who did not tell anyone about the incident was significantly lower for ransomware victims than for other malware victims (ransomware victims *n*=85, 28%; other malware victims *n*=1,044, *n*=40%). This may be because ransomware victims were more likely than other malware victims to lose money and to lose larger amounts (see Voce & Morgan 2021).

Age was significantly associated with the likelihood of seeking help from any source and from formal sources other than friends and family (Figure 2). In general, a higher proportion of younger respondents sought help from anyone (18–24 years *n*=49, 84%; 25–34 years *n*=63, 89%), from formal sources (18–24 years *n*=44, 76%; 25–34 years *n*=54, 76%) and from police or the ACSC (18–24 years *n*=15, 26%; 25–34 years *n*=20, 28%) than older respondents. However, older respondents sought help more often than middle-aged participants (sought help from anyone: 65–74 years *n*=21, 62%; 75 years and over *n*=19, 71%), but not from formal sources or from the police or ACSC, which suggests older ransomware victims tend to seek help from their informal social networks.

Figure 2: Help-seeking behaviour among ransomware victims, by age (%)



a: Includes all sources of help, advice or support except for friends and family and 'other' unspecified sources

b: Includes seeking help, advice or support from police and the Australian Cyber Security Centre (also referred to as ReportCyber/cyber.gov.au)

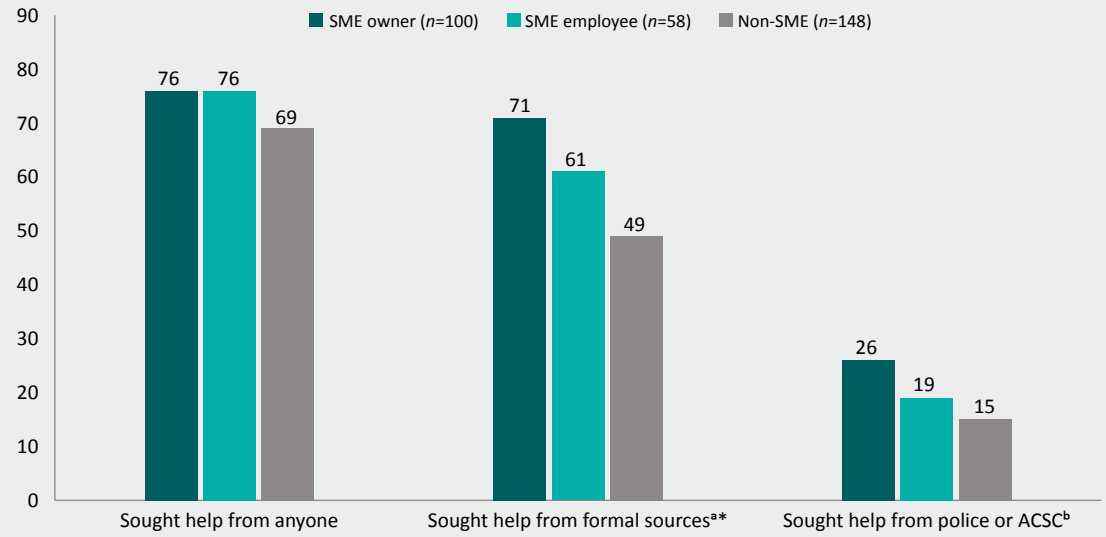
Note: Excludes 13 ransomware victims who did not indicate whether they sought help, advice or support. Statistically significant differences are marked by an asterisk (*). Statistically significant differences include: sought help from anyone: F=3.85, p<0.001; and sought help from formal sources: F=4.53, p<0.001. Percentages may not total 100 due to rounding. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: AIC Cybercrime Survey [weighted data]

Given recent evidence that small business operators have an elevated risk of ransomware victimisation (Voce & Morgan 2021), we then compared the help-seeking behaviours of small to medium enterprise (SME) owners, SME employees, and people who are not an SME owner or employee. Importantly, as with our previous research, we cannot be certain whether ransomware incidents occurred in the context of work or during personal computer use. A higher proportion of SME owners sought help from formal sources, which include persons or organisations other than friends and family (*n*=71, 71%) compared with SME employees (*n*=36, 61%) and individuals who did not own or work for an SME (*n*=72, 49%). This difference in seeking help, advice or support from formal sources was statistically significant (Figure 3). Among past-year ransomware victims, more than a quarter of SME owners made a report to police or the ACSC (*n*=26, 26%). There were no statistically significant differences between SME owners, SME employees and individuals who did not own or work for an SME in whether they made any report or whether they made a report to police or the ACSC.

Among past-year ransomware victims who sought help from anyone, around half sought help from only one source (*n*=106, 48%; see Figure 4). This was also true among victims who sought help from formal sources (*n*=91, 51%).

Figure 3: Help-seeking behaviour among ransomware victims, by SME status (%)



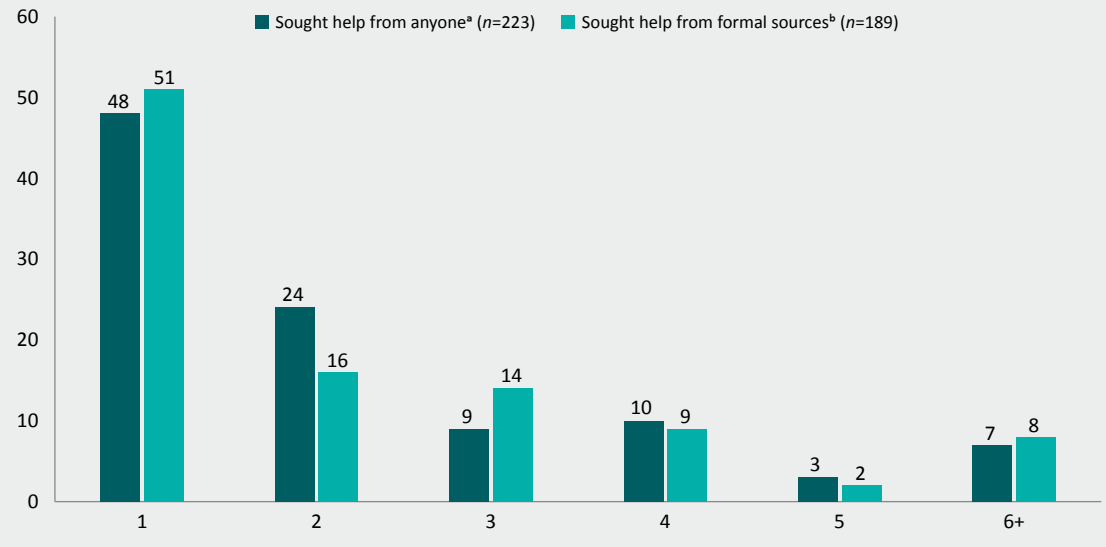
a: Includes all reports except those made to friends and family and 'other' unspecified reports

b: Includes reports to police and the Australian Cyber Security Centre (also referred to as ReportCyber/cyber.gov.au)

Note: Excludes 15 ransomware victims who did not indicate whether they owned or were employed by an SME or did not indicate to whom they had reported the incident. Categories of help-seeking sources are not mutually exclusive. Statistically significant differences are marked by an asterisk (*). Statistically significant difference in help-seeking from formal sources: F=5.94, p<0.05. Percentages may not total 100 due to rounding. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: AIC Cybercrime Survey [weighted data]

Figure 4: Number of different sources of help, advice or support among ransomware victims (%)



a: Range is 1–16 different sources of support (including 'other' unspecified sources)

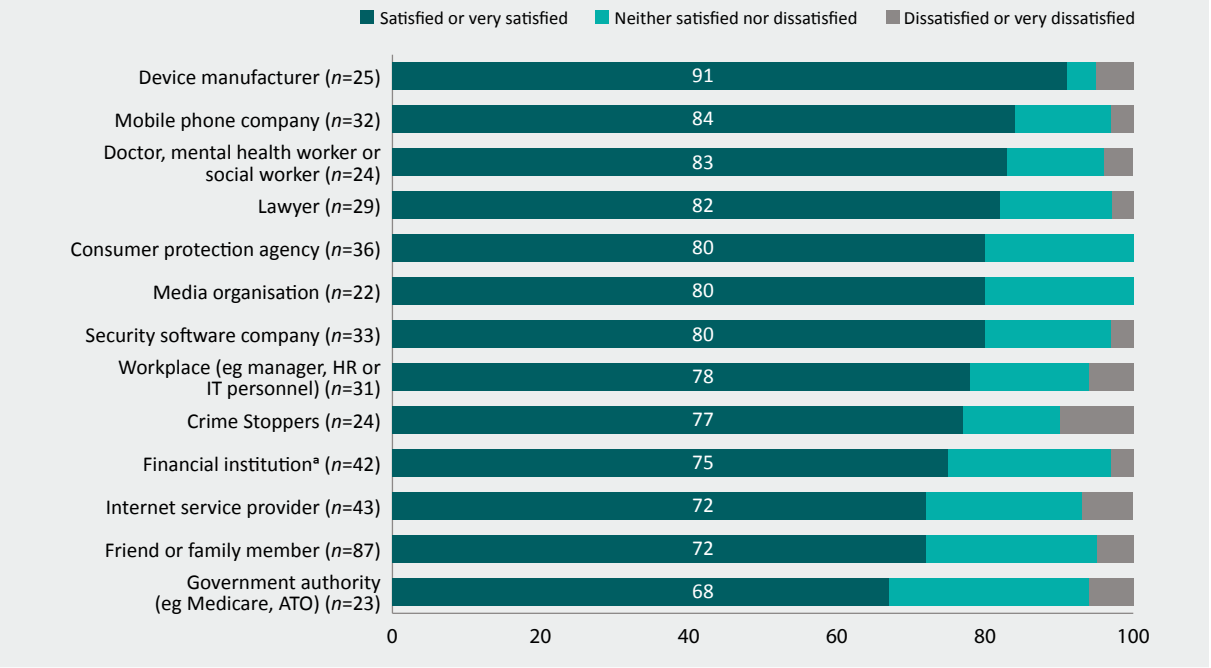
b: Range is 1–14 different sources of support, includes all sources except for friends and family and 'other' unspecified sources

Note: Excludes 13 respondents who did not indicate whether they sought help, advice or support and 85 respondents who did not seek help, advice or support from anyone. Percentages may not total 100 due to rounding. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: AIC Cybercrime Survey [weighted data]

Victims who reached out to people or organisations were generally satisfied with the help, advice or support they received, with a quarter stating that they were satisfied (*n*=55, 25%) and 46 percent stating they were very satisfied (*n*=102). Levels of satisfaction varied by the source of support victims reached out to (Figure 5).

Figure 5: Satisfaction with the quality of help, advice or support received by ransomware victims by source of help (%) (*n*=222)



a: A bank or credit union, a credit/debit card company (eg Visa or MasterCard) or an e-commerce provider (eg PayPal)

Note: Excludes 13 respondents who did not indicate whether they reported the incident, 85 respondents who did not report to anyone, and 1 respondent who selected 'Don't know/prefer not to say'. Satisfaction with reporting to police and/or ACSC is reported in Figure 8. Percentages may not total 100 due to rounding. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

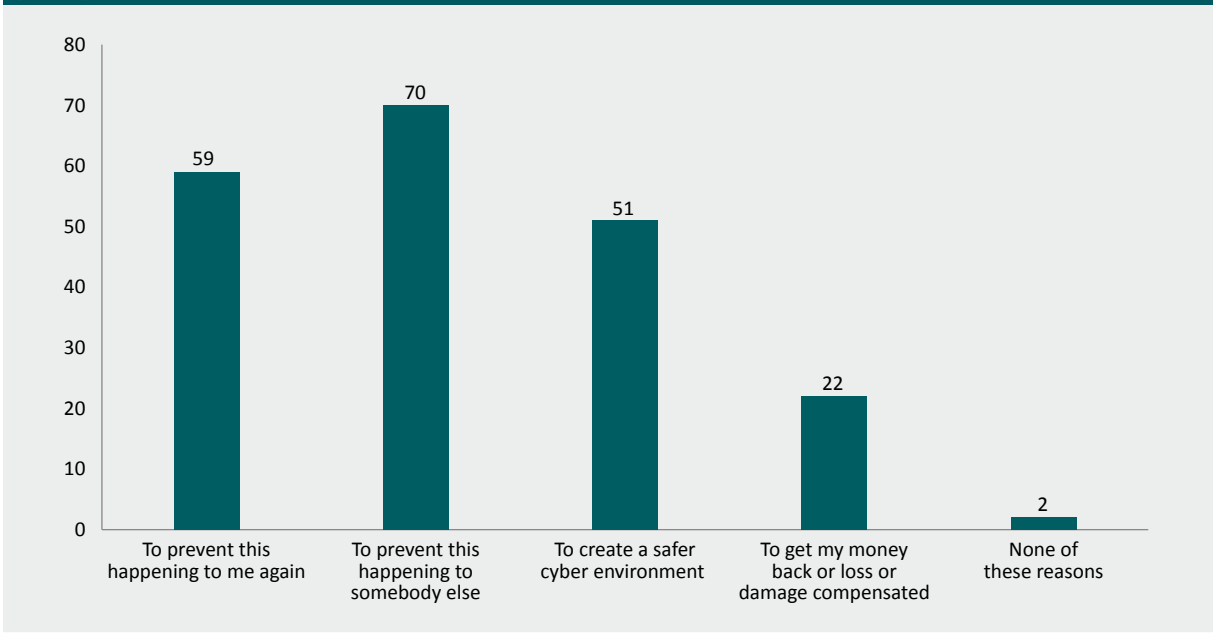
Source: AIC Cybercrime Survey [weighted data]

Victims were most satisfied with the help they received from device manufacturers; mobile phone companies; doctors, mental health workers and social workers; and legal professionals. Importantly, because victims could report to multiple organisations and were asked about their satisfaction with reporting overall, there was no way of determining satisfaction with specific organisations (besides police and the ACSC—discussed below).

Reasons for, outcomes of and satisfaction with reporting to police

Nineteen percent of past-year ransomware victims (*n*=58) said they had sought help, advice or support from either the police or the ACSC, which is also referred to as ReportCyber or cyber.gov.au. These respondents were asked about their reasons for seeking help from police and the ACSC (Figure 6), the outcomes of their report and their satisfaction with the outcome. Victims most often stated that they made a report to police or ACSC to prevent the incident happening to somebody else (*n*=41, 70%), to prevent the incident happening to them again (*n*=35, 59%) and to create a safer cyber environment (*n*=30, 51%). Only a fifth of victims reported the incident because they wanted to get their money back or compensation for the loss or damage (*n*=13, 22%).

Figure 6: Reasons for reporting incidents to the police or ACSC among ransomware victims (%) (*n*=58)

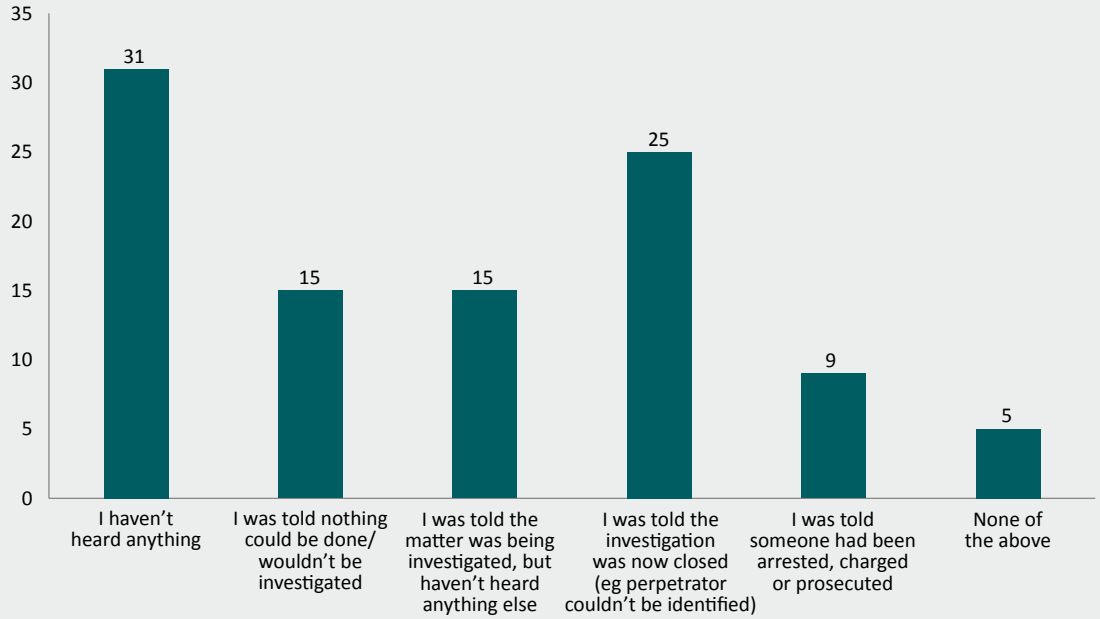


Note: Categories are not mutually exclusive; respondents could select multiple answers. Percentages may not total 100 due to rounding. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: AIC Cybercrime Survey [weighted data]

In 46 percent of cases (*n*=27), victims either did not hear back from police or the ACSC about their report or were told the matter would not be investigated (Figure 7). Half of the cases were investigated (*n*=29), and 25 percent (*n*=15) were closed without an arrest, charge or prosecution. Nine percent (*n*=5) resulted in an offender being arrested, charged or prosecuted.

Figure 7: Outcome of ransomware incidents reported to the police or ACSC (%) (*n*=58)

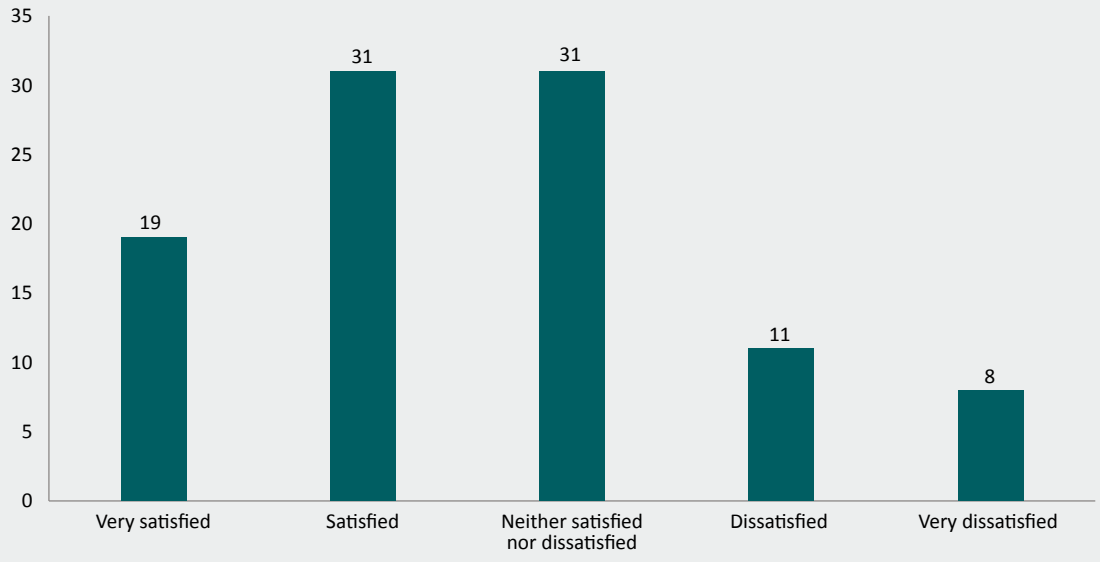


Note: Categories are not mutually exclusive; respondents could select multiple answers. Percentages may not total 100 due to rounding. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: AIC Cybercrime Survey [weighted data]

Victims were generally satisfied with the outcomes of their reports to police or ACSC (Figure 8). Fifty-one percent of victims stated that they were satisfied or very satisfied (*n*=28), while 31 percent said they were neither satisfied nor dissatisfied (*n*=17).

Figure 8: Satisfaction with reporting to the police or ACSC among ransomware victims (%) (*n*=56)



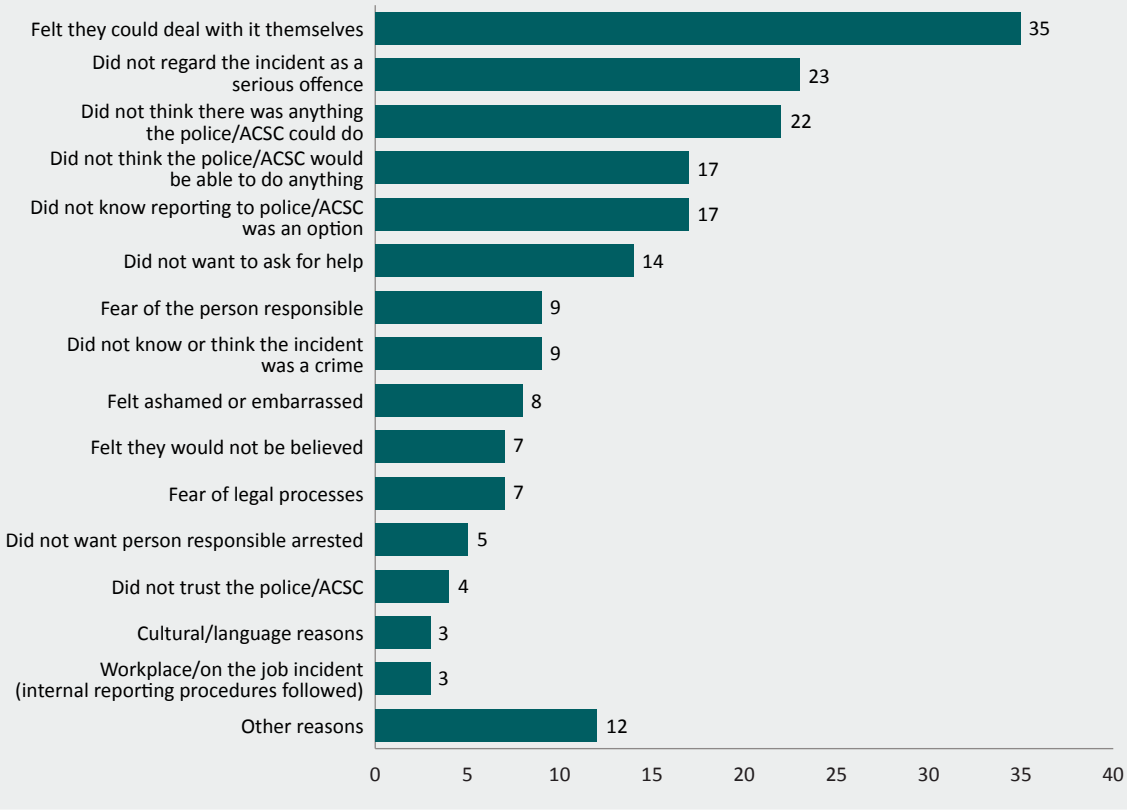
Note: Excludes 2 respondents who answered 'Don't know/prefer not to say'. Percentages may not total 100 due to rounding. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: AIC Cybercrime Survey [weighted data]

Reasons for not reporting to the police or ACSC

Respondents could nominate multiple reasons for not having reported incidents to the police or ACSC. Most often, respondents who had been a victim of ransomware did not seek help from police or ACSC because they felt they could deal with the incident themselves (*n*=82, 35%), they did not think there was anything the police or ACSC could do (*n*=67, 28%), they did not regard the incident as a serious offence (*n*=55, 23%) or they did not know that reporting to the police or ACSC was an option (*n*=41, 17%; Figure 9).

Figure 9: Reasons for not reporting incidents to the police or ACSC among ransomware victims (%) (*n*=237)



Note: Only includes respondents who did not report to police or the ACSC. Excludes 13 ransomware victims who did not indicate whether they had reported the incident and 12 respondents who did not answer the question. Categories are not mutually exclusive; respondents could select multiple answers. Percentages may not total 100 due to rounding. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: AIC Cybercrime Survey [weighted data]

Discussion

Ransomware victims seek help, advice and support from a range of sources. Nearly three-quarters of ransomware victims sought advice or support from at least one person or organisation, and nearly 60 percent sought help from at least one formal source (ie they told someone other than a family member or friend), and over half sought help from multiple sources. Most commonly, victims sought help from their friends and family, police or the ACSC, internet service providers, a financial institution, or a consumer protection agency (including Scamwatch). Formal help-seeking was higher among younger respondents and small to medium enterprise owners.

Nineteen percent of victims sought advice or support from either the police or the ACSC. This suggests that the true number of ransomware incidents in the community is significantly underestimated by official law enforcement data using reports made to police and ACSC. Most often, victims did not seek advice or support from the police or ACSC because they felt they could deal with the ransomware attack themselves, they did not think there was anything the police or ACSC could do, they did not regard the incident as a serious offence or they did not know that reporting to the police or ACSC was an option.

The most common reasons for reporting to police or the ACSC were to prevent the incident happening to somebody else or to prevent revictimisation. Only a fifth of victims reported because they wanted to get their money back or to be compensated for the loss or damage. This is largely consistent with the findings of previous research into reporting by malware victims (van de Weijer, Leukfeldt & Van der Zee 2020). Half of the reports resulted in the matter being investigated, and nine percent resulted in an offender being arrested, charged or prosecuted. Fifty-one percent of victims said they were satisfied or very satisfied with the outcome of their report to police or ACSC.

Overall, these findings show that ransomware victims actively seek information on dealing with their victimisation, and highlight the importance of providing advice and support to victims to minimise the impact of ransomware attacks and reduce the risk of repeat victimisation. Critically, because victims seek help from a wide range of sources in the law enforcement, government and private sectors (such as banks and internet services providers), there is a need for consistent, up-to-date and accurate messaging, both at the broad community level and targeted to the organisations that provide support to victims.

References

URLs correct as at December 2021

Australian Bureau of Statistics (ABS) 2021. *Population by age and sex - national. National, state and territory population, Dec 2020*. https://www.abs.gov.au/statistics/people/population/national-state-and-territory-population/dec-2020#data-downloads-data-cubes

Australian Cyber Security Centre (ACSC) 2020a. *ACSC annual cyber threat report: July 2019 to June 2020*. Canberra: ACSC. https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-july-2019-june-2020

Australian Cyber Security Centre (ACSC) 2020b. *Ransomware in Australia*. https://www.cyber.gov.au/acsc/view-all-content/publications/ransomware-australia

Cobb S 2015. *Sizing cybercrime: Incidents and accidents, hints and allegations*. Virus Bulletin International Conference, Prague, Czech Republic, 30 September to 2 October 2015. https://www.virusbulletin.com/conference/vb2015/abstracts/sizing-cybercrime-incidents-and-accidents-hints-and-allegations

Graham A, Kulig TC & Cullen FT 2020. Willingness to report crime to the police: Traditional crime, cybercrime, and procedural justice. *Policing: An International Journal* 43(10): 1–16. https://doi.org/10.1108/PIJPSM-07-2019-0115

Morgan A, Dowling C, Brown R, Mann M, Voce I & Smith M 2016. *Evaluation of the Australian Cybercrime Online Reporting Network*. Report prepared for CrimTrac. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/sites/default/files/2020-06/acorn_evaluation_report_.pdf

Pennay DW, Neiger D, Lavrakas PJ & Borg K 2018. *The Online Panels Benchmarking Study: A total survey error comparison of findings from probability-based surveys and non-probability online panel surveys in Australia*. CSRM & SRC Methods Paper no. 2/2018. Canberra: Australian National University. https://csrm.cass.anu.edu.au/research/publications/online-panels-benchmarking-studytotal-survey-error-comparison-findings

Pereira B 2016. The fight against cybercrime: From the abundance of the standard has its perfectibility. *Revue Internationale de Droit Économique* 30(3): 387–409. https://doi.org/10.3917/ride.303.0387

van de Weijer SGA, Leukfeldt R & Bernasco W 2019. Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking. *European Journal of Criminology* 16(4): 486–508. https://doi.org/10.1177/1477370818773610

van de Weijer SGA, Leukfeldt R & Van der Zee S 2020. Reporting cybercrime victimization: Determinants, motives, and previous experiences. *Policing: An International Journal* 43(1): 17–34. https://doi.org/10.1108/PIJPSM-07-2019-0122

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

Isabella Voce is a Senior Research Analyst in the Australian Institute of Criminology's Serious and Organised Crime Research Laboratory.

Anthony Morgan is the Research Manager of the Australian Institute of Criminology's Serious and Organised Crime Research Laboratory.

General editor, Statistical Bulletin series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology.
For a complete list and the full text of the papers in the Statistical Bulletin series, visit the AIC website at: aic.gov.au

ISSN 2206-7302 (Online) ISBN 978 1 922478 50 4 (Online)
https://doi.org/10.52922/sb78504

GPO Box 1936
Canberra ACT 2601, Australia
Tel: 02 6268 7166