Australian Government
Australian Institute of Criminology

Statistical Bulletin 35

October 2021

Abstract | This study presents the results from a survey of 14,994 Australian adult computer users conducted in June 2021.

Nearly five percent of all respondents had ever experienced ransomware victimisation, while two percent of respondents had experienced ransomware in the last 12 months.

Small to medium enterprise (SME) owners were twice as likely as other respondents to have been the victim of ransomware attacks in the past year and were more likely to have paid the ransom. The prevalence of ransomware victimisation varied according to the industry in which respondents were currently employed.

Most ransomware victims did not pay the ransom. The advice given to ransomware victims was identified as the most common reason for a respondent's decision about whether or not to pay the ransom, particularly in the case of SME owners.

Serious & Organised Crime
Research Laboratory

Ransomware victimisation among Australian computer users

Isabella Voce and Anthony Morgan

Ransomware is a type of malicious software (commonly referred to as malware) that blocks and encrypts a computer user's access to their data unless a ransom is paid to recover it. Ransomware has recently been identified as one of the most significant threats to Australian businesses and government (ACSC 2020a). The 2018 Internet Organised Crime Threat Assessment by Europol found that ransomware is the key malware threat in law enforcement and industry reporting (Europol 2018), while the Symantec Global Intelligence Network has reported that ransomware infections steadily increased year-over-year from 2013, reaching a record high of 1,271 detections per day in 2016 (Symantec 2017).

An increasing concern is the impact of ransomware on Australian businesses. A recent report by cybersecurity firm Mimecast (2021), based on a global survey of 1,225 companies that included Australia, found that 61 percent of businesses were disrupted by ransomware at some point during the past year. Among the affected companies, 52 percent paid the ransom and, of these, 34 percent did not get their data back despite paying the ransom.

Ransomware attacks often begin through phishing, in which emails are sent out to individuals with the aim of deceiving them into clicking on a malicious link or opening a file (Gendre 2019). As with many other cybercrimes, ransomware attacks have traditionally been employed by criminals using a 'scattergun' approach, whereby hackers cast a wide net, hoping to infect as many individual devices as possible (Groenfeldt 2016). However, ransomware attacks are becoming increasingly professional, organised and targeted at specific businesses and companies, where greater potential profits are available (Europol 2018). According to the Australian Cyber Security Centre, cybercrime offenders often launch targeted phishing attacks to illicitly obtain user logins and credentials, before using remote desktop protocol services to deploy ransomware on their targets (ACSC 2020a).

The prevalence of ransomware in the Australian community has not been measured outside of law enforcement data or broad global cybersecurity data. Ransomware attacks are likely to be under-reported, as cybercrime activity in general is often difficult to detect, even by victims (Cobb 2015), and businesses have traditionally been reluctant to divulge information on cyberattacks, in part to protect their reputations and guard against possible legal proceedings (Pereira 2016). Law enforcement data is limited to offences reported to or detected by police, reflect activities that are considered (in legislation and by law enforcement agencies) to be crimes, and provide a limited picture of overall cybercrime activity. In contrast, self-report surveys provide information on victim prevalence and crime trends, independent of victim reporting behaviour and recording practices by the police (Reep-van den Bergh & Junger 2018).

The current study aimed to measure the prevalence of ransomware victimisation among a sample of adult Australian computer users, along with victim characteristics, their decisions about whether to pay the ransom, and financial losses. Given the apparent risk to businesses from ransomware, particularly smaller businesses (ACSC 2020b; Mason 2021), we focus on the differences between respondents who own or work for small to medium enterprises (SMEs), and those who do not.

Method

A large-scale survey of 15,000 members of the public was conducted in June 2021. The survey was conducted in partnership with JWS Research. Non-proportional quota-based sampling was used to ensure the sample was representative of the spread of the Australian population. An invitation to the survey was sent out to 171,537 individuals who were members of the online 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 through 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, reporting behaviour, risk factors for victimisation and harms resulting from victimisation. A range of sociodemographic information was also collected.

Respondents were identified as ransomware victims if they had received instructions on their device for paying a ransom. 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 known to them had been receiving suspicious messages and links from them 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 keep 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.

Participants were asked to only report incidents that they believed were not just the result of genuine device malfunction or aging. Respondents were also asked whether they had ever been a victim and, if so, whether it had occurred within the last year. The survey included several ransomware-specific questions including whether victims had paid the ransom and their reasons for choosing to pay or not.

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 ABS demographic data as of December 2020 (ABS 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 to the survey. Of the 15,000 respondents, six respondents were removed from the sample for providing illogical responses to sets of questions that implied they were answering the survey randomly, resulting in a final survey sample of 14,994 respondents.

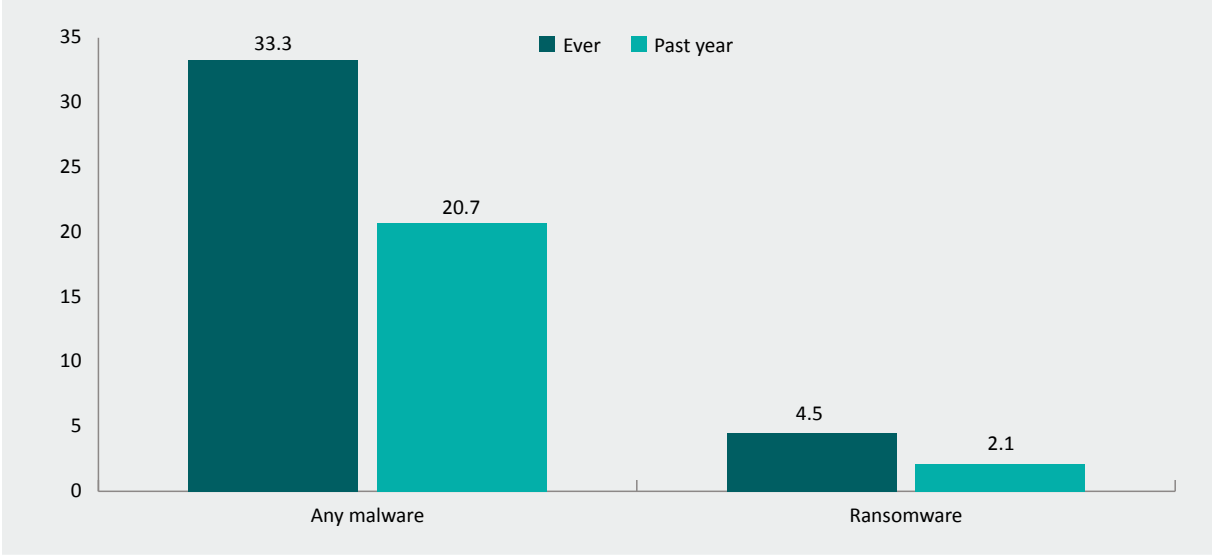
Online panels allow for rapid collection of data from large samples, which is particularly useful where the prevalence of an outcome is relatively rare (as is the case with many cybercrimes), and where the main population of interest is computer users. There are limitations to this approach. While the sample in this survey was large, and comparisons between secondary (ie non-sampling) demographics and population-level characteristics revealed a high degree of concordance, we are cautious not to generalise the results to the wider population, or assume the results are representative of non-respondents. It should also be acknowledged that this was a survey of Australian individuals, rather than being specifically targeted at business owners, meaning the findings may not be representative of all small to medium business owners. Efforts were made to ensure the questions about cybercrimes and prevention strategies were as accessible as possible for a non-technical audience, and a unique bottom-up approach to asking about victimisation was adopted; however, it is possible that some respondents may not have been aware they were a victim of cybercrime. Similarly, some respondents may have been reluctant to disclose experiences of victimisation due to shame or embarrassment.

Results

Prevalence

As shown in Figure 1, 33.3 percent of the weighted sample (*n*=4,990) had ever experienced any kind of malware, while 20.7 percent (*n*=3,106) had experienced malware in the last 12 months. Nearly five percent of respondents (*n*=669, 4.5%) had ever experienced ransomware, with two percent (*n*=321, 2.1%) experiencing it in the last 12 months.

Figure 1: Ransomware and malware victimisation at any time in the past and in the last 12 months (%) (*n*=14,994)

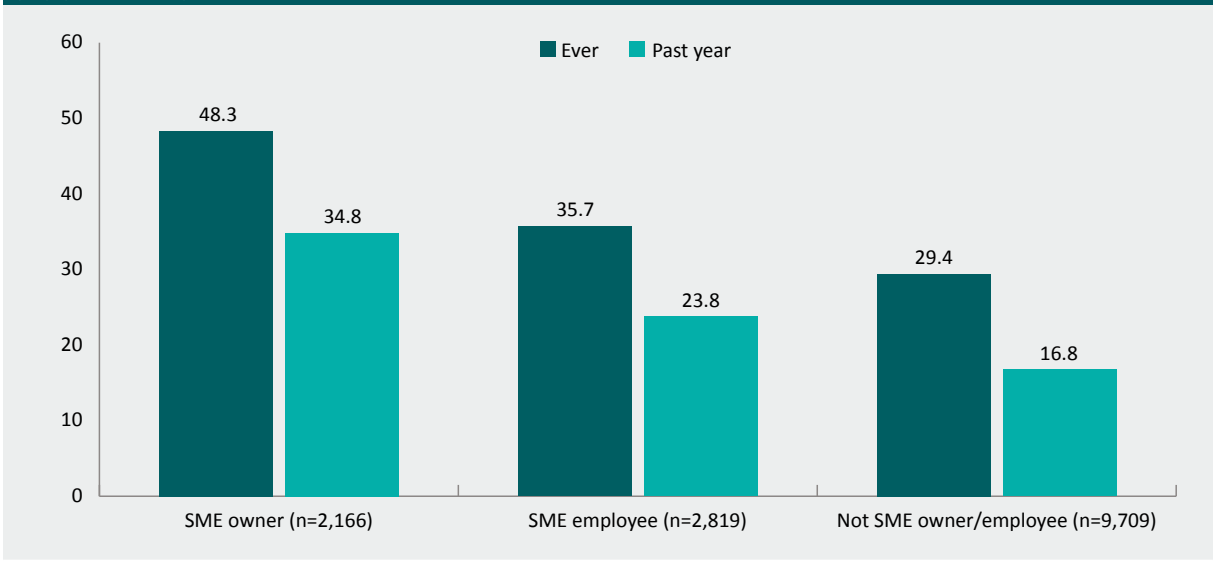


Note: Denominator for lifetime malware and ransomware prevalence includes 689 respondents who answered 'don't know' or preferred not to answer; lifetime prevalence estimates excluding non-responders are 34.9% for malware and 4.7% for ransomware. Denominator for past-year malware and ransomware prevalence includes 967 respondents who answered 'don't know' or preferred not to answer; past-year prevalence estimates excluding non-responders are 22.1% for malware and 2.3% for ransomware

Source: AIC Australian Cybercrime Survey [weighted data]

Small to medium business owners had a higher prevalence of malware victimisation in their lifetime and in the past year compared with SME employees and individuals who were not owners or employees of SMEs (see Figure 2). Forty-eight percent of SME owners had ever been the victim of any kind of malware (*n*=1,047), with 34.8 percent reporting victimisation in the past year (*n*=754). Thirty-six percent of SME employees had ever been the victim of any kind of malware attack (*n*=1,007), with 23.8 percent reporting victimisation in the past year (*n*=672). Twenty-nine percent of individuals who reported that they did not own or work in an SME had ever been the victim of any kind of malware attack (*n*=2,854), with 16.8 percent reporting victimisation in the past year (*n*=1,634). There was a statistically significant relationship between SME status and malware victimisation (see Figure 2 notes).

Figure 2: Malware victimisation at any time in the past and in the last 12 months, by SME status (%) (*n*=14,694)



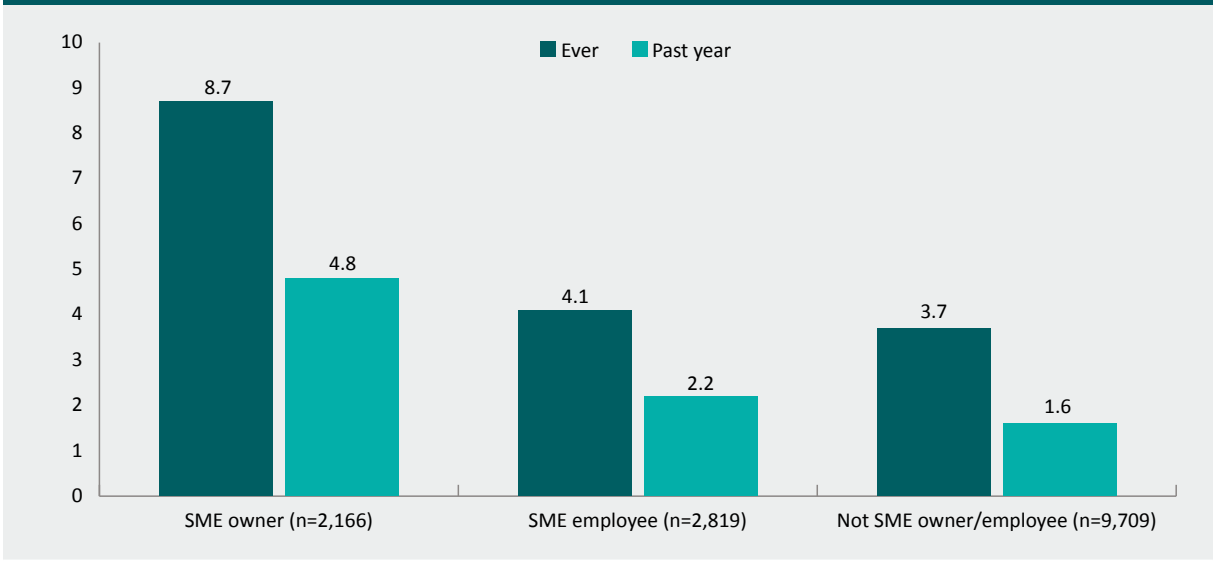
Note: Excludes 300 respondents who did not indicate whether they owned or were employed by an SME. Denominator for lifetime malware prevalence includes 622 respondents who answered 'don't know' or preferred not to answer. Denominator for past-year malware prevalence includes 892 respondents who answered 'don't know' or preferred not to answer.

Statistically significant difference in lifetime malware prevalence (excluding non-responders: SME owners, 50.4%; SME employees, 37.1%; individuals who did not own or work within an SME, 30.8%): $\chi^2(2, n=14,072)=315.52$, $F=138.47$, $p<0.001$. Statistically significant difference in past-year malware prevalence (excluding non-responders: SME owners, 37.2%; SME employees, 25.3%; individuals who did not own or work within an SME, 17.9%): $\chi^2(2, n=13,802)=406.66$, $F=174.75$, $p<0.001$

Source: AIC Australian Cybercrime Survey [weighted data]

As shown in Figure 3, SME owners also had a higher prevalence of ransomware attacks, both in their lifetime (*n*=187, 8.7%) and in the last year (*n*=103, 4.8%), compared to individuals who were SME employees (lifetime *n*=116, 4.1%; past year *n*=61, 2.2%) and individuals who were not SME owners or employees (lifetime *n*=357, 3.7%; past year *n*=153, 1.6%). These differences in lifetime and past-year ransomware prevalence were statistically significant (see Figure 3 notes).

Figure 3: Ransomware victimisation at any time in the past and in the last 12 months, by SME status (%) (*n*=14,694)



Note: Excludes 300 respondents who did not answer the question about being an SME owner or employee. Denominator for lifetime ransomware prevalence includes 622 respondents who answered 'don't know' or preferred not to answer. Denominator for past-year ransomware prevalence includes 892 respondents who answered 'don't know' or preferred not to answer.

Statistically significant difference in lifetime ransomware prevalence (excluding non-responders: SME owners, 9.0%; SME employees, 4.2%; individuals who did not own or work within an SME, 3.9%): $\chi^2(2, n=14{,}072)=109.48$, $F=48.29$, $p<0.001$. Statistically significant difference in past-year ransomware prevalence (excluding non-responders: SME owners, 5.1%; SME employees, 2.3%; individuals who did not own or work within an SME, 1.7%): $\chi^2(2, n=13{,}802)=93.06$, $F=39.89$, $p<0.001$

Source: AIC Australian Cybercrime Survey [weighted data]

Compared to females, ransomware victimisation was significantly higher among males in their lifetime (males *n*=409, 5.6%; females *n*=256, 3.4%) and in the past year (males *n*=191, 2.6%; females *n*=128, 1.7%; Table 1). There was also a statistically significant relationship between age and lifetime and past-year ransomware victimisation (see Table 1 notes). Respondents aged 18 to 24 years (lifetime *n*=107, 6.1%; past-year *n*=61, 3.5%) and 25 to 34 years (lifetime *n*=158, 5.5%; past-year *n*=75, 2.6%) were most likely to have been victims of ransomware, although lifetime victimisation rates were notably higher among respondents aged 65 years and over when compared with respondents aged 35 to 64 years.

Table 1: Ransomware victimisation by respondent age and gender (%) (*n*=14,994)

	Number in sample	Lifetime prevalence	Past-year prevalence
Gender			
Female	7,610	3.4	1.7
Male	7,326	5.6	2.6
Non-binary	39	10.3	5.1
Age			
18–24	1,749	6.1	3.5
25–34	2,865	5.5	2.6
35–44	2,583	3.4	1.5
45–54	2,426	3.6	1.8
55–64	2,237	3.8	1.8
65–74	1,766	4.4	2.0
75+	1,368	4.8	2.0

Note: Data for gender excludes 19 respondents who did not answer the question. Denominator for lifetime ransomware prevalence includes 677 respondents who answered 'don't know' or preferred not to answer. Denominator for past-year ransomware prevalence includes 955 respondents who answered 'don't know' or preferred not to answer. 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.

Statistically significant difference between males and females for lifetime ransomware victimisation (excluding non-binary due to low number, and non-responders: males, 5.8%; females, 3.5%): $\chi^2(1, n=14{,}266)=44.86$, $F=39.24$, $p<0.001$. Statistically significant difference between males and females for past-year ransomware victimisation (excluding non-binary due to low number, and non-responders: males, 2.8%; females, 1.8%): $\chi^2(1, n=13{,}992)=15.55$, $F=13.34$, $p<0.001$. Statistically significant relationship between respondent age and lifetime ransomware victimisation (excluding non-responder ages 18–24, 6.6%; ages 25–34, 5.9%; ages 35–44, 3.6%; ages 45–54, 3.7%; ages 55–64, 3.9%; ages 65–74, 4.5%; age 75+, 5.0%): $\chi^2(6, n=14{,}305)=38.39$, $F=5.68$, $p<0.001$. Statistically significant relationship between respondent age and past-year ransomware victimisation (excluding non-responder ages 18–24, 3.8%; ages 25–34, 2.9%; ages 35–44, 1.6%; ages 45–54, 1.9%; ages 55–64, 1.8%; ages 65–74, 2.1%; age 75+ 2.1%): $\chi^2(6, n=14{,}027)=31.12$, $F=4.45$, $p<0.001$

Ransomware victimisation also varied by employment status (Table 2). Respondents studying full time had the highest lifetime prevalence (*n*=13, 5.1%) while semi-retired respondents had the highest prevalence in the last year (*n*=11, 3.1%), though numbers were small overall. More broadly, respondents who were currently working (working full-time, part-time or semi-retired) were significantly more likely to have experienced ransomware in the last 12 months (*n*=230, 2.3%) than respondents who were not working (*n*=83, 1.7%), but this difference was not statistically significant for lifetime ransomware victimisation (working *n*=465, 4.7%; not working *n*=194, 4.0%; see Table 2 notes).

Table 2: Ransomware victimisation by respondent employment status (%) (*n*=14,683)

	Number in sample	Lifetime prevalence	Past-year prevalence
Employment status			
Working full-time	6,598	5.0	2.4
Working part-time	2,856	4.1	2.2
Semi-retired	373	4.9	3.1
Unemployed	688	3.2	1.0
Full-time homemaker	696	3.4	1.6
Full-time student	261	5.1	2.6
Retired/pension	3,211	4.2	1.8
Currently working[a]	4,856	4.7	1.7
Not currently working[a]	9,827	4.0	2.3

a: 'Currently working' only includes respondents working full-time, part-time or semi-retired, while 'not currently working' includes all other categories

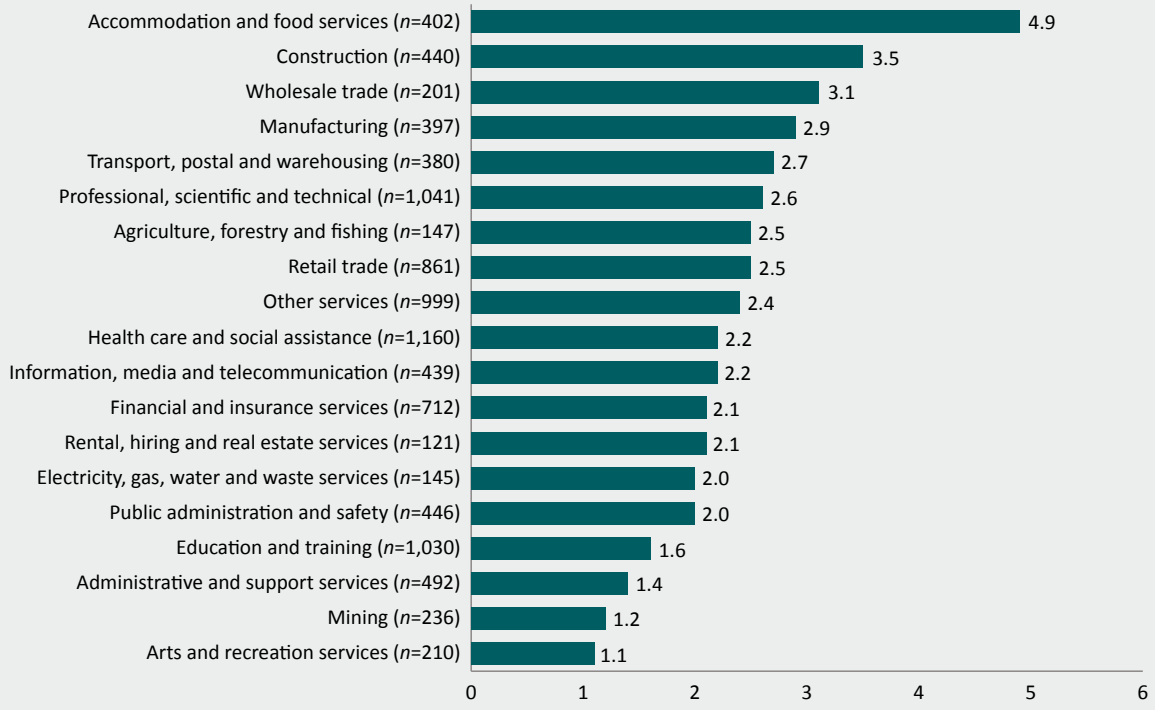
Note: Missing data includes 96 respondents who preferred to not answer the question, and 215 respondents who selected 'other' employment status. Denominator for lifetime ransomware prevalence includes 378 respondents who answered 'don't know' or preferred not to answer. Denominator for past-year ransomware prevalence includes 656 respondents who answered 'don't know' or preferred not to answer. 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.

Lifetime prevalence excluding non-responders: working full-time, 5.2%; working part-time, 4.4%; semi-retired, 5.0%; unemployed, 3.6%; full-time homemaker, 3.5%; full-time student, 5.4%; retired/pension, 4.3%. Past-year prevalence excluding non-responders: working full-time, 2.5%; working part-time, 2.4%; semi-retired, 3.2%; unemployed, 1.2%; full-time homemaker, 1.7%; full-time student, 2.8%; retired/pension, 1.9%. Statistically significant difference between respondents who were currently working and not currently working for past-year ransomware victimisation (excluding non-responders working, 2.5%; not working, 1.8%): $\chi^2(1, n=13{,}769)=6.87$, $F=5.67$, $p<0.05$

Source: AIC Australian Cybercrime Survey [weighted data]

Among those respondents who were currently employed, the highest prevalence of past-year victimisation was among those working in accommodation and food services (*n*=20, 4.9%) and the construction industry (*n*=15, 3.5%; Figure 4). It was not possible to determine whether respondents experienced ransomware while at work or at home or using their personal or professional computer network.

Figure 4: Prevalence of past-year ransomware victimisation, by industry (%) (*n*=9,859)

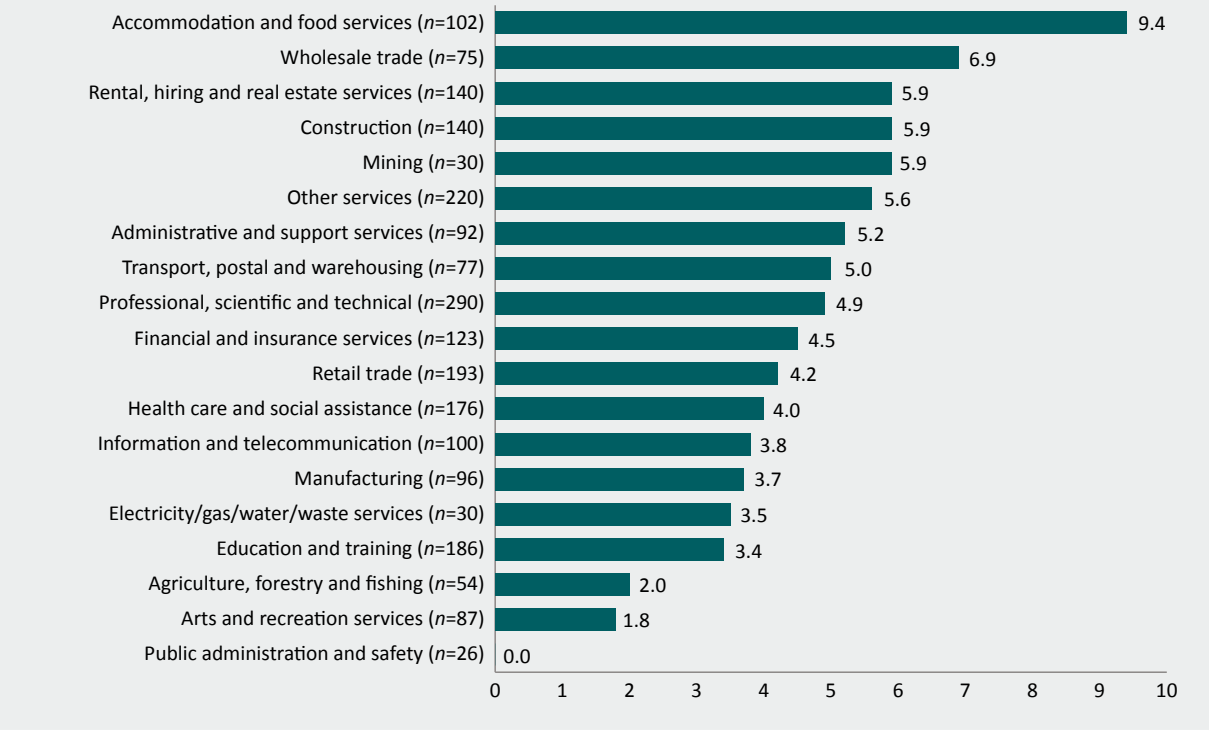


Note: Only includes respondents who were working full-time, working part-time, semi-retired or had selected 'other' employment status, and excludes 183 respondents who fell into these work categories but did not indicate which industry they worked in. Denominators for past-year ransomware prevalence include 447 respondents who answered 'don't know' or preferred not to answer. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: AIC Australian Cybercrime Survey [weighted data]

Among respondents who indicated they were SME owners, past-year ransomware victimisation was most common among those in the accommodation and food services (*n*=10, 9.4%) and wholesale trade (*n*=5, 6.9%) industries (Figure 5), though the sample of SME owners in some industries was relatively small. Importantly, being an owner of an SME does not necessarily mean the ransomware attack was related to their business.

Figure 5: Prevalence of past-year ransomware victimisation, by industry, SME owners only (%) (*n*=2,139)



Note: Only includes SME owners and excludes 40 respondents who did not indicate which industry they worked in. Denominator for past-year malware and ransomware prevalence include 141 respondents who answered 'don't know' or preferred not to answer. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

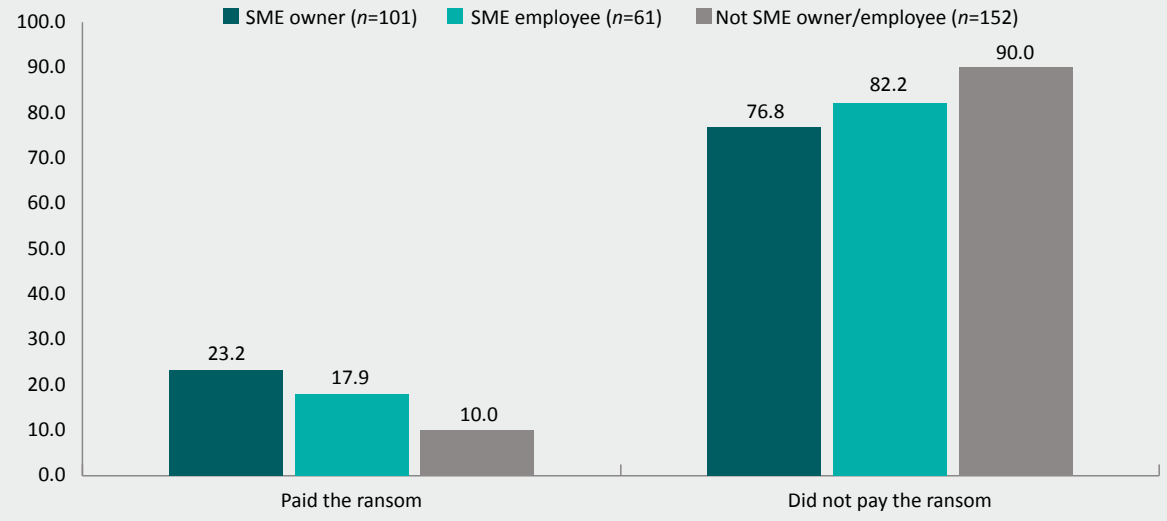
Source: AIC Australian Cybercrime Survey [weighted data]

Paying the ransom

Respondents who had been the victim of ransomware in the past year (*n*=321) were asked whether they had decided to pay the ransom. Among those victims who answered this question (*n*=314), most indicated that they had decided to not pay the ransom (*n*=266, 83.6%), while 15 percent (*n*=49, 15.4%) indicated that they had paid the ransom.

Among past-year ransomware victims, 23.2 percent of SME owners indicated that they had decided to pay the ransom (*n*=24), while 17.9 percent of SME employees paid the ransom (*n*=11) and 10.0 percent of individuals who did not own or work for an SME paid the ransom (*n*=15; Figure 6). There was a statistically significant relationship between SME status and whether a victim paid the ransom (see Figure 6 notes).

Figure 6: Ransom payment among past-year ransomware victims, by SME status (%) (*n*=314)



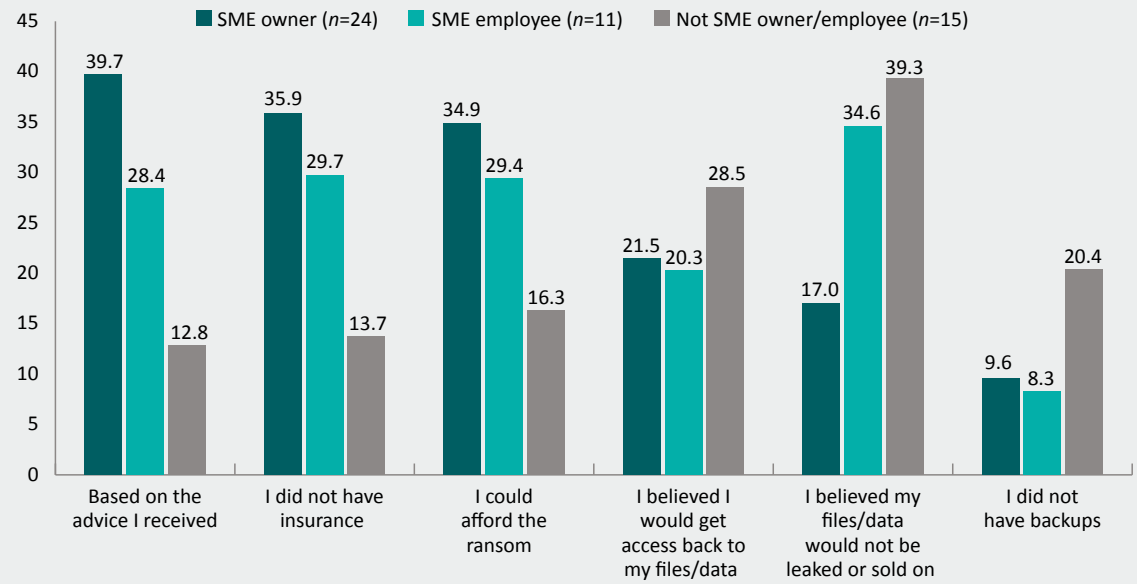
Note: Data excludes 7 respondents who did not indicate whether they paid the ransom or whether they owned or were employed by an SME. Statistically significant relationship between SME status and ransomware payment: $\chi^2(2, n=314)=393.56$, $F=3.46$, $p<0.05$. Percentages may not total 100 due to rounding. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: AIC Australian Cybercrime Survey [weighted data]

According to respondents who had paid the ransom, the most common reasons for paying the ransom were the advice they received (*n*=14, 29.0%), their ability to afford the ransom (*n*=14, 28.0%), their belief that their files/data would not be leaked or sold on if they paid the ransom (*n*=14, 27.7%) and that they did not have insurance (*n*=14, 27.7%).

Reasons for paying the ransom differed between SME owners, SME employees and individuals who did not own or work for an SME (Figure 7). Compared with SME employees and individuals who did not own or work for an SME, a higher proportion of SME owners paid the ransom based on the advice they received (*n*=9, 39.7%), because they did not have insurance (*n*=8, 35.9%), and because they could afford the ransom (*n*=8, 34.9%). Conversely, non-SME owners or employees more often paid the ransom because they believed their files or data would not be leaked or sold on (if they paid; *n*=6, 39.3%), they believed they would receive access to their files or data (*n*=5, 28.5%), and because they did not have backups (*n*=3, 20.4%). While these differences were not statistically significant, possibly due to the small sample size (*n*=49), they do suggest different motives for paying ransom according to whether respondents owned, were employed by or did not work for an SME.

Figure 7: Reasons for paying the ransom among past-year ransomware victims (%) (*n*=49)



Note: Data excludes 2 'Other' responses. Corresponding numbers and percentages may be slightly unequal due to rounding of weighted data. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding

Source: AIC Australian Cybercrime Survey [weighted data]

The most common reasons respondents provided for not paying the ransom were the advice they received (*n*=77, 30.7%), a perception that the ransom demands were not genuine (*n*=72, 28.7%), and that they had backups (*n*=61, 24.3%).

These reasons were also the most common reasons for not paying the ransom among SME owners (Figure 8). Compared with SME employees and individuals who did not own or work for an SME, a higher proportion of SME owners stated that they did not pay the ransom because they had insurance (*n*=9, 12.6%), which was a statistically significant difference (see Figure 8 notes). A higher proportion of SME owners also believed their files or data would be leaked or sold on regardless of whether they made the payment (*n*=11, 14.5%), although this difference was not statistically significant.

Figure 8: Reasons for not paying the ransom among past-year ransomware victims (%) (*n*=249)

Note: Data excludes 16 respondents who preferred not to answer the question and 2 respondents who did not indicate whether they owned or were employed by an SME. Frequencies produced in the weighted analysis are not presented as integers, meaning that frequencies may not equal totals due to rounding. Statistically significant difference for 'I had insurance': $\chi^2(2, n=249)=401.12$, $F=3.42$, $p<0.05$

Source: AIC Australian Cybercrime Survey [weighted data]

Amount lost

Ten percent of ransomware victims (*n*=30, 9.5%) reported that they had money stolen as a result of their victimisation, compared with 7.3 percent of victims who experienced other forms of malware (*n*=199). The median amount lost by ransomware victims was $500 (*n*=25, range: $50–$24,000), while the median amount lost by other malware victims was $200 (*n*=167, range: $1–$250,000).

Forty-three percent of ransomware victims who paid the ransom had money stolen (*n*=21), while three percent of ransomware victims who paid the ransom (*n*=8) reported having money stolen. On average ransomware victims who did pay the ransom lost more money (median $500, *n*=18, range: $50–$24,000) than those who did not pay the ransom (median $300, *n*=8, range: $149–$10,000). While ransomware victims were asked specifically about money that was stolen, it is possible that these respondents considered money spent paying the ransom as money that had been stolen, particularly if they did not get access to their files or data restored.

Among past-year ransomware victims, the median amount lost by SME owners was $500 (*n*=10, range: $50–$24,000), the median amount lost by SME employees was $300 (*n*=6, range: $120–$2,000) and the median amount lost by victims who did not own or work at an SME was $1,000 (*n*=9, range: $60–$10,000).

Co-occurring issues

Fifty percent of past-year ransomware victims (*n*=160) also reported at least one other malware issue within the last year (Table 3). The most common co-occurring issues were that pop-up ads started appearing everywhere (*n*=61, 18.9%), people known to them had been receiving suspicious messages and links from them over social media or email (*n*=51, 15.9%), and their device was working excessively while no programs were running (*n*=45, 13.9%) or had slowed down or was acting strangely (*n*=44, 13.6%).

Table 3: Other malware issues reported by past-year ransomware victims (%) (*n*=321)

	%
Pop-up ads started popping up everywhere	18.9
People I knew told me that I had been sending them suspicious messages and links over social media or email	15.9
My device was working excessively while no programs were running	13.9
My device slowed down and acted strangely	13.6
My browser kept getting redirected when I tried to search for a familiar site	12.6
My devices keep crashing for some reason	10.2
Programs were opening and closing automatically	9.1
My files have gone missing or been replaced with odd file extensions (such as .crypted or .cryptor) and the icons for the files were blank	8.8
There was a lack of storage space that I couldn't explain	8.1
Previously accessible system tools (such as personalised or security settings) were disabled	6.4
At least one of the above	49.9

Source: AIC Australian Cybercrime Survey [weighted data]

The experience of other forms of cyber-enabled crime in the same 12 months may indicate that a victim of ransomware has had their personal or business information compromised. Fifty-nine percent of past-year ransomware victims reported that they had also experienced signs of identity theft, compromise or misuse in the past year (*n*=185), most commonly:

- 18.6 percent said they received notification from a bank, financial institution or credit card company that their identity had been stolen or that there was suspicious activity on their account that they didn't recognise (*n*=59);
- 18.4 percent said they were notified that their information was exposed in a data breach (*n*=57);
- 10.7 percent received calls from debt collectors asking about unpaid bills they did not recognise (*n*=34); and
- 9.5 percent said suspicious transactions had appeared in their bank statements or accounts, or their cheques bounced (*n*=30).

Thirty-four percent of past-year ransomware victims had also been a victim of a fraud or scam in the past year (*n*=109), most commonly:

- seven percent said they provided their personal/financial details in response to a phishing scam (*n*=21);
- seven percent said they paid money or provided their personal/financial details in response to being sent a fake bill or invoice (*n*=21);
- seven percent said they had sent money to a fake seller or buyer on an online classifieds or marketplace website, such as Facebook Marketplace or eBay (*n*=23); and
- seven percent said they allowed someone pretending to be a telecommunications or computer company to remote access their computer, or paid them money or provided them with their personal or financial details (*n*=22).

Overall, ransomware victims were significantly more likely to experience other profit-motivated cybercrimes than malware victims and respondents who did not experience any form of malware (Table 4). The prevalence of identity theft, compromise or misuse among ransomware victims (*n*=185, 57.8%) was higher than among other malware victims (*n*=1,326, 47.6%) and the rest of the sample (*n*=2,293, 19.3%). Similarly, ransomware victims had a higher prevalence of fraud and scam victimisation in the past year (*n*=108, 33.8%) than other malware victims (*n*=756, 27.1%) and the rest of the sample (*n*=586, 4.9%).

Table 4: Prevalence of profit-motivated cybercrime in the past year, by cybercrime type (%) (*n*=14,994)

	Prevalence of identity theft, compromise or misuse	Prevalence of fraud and scams
Ransomware victims (*n*=321)	57.8	33.8
Other malware victims[a] (*n*=2,785)	47.6	27.1
Rest of the sample[b] (*n*=11,888)	19.3	4.9

a: Only includes past-year victims of malware who did not experience ransomware

b: Includes all respondents except those who experienced any malware and/or ransomware in the past year

Note: Statistically significant differences in prevalence of identity theft, compromise or misuse (excluding non-responder ransomware victims, 58.7%; other malware victims, 48.6%; rest of the sample, 20.1%): $\chi^2(2, n=14{,}458)=1136.33$, $F=509.77$, $p<0.001$. Statistically significant differences in prevalence of fraud and scams (excluding non-responder ransomware victims, 34.2%; other malware victims, 27.5%; rest of the sample, 5.1%): $\chi^2(2, n=14{,}579)=1{,}499.44$, $F=66{,}540$, $p<0.001$

Source: AIC Australian Cybercrime Survey [weighted data]

Discussion

This paper draws on data from a large sample of Australian computer users to explore patterns of ransomware victimisation, which has been identified as significant threat to Australian businesses and individuals. Ransomware victimisation was relatively uncommon, with 4.5 percent of respondents having ever been a victim, and 2.1 percent of respondents being a victim in the past year. However, SME owners were significantly more likely to report ransomware victimisation both in their lifetime and in the past year compared with SME employees and individuals who did not own or work for an SME. Past-year ransomware victims often experienced other technical issues suggestive of malware attacks in the past year, along with high prevalence of identity theft, compromise or misuse, and frauds and scams. These findings indicate that SME owners are significant targets for ransomware attacks, and highlight the co-occurrence of cybercrime offences and the need to identify and assist those individuals at risk of victimisation and repeat victimisation.

While the majority of ransomware victims chose to not pay the ransom, SME owners were significantly more likely to pay the ransom. The advice given to ransomware victims was consistently identified as the most common basis upon which they decided whether or not to pay the ransom. This was more often a deciding factor for SME owners compared with other respondents. Other reasons for paying the ransom included being able to afford the ransom or not having insurance. Victims who did not pay the ransom often had backups or did not believe the ransom demands were credible. Compared with other respondents, a higher proportion of SME owners said that having insurance was a factor in their decision to not pay the ransom. These findings show that ransomware victims rely on advice on how to resolve attacks and highlight the importance of providing consistent and accurate advice to victims on what action they should take and whether or not they should pay the ransom.

References

URLs correct as at September 2021

Australian Cyber Security Centre (ACSC) 2020a. *ACSC annual cyber threat report: July 2019 to June 2020*. 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. Cyber security and Australian small businesses: Results from the Australian Cyber Security Centre Small Business Survey. https://www.cyber.gov.au/acsc/small-and-medium-businesses/small-business-survey-results

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

Europol 2018. *Internet organised crime threat assessment 2018*. https://www.europol.europa.eu/internet-organised-crime-threat-assessment-2018

Gendre A 2019. 4 ways hackers use phishing to launch ransomware attacks. Vade, 12 September. https://www.vadesecure.com/en/blog/3-ways-hackers-use-phishing-to-launch-ransomware-attacks

Groenfeldt T 2016. Cyber criminals target banks because that's where the money is. Forbes, 28 September. https://www.forbes.com/sites/tomgroenfeldt/2016/09/28/cyber-criminals-target-banks-because-thats-where-the-money-is/?sh=3a5ef8e635b9

Mason M 2021. More than half of Australian businesses disrupted by cyber attacks. *Australian Financial Review*, 23 April. https://www.afr.com/policy/foreign-affairs/more-than-half-of-australian-businesses-disrupted-by-cyber-attacks-20210423-p57lvs

Mimecast 2021. *The state of email security report 2021*. https://www.mimecast.com/state-of-email-security/

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-study-total-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

Reep-van den Bergh CMM & Junger M 2018. Victims of cybercrime in Europe: A review of victim surveys. *Crime Science* 7(5). https://doi.org/10.1186/s40163-018-0079-3

Symantec 2017. *2017 Norton cyber security insights report: Global results*. https://www.nortonlifelock.com/us/en/newsroom/press-kits/ncsir-2017/

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 38 2 (Online)
https://doi.org/10.52922/sb78382

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