Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

No. 724 November 2025

Ransomware targeting individuals and small businesses: Vulnerabilities and impacts

Isabella Voce and Anthony Morgan

Abstract | This study examines the experiences of 331 Australian individuals and small to medium enterprise (SME) owners who were victims of ransomware. We used survey data to understand how they were targeted and the vulnerabilities that were exploited in private and work-related settings.

Most ransomware victims had received multiple ransom messages in the past 12 months. SME owners were more likely to have received multiple messages and to have previously paid a ransom. Strong messaging should dissuade SME owners from making these payments, which increase the chances of repeat victimisation.

SME owners reported impacts on many devices. The affected devices were also more likely to have been a work-issued device or a personal device used for work. SME owners were also more likely than other victims to report that the ransomware had spread to other workplace devices, systems or email accounts. The results highlight both the human element in victimisation and the need for technological solutions to protect business owners from ransomware and its harmful effects.

Ransomware refers to a type of malicious software that encrypts or blocks access to files until a user has paid a ransom (Australian Cyber Security Centre (ACSC) 2023a). Ransomware is a multi-billion-dollar global industry (Wall 2021), with attacks targeting major infrastructure, government services, businesses and individuals increasing significantly in the past decade. This increase can be attributed to many factors, including the growing reliance of individuals and organisations on their IT and data systems, which make them valuable targets to criminals (Connolly & Wall 2019), and the professional ecosystem that has grown to enable and support ransomware offenders (Wall 2021). This includes easily accessible ransomware toolkits and ransomware-as-a-service, which allow cybercriminals to launch attacks without having advanced technical knowledge themselves (Sharmeen et al. 2020).

Within this changing and growing ransomware landscape, it is crucial to understand how ransomware targets individuals and organisations, including the techniques used and the vulnerabilities exploited. Ransomware research has ballooned in the past decade, yet most of this research has focused primarily on its technical aspects, with little attention to the human factor in victimisation (Connelly & Wall 2019). In particular, few studies have examined the ransomware experiences of small to medium enterprise (SME) owners, who are at high risk of cybercrime victimisation and often have low levels of cybersecurity understanding and practices (Matthijsse et al. 2025), despite most rating cybersecurity as important (ACSC 2023b). Understanding this helps in developing effective prevention strategies and support for victims.

In the 2023 Australian Cybercrime Survey, comprising 13,887 Australian adults, nearly five percent of survey respondents had received a ransom message on their device in the preceding 12 months (Voce & Morgan 2023a). This was an increase on the estimated 2.1 percent of respondents who had received a ransom message on their device in a 2021 Australian survey (Voce & Morgan 2021). Additional analysis of data from the 2023 Australian Cybercrime Survey revealed that SME owners were more likely to have been the victim of ransomware resulting in an encrypted or disrupted device (6.2%) than SME employees (3.2%) and other respondents (1.5%).

Australian SMEs face increasingly sophisticated ransomware attacks targeting their money, data and reputation (ACSC 2023b). While some ransomware groups specialise in ‘big game hunting’, or attacks against large companies, the majority tend to target SMEs, which have less sophisticated cybersecurity yet enough revenue, data and access to other victims within their supply chain to be valuable (Wall 2021). A study of 5,600 IT professionals in medium to large organisations across 31 countries found that ransomware attacks were on the rise and their complexity and impact were increasing (Sophos 2022). From 2020 to 2021, the proportion of organisations reporting that one or more devices had been impacted by an attack in the previous year increased from 37 percent to 66 percent, and the proportion of attackers successfully encrypting data increased from 54 percent to 65 percent.

Ransomware can be spread through many different means, including phishing or spam emails, password cracking or stolen credentials, remote desktop connection, infecting legitimate websites with malicious elements like links, worms that spread malware across different devices, and ransomware exploit toolkits (Beaman et al. 2021). In Australia, malicious actors persistently scan for any networks with unpatched systems, at times seeking to use these as entry points leading to higher value targets (ACSC 2023a). In 2021–22, the majority of significant incidents ACSC responded to were due to inadequate patching (ACSC 2023a). Different types of ransomware have different impacts on systems, files and devices. Some methods can often by easily resolved (Beaman et al. 2021), while other methods are irreversible (Gómez-Hernández, Álvarez-González & García-Teodoro 2018). Others rely on manipulation and social engineering to exploit the fear of computer users, rather than locking the device or encrypting any data, and install malware that can have longer-term effects (Andronio, Zanero & Maggi 2015).

Cybercriminals are also increasingly targeting the reputation of organisations by threatening to release or sell their data. One-quarter of the ransomware reports made to the ACSC involved 'double extortion', which is when ransomware victims who experience impacts on their devices or systems are also extorted for payment to prevent the data being leaked or sold online (ACSC 2023a). This was evident in 2021 and 2022, when ransomware groups stole and released the personal information of hundreds of thousands of Australians (ACSC 2023a). Such capabilities have been in development since at least 2015, with analysis of 57 variants of ransomware indicating that cybercriminals were increasingly building information-stealing capabilities into their ransomware (Kharraz et al. 2015). Moreover, cybercrime groups have also begun 'naming and shaming' victims on public forums to increase pressure on the victim to make the ransom payment (Wall 2021). This is particularly a risk for SMEs because, aside from any impacts on business systems and devices, breaches of customer data cause significant reputational damage (Biddle, Gray & McEachern 2022).

Traditionally cybercriminals use fully automated mass distribution ransomware, which is very fast in execution and hits as many targets as possible (Brewer 2016). This method is changing, with ransomware attacks becoming more targeted at specific businesses and companies, where there is the potential for higher profits (Europol 2018). Targeted ransomware attacks involve more sophisticated attackers who spend more time investigating a targeted system's design, cause significant system and device damage and disruption, and demand larger payments from victims (Al-Hawawreh, Den Hartog & Sitnikova 2019), causing more damage than opportunistic attacks (Connolly et al. 2020). The types of systems, devices and data that can be impacted by ransomware are also becoming more diverse (Al-Hawawreh, Den Hartog & Sitnikova 2019).

We know there are certain risk factors for ransomware victimisation. Data breaches have been closely linked to ransomware attacks (Europol 2021). Analysis of 2021 survey data from the Australian public found that respondents who had been notified of a data breach were 79.5 percent more likely to have also received a ransom message on their device (Morgan & Voce 2022). Further, being the victim of ransomware once increases the likelihood of becoming a repeat victim (Barracuda 2023). In particular, paying ransoms can incentivise attackers to target victims multiple times (Department of Home Affairs 2021).

Despite this evidence, our understanding of what makes individuals and organisations fall victim to ransomware is not well developed (Holt & Bossler 2014). There is a lack of studies examining the experiences of businesses and individuals that have fallen victim to ransomware attacks (Connolly et al. 2020). We aim to address this gap by using data from a sample of 331 ransomware victims who participated in the 2023 Australian Cybercrime Survey to understand the events leading up to the incident, the vulnerabilities exploited by perpetrators and the impacts on devices, systems and data for both work-related incidents and personal incidents.

Method

Australian Cybercrime Survey

The sample for this study was drawn from the 2023 Australian Cybercrime Survey, which was a national survey of 13,887 online Australians aged 18 years and over that measured cybercrime trends, victim characteristics, help-seeking behaviour, financial losses and other harms. Questions about ransomware victimisation were included in a section of the survey focused on malware. The survey was conducted by Roy Morgan Research in early 2023 using its Single Source panel and panels managed by PureProfile and Dynata. Proportional quota sampling, a non-probability sampling method, was used to ensure the sample was demographically representative of the Australian population. Quotas were based on the Australian adult population stratified by age, sex and usual place of residence, derived from Australian Bureau of Statistics population data. The data were subsequently weighted by age, sex and usual place of residence to ensure the data were representative of the spread of the Australian population. Additional random iterative method weights were applied to correct for education level, internet use and social media use. All findings presented in this report are based on weighted data.

Respondents who said they had received a ransom message on their device in the 12 months prior to the survey were directed to an addendum with follow-up questions. Respondents were asked about the most recent incident of ransomware they had experienced, including:

- how they received the ransom message;
- what impacts occurred to their devices, systems and data around the time of receiving the message;
- the amount demanded in the ransom message and the time limit given for payment;
- their reasons for deciding to pay or not; and
- actions taken to resolve, remedy or report the incident.

Because this paper is focused on the most recent incident reported by victims rather than incidents that occurred over the previous 12 months, results differ from those reported by Voce and Morgan (2023a).

Sample

In the 12 months prior to the survey, 673 respondents had received a ransom message on their device demanding payment (with or without device disruption or compromise). Of these victims, 331 participants indicated that either of the following had occurred:

- ‘My systems, devices or files had a virus or were inaccessible (eg locked or unreadable) and I received instructions for paying a ransom to restore access’; or
- ‘My devices, servers, service or networks were disrupted (eg slowed down, lost connection, had outages) and I received instructions for paying a ransom to restore functionality.’

Victims who experienced device, system or data disruption or compromise were included in the current analysis. The remaining 342 victims, who said their data had been stolen and they had to pay to prevent the information being sold or leaked online but who did not report that their device had been disrupted or compromised, were excluded from the current study. Of the 331 victims in the current sample:

- 110 respondents (33%) owned an SME, which was defined as a business with fewer than 200 employees;
- 219 respondents (66%) did not own an SME but may have been employed by one; and
- one respondent did not indicate their employment status (and was therefore excluded from any comparative analysis).

Limitations

To identify the sample for this study, we used a bottom-up approach to asking about victimisation. This was to ensure that identifying as a victim did not rely on a non-technical audience understanding the definition of ransomware. Given that cybercriminal modus operandi are constantly changing, the incident descriptions used in this study may not fully capture every type of ransomware, and some incidents may not easily fit with these categories. Relatedly, we excluded respondents who were the victim of hacking and data extortion where there were no signs indicating malware on their devices or systems, since the focus was on pure ransomware, but we note that the experiences of this other group may be different to those reported by victims whose devices were impacted.

Although respondents were assured that their responses to the survey were anonymous and private, some respondents may nevertheless have been excluded from the current sample because of their reluctance to disclose experiences of victimisation due to shame or embarrassment. This is particularly the case for SME owners or employees who experienced a work-related ransomware attack on their business. We also note the potential limitations of relying on respondents to accurately recall information about an incident that could have occurred up to 12 months prior to the survey.

Results

Receiving the ransom message

More than half of all ransomware victims had received more than one ransom message in the 12 months prior to the survey (51.7%, see Table 1), with SME owners significantly more likely to receive multiple ransom messages than other victims (63.7% vs 46.2%; $F(1, 246)=5.35$, $p<0.05$). When asked about the most recent incident, victims most commonly received the ransom message on their mobile phone (56.0%) or laptop or computer (49.1%), and this usually came in the format of an email, text or private online chat (59.1%) or pop-up notification (48.1%). There were no significant differences between SME owners and other victims in terms of which device the ransom appeared on or format of the ransom.

Table 1: Frequency, target and format of ransom messages

	SME owner		Not an SME owner		Total	
	n	%	*n*	%	*n*	%
Number of ransom messages received in the 12 months prior to survey						
One	26	36.3	83	53.8	109	48.3
Two	18	25.9	26	16.9	44	19.7
Three	18	25.2	17	10.8	35	15.3
Four	5	7.2	14	9.0	19	8.4
Five or more	4	5.5	15	9.6	19	8.3
The device on which the victim received message/s in the most recent incident[a]						
Mobile phone	56	61.4	102	53.4	158	56.0
Laptop or computer	44	48.4	94	49.4	138	49.1
Tablet	13	13.8	17	8.9	29	10.5
Other	0	0	1	0.6	1	0.4
The format of the message/s in most recent incident[a]						
Message in an email, text or private online chat	62	66.6	102	55.3	164	59.1
Pop-up notification on device	43	45.8	91	49.2	133	48.1
Other	3	3.6	6	3.2	9	3.3

a: Respondents could select multiple response options

Note: Excludes respondents who did not answer the question

Source: Australian Cybercrime Survey 2023 [weighted data]

Events precipitating the ransomware incident

Victims were asked whether they remembered clicking on any suspicious links, pop-ups, buttons, files or attachments prior to their device being impacted (Table 2). Only 43.2 percent of victims could specifically remember clicking on any suspicious elements prior to the incident, and while the difference was not statistically significant this was more common among SME owners than other victims (53.8% vs 37.8%; $F(1, 198)=3.71$, $p=0.06$). Victims most commonly clicked on a suspicious link, pop-up, button, file or attachment on a webpage (52.6%) or in an email (42.3%), followed by a text message (33.5%), a social media post (16.0%) or a private chat platform (13.6%). There were no statistically significant differences between SME owners and other victims in where they clicked on suspicious links, pop-ups, buttons, files or attachments.

Table 2: Events precipitating the most recent ransomware incident

	SME owner		Not an SME owner		Total	
	n	%	*n*	%	*n*	%
Whether they remember clicking on a suspicious link, pop-up, button, file or attachment[a]						
Victim remembered clicking on any suspicious links, pop-ups, buttons, files or attachments	33	53.8	28	37.4	78	43.2
Where they clicked on the suspicious link, pop-up, button, file or attachment[a,b]						
On a webpage	17	51.2	17	59.8	40	52.6
In an email	13	39.9	14	50.5	32	42.3
In a text message	11	33.4	10	36.0	26	33.5
On a social media post	3	9.3	5	19.1	12	16.0
On a private chat platform	4	11.2	3	12.3	10	13.6
Other (please specify)	3	8.6	0	0	3	3.7
Data breaches						
Victim had personal data leaked in previous year	56	58.6	95	48.7	151	51.9
Previous ransom payments[c]						
Victim paid the ransom in a separate incident in the past year	15	40.5	6	10.0	21	21.5

a: Limited to respondents who said they experienced loss of device functionality, impacts on data or files, a virus or software installed on devices, or disruption to networks, servers and services (*n*=214)

b: Respondents could select multiple options. Limited to respondents who remembered clicking on a suspicious link, pop-up, button, file or attachment (*n*=78)

c: Limited to respondents who received more than one ransom message in the 12 months prior to survey (*n*=117)

Note: Excludes respondents who did not respond

Source: Australian Cybercrime Survey 2023 [weighted data]

Over half of all ransomware victims reported having had their data exposed in a data breach in the 12 months prior to the survey (51.9%). While this was more common among SME owners (58.6%) than other victims (48.7%), this difference was not statistically significant.

Among the victims who reported receiving ransom messages multiple times in the 12 months prior to survey, 21.5 percent had paid a ransom following one of these previous threats. In comparison to other victims, SME owners were much more likely to have paid the ransom in response to a previous threat (40.5% vs 10.0%; $F(1, 108)=9.37$, $p<0.01$).

Impact on devices, systems and data

As shown in Table 3, the most common impacts reported by victims were that their servers, services or networks were disrupted (37.1%); data or files on their devices were altered, removed or locked (30.1%); or the device itself lost functionality (29.6%). One in five victims stated that their device had software or a virus installed (21.9%), and a quarter said that they experienced other unspecified impacts (24.0%). There were no statistically significant differences between SME owners and other victims.

Table 3: Impacts on devices and systems at the time of receiving the ransom message

	SME owner		Not an SME owner		Total	
	n	%	*n*	%	*n*	%
My servers, service or networks were disrupted (eg slowed down, lost connection, had outages)	39	41.0	65	35.1	104	37.1
Data or files on the device(s) were altered, removed or locked (eg inaccessible or password protected)	34	35.3	51	27.4	85	30.1
The device(s) lost functionality (eg it was locked, inaccessible or password protected)	28	28.9	55	29.9	83	29.6
Software or a virus was installed on my device(s)	20	21.0	41	22.5	62	21.9
Other	22	23.3	45	24.4	67	24.0

Note: Respondents could select multiple options. Excludes respondents who did not respond

Source: Australian Cybercrime Survey 2023 [weighted data]

The devices most commonly impacted were the victim's laptop computer (46.3%), smartphone (40.7%), desktop computer (22.4%) and tablet or iPad (22.3%). Compared with other victims, SME owners were more likely to experience impacts to their smart wearables (21.5% vs 6.1%; *F*(1, 229)=8.33, *p*<0.01) and security alarms or intercom entry systems (16.7 vs 1.9%; *F*(1, 299)=19.711, *p*<0.001; Table 4).

Table 4: Devices or systems that lost functionality or connection, had a virus, or had files or data blocked

	SME owner		Not an SME owner		Total	
	n	%	*n*	%	*n*	%
Laptop computer	37	49.8	60	44.4	97	46.3
Smartphone (eg iPhone, Samsung Galaxy)	26	35.4	59	43.6	85	40.7
Desktop computer	20	27.5	26	19.6	47	22.4
Tablet or iPad	22	30.1	24	18.1	47	22.3
Smart TV	14	19.4	15	10.9	29	13.9
Smart wearables (eg Fitbit, smart watch)**	16	21.5	8	6.1	24	11.5
A gaming console connected to the internet or your TV (eg PlayStation, Xbox)	13	17.9	7	5.4	21	9.8
Modem/router	10	13.1	7	5.5	17	8.2
Smart home devices (eg Google home, Amazon Home Family)	9	12.5	7	5.3	16	7.9
Smart security/alarm/intercom entry system***	12	16.7	2.6	1.9	15	7.2
Servers or networks	5	7.0	6	4.5	11	5.4
Home automation (eg appliances, lights etc)	3	3.8	2	1.8	5	2.5
Webpages/websites	2	2.7	0	0	2	1.0
Other	0	0	1	0.9	1	0.6

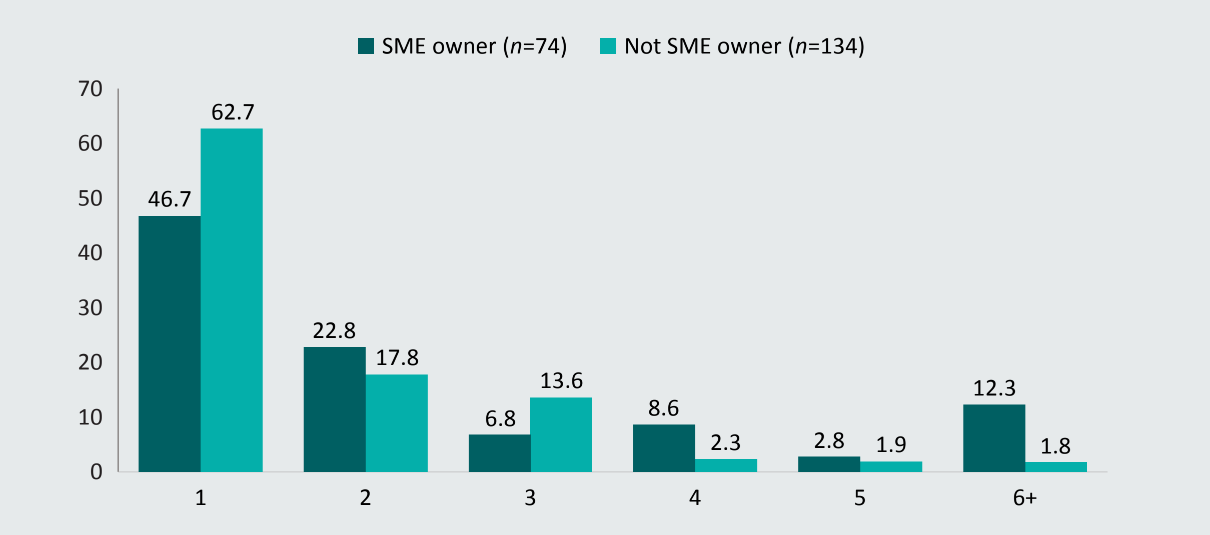
***statistically significant at *p*<0.001, **statistically significant at *p*<0.01

Note: Limited to respondents who said they experienced loss of device functionality, impacts on data or files, a virus or software installed on devices, or disruption to networks, servers and services (*n*=214). Respondents could select multiple options. Excludes respondents who did not respond

Source: Australian Cybercrime Survey 2023 [weighted data]

Overall, SME owners experienced impacts across significantly more types of devices than other victims (*F*(4, 1008)=2.90, *p*<0.05), with 23.7 percent experiencing impacts on four or more devices compared with just six percent of other victims (See Figure 1).

Figure 1: Number of device types impacted (%)



Note: Limited to respondents who said they experienced loss of device functionality, impacts on data or files, a virus or software installed on devices, or disruption to networks, servers and services (*n*=214). Excludes respondents who did not respond

Source: Australian Cybercrime Survey 2023 [weighted data]

As shown in Table 5, SME owners were significantly more likely than other victims who were currently working to report that the impacted device had been issued to them by their workplace (40.1% vs 19.5%; *F*(1, 163)=6.31, *p*<0.05) or that they used the personal device for work or business-related tasks (52.6% vs 28.1%; *F*(1, 170)=8.38, *p*<0.01). A higher proportion of SME owners said the data or files impacted by the incident were owned or used by their business or place of employment (49.2% vs 33.1%), but given the relatively small numbers this difference was not statistically significant.

Table 5: Features of ransomware incidents related to work

	SME owner		Not an SME owner		Total	
	n	%	*n*	%	*n*	%
The device impacted was issued by workplace*	26	40.1	14	19.5	41	29.2
The impacted personal device was also used for work- or business-related tasks**	36	52.6	23	28.1	59	39.1
The data or files impacted by the incident were owned or used by business or place of employment[a]	14	49.2	10	33.1	24	40.9

**statistically significant at *p*<0.01, *statistically significant at *p*<0.05

a: Limited to people who had data or files on the devices altered, removed or locked (*n*=85)

Note: Limited to respondents who were currently working (*n*=251). Limited to respondents who said they experienced loss of device functionality, impacts on data or files, a virus or software installed on devices, or disruption to networks, servers and services (*n*=214). Excludes respondents who did not respond

Source: Australian Cybercrime Survey 2023 [weighted data]

Victims who indicated that the ransomware event was work-related were asked whether the ransomware had spread to other devices, systems or email accounts in their workplace. SME owners were significantly more likely than other victims to report that the ransomware had spread to other workplace devices, systems or email accounts (52.5% vs 24.0%; $F(1, 86)=6.32$, $p<0.05$).

Features of the threats

Nearly a third of ransomware victims (29.6%) were threatened that their stolen data would be sold or shared if they did not pay the ransom. This was similar for SME owners (31.7%) and other victims (28.6%).

Ransomware perpetrators demanded payments in money, cryptocurrency and gift cards. The median total amount demanded was $300 for SME owners and $758 for other respondents. The mean value demanded was higher for SME owners ($12,287) than for respondents who were not SME owners ($7,213) for although this difference was not statistically significant (see Table 6).

Table 6: Ransom amounts and forms of payment demanded

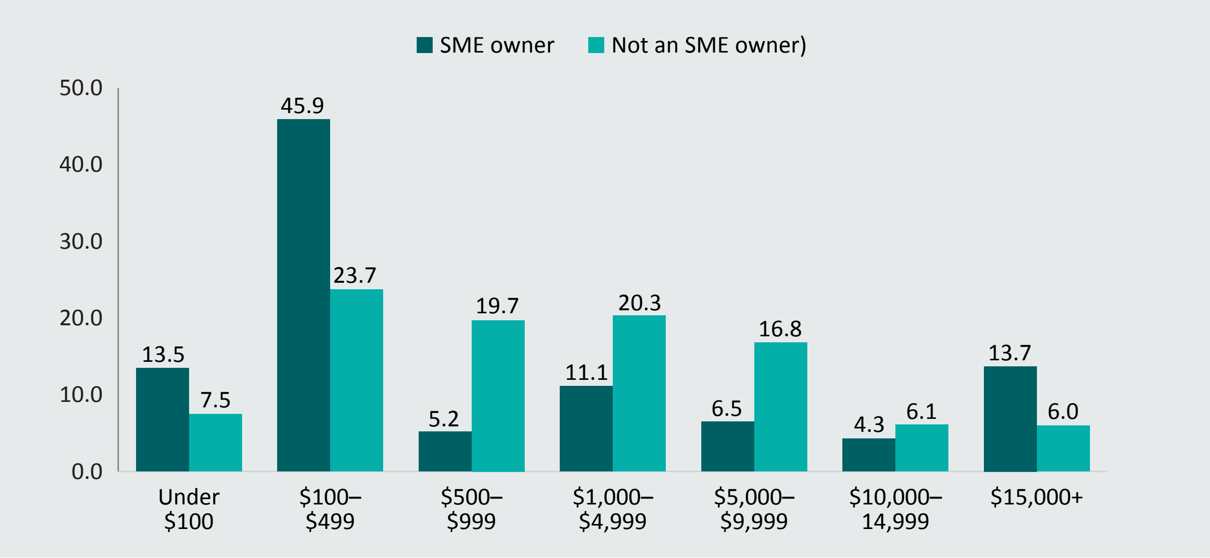
		SME owner	Not an SME owner	Total
Money	Median (mean)	$100 ($4,723)	$500 ($3,346)	$500 ($3,779)
	Range	$2–$50,000	$3–$100,000	$2–$100,000
Cryptocurrency	Median (mean)	$100 ($9,845)	$986 ($13,385)	$500 ($11,986)
	Range	$5–$500,000	$5–$350,000	$5–$500,000
Gift cards	Median (mean)	$100 ($1,714)	$100 ($734)	$100 ($1,184)
	Range	$1–$20,000	$1–$6,999	$1–$20,000
Total	Median (mean)	$300 ($12,287)	$758 ($7,213)	$555 ($8,728)
	Range	$1–$500,000	$3–$350,000	$1–$500,000

Note: No statistically significant differences were found between SME owners and other respondents. Excludes 169 respondents who did not respond (62 SME owners, 106 respondents who were not SME owners and 1 respondent who did not indicate whether they owned an SME)

Source: Australian Cybercrime Survey 2023 [weighted data]

The amounts demanded of SME owners were relatively small, with 59.4 percent being asked to pay less than $500 (see Figure 2). A small proportion of SME owners received demands for sums of $15,000 or more (13.7%). The amounts demanded of victims who were not SME owners varied greatly, with 80.5 percent of ransoms falling between $100 and $9,999. These differences in the ransom demands received by SME owners and other victims were statistically significant ($F(6, 1005)=3.38$, $p<0.01$).

Figure 2: Ransom amounts demanded (%)



Note: Excludes respondents who did not respond

Source: Australian Cybercrime Survey 2023 [weighted data]

Victims were asked whether the ransom message had given them a time limit within which to pay (see Table 7). Half of the ransom messages to SME owners (49.5%) gave a time limit, compared with 39 percent of messages to other victims. Of the 109 victims who were given a time limit for payment, SME owners were given significantly longer timeframes than victims who were not SME owners (median 30 days vs 1 day; *B*=0.004, *F*(1, *n*=102)=14.88, *p*<0.001).

Table 7: Time given for ransom payments

		SME owner	Not an SME owner	Total
Days	Median (mean)	30 (52)	1 (7)	2 (23)
	Range	0–360	0–68	0–360

Note: Excludes respondents who did not respond

Source: Australian Cybercrime Survey 2023 [weighted data]

Finally, victims were asked whether they had paid or attempted to pay the ransom in the most recent incident. Overall, relatively few respondents indicated that they had actually paid the ransom (12.2%). However, SME owners were more likely than other respondents to have paid the ransom (22.6% vs 7.8%, *F*(1, 307)=10.22, *p*<0.01).

Discussion

This paper draws on data from a sample of 331 Australian ransomware victims to better understand how ransomware attacks occur, how victims are targeted and the vulnerabilities exploited by cybercriminals. We had a specific focus on SME owners in light of recent evidence showing they are being targeted more often than large companies (Wall 2021), with attacks that are increasingly frequent, sophisticated and harmful (ACSC 2023b; Sophos 2022).

Typically, ransom messages first appeared on the victim's mobile phone or computer in the form of an email, text message or private online chat. More than half of all ransomware victims had been contacted multiple times over the previous 12 months with threats and demands for payment. This was significantly more common for SME owners, with nearly two-thirds being contacted more than once and more than third contacted three or more times. Importantly, over 40 percent of SME owners had paid in response to one of these previous ransom messages, a significantly higher proportion than among other victims. SME owners were also more likely to have paid following the most recent ransomware incident. This fuels the ransomware business model and can make SME owners appear to be easy to scare and manipulate, increasing their chances of repeat victimisation. Cybercriminals reportedly share between themselves 'sucker lists' of individuals and organisations who have made previous payments (Connolly & Borrion 2022). For this reason, along with the lack of a guarantee that files and systems will be restored and data will not be sold or shared, the Australian Government's advice is to never pay a ransom (ACSC 2023c). Stronger messaging is needed to ensure that SME owners understand and follow this advice.

More than half of all ransomware victims could not remember clicking on any suspicious links, pop-ups, buttons, files or attachments prior to their device being impacted. This speaks to the sophistication of malware attacks, which makes it increasingly hard to spot malicious elements hidden in websites, texts, emails and social media posts. The impacts may not be felt until days or weeks later, meaning attributing the ransomware attack to clicking on something specific can be difficult. For those who could remember, the suspicious element was most commonly in a webpage or email. Ransomware infections through email and webpages are common (Beaman et al. 2021), and prevention requires a combination of technological and human defences. There was some evidence that SME owners were more likely to have clicked on suspicious elements. Business owners are easily identifiable targets as they often have a more visible online presence than other potential victims. Many have public-facing websites, social media pages and email addresses, allowing anyone to contact the business for quotes or enquiries. Preventing ransomware attacks against small business requires cybersecurity measures, but there is an important human element.

Third-party data breaches were a common concurrent event for this sample of ransomware victims. Over half of the sample had experienced a third-party data breach in the 12 months prior to the survey, which is higher than the prevalence across the general Australian Cybercrime Survey sample, of whom 33.6 percent had experienced a data breach (Voce & Morgan 2023a). This is consistent with research showing that third-party data breaches significantly increase the likelihood of ransomware victimisation (Morgan & Voce 2022). A recent survey by the Office of the Australian Information Commissioner (2023) found that 52 percent of victims of third-party data breaches reported an increase in calls and spam texts, which can include hidden malware. Reducing data breaches and putting in place measures to protect affected individuals will help reduce ransomware victimisation.

Business owners experienced far-reaching impacts on their devices, with a higher number of devices and multiple types of devices impacted. These were most often laptop computers and smartphones; however, SME owners were significantly more likely to experience impacts to their smart wearables and security alarms and intercom entry systems—the latter posing clear risks to the physical security of their business. SME owners were also more likely to report that the impacted device had been issued to them by their workplace or that they used a personal device for work- or business-related tasks. They were also more likely to report that the ransomware had spread to other workplace devices, systems or email accounts.

Taken together, these findings reflect the variety of devices and systems that SME owners now use for personal and work-related tasks. With the growing availability of connected devices and systems, SME owners are using this technology to increase collaboration, productivity and revenue (AlphaBeta 2019). Almost all Australian businesses are connected to the internet, more than half have adopted cloud technology and over half have a web presence (Productivity Commission 2023), with one in three SMEs receiving orders via online platforms (AlphaBeta 2019). SMEs are constantly under pressure to be innovative and responsive and are increasingly connected to their customers, employees and supply chain (Baillette & Barlette 2018). They also have more difficulty managing information security because they lack technical and financial resources, and are increasingly targeted by cybercriminals because they can exploit their security weaknesses to access larger organisations of greater interest (Baillette & Barlette 2018).

SMEs and their employees often use their personal devices for work, including personal laptops, tablets and mobile phones. This phenomenon has been termed BYOD (bring your own device), and has become popular in recent years, particularly since working from home became common during the COVID-19 pandemic. While BYOD practices offer flexibility and productivity, they are considered one of the greatest security threats faced by SMEs (Baillette & Barlette 2018). When SME owners moved to working from home during the pandemic, their risk of falling victim to cybercrime increased (Voce & Morgan 2023b). When employees are using their own devices, they may not update the software (Singh 2012) and may be less likely to comply with internal security rules or policies (Hovav & Putri 2016). Guidance on how to manage BYOD-related security issues, especially for those working from home, may help mitigate these risks.

Cybercriminals draw on a number of techniques to extract payment from victims. This includes double extortion, where cybercriminals extort the victim for both device decryption and the non-publication of data. Nearly one-third of all victims were threatened that their stolen data would be sold or shared if they did not pay the ransom. This is higher than previous estimates (closer to one in eight, see Voce & Morgan 2023a), which highlights the importance of asking ransomware victims specifically about the threat of double extortion. Effective information management and data security practices may help better prepare individuals and SME owners for ransomware attacks and ensure they have the confidence to respond appropriately to the threat of double extortion attempts.

Taken as a whole, this study illustrates the vulnerabilities among Australian computer users to the threat of ransomware. Consistent with international research (Matthijsse et al. 2025; Wall 2021), we found that SME owners are viewed as lucrative targets and are especially vulnerable. Efforts to reduce ransomware targeting small businesses (and to limit the potential flow-on consequences for larger organisations that could be infiltrated) need to raise awareness of the ways in which ransomware attacks often happen. This includes education on how to spot suspicious links in emails or on websites, how to respond appropriately to third-party data breaches, and what security measures should be implemented when working from home or using personal devices for work. This also includes supporting victims to identify and remove malware that has spread across devices and systems, and options to mitigate the situation that do not include paying the ransom. This study also makes clear that awareness-raising efforts alone may be insufficient to prevent attacks, meaning there must also be technological solutions that can help protect business owners and avoid the wide-ranging harms that can be inflicted on small businesses (Voce & Morgan 2023a).

References

URLs correct as at July 2025

Al-Hawawreh M, Den Hartog F & Sitnikova E 2019. Targeted ransomware: A new cyber threat to edge system of Brownfield Industrial Internet of Things. *IEEE: Internet of Things Journal* 6(4): 7137–7151. https://doi.org/10.1109/JIOT.2019.2914390

AlphaBeta 2019. Australia's digital opportunity: Growing a $122 billion a year industry. https://digi.org.au/digitalopportunity/

Andronio N, Zanero S & Maggi F 2015. HelDroid: Dissecting and detecting mobile ransomware. In H Bos, F Monrose & G Blanc (eds), *Research in attacks, intrusions, and defenses*. https://www.springerprofessional.de/en/heldroid-dissecting-and-detecting-mobile-ransomware/6878340

Australian Cyber Security Centre (ACSC) 2023a. *ASD cyber threat report 2022–2023*. Canberra: ACSC. https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

Australian Cyber Security Centre (ACSC) 2023b. *Cyber security and Australian small businesses: Results from the Australian Cyber Security Centre Small Business Survey*. Canberra: ACSC. https://www.cyber.gov.au/sites/default/files/2023-03/2023_ACSC_Cyber%20Security%20and%20Australian%20Small%20Businesses%20Survey%20Results_D1.pdf

Australian Cyber Security Centre (ACSC) 2023c. *So, you've been held to ransom?* Canberra: ACSC. https://www.cyber.gov.au/sites/default/files/2023-03/ACSC_Ransomware_Emergency_Response_One_Page_Guide.pdf

Baillette P & Barlette Y 2018. BYOD-related innovations and organizational change for entrepreneurs and their employees in SMEs. *Journal of Organizational Change Management* 31(4): 839–851. https://doi.org/10.1108/JOCM-03-2017-0044

Barracuda 2023. *2023 ransomware insights: The prevalence and impact of ransomware attacks around the world*. https://www.barracuda.com/reports/ransomware-insights-report-2023

Beaman C et al. 2021. Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security* 111: 102490. https://doi.org/10.1016/j.cose.2021.102490

Biddle N, Gray M & McEachern S 2022. *Public exposure and responses to data breaches in Australia: October 2022*. ANU Centre for Social Research and Methods. Canberra: Australian National University. https://polis.cass.anu.edu.au/research/publications/public-exposure-and-responses-data-breaches-australia-october-2022

Brewer R 2016. Ransomware attacks: Detection, prevention and cure. *Network Security* 9: 5–9. https://doi.org/10.1016/s1353-4858(16)30086-1

Connolly AY & Borrion H 2022. Reducing ransomware crime: Analysis of victims' payment decisions. *Computers & Security* 119: 102760. https://doi.org/10.1016/j.cose.2022.102760

Connolly LY & Wall DS 2019. The rise of crypto-ransomware in a changing cybercrime landscape: Taxonomising countermeasures. *Computers & Security* 87: 101568. https://doi.org/10.1016/j.cose.2019.101568

Connolly LY, Wall DS, Lang M & Oddson B 2020. An empirical study of ransomware attacks on organizations: An assessment of severity and salient factors affecting vulnerability. *Journal of Cybersecurity* 6(1). https://doi.org/10.1093/cybsec/tyaa023

Department of Home Affairs 2021. *Ransomware Action Plan*. Canberra: Department of Home Affairs. https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/australias-ransomware-action-plan

Europol 2021. *Internet organised crime threat assessment 2021*. https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021

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

Gómez-Hernández J, Álvarez-González L & García-Teodoro P 2018. R-Locker: Thwarting ransomware action through a honeyfile-based approach. *Computers & Security* 73: 389–398. https://doi.org/10.1016/j.cose.2017.11.019

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

Hovav A & Putri FF 2016. This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing* 32: 35–49. https://doi.org/10.1016/j.pmcj.2016.06.007

Kharraz A, Robertson W, Balzarotti D, Bilge L & Kirda E 2015. Cutting the Gordian knot: A look under the hood of ransomware attacks. In M Almgren, V Gulisano & F Maggi (eds), *Detection of intrusions and malware, and vulnerability assessment*: 3–24. https://doi.org/10.1007/978-3-319-20550-2_1

Matthijsse SR, Moneva A, van 't Hoff-de Goede MS & Leukfeldt ER 2025. Examining ransomware payment decision-making among small- and medium-sized enterprises. *European Journal of Criminology* 22(4): 625–645. https://doi.org/10.1177/14773708241285671

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

Office of the Australian Information Commissioner 2023. *Notifiable data breaches report: January to June 2023.* Sydney: OAIC. https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-publications/notifiable-data-breaches-report-january-to-june-2023

Productivity Commission 2023. *5-year Productivity Inquiry: Australia's data and digital dividend*. Inquiry report vol 4. Canberra: Productivity Commission. https://www.pc.gov.au/inquiries/completed/productivity/report

Sharmeen S, Ahmed YA, Huda S, Koçer BŞ & Hassan MM 2020. Avoiding future digital extortion through robust protection against ransomware threats using deep learning based adaptive approaches. *IEEE Access* 8: 24522–24534. https://doi.org/10.1109/ACCESS.2020.2970466

Singh N 2012. B.Y.O.D. Genie is out of the bottle – 'devil or angel'. *Journal of Business Management & Social Sciences Research* 1(3): 1–12

Sophos 2022: *The state of ransomware*. https://www.sophos.com/en-us/whitepaper/state-of-ransomware

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

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

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

Wall DS 2021. The transnational cybercrime extortion landscape and the pandemic: Changes in ransomware offender tactics, attack scalability and the organisation of offending. *European Law Enforcement Research Bulletin*, Special Conference edition No. 5. https://ssrn.com/abstract=3908159

Isabella Voce is a Principal Research Analyst in the Serious and Organised Crime, Cybercrime and Radicalisation Research Program at the Australian Institute of Criminology.

Anthony Morgan is Research Manager of the Serious and Organised Crime, Cybercrime and Radicalisation Research Program at the Australian Institute of Criminology.

General editor, *Trends & issues in crime and criminal justice* series: Dr Rick Brown, Deputy Director, Australian Institute of Criminology. Note: *Trends & issues in crime and criminal justice* papers are peer reviewed. For a complete list and the full text of the papers in the *Trends & issues in crime and criminal justice* series, visit the AIC website: www.aic.gov.au

ISSN 1836-2206 (Online) ISBN 978 1 922878 10 6 (Online)

https://doi.org/10.52922/ti78106

GPO Box 1936
Canberra ACT 2601, Australia

Tel: 02 6268 7166

Disclaimer: This research paper does not necessarily reflect the policy position of the Australian Government