Australian Government
Australian Institute of Criminology

Trends & issues in crime and criminal justice

No. 675

Online behaviour, life stressors and profit-motivated cybercrime victimisation

Isabella Voce and Anthony Morgan

Abstract | This study analyses data from a survey of Australian adult computer users conducted in June 2021 to examine the influence of online routine activities and life stressors on the likelihood of profit-motivated cybercrime victimisation.

Compared with non-victims, victims spent more time online, more frequently engaged in recreational online activities and were more likely to employ higher-risk online practices. Small-to-medium enterprise owners working from home were more likely to be victims. Respondents who had experienced recent increases in financial stress and gambling and negative impacts on interpersonal relationships during the COVID-19 pandemic were also more likely to be a victim of cybercrime.

Being accessible online and a lack of personal and physical guardianship are associated with an increased risk of being a victim, but other factors may influence the susceptibility of computer users to cybercrime victimisation. This has important implications for cybercrime responses.

Cyber-enabled and cyber-dependent crimes pose a growing threat to the safety of individuals and businesses online. In the 2021–22 financial year the Australian Cyber Security Centre (ACSC 2022) received over 76,000 reports of cybercrime, an increase of nearly 13 percent from the previous financial year. The COVID-19 pandemic was associated with increases in reports of phishing and identity theft (ACCC 2021), ransomware (ACSC 2021), certain forms of hacking (Buil-Gil et al. 2021), and many types of cyber-enabled fraud (Buil-Gil, Zeng & Kemp 2021). The growing threat posed by cybercrime has recently led to significant government investment in enhanced cybersecurity capabilities and in law enforcement.

Serious & Organised Crime
Research Laboratory

At the same time, there is an important human factor in cybercrime victimisation, with some computer users more vulnerable to becoming a victim than others. Routine activity theory (Cohen & Felson 1979) describes how daily activities bring about three situational criteria necessary for a crime to occur: a suitable target, a motivated offender and the absence of capable guardianship. In the case of cybercrime, targets can include personal information or financial assets, while guardians may include computer users, antivirus software, identity authentication, or third parties such as network administrators and financial institutions (Leukfeldt & Yar 2016; Reyns 2018; Williams 2016).

While routine activity theory has its limitations—such as its inability to explain why certain individuals are motivated to offend, and challenges associated with translating key concepts to the online environment—it has been shown to be a useful lens through which to understand cybercrime victimisation (Reyns 2018). For example, research has consistently shown the importance of the visibility of potential targets—by virtue of the amount and type of online activity—in determining the risk of victimisation for different types of cybercrime (Leukfeldt & Yar 2016). Online forums, pornography websites, online gambling, dating websites, online gaming and online purchases are all associated with fraud and scam victimisation (Gainsbury, Browne & Rockloff 2018; van Wilsem 2013; Whitty 2019). Identity theft victimisation has been linked to online shopping, banking, emailing or instant messaging and downloading behaviours (Reyns 2013; Williams 2016). Malware and ransomware victimisation have also been linked to the frequency of internet use, number of internet devices, and online activities such as illegal downloading, using dating websites and blogging (Bergmann et al. 2018; Bossler & Holt 2010; Holt et al. 2020).

While there are risks associated with online routine activities, these risks are not evenly distributed among all computer users. Some individuals may be more vulnerable to victimisation than others. Some studies have linked cybercrime risk to low self-control (Holt et al. 2020; van Wilsem 2013; Whitty 2019), emotional instability, higher openness to experience and lower conscientiousness (van de Weijer & Leukfeldt 2017). Yet these factors may be difficult to modify, as research shows that personality and self-control are relatively fixed risk factors for most people, at least in the short term (Cobb-Clark, Kong & Schildberg-Hörisch 2021; Roberts 2009). Prior research has also produced mixed results as to the importance of these individual factors (Bossler & Holt 2010; Ngo & Paternoster 2011).

Recent life stressors may also increase vulnerability to cybercrime victimisation but have received less empirical attention. Online fraud victimisation has been linked with negative life events such as divorce, the death of a family member or close friend, injury or illness in one's family and job loss (Anderson 2013; Emami, Smith & Jorna 2019; Ross & Smith 2011). These types of events can lead to social isolation, loneliness and reduced psychological wellbeing, which can further increase vulnerability to financial exploitation and scams (James, Boyle & Bennett 2014). Socially isolated individuals may be unable to seek advice about scams from friends and family or be more open to engaging with strangers to fulfil social needs (Lee & Soberon-Ferrer 1997). Additionally, individuals who are stressed tend to make poorer decisions (Wemm & Wulfert 2017), with research showing that decision-making is negatively affected by sad emotional states (Baumeister et al. 2005; Lerner, Li & Weber 2012). None of this is intended to blame victims; rather, motivated offenders exploit the susceptibility of victims through manipulation, persuasion and coercion, making it hard to distinguish legitimate from illegitimate exchanges or determine whether a scenario is likely to be harmful (Carter 2023; Cross 2015).

The importance of understanding the intersection between online routine activities and the vulnerabilities of potential targets was particularly evident during the COVID-19 pandemic. The pandemic and associated containment measures brought about significant, abrupt changes in online activities. Many employees transitioned to working from home (WFH; Baxter & Warren 2021), including many small business operators, using their home internet connections and personal devices to undertake work tasks (Nabe 2021). This increased the accessibility of targets while simultaneously lowering capable guardianship. At the same time, there was significant concern during the COVID-19 pandemic about profit-motivated offenders exploiting the fear and anxiety that make individuals susceptible to scams, as evidenced by the large volumes of malicious emails and text messages with pandemic-related themes (ACSC 2021).

In this study, we explored how the significant changes in the online routine activities of computer users during the pandemic, coupled with the effects of the psychological, social and economic stress of the pandemic, influenced the risk of cybercrime victimisation. In doing so, we provide important insights into the human factor in profit-motivated cybercrime victimisation and identify several implications for prevention.

Method

This study used data collected as part of the Australian Institute of Criminology's pilot Australian Cybercrime Survey to examine the relationship between past-year profit-motivated cybercrime victimisation, the routine activities of computer users and presence of life stressors. The pilot survey asked 15,000 members of the public in June 2021 about a range of experiences related to cybercrime victimisation, reporting behaviour, risk factors for victimisation, and harms resulting from victimisation, as well as sociodemographic information. While this was a cross-sectional survey, we capitalised on the fact that the survey covered the first year of the pandemic and captured information about changes to respondents' online routine activities and individual circumstances.

Non-proportional quota-based sampling was used to ensure the sample was representative of the spread of the Australian population. Invitations to the survey were sent to 171,537 individuals who were members of a panel managed by 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). Post-stratification weights based on jurisdiction, age and sex were applied to male and female respondents using Australian Bureau of Statistics demographic data as of December 2020 (ABS 2021). Despite processes that excluded poor-quality responses from the total sample, six respondents were removed from the sample for providing illogical responses which implied they were answering the questions randomly, resulting in a final survey sample of 14,994 respondents. For further details on the sampling and weighting of the data used in this study, see the method section of Voce and Morgan (2021).

Changes to working arrangements during the pandemic, including WFH and work-related hours spent on the internet, represented a major shift in the routine activities of computer users. To explore how this may have influenced cybercrime risk, we limited the sample to respondents who were employed at the time of the survey (*n*=9,827). We then excluded respondents with missing data for any of the main variables of interest, resulting in a final sample of 8,914 respondents included in the study.

Data on risky online activities, the impacts of the pandemic and victimisation accounted for the largest proportion of missing data. We did not use missing data imputation because there is a strong possibility that missing data was correlated with the likelihood of the response to sensitive questions (eg victims being more likely to refuse to answer questions about their victimisation, or people who engaged in risky online behaviour being unwilling to admit that). We note the risk of bias and do not assume results from the regression model would apply equally to excluded respondents.

Dependent variables

The dependent variables in this study were whether, in the 12 months prior to the survey, the respondent was a victim of the following broad crime types, typically motivated by financial gain:

- identity theft, compromise or misuse (hereafter referred to as identity crime and misuse);
- malware; or
- fraud and scams.

We adopted a bottom-up approach that sought to capture a wide range of cybercrime modus operandi. For each broad crime type, individuals were presented with a list of incidents or symptoms associated with being a victim, and were categorised as a victim if they had experienced at least one incident or symptom related to that type of cybercrime. For identity crime and misuse, the victim had to suspect these issues were the result of a privacy breach or information compromise. For malware, victims had to believe the issues were not just the result of genuine device malfunction or aging.

Independent variables

We included several main variables of interest in our analysis. The first set related to the social, economic and psychological stress associated with the pandemic. Respondents were asked whether the COVID-19 pandemic had impacted them in the following ways at any point since early 2020, even if their current situation had improved:

- they had experienced an increase in financial stress;
- they had become more socially isolated;
- they had increased the amount of time or money they gambled;
- their relationships with family and friends had been negatively impacted;
- they had experienced mental or emotional distress;
- their overall physical health and wellbeing had deteriorated; and
- they had increased their consumption of alcohol or other drugs.

Responses to these questions were based on a five-point Likert scale (strongly disagree to strongly agree). For the purpose of analysis, these variables were all recoded as binary variables (0=no, 1=yes).

We also included several variables that related to the routine online activities of computer users. These included measures relating to the accessibility of computer users as potential targets, based on the extent and type of internet use:

- the average number of hours on a normal business day spent using the internet for work-related purposes (continuous variable);
- the average number of hours per day spent using the internet for personal use (continuous variable);
- the frequency with which they engaged in certain online activities in the previous 12 months, including using online blogs, forums and interest groups; purchasing items from online marketplaces or online stores; being active on romance or dating websites or apps; participating in online gaming or esports; and accessing sexually explicit adult websites or subscribing to sexually explicit interactive adult platforms (five-point scale ranging from daily to never, recoded to 0=less than weekly, 1=daily or weekly basis).

We included two measures of guardianship. The first related to personal guardianship—namely, whether the respondent had engaged in any risky online behaviours in the previous 12 months, based on their responses to questions about whether they had opened emails from unknown people or organisations, shared passwords with someone they knew, and used freely available wi-fi in public locations to conduct financial transactions (0=no, 1=yes).

The second was a measure of physical guardianship. We measured whether respondents were WFH at any point because of pandemic-related social distancing measures (0=no, 1=yes). Home internet connections may be less secure than those of workplaces, devices may no longer be protected by corporate security controls or may not get the updates and patching they need, and sensitive work information may be stored on or shared over unsecure personal devices.

Finally, we included a variable to identify small-to-medium enterprise (SME) owners and employees, and several socio-demographic variables including gender, age and relationship status, as these have been identified as correlates of cybercrime victimisation (Jorna & Hutchings 2013).

Analytic strategy

Following similar studies of cybercrime victimisation (Mikkola et al. 2020; Ngo & Paternoster 2011; Reyns 2013), we used logistic regression to measure the relationships between main variables of interest and the likelihood of past-year victimisation while controlling for other factors. The analysis was undertaken using weighted data. Model fit was assessed using a modified version of the Hosmer–Lemeshow goodness-of-fit test, which estimates the *F*-adjusted mean residual test following the estimation of logistic regression models using survey commands in Stata (Archer & Lemeshow 2006). Because there is evidence this test is susceptible to bias in large samples (Nattino, Pennell & Lemeshow 2020), further link tests were conducted to assess the goodness-of-fit. This test is used to detect specification errors and assumes that in a properly specified model it would not be possible to identify additional significant independent variables (Pregibon 1979). A weighted area under the receiver operating characteristic curve (AUROC) was also calculated for logistic regression models using Somers' *D* (Newson 2006).

For identity crime and misuse, initial model fit diagnostics indicated the model was not properly specified. An interaction between the variables WFH and SME ownership/employment was included and further tests revealed the revised model was a good fit for the data. The same interaction effect included in the other models and was also statistically significant.

Limitations

Online panels allow for rapid collection of data from large samples, which is particularly useful where the main population of interest is computer users. However, while the sample is large and representative of the spread of the Australian population, we are cautious not to generalise the results to the wider population, or assume the results are representative of non-respondents.

As this study uses cross-sectional data, the temporal order and causal relationships between the independent variables and outcomes of interest cannot be established. For instance, in the case of an association between psychosocial life stressors and cybercrime victimisation, these stressors may be both a risk factor for and consequence of being a victim. We attempted to overcome this by asking specifically about the effects of the COVID-19 pandemic. Similarly, it was not possible to compare respondents' online behaviour before and after the pandemic. While there is clear evidence that people's online behaviour changed during the pandemic, we can only highlight those behaviours that were associated with an increased risk of victimisation.

Results

Sample characteristics

In the past year, 28 percent (*n*=2,479) of the study sample had been a victim of identity crime and misuse, 22 percent (*n*=1,965) had been a malware victim, and 10 percent (*n*=912) had been a fraud or scam victim. Many victims of profit-motivated cybercrime had experienced more than one form of cybercrime in the previous 12 months. Thirty-five percent of victims said they experienced two or more forms of profit-motivated cybercrime (*n*=1,262) with 13 percent experiencing all three forms of cybercrime victimisation (*n*=483). This is not surprising, given that they are frequently interrelated (eg offenders may use an identity theft victim's personal information to carry out fraud or scams).

Sample characteristics for respondents included in the current study are presented in Table 1 (*n*=8,914). Fifty-three percent of the sample were male, 36 percent were aged 18 to 34 years, and 22 percent owned an SME. Pandemic-related stressors were common among respondents, including increases in social isolation (49%), mental or emotional distress (42%), deterioration in physical health and wellbeing (34%), increases in financial stress (33%), negative impacts on personal relationships (27%), and increases in alcohol and/or drug use (24%) and gambling (12%). Fifty-eight percent of respondents were WFH at some point in the previous year as a result of COVID-19 related social distancing measures.

In terms of the online behaviour of respondents, 28 percent frequently used online blogs, forums or interest groups; 38 percent frequently purchased items from online marketplaces or online stores; 11 percent were frequently active on romance and dating websites or apps; 17 percent frequently participated in online gaming or esports; and 22 percent frequently accessed sexually explicit adult websites or subscribed to sexually explicit interactive adult platforms. Twenty-eight percent of respondents had engaged in at least one risky online behaviour in the previous 12 months.

Table 1: Sample characteristics (*n*=8,914)

		(*n*)	%
Gender	Male	4,703	52.8
	Female	4,211	47.2
In a current relationship		5,842	65.5
Age	18–34 years	3,184	35.7
	35–64 years	5,186	58.2
	65+ years	544	6.1
Owns or operates an SME	SME owner	1,924	21.6
	SME employee	2,597	29.1
	Not an SME owner nor employee	4,394	49.3
Mean work hours using internet (*SD*)		4.68 (3.37)	
Mean personal hours using internet (*SD*)		3.74 (2.93)	
Risky online practices in past year		2,454	27.5
Online activities undertaken daily or weekly (vs less frequently)	Online blogs, forums, interest groups	2,527	28.4
	Purchasing from online marketplaces/stores	3,355	37.6
	Romance/dating websites or apps	971	10.9
	Online gaming/esports	1,550	17.4
	Sexually explicit adult websites or platforms	1,926	21.6
Negative impacts of pandemic experienced	Increase in financial stress	2,913	32.7
	More socially isolated	4,342	48.7
	Increased time and/or money gambling	1,089	12.2
	Negative impact on relationships with family and friends	2,368	26.6
	Mental or emotional distress	3,780	42.4
	Physical health and wellbeing deteriorated	3,057	34.3
	Increased consumption of alcohol or other drugs	2,170	24.3
WFH due to pandemic		5,183	58.1

Note: From the sample presented in Table 1, 272 respondents were excluded from the identity crime and misuse model, 423 respondents were excluded from the malware attacks model, and 196 respondents were excluded from the fraud/scams model due to data missing on the outcome variable. These respondents are included in the denominator for the prevalence rates reported in text. SME=small to medium enterprise

Source: AIC pilot Australian Cybercrime Survey, 2021

Multivariable analysis

Results from the three multivariate logistic regression models—for identity crime and misuse (model 1), malware attacks (model 2) and fraud and scams (model 3)—are presented in Table 2. We summarise the results for the main variables of interest below.

Respondents who reported engaging in risky online practices were more likely to have been a victim of identity crime and misuse (adjusted odds ratio (AOR)=1.54), malware (AOR=1.61) and fraud (AOR=1.53) than those who had not engaged in these behaviours in the last year (reference category). The number of hours respondents spent online in their personal time was a statistically significant predictor of fraud victimisation (AOR=1.05), as was the number of hours spent online for work (AOR=1.05). For every hour of personal time spent online, the odds that a respondent would fall victim to fraud increased by five percent.

Respondents who frequently used online blogs, forums and interest groups were significantly more likely to experience identity crime and misuse (AOR=1.24) but not malware or fraud. Frequently purchasing items from online marketplaces or online stores was also a significant predictor of identity crime and misuse (AOR=1.32), malware (AOR=1.32) and fraud (AOR=1.57). Frequently being active on romance and dating websites or apps was also a significant predictor of identity crime and misuse (AOR=1.46), malware (AOR=1.46) and fraud (AOR=2.21). Frequently participating in online gaming or esports was a significant predictor of malware (AOR=1.34) and fraud (AOR=1.52) but not identity crime and misuse. Similarly, frequently accessing sexually explicit adult websites or subscribing to sexually explicit interactive adult platforms was a significant predictor of malware (AOR=1.25) and fraud (AOR=1.50) but not identity crime and misuse.

Social, psychological and economic stressors were associated with all three types of victimisation. Respondents who spent an increased amount of time or money gambling were significantly more likely to experience identity crime and misuse (AOR=1.24), malware (AOR=1.59) and fraud (AOR=2.16). Respondents who experienced increased financial stress were more likely to have experienced identity crime and misuse (AOR=1.13), malware (AOR=1.32) and fraud victimisation (AOR=1.59). Respondents who experienced negative impacts on their relationships with family and friends were also significantly more likely to experience identity crime and misuse (AOR=1.16), malware (AOR=1.29) and fraud (AOR=1.46). Respondents who had increased their consumption of alcohol or other drugs were significantly more likely to experience identity crime and misuse (AOR=1.28) and malware (AOR=1.25) but not fraud. Deteriorating physical health and wellbeing was also associated with malware victimisation (AOR=1.22).

Table 2: Logistic regression model predicting profit-motivated cybercrime victimisation in the 12 months prior to the survey

		Model 1: Identity crime and misuse (*n*=8,644)		Model 2: Malware attacks (*n*=8,491)		Model 3: Fraud or scams (*n*=8,719)	
Variable		**AOR**	**95% CI**	**AOR**	**95% CI**	**AOR**	**95% CI**
Male (vs female)		1.00	0.90, 1.12	0.94	0.83, 1.06	1.08	0.90, 1.29
Current relationship (vs not in current relationship)		1.09	0.98, 1.22	1.17*	1.03, 1.33	1.13	0.95, 1.35
Age (vs 18–34 years old)	35–64 years	0.81**	0.72, 0.91	0.67***	0.59, 0.77	0.67***	0.56, 0.81
	65+ years	1.10	0.88, 1.39	0.87	0.67, 1.13	0.90	0.59, 1.37
Owns or operates an SME (vs neither)	SME owner	1.21	0.97, 1.53	1.75***	1.37, 2.24	1.52*	1.10, 2.11
	SME employee	1.04	0.86, 1.26	1.32*	1.07, 1.64	0.89	0.65, 1.23
Work hours using internet (continuous variable)		1.01	0.99, 1.03	1.01	0.99, 1.02	1.05***	1.02, 1.08
Personal hours using internet (continuous variable)		1.01	0.99, 1.03	1.02	0.99, 1.04	1.05***	1.02, 1.08
Risky online practices in past year (vs no)		1.54***	1.38, 1.72	1.61***	1.42, 1.82	1.53***	1.29, 1.80
Online activities undertaken daily or weekly (vs less frequently)	Online blogs, forums, interest groups	1.24**	1.10, 1.40	1.07	0.93, 1.23	1.10	0.92, 1.32
	Purchasing from online marketplaces/ stores	1.32***	1.19, 1.48	1.32***	1.17, 1.49	1.57***	1.32, 1.86
	Romance/ dating websites or apps	1.46***	1.22, 1.74	1.46***	1.21, 1.76	2.21***	1.76, 2.77
	Online gaming/ esports	1.11	0.96, 1.28	1.34***	1.15, 1.57	1.52***	1.25, 1.86
	Sexually explicit adult websites or platforms	1.12	0.97, 1.29	1.25**	1.07, 1.45	1.50***	1.22, 1.83

Table 2: Logistic regression model predicting profit-motivated cybercrime victimisation in the 12 months prior to the survey (continued)

		Model 1: Identity crime and misuse (*n*=8,644)		Model 2: Malware attacks (*n*=8,491)		Model 3: Fraud or scams (*n*=8,719)	
Experienced negative impacts of pandemic (vs did not)	Increase in financial stress	1.13*	1.01, 1.28	1.32***	1.15, 1.50	1.59***	1.32, 1.92
	More socially isolated	1.09	0.97, 1.23	1.14	0.99, 1.30	0.86	0.71, 1.05
	Increased time and/or money gambling	1.24**	1.06, 1.46	1.59***	1.34, 1.89	2.16***	1.76, 2.67
	Negative impact on relationships with family and friends	1.16*	1.02, 1.31	1.29***	1.13, 1.49	1.46***	1.20, 1.76
	Mental or emotional distress	1.05	0.92, 1.20	1.08	0.93, 1.24	0.92	0.75, 1.12
	Physical health and wellbeing deteriorated	1.12	0.99, 1.27	1.22**	1.06, 1.40	1.09	0.89, 1.34
	Increased consumption of alcohol or other drugs	1.28***	1.13, 1.46	1.25**	1.09, 1.44	1.19	0.99, 1.44
WFH due to pandemic (vs no)		1.36***	1.15, 1.60	0.90	0.74, 1.10	0.63**	0.47, 0.85
Interaction[a]	WFH and SME owner[a]	1.33*	1.01, 1.74	1.44*	1.07, 1.94	2.28***	1.52, 3.43
	WFH and SME employee[a]	0.97	0.76, 1.24	1.25	0.95, 1.66	1.92**	1.26, 2.92
Constant	0.15***	0.12, 0.18	0.09***	0.07, 0.12	0.02***	0.02, 0.03	

***statistically significant at $p<0.001$, **statistically significant at $p<0.01$, *statistically significant at $p<0.05$

a: Compared with respondents who did not own or operate an SME and were not WFH

Note: AOR=adjusted odds ratio, CI=confidence interval, SME=small to medium enterprise, WFH=working from home

Identity crime and misuse: Hosmer–Lemeshow $\chi^2(9)=1.34$, $p=0.21$; AUROC=0.791; $F(24, 14970)=26.99$, $p<0.001$

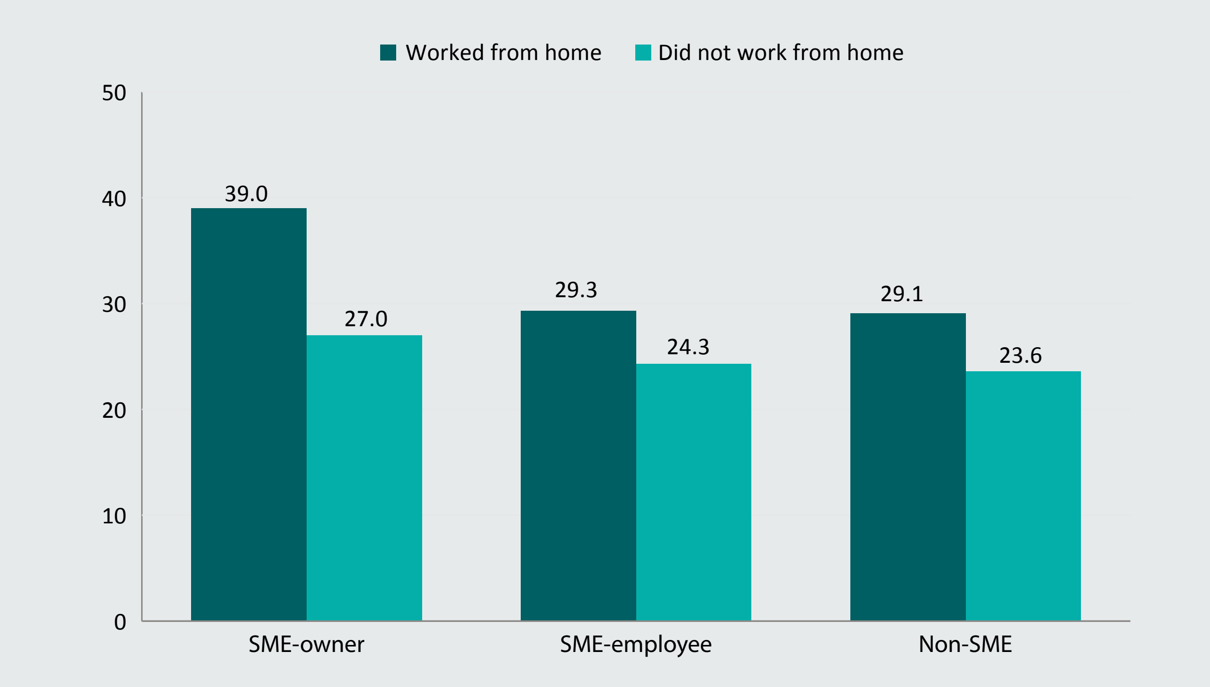
Malware: Hosmer–Lemeshow $\chi^2(9)=1.04$, $p=0.41$; AUROC=0.807; $F(24, 14970)=39.26$, $p<0.001$

Fraud and scams: Hosmer–Lemeshow $\chi^2(9)=0.425$, $p=0.92$; AUROC=0.816; F(24, 14970)=39.52, $p<0.001$

Source: AIC pilot Australian Cybercrime Survey, 2021

WFH in response to COVID-19 social distancing measures was associated with a higher likelihood of identity crime and misuse victimisation (AOR=1.36) and a lower likelihood of fraud victimisation (AOR=0.63). There was a significant interaction between owning an SME and WFH during the pandemic for identity crime and misuse (AOR=1.33), malware (AOR=1.44) and fraud victimisation (AOR=2.28). To demonstrate this relationship between SME ownership and WFH during the pandemic, Figures 1 to 3 display the average predictive margins, adjusted for covariates using marginal standardisation (Muller & MacLehose 2014), which represents the average predicted probability of each type of victimisation. The predicted probability of identity theft was 1.4 times higher for SME owners who were WFH than for those who were not (39% vs 27%; Figure 1). The predicted probability of malware attacks was 1.2 times higher (33% vs 28%; Figure 2), and the predicted probability of fraud and scams was 1.3 times higher (17% vs 13%; Figure 3). For fraud and scams, the risk of victimisation for respondents who did not own or operate an SME was higher among those who did not work from home (9.7%) than those who did work from home (6.8%).

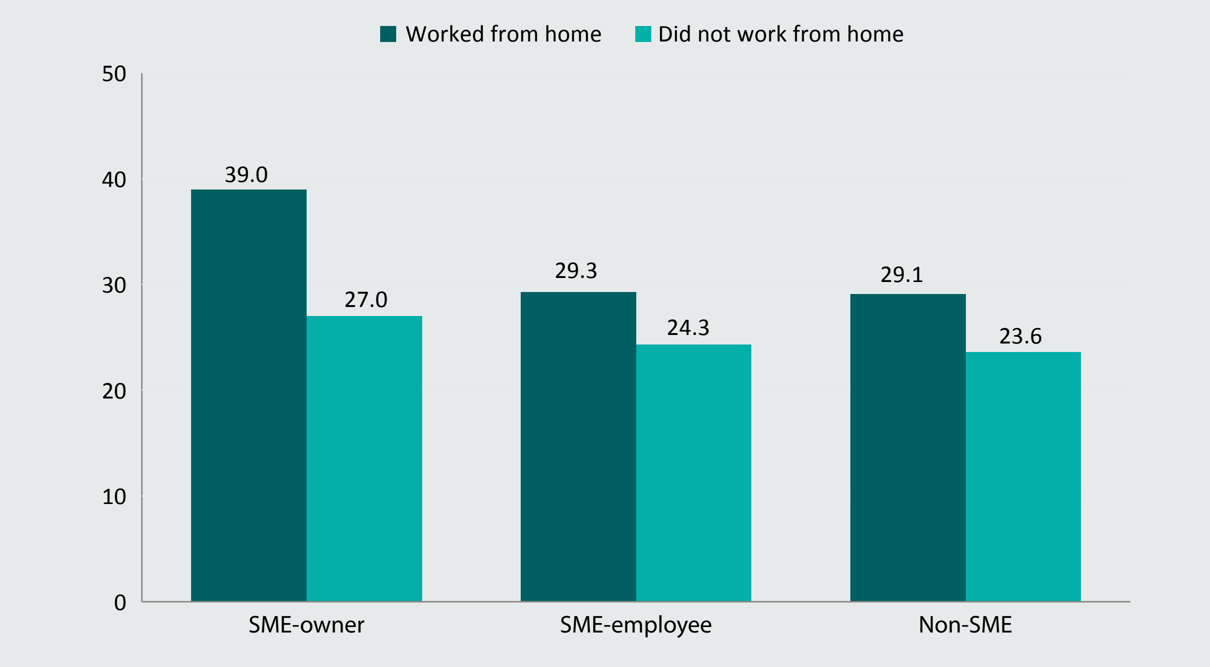
Figure 1: Predicted probability of identity crime and misuse by SME status and WFH due to COVID-19 social distancing measures (%)



Note: Predictive margins based on the logistic regression model reported in Table 2 (Model 1). SME=small to medium enterprise, WFH=working from home

Source: AIC pilot Australian Cybercrime Survey, 2021

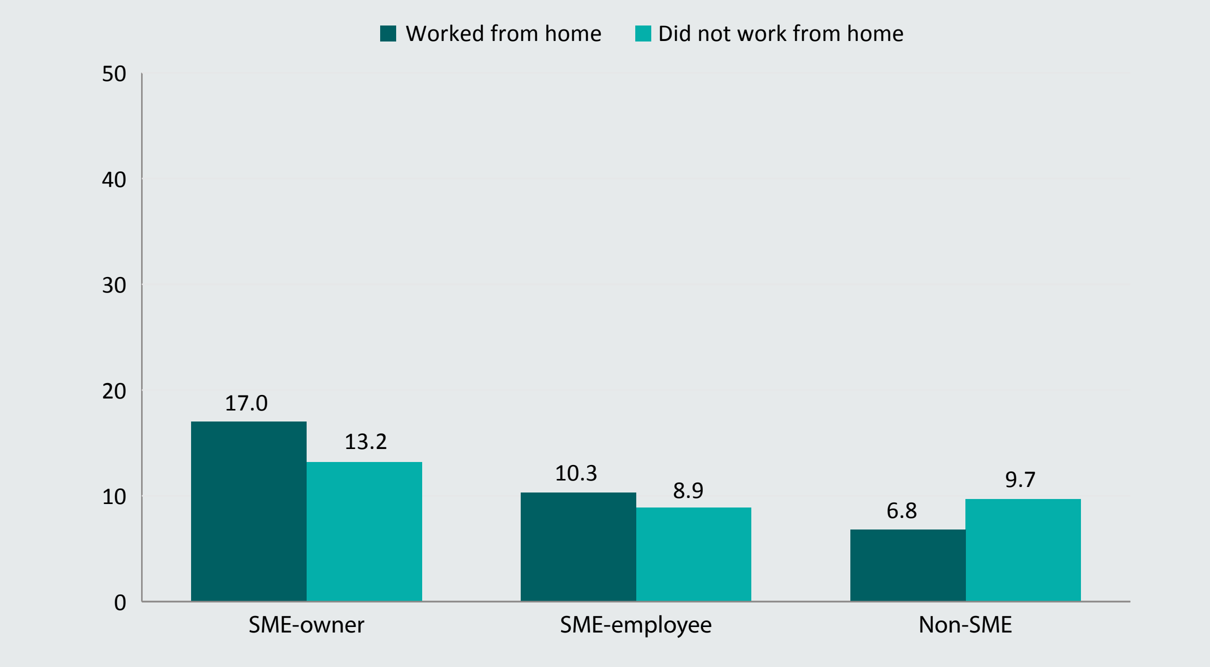
Figure 2: Predicted probability of malware attacks by SME status and WFH due to COVID-19 social distancing measures (%)



Note: Predictive margins based on the logistic regression model reported in Table 2 (Model 2). SME=small to medium enterprise, WFH=working from home

Source: AIC pilot Australian Cybercrime Survey, 2021

Figure 3: Predicted probability of fraud and scams by SME status and WFH due to COVID-19 social distancing measures (%)



Note: Predictive margins based on the logistic regression model reported in Table 2 (Model 3). SME=small to medium enterprise, WFH=working from home

Source: AIC pilot Australian Cybercrime Survey, 2021

Discussion

This study explored how the online routine activities of computer users, coupled with the effects of the psychological, social and economic stress of the pandemic—which we collectively described as the human factor in cybercrime—influenced the risk of profit-motivated cybercrime victimisation among a large sample of Australian adults. We capitalised on the fact that our survey covered the first year of the pandemic and captured self-reported changes in online routine activities and individual circumstances.

Victimisation was linked to the amount of recreational time individuals spent online and the specific online activities that they engaged in, both of which increase their accessibility or exposure to motivated offenders as a suitable target (Leukfeldt & Yar 2016; Reyns 2018). Purchasing items from online marketplaces or online stores and being active on romance or dating platforms exposes users to profit-motivated offenders. These activities involve communicating with strangers on the internet, and registration processes require users to enter financial information, which can be targeted. Alternatively, the source of risk might not be the platforms themselves but the opportunity they create for malicious actors to exploit them. Offenders may lure victims off legitimate platforms onto platforms with lower levels of monitoring (and therefore guardianship) to ask for personal information or money or to send malicious links. Malicious actors may also trick online shoppers by sending scam text messages pretending to be from couriers and post office companies. These scams proliferated during the COVID-19 pandemic. Other online activities were also related to increased risk of victimisation, reflecting the diverse methods profit-motivated cybercrime offenders use to target victims.

Risky online behaviour was associated with all three forms of victimisation, emphasising the importance of personal guardianship in preventing cybercrime (Williams 2016). This finding highlights the need for public messaging about the threat of cybercrime, the value of data and privacy, and what constitutes risky online behaviour. Given users of certain platforms were at elevated risk of victimisation, educating users of these platforms who also engage in other risky online behaviours may be an effective means of reducing cybercrime victimisation.

It was anticipated that WFH due to COVID-19 social distancing measures would increase vulnerability to cybercrime by reducing the guardianship afforded by secure workplace settings and networks. Whether WFH was a risk factor for victimisation depended on the respondent's working arrangements. SME owners who worked from home were at significantly increased risk of all three types of cybercrime victimisation. Unlike large companies and government departments, SME owners may lack the resources to employ cybersecurity personnel and implement strong cybersecurity measures at home. SME owners may also lack the necessary knowledge when assessing risks and vulnerabilities. This research highlights the need to better support small business.

While online routine activities were important, profit-motivated cybercrime victimisation was also associated with psychosocial, economic and health-related stressors. Respondents who reported pandemic-related increases in financial stress, gambling and relationship difficulties were significantly more at risk of all three types of cybercrime than those who did not report these types of pandemic-related impacts. This is consistent with previous research linking stressful life events to fraud victimisation (Anderson 2013; Ross & Smith 2011). Financial pressures, exacerbated by frequent gambling or substance use, may increase a person's vulnerability to exploitation by offenders promising quick and easy money (Levi & Smith 2021). The link between low self-control and cybercrime victimisation may also explain the link between increased gambling and substance use and victimisation, especially for cyber-enabled crimes (Reyns et al. 2019; van Wilsem 2013). While we cannot establish the temporal order of these stressors and victimisation from a cross-sectional survey, we asked respondents whether they experienced these stressors because of the pandemic, giving us some confidence that they were not the effects of being a cybercrime victim. We therefore conclude that the risk of cybercrime victimisation is explained by both the online activities of individuals and the life circumstances that may make them vulnerable to manipulation, coercion and exploitation.

While awareness campaigns that promote personal or physical guardianship of personal and financial information are important, this study echoes others that have pointed to the fact that the risk of victimisation will not be eliminated solely by encouraging people to use appropriate safeguards when online (Carter 2023). The findings from this study may help inform targeted prevention strategies focused on those most vulnerable to victimisation, or awareness campaigns based on the understanding that certain stressors may affect people's decision-making when online. These findings may also guide the development of interventions that simultaneously aim to promote safe online practices and address broader vulnerabilities of potential victims experiencing life stressors. For example, victim support services could assess victim needs and offer referrals to different sources of help to reduce the likelihood of repeat victimisation. Finally, these findings may assist in planning and resourcing for support services and cybercrime prevention efforts, noting that many of the stressors amplified during the pandemic—such as financial stress—are by no means unique to that period.

References

URLs correct as at May 2023

Anderson K 2013. *Consumer fraud in the United States, 2011: The third FTC survey.* https://www.ftc.gov/reports/consumer-fraud-united-states-2011-third-ftc-survey

Archer KJ & Lemeshow S 2006. Goodness-of-fit test for a logistic regression model fitted using survey sample data. *Stata Journal* 6(1): 97–105. https://doi.org/10.1177/1536867X0600600106

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

Australian Competition and Consumer Commission (ACCC) 2021. *Targeting scams: Report of the ACCC on scams activity 2020.* Canberra: ACCC. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-report-of-the-accc-on-scam-activity-2020

Australian Cyber Security Centre (ACSC) 2022. *Annual cyber threat report: July 2021 – June 2022.* Canberra: ACSC. https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2021-june-2022

Australian Cyber Security Centre (ACSC) 2021. *Annual cyber threat report: 1 July 2020 to 30 June 2021.* Canberra: ACSC. https://www.cyber.gov.au/about-us/reports-and-statistics/acsc-annual-cyber-threat-report-july-2020-june-2021

Baumeister RF, DeWall CN, Ciarocco NJ & Twenge JM 2005. Social exclusion impairs self-regulation. *Journal of Personality and Social Psychology* 88(4): 589–604. https://doi.org/10.1037/0022-3514.88.4.589

Baxter J & Warren D 2021. *Families in Australia Survey: Report no. 2: Employment & work–family balance in 2020*. Australian Institute of Family Studies. https://aifs.gov.au/research/research-reports/towards-covid-normal-employment-work-family-balance

Bergmann MC, Dreißigacker A, von Skarczinski B & Wollinger GR 2018. Cyber-dependent crime victimization: The same risk for everyone? *Cyberpsychology, Behavior, and Social Networking* 21(2): 84–90. https://doi.org/10.1089/cyber.2016.0727

Bossler AM & Holt TJ 2010. The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice* 38(3): 227–236. https://doi.org/10.1016/j.jcrimjus.2010.03.001

Buil-Gil D, Miró-Llinares F, Moneva A, Kemp S & Díaz-Castaño N 2021. Cybercrime and shifts in opportunities during COVID-19: A preliminary analysis in the UK. *European Societies* 23(S1): S47–S59. https://doi.org/10.1080/14616696.2020.1804973

Buil-Gil D, Zeng Y & Kemp S 2021. Offline crime bounces back to pre-COVID levels, cyber stays high: Interrupted time-series analysis in Northern Ireland. *Crime Science* 10: article 26. https://doi.org/10.1186/s40163-021-00162-9

Carter E 2023. Distort, extort, deceive and exploit: Exploring the inner workings of a romance fraud. *British Journal of Criminology* 61(2): 283–302. https://doi.org/10.1093/bjc/azaa072

Cobb-Clark DA, Kong N & Schildberg-Hörisch H 2021. *The stability of self-control in a population representative study.* IZA Institute of Labor Economics, Discussion paper No. 14976. Germany: IZA – Institute of Labor Economics

Cohen LE & Felson M 1979. Social change and crime rate trends: A routine activity approach. *American Sociological Review* 44(4): 588–608. https://doi.org/10.2307/2094589

Cross C 2015. No laughing matter: Blaming the victim of online fraud. *International Review of Victimology* 21: 187–204. https://doi.org/10.1177/0269758015571471

Emami C, Smith RG & Jorna P 2019. *Online fraud victimisation in Australia: Risks and protective factors.* Research Report no. 16. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/rr/rr16

Gainsbury SM, Browne M & Rockloff M 2018. Identifying risky internet use: Associating negative online experience with specific online behaviours. *New Media & Society* 21(6): 1232–1252. https://doi.org/10.1177/1461444818815442

Holt TJ, van Wilsem J, van de Weijer S & Leukfeldt R 2020. Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review* 38(2): 187–206. https://doi.org/10.1177/0894439318805067

James BD, Boyle PA & Bennett DA 2014. Correlates of susceptibility to scams in older adults without dementia. *Journal of Elder Abuse & Neglect* 26(2): 107–122. https://doi.org/10.1080/08946566.2013.821809

Jorna P & Hutchings A 2013. *Australasian Consumer Fraud Taskforce: Results of the 2012 online consumer fraud survey.* Technical and background paper no. 56. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tbp/tbp56

Lee J & Soberon-Ferrer H 1997. Consumer vulnerability to fraud: Influencing factors. *Journal of Consumer Affairs* 31(1): 70–89. https://doi.org/10.1111/j.1745-6606.1997.tb00827.x

Lerner JS, Li Y & Weber EU 2012. The financial costs of sadness. *Psychological Science* 24(1): 72–79. https://doi.org/10.1177/0956797612450302

Leukfeldt ER & Yar M 2016. Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behavior* 37(3): 263–280. https://doi.org/10.1080/01639625.2015.1012409

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

Mikkola M et al. 2020. Situational and individual risk factors for cybercrime victimization in a cross-national context. *International Journal of Offender Therapy and Comparative Criminology*. Advance online publication. https://doi.org/10.1177/0306624x20981041

Muller CJ & MacLehose RF 2014. Estimating predicted probabilities from logistic regression: Different methods correspond to different target populations. *International Journal of Epidemiology* 43(3): 962–970. https://doi.org/10.1093/ije/dyu029

Nabe C 2021. Impact of COVID-19 on cybersecurity. https://www2.deloitte.com/ch/en/pages/risk/articles/impact-covid-cybersecurity.html

Nattino G, Pennell ML & Lemeshow S 2020. Assessing the goodness of fit of logistic regression models in large samples: A modification of the Hosmer-Lemeshow test. *Biometrics* 76(2): 549–560. https://doi.org/10.1111/biom.13249

Newson R 2006. Confidence intervals for rank statistics: Somers’ D and extensions. *Stata Journal* 6(3): 309–334. https://doi.org/10.1177/1536867X0600600302

Ngo FT & Paternoster R 2011. Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology* 5(1): 773–793.

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

Pregibon D 1979. *Data analytic methods for generalized linear models.* University of Toronto.

Reyns BW 2018. Routine activity theory and cybercrime: A theoretical appraisal and literature review. In KF Steinmetz & MR Nobles (eds), *Technocrime and criminological theory*. New York: Routledge: 35–54. https://doi.org/10.4324/9781315117249-3

Reyns BW 2013. Online routines and identity theft victimization: Further expanding routine activity theory beyond direct-contact offences. *Journal of Research in Crime and Delinquency* 50(2): 216–238. https://doi.org/10.1177/0022427811425539

Reyns BW, Fisher BS, Bossler AM & Holt TJ 2019. Opportunity and self-control: Do they predict multiple forms of online victimization? *American Journal of Criminal Justice* 44(1): 63–82. https://doi.org/10.1007/s12103-018-9447-5

Roberts BW 2009. Back to the future: Personality and assessment and personality development. *Journal of Research in Personality* 43(2): 137–145. https://doi.org/10.1016/j.jrp.2008.12.015

Ross S & Smith RG 2011. Risk factors for advance fee fraud victimisation. *Trends & issues in crime and criminal justice* no. 420. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/tandi/tandi420

van de Weijer SGA & Leukfeldt ER 2017. Big Five personality traits of cybercrime victims. *Cyberpsychology, Behavior, and Social Networking* 20(7): 407–412. https://doi.org/10.1089/cyber.2017.0028

van Wilsem J 2013. 'Bought it, but never got it' assessing risk factors for online consumer fraud victimization. *European Sociological Review* 29(2): 168–178. https://doi.org/10.1093/esr/jcr053

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

Wemm SE & Wulfert E 2017. Effects of acute stress on decision making. *Applied Psychophysiology and Biofeedback* 42(1): 1–12. https://doi.org/10.1007/s10484-016-9347-8

Whitty MT 2019. Predicting susceptibility to cyber-fraud victimhood. *Journal of Financial Crime* 26(1): 277–292. https://doi.org/10.1108/JFC-10-2017-0095

Williams ML 2016. Guardians upon high: An application of routine activities theory to online identity theft in Europe at the country and individual level. *British Journal of Criminology* (56)1: 21–48. https://doi.org/10.1093/bjc/azv01

Isabella Voce is an Acting Principal 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, *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 922877 06 2 (Online)

https://doi.org/10.52922/ti77062

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

www.aic.gov.au