Australian Government
Australian Institute of Criminology

Statistical Bulletin 34

July 2021

Abstract | This report estimates the cost of pure cybercrime to individuals in Australia in 2019. A survey was administered to a sample of 11,840 adults drawn from two online panels—one using probability sampling and the other non-probability sampling—with the resulting data weighted to better reflect the distribution of the wider Australian population.

Thirty-four percent of respondents had experienced some form of pure cybercrime, with 14 percent being victimised in the last 12 months. This is equivalent to nearly 6.7 million Australian adults having ever been the victim of pure cybercrime, and 2.8 million Australians being victimised in the past year.

Drawing on these population estimates, the total economic impact of pure cybercrime in 2019 was approximately $3.5b. This encompasses $1.9b in money directly lost by victims, $597m spent dealing with the consequences of victimisation, and $1.4b spent on prevention costs. Victims recovered $389m.

Estimating the cost of pure cybercrime to Australian individuals

Coen Teunissen, Isabella Voce and Russell G Smith

Cybercrime is a growing, borderless and continually evolving body of crimes which can threaten individuals, businesses, government and national security. Concerns about the economic impact of cybercrime have continued to grow as society becomes increasingly reliant upon technology and thus increasingly vulnerable to cybercrime. In 2019, a global cybercrime survey of 10,063 adults in 10 countries (NortonLifeLock 2020) showed that over a third of respondents experienced a cybercrime of some kind between 2018 and 2019. In Australia, 57 percent of respondents indicated they had ever been a cybercrime victim, with 33 percent indicating they had been victimised in the previous 12 months (NortonLifeLock 2020).

This report describes the methodology and findings of a study estimating the cost of pure cybercrime to individuals in Australia in 2019. It is imperative that the financial harms associated with cybercrime are assessed so that resources for prevention and response activities can be targeted most effectively, and a baseline can be developed against which to measure the impact of future policy responses.

Serious & Organised Crime
Research Laboratory

Defining cybercrime

Cybercrime encompasses a range of crime types (Anderson et al. 2019). Cyber-dependent crimes are those that can only be committed using information and communications technologies (McGuire & Dowling 2013). These activities—such as hacking, spreading viruses and other malware, and distributed denial-of-service attacks—are considered to be 'pure cybercrimes'. They are primarily directed *against* machines and networks.

In contrast, cyber-enabled crimes are traditional crimes which could be committed without using computers, computer networks or other technology but which employ these methods to increase their scale or reach (Furnell & Dowling 2019). Cyber-enabled offences are crimes *using* the machine—such as identity theft, fraud, stalking and harassment—in which technology makes conventional crimes easier to commit and with a lower risk of detection.

Pure cybercrime is the focus of the present study. The main forms of pure cybercrime involve illicit intrusions into computer networks (eg hacking), and the disruption or downgrading of computer functionality and network space (eg viruses and distributed denial-of-service attacks; HM Government 2016; McGuire & Dowling 2013). These acts can result in disruption to networks and business operations, the loss of important data and serious financial consequences (Australian Cyber Security Centre 2021). They may lead to secondary crimes, such as when data gathered by hacking into an email account is subsequently used to commit fraud (Furnell & Dowling 2019).

Costs of pure cybercrime

There remains limited evidence of the financial costs of pure cybercrime to individuals in Australia (see, for example, Bergmann et al. 2018). However, international estimates of the total cost of cybercrime are frequently produced by cybersecurity organisations. For example, in November 2020, one cybersecurity company estimated that global cybercrime costs will grow by 15 percent per year over the next five years, reaching US$10.5t annually by 2025, up from US$3t in 2015 (Cision 2020). Country-specific estimates tend to be much smaller in relative terms. The Home Office (2018) estimated the cost of cybercrime in the United Kingdom—based on prevention, property loss and response costs—was £1.1b in the 2015–16 financial year.

Conversely, there is better evidence of the costs of cyber-enabled crime. For example, the Australian Cyber Security Centre (2020) received approximately 144 reports of cybercrime relating to small business per day in 2019, costing small businesses an estimated $300m per year, but it is unclear which types of cybercrime were included in the cost estimates. Research conducted by the Australian Institute of Criminology (AIC) estimated that the total direct costs of identity crime to Commonwealth entities, state and territory agencies (including police), individuals and businesses in Australia were $3.1b in 2018–19 (most of which, but not all, was a consequence of cyber-enabled identity crime; Smith & Franks 2020). The Australian Competition and Consumer Commission (2020) found that Australians reported losing over $634m to scams in 2019, which likely under-estimates the true extent of economic harm due to the well-known under-reporting of all forms of cybercrime. In the United States, the Federal Bureau of Investigation's Internet Crime Complaint Center (2020, 2019) estimated the total losses from cyber-enabled crime to be US$3.5b in 2019 and US$4.2b in 2020.

In one of the few estimates of pure cybercrime available for Australia, Smith (2018) estimated the cost of pure cybercrime by serious and organised crime groups to be up to A$937m in 2016–17. This included the costs associated with hacking, malware/ransomware, denial-of-service attacks, business email compromise and remote access intrusion. It was a conservative estimate due to efforts to avoid the double-counting of costs counted in other crime categories.

The current study

This study aimed to measure the prevalence of pure cybercrime and associated costs among Australian users of digital devices. The study used a large sample of adult Australians, representing one of the first attempts to assess how individual users of digital devices are economically affected by pure cybercrime.

Method

Defining pure cybercrime

The current study categorised pure cybercrime into three broad types:

- computer access crimes (CAC)—getting into a computer network or device without permission to obtain information or data. Victims may discover that another person has gained access to their digital device without their permission and has added, removed or made use of information or data, such as credit card numbers, a document, photos or video files or taken personal identity information for illegal purposes. Computer access crimes do not include the acquisition and misuse of credit card information simply through theft, misuse of a card during a normal transaction, nor when a victim is scammed into freely disclosing information;
- computer disruption crimes (CDC)—the disruption of computer or network resource operations. Signs that an individual's device has been attacked include the device not working properly or ceasing to work completely, slowed data processing, unusual messages appearing on the device, or the owner being blocked from using the device or being unable to access files because they have been encrypted. These attacks may be accompanied by a ransom message demanding payment to restore the system or decrypt the data; and
- computer malfunction crimes (CMC)—when users are uncertain if they have experienced a computer access crime or a computer disruption crime, but have experienced a computer malfunction affecting the operation of their devices, networks or information and they believe this was caused by criminally-motivated people.

An individual was considered to have experienced one of these three types of pure cybercrime when they first became aware of a problem or symptom of victimisation. This awareness can come in the form of a notification from a service provider or automated computer scanning software, or because the victim has observed the problems themselves. Instances where cybersecurity software simply detected a virus or other problem and prevented it from harming a device were excluded.

This survey did not look at problems associated with using devices caused by user error, or problems caused by manufacturers of devices or software. For example, respondents were asked not to include instances in which a device stopped working because the user failed to renew a contract, or problems that developed after a device was dropped or otherwise damaged physically.

This research focused on individual victims of pure cybercrime, excluding victimisation of corporate entities and businesses. Respondents were not asked about attacks on devices that were used solely for business or work purposes, nor attacks on digital devices and systems used in vehicles, for energy supply or other monitoring devices at their residence. In cases where a respondent's device was used for both business purposes and personal use, costing estimates were limited to those associated with victimisation through personal use.

Survey

The survey instrument was administered online and comprised 30 open and closed-choice questions. It took respondents approximately 10–15 minutes to complete if they had experienced one of the types of pure cybercrime examined. The questionnaire asked participants to report experiences of CAC, CDC and CMC that had occurred at any time in the past, and during the preceding 12 months (between June 2018 and May 2019). Data were collected between 6 and 19 May 2019.

Respondents were asked about the extent to which they used various digital devices, whether they owned these devices, the costs of the devices, their knowledge of and ability to use digital technologies, their experience of the three types of cybercrime and associated financial losses.

Sample

The Social Research Centre (SRC) and i-Link Research Solutions were engaged to undertake the survey using their respective platforms, before the two samples were combined.

i-Link Research Solutions hosts a panel of over 250,000 Australians who voluntarily participate in research projects and surveys in exchange for incentives such as reward points and entry into cash prize draws. The AIC engaged i-Link to provide a large sample of Australians to participate in the present survey. The sample obtained was a non-probability sample of 10,002 participants from across Australia aged 18 years and over (with a maximum age of 96 observed in the panel). Participants completed the survey online and i-Link offered several incentives.

The SRC hosts the Life in Australia (LinA) survey, which uses random probability-based methods to sample both online and offline populations. Participants in the LinA panel were recruited randomly through their landline or mobile phone, and a dual-frame random digit dialling sample design was employed to facilitate their recruitment. A 30:70 split was present between those who were recruited via a landline and a mobile phone. For the landline sample, only one member per household was invited to join the panel, and for the mobile sample the person who answered became the selected respondent. Members of the LinA panel were Australian residents aged 18 years or over, with a total of 2,672 active members being invited to take part in the survey, of whom 1,838 (68.8%) completed the survey. The average duration of the survey was 12 minutes for pure cybercrime victims and five minutes for non-victims. Respondents were provided with a $10 gift card or charitable donation for their participation in the survey.

The SRC initially weighted the LinA sample to population benchmarks using Australian demographic statistics from the Australian Bureau of Statistics (ABS). The SRC assigned pseudo-weights to the non-probability dataset using several variables: self-perception of sociability, how often you look for information over the internet, self-assessed ability to use digital devices, age group, highest level

of education, concession card holder status and volunteer status. Information on these additional variables was derived from a set of benchmark questions that selected members of the two panels were asked.

The SRC then used proprietary calibration and statistical models to blend the results from the non-probability sample obtained from i-Link participants and the probability sample obtained from the LinA participants. Data were re-weighted to match the same population benchmarks from the ABS, obtaining a total sample size of 11,840. This methodology reduced the bias arising from the use of a non-probability sample. The benefit of this approach is that it allows for a larger online sample than would be possible using only probability sampling, which provides opportunities for more detailed analysis, while the application of proprietary calibration allows for results from the sample to be extrapolated to the wider Australian population.

Data blending and extrapolation

To extrapolate findings to the wider Australian population, the data obtained from this weighted sample were applied to the Australian Bureau of Statistics demographic statistics for 2019 (ABS 2019). For example, the total losses occurring in Australia were estimated by obtaining a total observed loss from the weighted sample, dividing by the entire sample size and then multiplying by the number of Australians aged 18 years or over based on the ABS data for 2019.

This method was chosen over obtaining individual means or medians and applying these to proportions of the wider population due to large variations in mean size, but also due to inconsistencies in the results where those who experienced losses or recoveries could not recall the exact figures, and large proportions of individuals who reported experiencing multiple crime types.

Costing methodology

Four types of costs were included in the analysis, which only included money lost or spent in the year 2019:

- money directly lost—the amount of money taken from victims as a result of CAC, CMC and/or CDC that they experienced during the last 12 months;
- money spent on consequences—the amount of money victims spent as a result of directly dealing with the consequences of CAC, CMC and/or CDC that they experienced during the last 12 months (such as the costs of buying new hardware or software and repairing devices). See Table 6 for the full list of costing items;
- money spent on prevention—the amount of money respondents (both victims and non-victims) spent in order to protect themselves from CAC, CMC and/or CDC during the last 12 months (such as the costs of new hardware, backup data storage or storage devices, insurance etc). See Table 9 for the full list of costing items; and
- money recovered—the amount of money victims recovered or were reimbursed following their experience of CAC, CMC and/or CDC during the last 12 months.

For each of these costs, the total amount lost or spent was divided by the number of respondents in the sample (*n*=11,840), then multiplied by the Australian population aged 18 years or over based on the ABS data for 2019. The total amount lost or spent was based on respondents' estimates only where this information was known to them. The final cost after recoveries was calculated by summing the total money directly lost, total money spent on consequences, and the total money spent on prevention, then subtracting the total money recovered.

Limitations

There are limitations to this survey. These include the ability of respondents to determine whether they were a victim of particular forms of cybercrime, to accurately recall the amount of money lost due to cybercrime, and to distinguish between money spent on prevention (by victims and non-victims) and money spent on general computer hardware upgrades. While the use of probability and non-probability surveys allows for a large sample, and the use of the probability sample to calibrate the data from the non-probability sample improves the representativeness of the data, it is possible that unidentified biases may have been introduced during the weighting or calibration process that could not be accounted for.

Sample characteristics

Tables 1 and 2 outline the sample characteristics in terms of device ownership, usage and knowledge. On average, participants spent 39.2 hours using any digital device in the week prior to the survey (range: 0–168 hours), of which 12.5 hours were spent on work or business-related activities only (range 0–168).

Table 1: Device ownership and frequency of use (weighted data, *n*=11,840)

Device	Percent of sample owning device[a]	Frequency of device use for personal use (%)[b]			
		Frequently	Occasionally	Rarely	Never
Desktop	58.3	46.1	18.9	18.3	16.7
Laptop	77.7	59.6	22.4	13.4	4.7
Tablet	62.5	46.0	28.4	19.4	6.3
Mobile phone	95.5	85.7	10.4	3.3	0.6
Smart device[c]	55.2	58.8	23.2	11.9	6.1
Modem	70.7	64.2	17.3	12.6	5.9
Printer/scanner	75.7	25.1	39.9	26.7	8.3
Digital camera	54.0	14.4	35.0	37.7	12.9

a: This includes both personal devices and devices used for work or business. Missing data on device ownership includes: desktop *n*=9, laptop *n*=3, tablet *n*=10, mobile *n*=3, smart devices *n*=7, modem *n*=12, printer *n*=6, digital camera *n*=14

b: Frequency of use refers to personal use only, and does not include devices used solely for business or work purposes. Figures only include respondents who reported that they owned each device. Missing data on frequency of use includes: desktop *n*=3,114, laptop *n*=2,156, tablet *n*=3,899, mobile *n*=402, smart devices *n*=5,587, modem *n*=2,764, printer/scanner *n*=1,256, digital camera *n*=4,846

c: Smart devices included watches, TVs, and other 'smart' devices not including mobile phones and computers

Note: Percentages may not total 100 due to rounding

Source: Cost of cybercrime survey [AIC data file]

Table 2: Knowledge of and ability to use devices (weighted data, *n*=11,840) (%)

	Very low	Low	Moderate	High	Very high
Knowledge	11.6	17.7	44.9	18.4	7.4
Ability	9.0	12.8	41.4	25.4	11.4

Note: Percentages may not total 100 due to rounding. Excludes 3 respondents who did not report their self-rated knowledge of technological devices, and 22 respondents who did not report their self-rated ability to use technological devices

Source: Cost of cybercrime survey [AIC data file]

Results

Prevalence of pure cybercrime

As shown in Figure 1, 34 percent of the weighted sample had ever experienced at least one form of pure cybercrime, with 14 percent having experienced pure cybercrime in the last 12 months. The most prevalent type of victimisation was CDC, with 29 percent of all respondents indicating they had experienced a CDC at any time in the past, compared with 12 percent for CAC and nine percent for CMC (11%, 6% and 4% in the last 12 months, respectively).

Extrapolating these findings out to the entire Australian population of individuals aged 18 and over (*n*=19,753,290; ABS 2019), it is estimated that 6,690,439 Australians have been the victim of pure cybercrime at some point in the past, with 2,822,027 Australians being victimised in the past year.

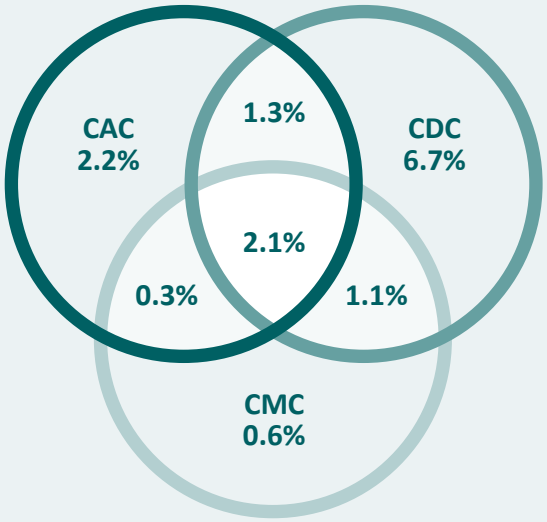
Figure 1: Experience of pure cybercrime at any time in the past and in the last 12 months (weighted sample, *n*=11,840) (%)

Note: CAC=computer access crimes; CDC=computer disruption crimes; CMC=computer malfunction crimes

Source: Cost of cybercrime survey [AIC data file]

Figure 2 presents the prevalence of pure cybercrime victimisation in the last 12 months, by cybercrime type. This shows the significant overlap between the three major categories of pure cybercrime. Among the 14 percent of respondents who experienced any form of pure cybercrime in the last 12 months, 15 percent (2% of all respondents) experienced all three forms. A further 19 percent (3% of all respondents) experienced two forms of cybercrime.

Figure 2: Pure cybercrime victimisation in the last 12 months by crime type (weighted sample, *n*=11,840)



Note: CAC=computer access crimes; CDC=computer disruption crimes; CMC=computer malfunction crimes
Source: Cost of cybercrime survey [AIC data file]

Economic impact of pure cybercrime

Using the weighted data extrapolated to the entire adult Australian population of individuals aged 18 and over (ABS 2019), the overall economic harm caused to the population by these crime types in the past 12 months was calculated (see Table 3). In the past 12 months, it is estimated that Australians had a total of $1.9b directly taken from them during a pure cybercrime, in addition to losing $597.4m dealing with the consequences of that victimisation. During this period, Australians (both victims and non-victims) also spent an estimated $1.4b on prevention costs. However, the true expenditure on prevention may be close to $1.6b after accounting for the individuals who spent money but could not recall how much. Even though Australians were able to recover $388.7m of the $1.9b lost, the total economic impact of pure cybercrime on Australian individuals as a whole in 2019 was approximately $3.5b.

Table 3: Extrapolated costs of pure cybercrime to Australian individuals (A$m)				
	All types	CAC	CDC	CMC
Total money directly lost	1,914.3	1,757.2	107.8	49.3
Total money spent on consequences	597.4	140.9	389.4	67.0
Total money spent on prevention by victims[a]	340.8	–	–	–
Total money spent on prevention by non-victims	1,035.0	–	–	–
Total money recovered	388.7	315.2	36.8	36.7
Final cost after recoveries[b]	3,498.7	1,737.0	707.1	166.9

a: The total money spent on prevention by victims also includes $103.9m for victims who experienced multiple types of cybercrime victimisation. This is because respondents were asked if they had spent any money on prevention measures, and then the results were analysed according to whether or not they had been a victim, and by crime type

b: Total money recovered is subtracted from the subtotal to provide the final cost after recoveries

Note: CAC=computer access crimes; CDC=computer disruption crimes; CMC=computer malfunction crimes

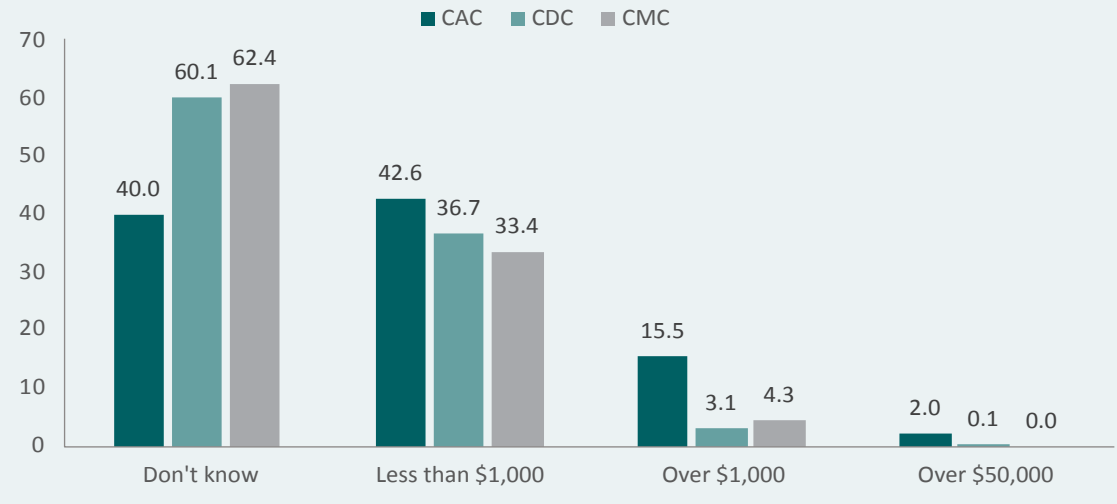
Source: Cost of cybercrime survey [AIC data file]

CAC resulted in the greatest direct losses and amounts recovered, while CDC incurred the highest cost to victims in dealing with the consequences. Non-victims spent more money on prevention than victims.

Money directly lost

A total of 42 percent of CAC victims, 15 percent of CDC victims and 16 percent of CMC victims reported losing money due to victimisation. More often than not for CDC and CMC, cybercrime victims knew they had lost money to the crime but were unsure how much they had lost. However, for all three types, when victims knew how much they had lost, the amount was most often less than $1,000 (see Figure 3).

Figure 3: Amounts lost to pure cybercrime in past 12 months, by crime type (weighted sample, *n*=1,792) (%)



Note: CAC=computer access crimes; CDC=computer disruption crimes; CMC=computer malfunction crimes

Source: Cost of cybercrime survey [AIC data file]

To obtain the total amount of money lost by victims, respondents were asked how much money they had lost in the last year as a result of experiencing each type of cybercrime: CAC, CDC and CMC. Victims of multiple types of pure cybercrime attributed the costs separately to each type.

The total amount lost by victims was $1,053,227 for CAC, $64,637 for CDC, and $29,522 for CMC (see Table 4). These totals were then extrapolated out to the Australian population, resulting in $1.8b for CAC, $107.8m for CDC and $49.3m for CMC.

Table 4: Money directly lost by victims

	CAC	CDC	CMC
Number of victims in past year	724	1,402	484
Number of victims who lost money (%)[a]	305 (42%)	208 (15%)	76 (16%)
Number of victims who could report how much they lost (%)[a]	171 (24%)	87 (6%)	30 (6%)
Amount taken per victim			
Mean (SD)	$5,033 (24,564)	$1,648 (9,696)	$1,556 (5,782)
Median	$300	$200	$300
Maximum lost	$215,000	$90,000	$32,000
Extrapolations			
Total amount lost in sample[b]	$1,053,227	$64,637	$29,522
Extrapolated total[c]	$1,757,153,578	$107,838,098	$49,254,562

a: Presented as the proportion of all victims of that crime type in the past 12 months

b: Estimated total based on the weighted population

c: Total amount divided by the sample (*n*=11,840), multiplied by the Australian population aged 18 years or over based on the ABS data for 2019 (*n*=19,753,290)

Note: CAC=computer access crimes; CDC=computer disruption crimes; CMC=computer malfunction crimes. Money figures rounded to nearest dollar

Source: Cost of cybercrime survey [AIC data file]

Money spent on consequences

To obtain the total amount of money spent dealing with the consequences of pure cybercrime, victims were asked how much money they spent on various responses taken in the last year. Respondents were asked to estimate this separately for CAC, CDC and CMC. Victims of multiple types of pure cybercrime attributed the costs separately to each type (see Table 5).

The total amount victims spent dealing with the consequences of pure cybercrime was $84,445 for CAC, $233,425 for CDC and $40,181 for CMC (see Table 6). These totals were then extrapolated to the Australian population, resulting in estimated costs of $140.9m for CAC, $389.4m for CDC and $67.0m for CMC (see Table 7).

Table 5: Money victims spent on consequences of pure cybercrime, by crime type			
	CAC	CDC	CMC
Number of victims in past year	724	1,402	484
Number of victims who spent money on consequences (%)[a]	219 (30%)	422 (30%)	115 (24%)
Number of victims who could report how much they spent (%)[a]	110 (15%)	251 (18%)	58 (12%)

a: Presented as the proportion of all victims of that crime type in the past 12 months

Note: CAC=computer access crimes; CDC=computer disruption crimes; CMC=computer malfunction crimes

Source: Cost of cybercrime survey [AIC data file]

Table 6: Mean cost of dealing with consequences of cybercrime victimisation when expenditure was known (A$)						
Cost item	Mean cost			Total cost (weighted)		
	CAC	CDC	CMC	CAC	CDC	CMC
Buying new hardware	552	400	589	38,166	40,373	15,969
Buying new additional software	177	173	194	4,326	10,139	1,183
Buying peripheral hardware to use with new systems	274	185	563	2,199	5,151	3,572
IT repair shop costs	237	185	249	11,793	27,909	12,457
Re-installing lost data	361	148	147	10,326	11,660	2,728
Increased insurance premiums	107	128	198	601	873	682
Bank fees	161	73	367	2,884	643	1,219
Service provider charges	126	94	55	2,511	2,094	159
Cost of physical security	190	327	60	1,673	2,651	73
Value of time off work	903	2,607	222	8,410	69,419	813
Travel costs for repairs/purchases	98	64	38	1,514	3,292	478
Other	100	262	300	42	59,222	838
Total combined[a]				84,445	233,425	40,181

a: Item costs may not equal the combined total due to rounding

Note: CAC=computer access crimes; CDC=computer disruption crimes; CMC=computer malfunction crimes. Money figures rounded to nearest dollar

Source: Cost of cybercrime survey [AIC data file]

Table 7: Extrapolated costs of dealing with the consequences of cybercrime victimisation (A$)			
	CAC	CDC	CMC
Total amount spent in sample[a]	84,445	233,425	40,181
Extrapolated total[b]	140,884,201	389,433,610	67,035,409

a: This uses an estimate of the total based on the weighted population

b: Total amount divided by the sample (*n*=11,840), multiplied by the Australian population aged 18 years or over based on the ABS data for 2019 (*n*=19,753,290)

Note: CAC=computer access crimes; CDC=computer disruption crimes; CMC=computer malfunction crimes. Money figures rounded to nearest dollar

Source: Cost of cybercrime survey [AIC data file]

Money spent on prevention

To obtain the total cost of prevention measures implemented by victims and non-victims, all respondents were asked how much money they had spent on various prevention measures in the last year. Unlike the costing for direct losses and consequences, respondents were not asked about prevention costs separately for CAC, CDC and CMC. Because respondents could be victims of multiple cybercrime types, prevention costs were estimated for all victims to avoid double-counting costs (see Table 8).

The total amount spent on prevention was $204,253 for victims and $620,391 for non-victims (see Table 9). These totals were then extrapolated out to the Australian population, resulting in estimated costs of $340.8m for victims and $1.0b for non-victims (see Table 10).

Table 8: Descriptive and costing statistics for money spent on prevention in the past year

	Victims[a]	Non-victims[b]
Number of respondents	1,792	10,048
Number who spent money on prevention (%)	1,118 (62%)	3,981 (40%)
Number who could report how much they spent (%)	645 (36%)	2,464 (25%)

a: Presented as proportion of victims in the past year
b: Presented as proportion of non-victims in the past year
Source: Cost of cybercrime survey [AIC data file]

Table 9: Mean cost of prevention when expenditure was known (A$)

Cost item	Mean cost		Total cost (weighted)	
	Victims	Non-victims	Victims	Non-victims
Buying new hardware	375	388	63,665	205,410
Buying backup data storage or storage devices	204	175	55,171	183,635
Buying new security or other software	152	131	40,587	125,070
Cyber security training costs	336	316	8,403	5,387
Taking out insurance	302	486	5,528	53,494
Changing service providers	253	179	9,559	20,027
Buying physical security	297	282	4,416	21,042
Time off work to install new devices and software	474	184	15,872	4,973
Other	202	183	1,053	1,353
Total combined[a]			204,253	620,391

a: Item costs may not equal the combined total due to rounding
Note: Money figures rounded to nearest dollar
Source: Cost of cybercrime survey [AIC data file]

Table 10: Extrapolated cybercrime prevention costs (A$)

	Victims	Non-victims
Total amount spent in sample[a]	204,253	620,391
Extrapolated total[b]	340,765,067	1,035,031,021

a: Estimated total based on the weighted population
b: Total amount divided by the sample (*n*=11,840), multiplied by the Australian population aged 18 years or over based on the ABS data for 2019 (*n*=19,753,290)
Note: Money figures rounded to nearest dollar
Source: Cost of cybercrime survey [AIC data file]

Money recovered

The total amount that victims recovered or were reimbursed was $188,907 for CAC, $22,049 for CDC and $22,010 for CMC (see Table 11). These totals were then extrapolated out to the Australian population, resulting in recoveries of $315.2m for CAC, $36.8m for CDC and $36.7m for CMC.

Table 11: Descriptive and costing statistics for money recovered by victims

	CAC	CDC	CMC
Number of victims in past year	724	1,402	484
Number of victims who recovered money (%)[a]	203 (28%)	149 (11%)	73 (15%)
Number of victims who could report how much they recovered (%)[a]	114 (16%)	56 (4%)	20 (4%)
Amount recovered per victim			
Mean (SD)	$1,601 (6,816)	$614 (1,466)	$731 (1,710)
Median	$321	$200	$235
Maximum recovered	$70,000	$10,000	$9,000
Extrapolations			
Total amount recovered in sample[b]	$188,907	$22,049	$22,010
Extrapolated total[c]	$315,163,909	$36,785,498	$36,720,081

a: Presented as the proportion of all victims of that crime type in the past 12 months

b: Estimated total based on the weighted population

c: Total amount divided by the sample (*n*=11,840), multiplied by the Australian population aged 18 years or over based on the ABS data for 2019 (*n*=19,753,290)

Note: CAC=computer access crimes; CDC=computer disruption crimes; CMC=computer malfunction crimes. Money figures rounded to nearest dollar

Source: Cost of cybercrime survey [AIC data file]

Discussion

This study represents the first large-scale Australian study of pure cybercrime prevalence and financial harm. Over a third of the sample had been a victim of pure cybercrime at some point in the past, while 14 percent had been victimised within the previous 12 months. CDC was the most commonly experienced pure cybercrime in terms of both lifetime and past year prevalence, although CAC had the highest financial impact in money directly lost and spent dealing with the consequences.

A significant number of victims had experienced multiple types of pure cybercrime over the previous 12 months. This speaks to the co-occurrence of cybercrime offences and highlights the need to identify those individuals who are at risk of repeat victimisation so they can be offered tailored and accessible guidance and support to reduce their risk going forward.

The total economic impact of pure cybercrime to individuals in Australia in 2019 was estimated to be approximately $3.5b. Importantly, this is a conservative estimate, as many victims were unable to report how much they had lost or how much they had spent dealing with the consequences of cybercrime. This also excludes the cost to business and government from pure cybercrime. Only a small proportion of financial losses are recovered by victims. Pure cybercrime is a highly profitable criminal activity and results in significant financial losses to Australians.

References

URLs correct as at May 2021

Anderson R, Barton C, Böhme R, Clayton R, van Eeten MJG, Levi M, Moore T & Savage S 2019. Measuring the cost of cybercrime. *The 18th Annual Workshop on the Economics of Information Security*. https://doi.org/10.17863/CAM.41598

Australian Bureau of Statistics (ABS) 2019. *Australian Demographic Statistics, Jun 2019*. ABS cat. no. 3101.0. Canberra: ABS. https://www.abs.gov.au/AUSSTATS/abs@.nsf/Lookup/3101.0Main+Features1Jun 2019

Australian Competition and Consumer Commission (ACCC) 2020. *Targeting scams 2019: A review of scam activity since 2009*. Canberra: ACCC. https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity/targeting-scams-2019-a-review-of-scam-activity-since-2009

Australian Cyber Security Centre (ACSC) 2021. View all threats. Canberra: ACSC. https://www.cyber.gov.au/acsc/view-all-content/threats

Australian Cyber Security Centre (ACSC) 2020. *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/2020-07/ACSC Small Business Survey Report.pdf

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. DOI: 10.1089/cyber.2016.0727

Cision 2020. Cybercrime to cost the world $10.5 trillion annually by 2025. 13 November. https://www.prnewswire.com/news-releases/cybercrime-to-cost-the-world-10-5-trillion-annually-by-2025--301172786.html

Furnell S & Dowling S 2019. Cyber crime: A portrait of the landscape. *Journal of Criminological Research, Policy and Practice* 5(1): 13–26

HM Government 2016. *National cyber security strategy 2016–2021*. https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021

Home Office 2018. *The economic and social costs of crime*, 2nd ed. London: UK Home Office

Internet Crime Complaint Center (IC3) 2020. *2020 Internet crime report*. Washington, DC: IC3. https://www.ic3.gov/Home/AnnualReports

Internet Crime Complaint Center (IC3) 2019. *2019 Internet crime report*. Washington, DC: IC3. https://www.ic3.gov/Home/AnnualReports

McGuire M & Dowling S 2013. *Cyber crime: A review of the evidence: Research Report 75: Chapter 1: Cyber-dependent crimes*. London: UK Home Office. https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence

NortonLifeLock 2020. *2019 cyber safety insights report*. https://au.norton.com/nortonlifelock-cyber-safety-report

Smith RG 2018. *Estimating the costs of serious and organised crime in Australia 2016–17*. Statistical Report no. 9. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/sr/sr9

Smith RG & Franks C 2020. *Counting the costs of identity crime and misuse in Australia, 2018–19*. Statistical Report no. 28. Canberra: Australian Institute of Criminology. https://www.aic.gov.au/publications/sr/sr28

Coen Teunissen is a Senior Research Analyst at the Australian Institute of Criminology.

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

Dr Russell G Smith is an Honorary Fellow at the Australian Institute of Criminology and a Professor in the College of Business, Government and Law at Flinders University.

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 26 9 (Online)
https://doi.org/10.52922/sb78269

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