Australian Cybercrime Victim Experiences and Needs (2024-2025)

IDCARE Discussion Paper and Submission to Horizon 2

28 August 2025

Connect with IDCARE at www.idcare.org

Contents

Introduction and Overview

IDCARE welcomes the opportunity to contribute to national debate and discussion in relation to Horizon 2 of the Australian Cyber Security Strategy and the Department's discussion paper.

In the 12 months prior to the release of the Discussion Paper (1 August 2024 – 31 July 2025), IDCARE responded to over 100,000 cases of individuals experiencing harm from online cybercrimes and related crimes of deception. Around half of these community members had not reported to law enforcement and many continue to experience profound and enduring impacts. Total financial losses from these scams and cybercrimes amounted to over $601 million in just one year, a 5.7% increase (+32.7 million) from 2023/24. Demand for our national support services increased by 21% over the same period when compared to the prior year.

These direct community experiences provide an opportunity for IDCARE to respond to the Discussion Paper in the following areas:

- Key impacts and needs from the Australian community.
- Small business experiences and the applicability of national guidance.
- The current state and performance of Australia's response system.
- Uplifting national efforts to effect enhanced cyber security response and resilience.

This paper concludes with a short number of strategic recommendations that are made with the intention of uplifting response and resilience to cybercrime threats impacting our community (see page 20).

1. About IDCARE

IDCARE provides the Australian community with specialist case management and response services to victims of cybercrimes and other online crimes of deception. Our national service was launched over a decade ago as a unique joint public-private initiative and not-for-profit. The blending of specialist case management, cyber-psychological and technical support interventions continue to be a world-first and demand for our services from across the Australian community continues to grow at a rate typically exceeding 15% per annum.

IDCARE frontline services to the community are without cost to victims. Our funding model, like many charities, is variable and at times perilous, and relies upon IDCARE to deliver services to industry and government to sustain our charitable efforts. We are extremely grateful for the support we do receive to enable us to deliver the critical work provided to the Australian community who are most in need.

Today more than 2,000 large organisations refer customers and communities members to IDCARE. Around one in five individuals come to IDCARE directly without being referred by an agency, police service or private sector institution. Many of those organisations that refer people do not contribute financially or in other ways to sustain our service. Those that do contribute, carry the burden on behalf of those that do not. A more robust sustainability model is needed and we encourage the participation by Governments to work with IDCARE to achieve this on behalf of the many thousands of people at present we cannot assist.

Awareness of our critical services are not the only driver for growth in community demand. If we have learnt anything over the last decade, it is that for every action in terms of prevention, there is an equal (often unequal) reaction and counter-measure by threat actors. The exponential growth in deepfake and cloning technologies and exploitative large language models are some areas already well-advanced that are aiding in facial verification and digital identity exploitation. Coupled with an absence of effective deterrence, there will predictably be a continuation of an increase in demand for our services from community members and small businesses that experience serious harms caused by such crimes despite the great initiatives identified within the Australian Cyber Security Strategy.

2. Impacts and Needs of the Community

Key Observations

Victims of cybercrimes, online scams and identity misuse are increasingly coming to IDCARE in favour of reporting through Government channels. This has underpinned the more than 200% growth in demand for IDCARE services in the last four years alone and a view by the community that the only solution offered by Governments is to ask victims to complete online forms where reporting is perceived to be the outcome.

Many victims share views about their response journey to these crimes as being just as harmful (if not more harmful) than the actual crimes themselves, yet it is likely that the response system is much more controllable than the offending. The absence of any national victim response charter or policy on cybercrime victim response exacerbates the response journey harms experienced by the community. In some extreme cases, victims feel that changing their name and moving interstate or overseas is the only solution left for them.

Little to no deterrence exists for offenders and with declining barriers to entry due to enhanced enabling technologies it is likely that the Australian community will experience greater levels of criminal offending into the future.

The growth in crimes committed where community members have no knowledge of how threat actors obtained their information is likely to speak directly to the gaps between prevention and threat actor exploitation, as well as limitations on current detection capabilities. There is a growing community need to present individuals with aggregate views of their exposed online information to aide with their understanding of risk and response priorities.

The self-detection rate where more than seven out of ten community members are the first to detect their crimes reveals clear gaps in organisational, market and government detection capabilities OR a preference to not inform individuals when exploitation is detected. Consideration in developing a national victim of cybercrime charter with appropriate coordination and oversight, such as via the National Office of Cyber Security, needs urgent consideration to address this critical detection, response and support gap.

Community Experiences

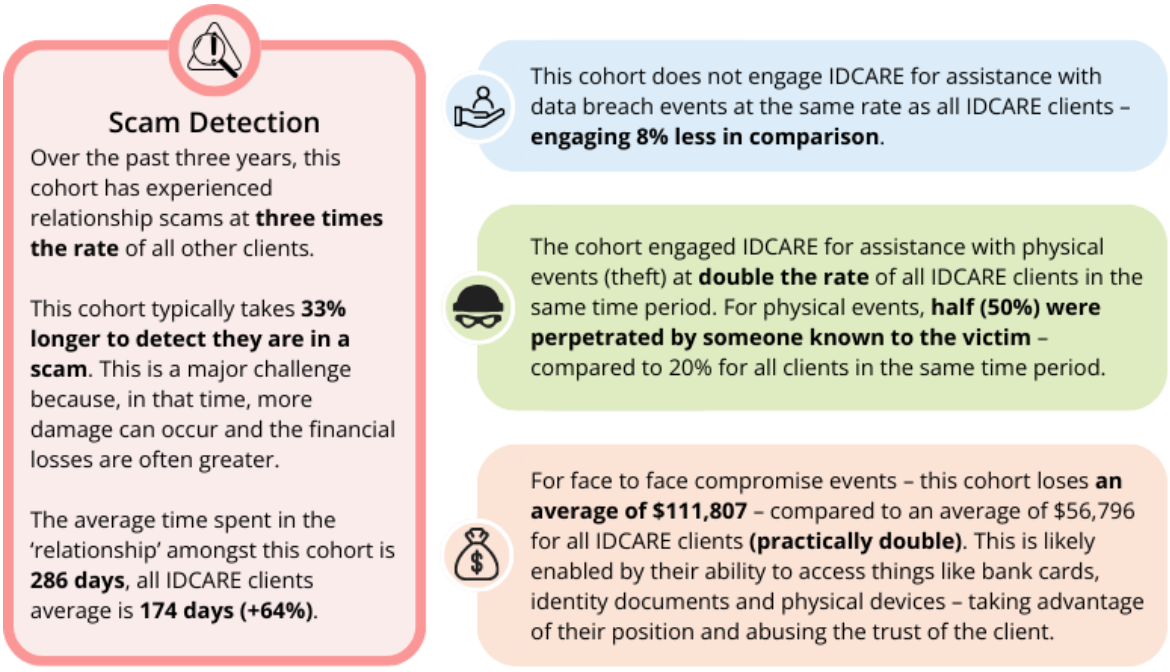
The primary experiences of Australians to engage IDCARE support services from 1 April 2025 to 30 June 2025 (3 months) are captured as follows:

- More than 27,000 Australians sought specialist help from IDCARE, resulting in more than 70,000 individual engagements over a three-month period.
- Australians lost close to $135 million dollars in savings, superannuation and other assets that has created additional demand on welfare and the community sector;
- Around 30 percent of community members had no idea how the threat actor first obtained their personal, account and credential information. This has more than doubled over the last five years despite the implementation of the notifiable data breach regime.
- The most commonly known source of cybercrime originated from over the phone, resulting in average losses of just over $42,385, where government and industry brands are being impersonated (the most frequent being Services Australia, Telstra and Australia

Post). This preferred channel of initial engagement by cyber criminals is up around 30% compared to the same period 12 months prior.

- Facebook is more prevalent as the primary means of engagement by cybercriminals than any other social media platform combined. Secondary engagement, where criminals move their engagements to another channel, primarily focuses upon WhatsApp and Telegram services.
- The most common non-financial impacts from cybercrimes and online crimes of deception reported by the community involve anxiety, fear, and suicidal ideation. These experiences appear to bear no relationship with either the amount of money lost, nor the nature of the identity, account and credential information stolen.
- Around 72% of cybercrimes and online crimes of deception are detected by the victim or a member of their family and not organisations that are then targeted by criminals using the individual's credentials.
- The most financially impactful cybercrime and online deception resulted from investment fraud cases. Average losses over the quarter were around $86,670 per case, with more than 70% originating on social media, namely Facebook.
- The most common age range of people connecting with IDCARE is 35-44 years, with around 55% identifying as female.
- Since the banking industry commenced increased efforts to prevent and detect scam activities in 2024, such as improved information sharing between institutions and blocking of cryptocurrency transactions by some, IDCARE has observed a noticeable shift by threat actors moving from targeting financial institutions to targeting the Commonwealth.

Various community cohorts experience heightened impacts from cybercrimes than the general trends reveal. For example, Australians living in regional and remote communities often find responding to these crimes much more arduous than those living in metropolitan locations. The following summary statistics reveal startling trends in relation to Australians living with disabilities who experience cybercrimes and other forms of online scams.



Vulnerable communities are recognised in the Strategy, and to advance upon maturing efforts in relation to this priority area IDCARE recommends that the Government commit further resources to research that better understands the unique needs and challenges of these communities. In doing so, we support efforts in trialling new measures in relation to outreach, engagement and support channels. There is some great work being done in some parts of academia on this issue, including Monash University and the University of Sydney. But much more is needed to ensure that all Australians, not just those who are able and living in metropolitan locations are supports and their needs understood and addressed. Cybercrime tends not to discriminate by location, and as IDCARE's demand reflects, every community in Australia experiences loss and harm from these crimes.

Nature of Community Support

IDCARE case management is a trauma-informed victim-centred service that works with community members to understand what has occurred, their main concerns and needs, leading to an assessment of risk and development of a personalised response plan. The assessment of risk leans on IDCARE's understanding of how the Australian community over time is being exploited, in what ways, and the impacts such risks present. Underpinning this work is an intimate and ongoing assessment of Australia's response system. The response system is made up of government and industry responders, such as law enforcement, financial institutions, credit bureaus, State and Commonwealth document issuers and other stakeholders that engage directly with victims.

Over the last four years, demand from community members for this specialist support has increased more than 200%. Our service model has had to adapt to this demand, and recognise that with limited resources, the priority remains on those community members presenting with the greatest needs and serious harm experiences. This has meant turning many people away or limiting engagement for some to 'email-only' advice, particularly in relation to individuals who have received data breach notifications but have yet to experience actual serious harm.

The growing complexity of case management, in turn, has necessitated IDCARE to design and deliver more specialised services in relation to technical and psychological interventions and support mechanisms. In 2023-2024, IDCARE established the IDCARE Foundation to deliver research-informed cyberpsychological care and advanced technical remediation to address the most serious community impacts from these crimes. We found a gap in such services, which are traditionally oriented towards supporting other important community needs, such as family and domestic violence survivors, or more generalised advice without expertise in cybercrimes and online crimes of deception.

Our work with leaders in clinical care and technical remediation across academia and practice nationally and internationally is helping IDCARE and our Foundation further enhance our work with community members. We've learnt over the last 14 months that there is no relationship between monetary losses experienced by Australians and psychological trauma and injury caused by these crimes. The same can be said of the nature of the attributes exposed, that is, there is no relationship between community members experiencing psychological harms and the nature of personal information compromised and/or misused. These findings have profound implications for organisations responsible for data breaches and their own assessment of serious harm.

Nature of Criminal Exploitation Impacting Australia

It is difficult for IDCARE to measure with confidence the location of criminals seeking to exploit the Australian community. Attributes provided by community members point to both domestic and offshore locations, including IP Addresses, phone numbers, and financial accounts. It is evident that the growth in technologies, such as artificial intelligence and deepfakes, are having a profound effect in scaling cybercrime efforts and reach across our community. So too are technologies that further enable cloning and the harvesting of credential information to support what is referred to as credential stuffing activities.

We are observing a number of specialist threat actors that offer data aggregation services to capitalise on historical breached information. This is a scenario that is not contemplated by Australian privacy laws – the aggregate serious harm risk confronting Australians that are victim to multiple breaches. It remains a common concern of many that seek support in responding to data breach notifications where the latest breach risk alone may not present a real risk of serious harm, but an aggregate view of historical exposure does for that person (for example, the accumulated risks from Optus, Latitude and Medibank breach data). Put simply, privacy laws are oriented towards a point-in-time assessment of risks to a person, which in turn, leaves IDCARE in the position of having to manage the enduring risks well after a breached entity has notified persons and captured the regulator's attention. This includes efforts to assess the changing nature of serious harm risks to individuals who may have had their information exposed years before against the backdrop of a response system which keeps evolving (i.e. what is possible now in terms of mitigation can be very different to what may have been extended to an individual when they were notified by a breach organisation).

By virtue of what threat actors exploit, there is also a clear blurring of boundaries between victims of cybercrimes, victims of identity theft, and victims of scams, and a growing irrelevance by response system stakeholders in seeking to define or demarcate resources and responsibilities along these lines. In fact, these artificial boundaries themselves create more friction and harm to Australians because of the need to re-tell their stories, re-file their complaints, and re-engage to prevent, detect and respond. This is further explored in Part 3 of this submission (Response System Performance).

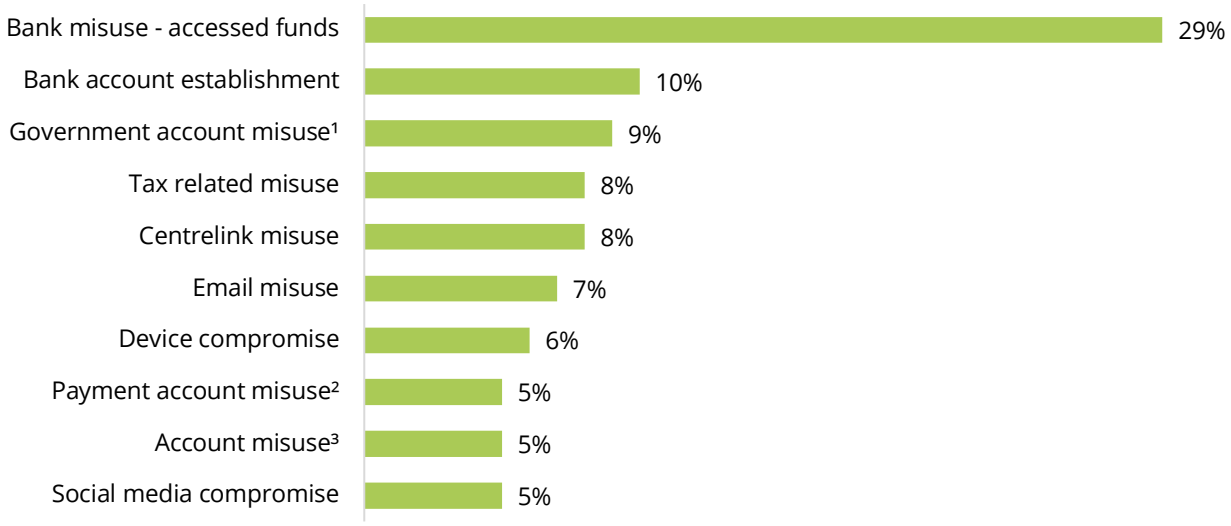
With these technologies, the barriers to entry in terms of criminal exploitation are reducing. It is likely that the Australian community will be seen by an increasing number of people that seek to pursue high criminal profits with little chance of capture or deterrence as an attractive target. The strategic-political environment and broader state of world affairs will only increase this risk to the Australian community. It is a risk that remains well below the threshold and interest of many Government agencies and the broader national security apparatus. A community member that presents to law enforcement because they have lost $86,670 to an investment fraud that commenced from a Facebook Ad over 12 months earlier is not likely to be prioritised over other crimes that deserve higher and immediate priority, such as sexual assaults. Therein lies one of the very complexities of the current situation – there is little to no obstacles for individuals to enact these crimes, little to no deterrence, high criminal profits, and a mostly impotent response.

We hear from Australians every day who experience further crimes and acts of exploitation beyond their initial criminal engagement. The most common of these, focus upon the victim's bank accounts or a desire by criminals to create new bank accounts to enable other offending, such as claiming fraudulent tax refunds or Government support payments (prevalent in around one-in-four secondary crimes). The advent of Confirmation of Payee controls, a necessary

measure, is almost certainly having a perverse impact on the growth in criminals establishing bank accounts in the names of cybercrime and scam victims in order to overcome this control measure (i.e. using the real name of the victim when creating a bank account to fraudulently access funds by third-parties in the victim's name, such as fraudulent tax returns).

The top ten most common cyber-enabled misuse is presented at Figure 1 from community engagements to IDCARE over the last 12 months.

Figure 1: Top 10 of the Most Common Misuse Types for Individuals



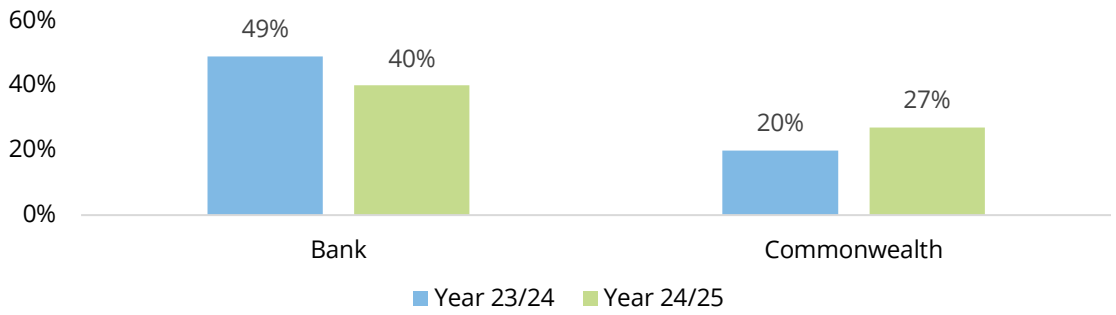
[1] This excludes Centrelink, Medicare or ATO misuse.

[2] Excludes bank misuse, but includes other online accounts, such as superannuation.

[3] Account misuse relates to unauthorised access of online accounts, such as email and non-banking accounts, resulting in changes to account information or actions that result in clients being locked out.

The community experiences crimes in a manner that shifts and evolves as market and government policies change. It is naive to assume that without any real deterrence, the threat actors responsible for impacting the Australian community will not also adapt to these changes, morphing their operations and focus of their exploitation accordingly. A real example of this is unfolding at present in relation to enhanced measures taken across financial institutions, and a corresponding displacement effect towards targeting Commonwealth services. Figure 2 represents this shift based on reported cases of online account creation and/or online account misuse over the last two financial years.

Figure 2: Types of cases involving bank and Commonwealth misuse.



Since the 2023-2024 financial year, there has been a shift in Commonwealth and bank related misuse events. There has been a 9% reduction in bank related misuse events, while there has been a 7% increase in Commonwealth related misuse events. This displacement effects speaks to the adaptability of the threat environment and the corresponding attractiveness Commonwealth credentials are to threat actors, such as MyGov logins, Tax File Number and Medicare Card details.

A further concerning development over the same period which reflects the actions of criminals has been the reclaimed volumes of unauthorised mobile phone porting and SIM-swapping. Following the introduction of reforms to the telecommunications industry that resulted in an uplift of identity verification, IDCARE observed a dramatic decline in reported instances of unauthorised porting and SIM-swapping. It was, at the time, a positive policy development with tangible impact.

However, over the last 12 months, the number of reports has increased by 65%. Like the establishment of transactional accounts, unauthorised porting and SIM-swapping are enabling crimes, where threat actors seek to intercept messages, including Multi-Factor Authentication codes relating to other online accounts. Aside from laxed identity controls, such as confirmation of the real owner of the device of the application to port or swap, it is difficult to determine the reason for such an increase following what appeared to be a successful policy implementation.

Like effective deterrence strategies, more needs to be done in understanding these shifts and predicting the likely consequence of policy development and its implementation on cybercrime and online deception impacts on the Australian community. This requires policy makers to increasingly think carefully about anticipated threat actor reactions, particularly in relation to prevention measures across the economy. Just like our observations in relation to vulnerable communities, the Commonwealth would benefit from supporting greater research and independent evaluation on policy development modelling specific to the needs and impacts of victims of cybercrime and community exposure to such crimes. This has been a repeated weakness across many policy decisions involving the combatting of cybercrimes and online crimes of deception. Australia has world leading researchers across many institutions that can directly contribute to enhanced understanding of the levers of Government and their likely impacts on the community that confront and respond to these crimes. Building a Centre of Excellence, with Government participation and input, across institutions to maximise contribution and value to the enhanced design of prevention, detection and response mechanisms for cybercrime and online crimes of deception is overdue.

3. The Experiences of Small Business

Key Observations

More than twice the number of small businesses to engage IDCARE do so because they experienced a cybercrime or online crime of deception than small businesses that seek help to build their cyber maturity in order to prevent such crimes.

Around 75% of small businesses self-detect the cybercrime or online deception first before any other entity (for example, their financial institution).

More than half of small businesses to detect cybercrimes impacting their business had no knowledge of how the threat actor got the account, credential or related information or access being exploited.

Unauthorised access of small business bank accounts, including via scam activities, unauthorised access of email accounts and the hacking of social media accounts are the most prevalent types of exploitation impacting Australian small businesses.

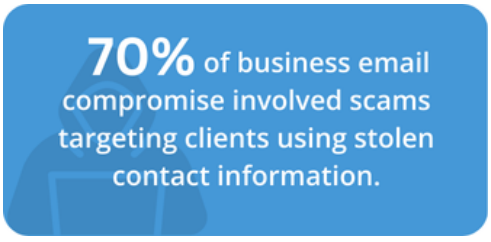
There are less response system affordances for small businesses when compared to individuals, such as an absence of any credit ban opportunities to prevent unauthorised credit being extended to criminals in the name of small businesses.

Small businesses are not incentivised to build their cyber maturity when consideration is given to all other competing priorities small business owners confront. The development of alternative maturity channels and advice may add to small business owners feeling dissuaded to proactively advance cyber maturity and a lack of connection and coherence between such measures and the actual threats impacting small business owners exacerbates this problem.

Small Business Experience

Small businesses often rely solely on themselves to detect signs of criminal exploitation (i.e. around 78% of all small business to present to IDCARE). This self-reliance poses several risks, including:

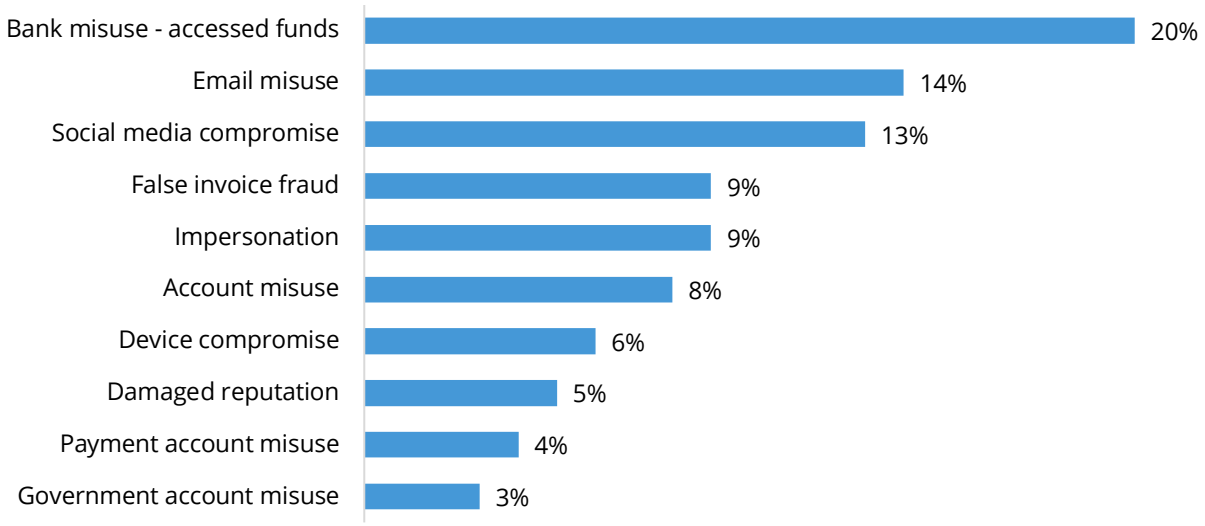
- Extended access for cybercriminals, allowing them to remain undetected longer.
- Delayed and uncertain response and recovery, increasing financial and operational impact.
- Greater damage to business operations, data and reputation.
- Higher risk to customer and staff data, due to lack of early containment.



Small businesses can be exploited as intermediaries or enablers of scams. For instance, cybercriminals may hijack a small business' social media account to impersonate the business and deceive customers. Due to the established reputation of the business, individuals are more likely to trust the account. This is evident as the top five individual misuse relate to gaining some sort of financial gain by compromising or

establishing accounts. However, for small businesses, the top five common misuse types relate to ways that scammers can exploit the trust and community the small business has built to target and scam a wider audience. Figure 3 captures the most common cybercrime exploitation confronting small businesses to engage IDCARE over the last 12 months.

Figure 3: Top 10 of the Most Common Misuse Types for Small Businesses.



Like individuals, the attraction of criminals to the retained earnings and savings of small business owners held in bank accounts has resulted in this being the most prevalent reported misuse. There is likely to be a coupling of unauthorised email access (or email misuse), along with social media compromise. The most prevalent of these relates to small business Facebook accounts that for many have email username and password credentials used as their access credentials. The absence of mandatory multi-factor authentication is a commonly exploited weakness when it comes to social media and email account exploitation. Efforts within the Strategy to uplift 'out of the box' security measures is a positive step in seeking to address this vulnerability.

Unique to small business (and no doubt larger business) are false invoice fraud events. Again, these rely heavily upon threat actors gaining unauthorised access to business email accounts.

47% of small business data breaches were the result of a compromised email system.

While the rate of device compromise is similar between individuals and small businesses, the impact on small businesses is significantly more severe. Notably, 13% of small businesses reported a full system compromise, affecting their critical systems such as email accounts, websites, bookkeeping software and data storage systems. These breaches not only disrupt business operations but also have cascading effects on customers and staff. The consequences are particularly pronounced in cases of email and social media account compromises, where the broader reach of small businesses amplifies the damage, ultimately affecting the wider community.

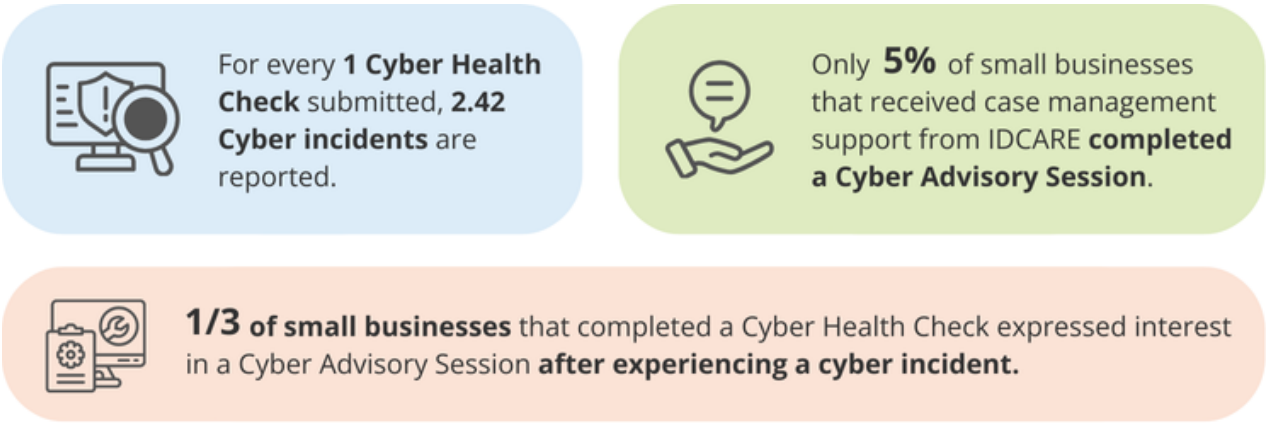
The access to cyber insurance is also limited with many small businesses that intersect with IDCARE. Some have remarked that they need some independent authority to review terms and conditions against what realistically are the most likely threats. Over the years IDCARE has assisted many small businesses that have cyber insurance and were told by their insurer they had to use service providers that in our view were inadequate and overly expensive. In one case, a School was quoted $300,000 for a templated policy set following a cyber incident by a law firm,

one policy of which when reviewed by IDCARE contained a number of response advice inaccuracies. These are measures that Government can better assist with, rather than leave it for the market to work out. The market, in our observation, consists of many genuine and reliable service providers, but are tarred by the brush of those that are exploitative and disingenuous. It is our view that the challenges confronting small business in uplifting their resilience needs greater government intervention, both in terms of incentivisation, but also in terms of providing greater regulatory oversight of operators across the cyber security continuum.

Nature of Services Extended to Small Business

IDCARE defines a small business in alignment with the Australian Bureau of Statistics (ABS) – an entity with less than 20 full time employees. Small businesses that come to IDCARE, benefit from investment made by the Commonwealth under the Small Business Cyber Resilience Service. These services focus on the delivery of the following:

- **Cyber Advisory Sessions** – Our sessions focus on helping small businesses adopt essential cyber security practices. We simplify complex cyber terminology and explain the importance of each recommendation.
- **Case management** – Our case management services offer expert guidance to small business on the containment, detection, and response of an incident, along with strategies to prevent future misuse.
- **Cyber First Aid** – Our cyber first aid sessions focus on supporting small businesses respond to compromised devices and reviewing accounts with a high risk of misuse – including social media accounts and Microsoft accounts.



Through IDCARE's Cyber Advisory Sessions and incident response services, we frequently encounter small business owners who request our help in implementing basic protections, such as multi-factor authentication, data encryption, and secure communication practices. This reliance on external support underscores a widespread gap in foundational cyber knowledge, capacity to enact, and time.

It is evident that addressing these shortcomings requires more than education. IDCARE does urge the Government under Horizon 2 to explore incentives for small businesses to uplift their cyber security posture. The advertising and embedding of services, like IDCARE's cyber advisory service, should be connected to national touchpoints for small business owners from the very commencement or registration of the Australian Business Number, through to the establishment

of the first business banking account, phone and internet service. Improving the reach to small business is one step, but an important one to advance upon national resilience and uplift. Small business owners are very busy and focused on primal needs. Many do not view cyber security as a primal need until it is. Our data on the mix of our engagement with small business reinforces this view.

4. Response System Affordances and Performance

Key Observations

Response is as much about prevention, as it is about detection and correction. For most victims it is never a linear process as represented in many frameworks and policies.

More than half of victims to experience cybercrimes experience further harms from the response system. The absence of any national victim of cybercrime charter or response standard exacerbates these experiences and retards efforts that could maximise victim insights for national prevention and system resilience.

The worst performing sectors and industries in addressing the needs of cybercrime and online deception victims to report to IDCARE over the financial year 2024-2025 were State Government, Credit Reporting and Law Enforcement agencies. The Commonwealth and financial institutions were the highest performers in terms of satisfaction levels by victims in assisting their response.

The main contributors to victim harm and traumatisation from the response system relate to convoluted reporting mechanisms, including multiple Government reporting measures, the onus on victims to carry the response load (particularly in light of the number of victims who self-detect – i.e. are the first to detect these crimes), and a general unwillingness and inconsistent approach to respond to these crimes and support the needs of victims.

As a matter of urgency, the Commonwealth, along with States and Territories, should develop a national cybercrime victims charter and regulatory model to uplift the standards of response for victims of these crimes and maximise on prevention opportunities for others.

Australia's Response to Cyber Security Threats – Victim Perspectives

As presented, the response to cybercrimes and other online crimes of deception is not linear nor does the lived experience neatly fit cyber security and risk frameworks where there is sequential progression of effort across detection, investigation, assessment and response. An individual or small business owner when faced with a response to a cybercrime event needs to concern themselves with detecting and investigating whether other crimes are occurring, as much as they need to protect and respond to the initial crime itself.

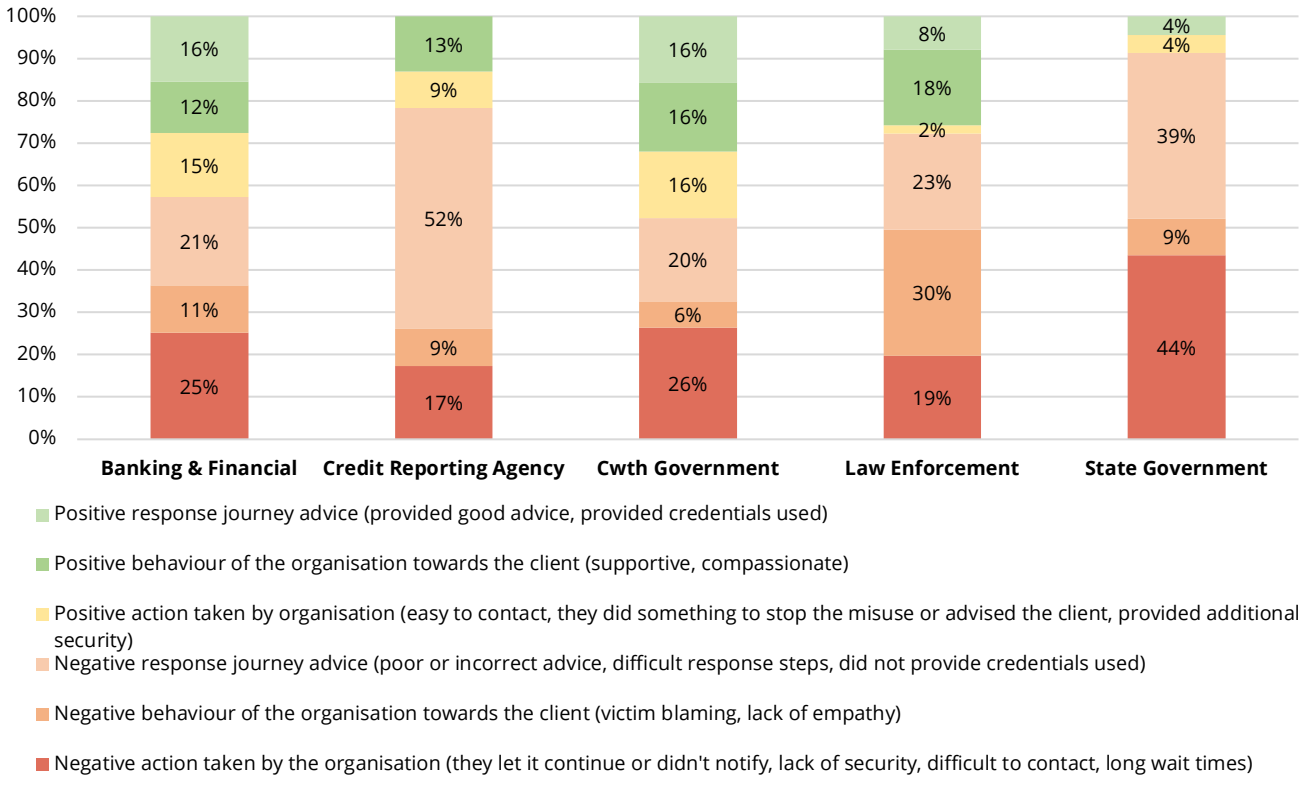
What exacerbates this problem is that most victims are the ones to detect and therefore have the job of convincing response system stakeholders that they are a victim and not a perpetrator or enabler of such crimes.

Furthermore, what individual and small business victims do to respond are actually efforts designed to protect 'the system' (but they don't know this), where their needs are often divergent from the needs of response system stakeholders. For example, a victim of a cybercrime that results in unauthorised access of their bank account is primarily concerned with getting their money back and securing their account. The financial institution is primarily concerned about determining whether the crime actually occurred and whether the individual enabled it. This determines liability. In our experience, the greater the divergence between the needs, the greater the harm is to the victim. In the absence of any national standards or any national cybercrime victim charter, these harms will persist and the system will continue to operate sub-optimally and

miss critical opportunities to actual lift system resilience. Feedback from IDCARE clients captured throughout the 2024-2025 financial year reveal significant variation between industries in victim experience, accessibility, and response effectiveness.

- Across all industry types, negative feedback outweighed positive feedback. State Government received the highest proportion of negative feedback (90%), with the main issues being response journey advice (44%) and a lack of action taken (39%).
- Law enforcement stood out for having significantly higher levels of feedback relating to negative behaviour (30%)- such as victim blaming or a lack of empathy- in comparison to other sectors. Additionally, less than 2% of feedback referred to positive action taken by law enforcement to stop the misuse.
- Commonwealth Government received the highest proportion of positive feedback (48%) in comparison to other industries, scoring equally well across all 'positive' categories (response advice, behaviour, action taken). The key area of concern for Commonwealth Government relates to negative action taken (26%), which can likely be attributed to victims frequently citing issues contacting the agencies (e.g. long wait times).
- Credit Reporting Agencies received overwhelming feedback for providing negative response journey advice (52%)- specifically where staff provided no response advice and reflected an inability to answer victims' questions.
- The Banking and Financial sector received the second-highest proportion of positive feedback (43% of total), with response journey advice being its strongest (positive) area. Considering the critical role financial services play in responding to cybercrime misuse, it is assuring to see it embracing the opportunity to provide guidance to victims.

Figure 4: Response System Feedback from Victims Engaging IDCARE (2024-2025)



The results from the experiences of victims in their response journey presents a sobering view of how well Australia is responding to these crimes. It is never about 'recovery' as presented by some quarters in Government, as this language is fraught and offers a false promise, when in reality the victim of a breach or cybercrime event never recovers the information that has been exposed.

Adding to this complexity is the disjointed nature of national efforts or an absence of any real need to consider and advance response system performance and efficiencies. IDCARE conducts independent testing of response plans across organisations within Australia's response system, with an aim to document and test the standards of responses to cyber and identity crime affecting victims. These lived experiences inform our work in how effective the response system is at preventing and responding to these crimes. It is evident that much more needs to be done in uplifting performance.

Victims of these crimes are not eligible for Government victim of crime support. Often crimes are not investigated, and prosecutorial outcomes are extremely rare. Many millions of Australians are left to deal with the fall out themselves and engage a system that is only interested in its own priorities. Put simply, if you are not harmed by the crime, you will be by the response. IDCARE strongly encourages the Commonwealth, along with States and Territories, to consider a national cybercrime victims charter and regulatory model to uplift the standards of response for victims of these crimes. If Australia is going to lift our resilience to these crimes, we must first ensure that those who are victim of such crimes have needs recognised and a system operating in a manner that addresses them. One person's unfortunate experience can be a lightning rod for prevention, but at present, the current response system is too immature to capitalise on such opportunities. Of all of the efforts under Horizon 2, IDCARE believes this one offers the greatest opportunity to effect positive change to the lives of many, and to genuinely uplift future resilience.

Major barriers facing victims within Australia's response ecosystem

Drawing on insights from the latest quarterly round of testing and client feedback, IDCARE analysts consistently identity the following systemic issues:

Fragmented and Convoluted Response Journeys

Due to the absence of a single, streamlined pathway, victims are forced to navigate complex and lengthy response journeys, involving multiple organisations across sectors such as banking, telecommunications, federal and state government, and reporting bodies. Often without clear guidance, individuals are expected to initiate and coordinate their own response journeys to remediate the impacts of a cyber incident, including renewing identity documents and credit cards, changing log-in details and security settings, ordering credit reports, or regaining access to government services.

Inconsistent Organisational Willingness to Share Information or Enable Protective Actions

Another barrier inhibiting the response journey of victims is the significant variability in the maturity of organisational response systems, which creates uncertainties around whether the organisations involved will conduct the necessary response actions. Victims have limited oversight or control over the internal systems of organisations that manage their accounts and personal information, making them heavily reliant on the willingness of organisations to act and disclose the information needed to respond to cybercrime.

The Banking and Financial industry is a prime example of how variances in the maturity of the varying maturity of response practices can within between organisations.

When an individual presents with a fraudulent bank account being created in their name, the financial institution involved determines (a) whether the victim can confirm the accounts existence; (b) what identity of theirs was used to create the fraudulent account; (c) whether the bank is willing to look for other accounts or attempted account creation events using the victim's details; (d) whether the bank will put in place measures to prevent future attempts; and (e) whether any of those needs will be communicated to the victim, and if so, when. While all of these actions are fundamental to detecting and responding to identity theft, many banks still prohibit the ability for victims to take these steps.

35% of banks do not allow individuals to detect whether a fraudulent account exists using their basic details.

20% of banks will not disclose to identity theft victims what form of ID was used to open an account in their name.

67% of banks will only disclose the type of ID stolen if the victim can pass the account's security or provide further documents.

The statistics presented to the right represent current response system testing results by IDCARE when examining what response affordances are provided by banks to victims. This is reinforced from a direct, but anonymised, quote from a cybercrime victim below.

"I had a fraudulent account opened at two different banks and Bank A's response was much worse [than Bank B]. They didn't seem to care, didn't give me any ID protection advice and did not tell me what documents were used or tell me if there was a plan to tell me this information in the future. These are all things the other bank did."

Despite the above presenting a negative view on the performance of financial institutions, this industry is actually one of the top performers when compared with other industries and governments. For example, different state agencies that issue drivers licences have their own stance on which circumstances they will consider changing driver licence numbers, or whether they offer the ability for individuals to place a block on their driver licence to prevent it from being authorised through the Document Verification Service.

Law Enforcement Responses Fall Short of Victims Expectations

IDCARE receives consistent feedback from clients expressing the view that the available reporting channels for victims of cybercrime are not meeting expectations.

For many victims who choose to lodge a report through ReportCyber, the decision is driven by the desire for their case to be investigated, resulting in some kind of follow-up with assistance and possible action against the offender. Given that this isn't the reality for most victims, many victims feel a sense of injustice and dissatisfaction with law enforcement. We recognise that this is the lesser of two evils, one being that without a mechanism to receive reporting about such crimes, Government would be oblivious to the effects these crimes are having on the Australian community. In addition, there is a genuine lack of resource and opportunity for intervention held by law enforcement. IDCARE doesn't make these observations as a criticism of law enforcement. We are well aware of the limitations, but it is necessary to provide these views on behalf of the

many victims who express them and aren't either aware or appreciative of such constraints. It is a 'no win' situation for all concerned, except the threat actor themselves.

While this response from victims can be attributed in part to a lack of understanding of ReportCyber's functions, there is a clear absence of a more suitable alternative for victims to turn to which can meet these expectations. Victims frequently remark that when they did present to a police station, they were turned away or refused help, often accompanied by the direction to ReportCyber which may be of little use if their device is compromised because of the cybercrime experienced. A national victim of cybercrime charter may assist in managing such expectations and developing consistent response frameworks across the Commonwealth, States and Territories with all main response system stakeholders.

We remain sensitive to the unique challenges confronting law enforcement when it comes to cybercrimes and online crimes of deception. But we are equally sensitive to the variable standards of response, and the traumatising effects the response system continues to have on victims. If there is one area that Horizon 2 can control with confidence when it comes to cyber threats, it is how Australia chooses to respond and treat victims. This is controllable and something that IDCARE feels compelled to advance upon as a priority interest and requirement for national change.

5. Uplifting Response and Resilience - Recommendations

Based upon our observations of individual community and small business needs and experiences, this final section of IDCARE's submission summarises the key recommendation across the specific areas of interest discussed that we believe present the best opportunities for Australia to advance national cyber resilience.

Addressing Response System Performance and Harm

Recommendation 1: The Commonwealth, with States and Territories, guided by victim groups and response system stakeholders, establish a National Victim of Cybercrime Charter coordinated by the National Office of Cyber Security that is inclusive and cognisant of the needs and experiences of all Australians, including vulnerable communities, captured in national standards that safeguard such interests.

Recommendation 2: The Commonwealth, States and Territories, develop in consultation with victim groups and response system stakeholders, national response standards that recognise the needs of victims, their unique circumstances in light of their distinct experiences outside of established victim of crime frameworks, to address urgent needs and improve the timeliness of reporting, and the advancement of prevention, detection and response outcomes.

Recommendation 3: There is a rationalisation of Commonwealth, State and Territory cybercrime and online deception victim reporting portals and direct linkages to national support capabilities, such as IDCARE, to reduce the time and burden placed on victims and their re-traumatisation. This rationalisation should also provide sufficient investment to enable the efficient consent-based transfer of victim information in order to protect against secondary exploitation and be directly guided by national standards (as per Recommendation 2).

Uplifting Small Business

Recommendation 4: The Commonwealth develop an incentivisation plan for small businesses to uplift their cyber resilience, including consideration of tax incentives, a rationalisation of standards which are informed by actual exploitation events experienced, and mandatory engagement channels that leverage existing company and tax registration processes.

Enhancing National Awareness and Policy Development

Recommendation 5: The Commonwealth fund a Centre of Excellence that brings together expertise across academic institutions to better enable modelling of likely policy outcomes from a cyber security and cybercrime threats and impacts perspective on the Australian community. This would complement existing arrangements which are focused on fraud against the Commonwealth and privacy compliance risks.

6. Concluding Remarks

IDCARE welcomes the opportunity extended by the Department of Home Affairs in contributing views in relation to the important work underway in Horizon 2 of the Australian Cyber Security Strategy. The views expressed have focused upon the areas that IDCARE maintains an intimate connection with – namely the journey of individuals and small businesses that respond to acts of cybercrime and other online forms of deception. This is a massive issue for the Australian community and not one, sadly, that is likely to dissipate.

There are things that are difficult to control, least of which is the desire and resources of the threat actors who continue to operate largely with impunity against our country. But one thing we can control, is how we respond to victims of these crimes. The trauma our response system inflicts on community members needs urgent attention and it needs to benefit from the lived experience of victims and the collective wisdom of stakeholders and interest groups. Australia already has a number of mechanisms in place to advance positive change on this front. It would be a tangible contribution towards our maturity under Horizon 2 to take on this important challenge. Not doing so means that totally avoidable trauma and re-victimisation will persist. The volume of crime we confront is more than enough without adding to this pain felt by so many across our country.