Submission to the Parliamentary Joint Committee on Law Enforcement:

The capability of law enforcement to respond to cybercrime

December 2023

IDcare

Connect with IDCARE at www.idcare.org

Submission overview and scope

Identity Care Australia and New Zealand (**IDCARE**) welcomes the Joint Committee's Inquiry into the capability of law enforcement to respond to cybercrime. IDCARE's Whole of Law Enforcement agreement includes the AFP and all states. In this capacity IDCARE frequently liaises with law enforcement agencies across all Australian states, territories and the Commonwealth. IDCARE also receives referrals from the Australian Cyber Security Centre, assisting people that have made a report to Report Cyber.

IDCARE's submission is informed by this relationship and our extensive experience in working with individuals and organisations that have been affected by identity theft, data breaches originating from online threats, scams and fraud. Our submission focuses on those areas in which IDCARE has direct experience; it does not respond to all questions in the consultation.

IDCARE has identified improvements that could be made to better improve the capacity of law enforcement to respond to cybercrime. Our three key recommendations are:

1. While there have been considerable efforts made to capture the nature and impact of these crimes on Australia, the resourcing orientation has some way to go in order properly advance disruption and response efforts to what is now an international volume-organised crime impact on our community.
2. IDCARE's significant community intelligence insights on cybercrimes, scams and related crimes present a tremendous opportunity for law enforcement, industry and government to support strategic intervention, build national resilience, and deliver meaningful outcomes for the community. The meaningfulness of these outcomes will need to continue to work towards bridging the divide between community norms and expectations of law enforcement and what is possible in terms of intervention and disruption. It will also need sufficient resourcing, which for IDCARE and its connections with all law enforcement agencies, is extended only as part of a one-off trial until early 2025. Beyond that period, IDCARE support of serious harm cases from ReportCyber and direct from law enforcement, will not continue without renewed funding support.
3. The advancements in generative AI, deep fakes and related technologies, combined with ongoing challenges with encryption, cryptocurrency detection, and identity obfuscation, is likely to mean that cybercrimes will continue to grow along with their sophistication. Law enforcement will need access to leading research, development and talent management to effectively counter these threats into the future.

About IDCARE

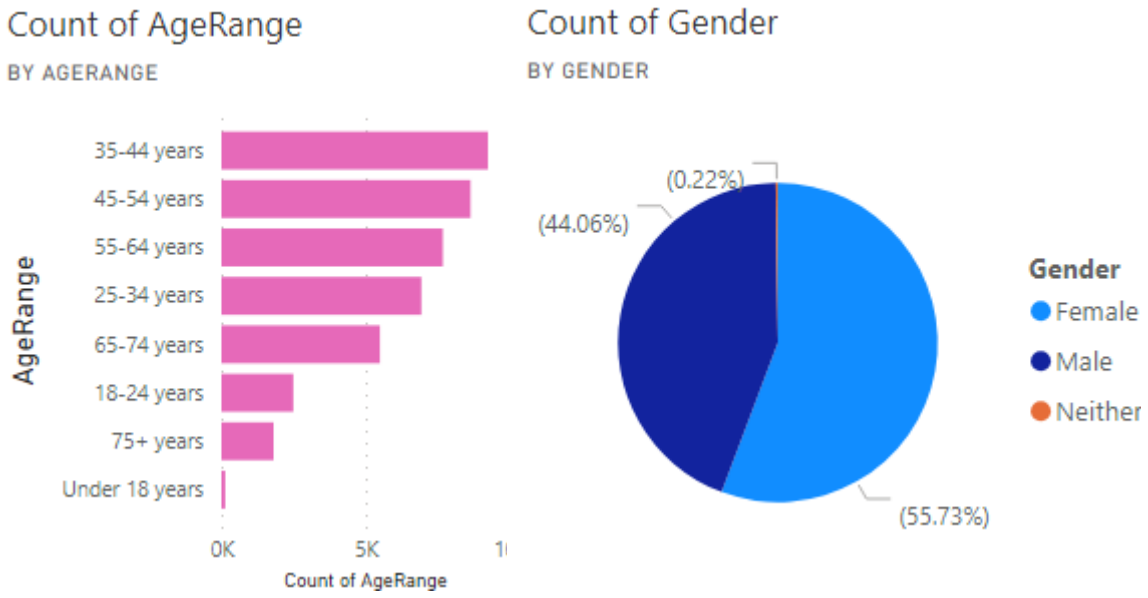
As Australia's only independent specialist identity and cyber support service, IDCARE occupies a niche within the cybercrime response framework. Our national community support service was launched in 2014 as a unique joint public-private and not-for-profit, to support people affected by identity theft, cybercrimes, scams, fraud, and personal information compromise and misuse. This was in direct response to a Council of Australian Governments national identity security strategy, which called for dedicated community remediation and support for victims of identity compromise and misuse. Since then, the Cyber Security Strategy and the National Plan to Combat Cybercrime recognises the critical role played by IDCARE in extending highly specialist victim support services to the community that is independent, confidential, and directly addresses the vulnerability of those impacted by these crimes.

These specialist services are centred on an allied health and technical care model directed towards individuals across the community that experience the most serious harms from these crimes. Our Case

Mangers provide independent and expert advice to help them understand the risks and take steps to address the compromise they have experienced. IDCARE also provides incident support to private and public sector entities that experience information breaches, assisting with their incident response or providing incident response training and preparation. In speaking to people and organisations every day who have been affected by cybercrime, IDCARE is at the frontline of cybercrime.

About IDCARE's individual clients (excluding organisations)

In the last 12 months alone, IDCARE demand from the community has increased over 20%, recording over 81,000 individual cases that resulted in over 260,000 community engagements. This was our busiest year to date. The most common age range of Australians to engage IDCARE specialist services over the last 12 months was 35-44 years, with slightly more people identifying as female compared to other gender groupings.



The vast majority of these community contacts results from crimes enabled via the online environment, resulting in nearly half a billion dollars in loss value. Less than 15% of these reports from community members came via ReportCyber or law enforcement. A large number of our clients report that prior to coming to IDCARE, they did not see the immediate value in reporting to law enforcement.

Emerging threats affecting Australian entities and individuals

On a global scale, IDCARE is aware of the pervasive threat that ransomware has posed and continues to pose on the Australian community. Ransomware operators are often sophisticated experienced cybercriminals who leverage international affiliate networks to carry out their exploits. By November 2023, the number of ransomware attacks detected by IDCARE's monitoring was 126% higher than that which we identified almost 12 months earlier.

While the ransomware industry rightfully soaks up a great deal of public attention, a companion industry, involving the trade of exposed network accesses also continues to boom. The access brokerage industry, characterised by a breed of cybercriminal known as an Initial Access Broker (IAB), serves as a direct precursor to the ransomware industry. IAB's gain unauthorised access to organisational networks through various means, maintain that access and list it for sale across underground forums.

Our national community services include notifying organisations and individuals where we detected that their systems or information repositories have been compromised and/or exploited. We work with law enforcement when necessary to identify these persons where such risks present. This is not done commercially but as a public good. Oftentimes, particularly with regard to small to medium entities, who may not have internal capacity to address a situation as such, our notification is met with suspicion or indifference. While with others, the engagement we have either validates other observed indicators from the victims themselves or is embraced as an opportunity to take control and respond.

There also continues to be heavy reliance on encryption in terms of both messaging platforms and cryptocurrencies. The former are favoured in terms of supporting the advertisement of criminal endeavours, the distribution of compromised data and as a communication services. Telegram in particular has proved to be an appealing landing place for many entry-level and experienced criminals, particularly interested in domestic exploitation. Throughout 2023, 45% of the listings detected by IDCARE analysts which pertained to the sale or distribution of compromised Australian identity data were found on Telegram, and over 100 new threat actors were identified via the platform.

As these crimes continue to go on undisturbed, IDCARE has observed a cohort of threat actors on Telegram who place much less emphasis on maintaining their operational security (OPSEC). Rather, they appear comfortable with sharing details of their work within a forum of fellow threat actors, readily seeking and receiving support and advice.

Profiling case study

In March 2023, IDCARE analysts discovered multiple images of Medicare cards and New South Wales driver's licenses shared within a Telegram group dedicated to Australian fraud activity. Although the identity documents belonged to different individuals, all sets were photographed in front of the same computer, indicating a potential breach. IDCARE was able to marry the details of two exposed credential holders with two former clients who had engaged our services within the preceding 12 months following the misuse of their identity information. Neither client knew how or when their details were initially compromised.

In an effort to identify the source of the breach, we engaged each individual, although neither client could recall providing the documents in the depicted format nor could they recognise the background of the photos. Despite not being able to ascertain a source, we were able to get an update on their experiences following their initial misuse events.

One client, in particular, continued to suffer misuse for up to 24 months after initially seeking our services. Despite a multitude of fraud events committed in their name, including the establishment of transactional bank accounts (even after the client had received a new driver licence card number) this client was not able to get their driver's licence number changed until appearing before a magistrate. Beyond the financial strain of addressing the misuse and correcting their identity information, the client explained how they were still, over 24 months after they initially engaged IDCARE, facing challenges in accessing services in their own name. Their phone bill, car loan and even their lease all had to be registered under their parent's name.

The ongoing trends in relation to encrypted communications is also seen in the preference towards cryptocurrencies. The ability for threat actors to move proceeds of crime from traditional banking to cryptocurrency environments is well proven. This enables the transfer of proceeds seamlessly offshore. There are ongoing efforts across industry to improve detection and response measures in this regard, however, the recently announced consultation paper by Treasury on the *Scams – Mandatory Industry Codes* does not place this industry amongst the current priorities. Although separate to this inquiry, the

Parliamentary Joint Committee may wish to consider where recommendations may extend to support this important work, particularly in advancing work to consider whether cybercrimes should be reported mandatorily under such Codes.

In addition to the persistent use of encryption services, over the past 12 months, IDCARE analysts have observed a concerning increase in the trade of username/password combinations (logs) across darknet repositories. Access to these logs is considered directly related to another growing trend involving the distribution of malicious software families known as 'infostealers' or 'stealers'. There are a number of different stealers on the market, each delivering similar services. Known brands include RedLine, Raccoon and Mars, although strains continue to mutate. The data harvested by infostealers is distributed in troves by threat actors within underground communities. Access to cloud servers which provide constant supply of newly harvested stealer logs are also offered on a subscription-like basis.

Almost immediately after a device is infected by a stealer, data acquisition begins with the malware in pursuit of login credentials and credit card information stored in search browsers, cookies, device-specific properties (IP address, antivirus software in use and applications installed), and files which may contain sensitive information. Once collected this data is transposed to another computer controlled by a malicious actor. In exploiting the acquired data, a malicious actor can use locational proxies (harvested through the stealer infection) to bypass anomaly triggers that prompt multi-factor authentication requests, or detection of fraudulent login attempts by the online service.

These logs may also act as a precursor for data extortion events, particularly when users access work or school networks from an infected personal device. Once garnered, the credentials used to access work applications remotely are then used by initial access brokers attempting to infiltrate corporate networks and sell this access on to ransomware affiliates looking to carry out an attack.

The most significant concern lies in Infostealer's capacity to circumvent anti-virus solutions and evade endpoint detection and response (EDR) platforms. This poses a major problem as the false negatives triggered may go undetected unless actively and specifically investigated.

Like most malwares, stealer infections are generally a result of engagement with malicious links or attachments distributed in spam emails, as well as through exploit packs which feature widely on platforms like YouTube, disguised as links to download cheats or upgrades for online gaming. IDCARE believes that many community members to have experienced cybercrimes committed in their name and do not know how the criminal first got their details may well be victims of this type of crime. The treatment of these individuals and compromised devices requires highly specialised capabilities deployed by IDCARE that requires ongoing government support to scale to the community. Since October 2023, IDCARE has had to scale back its provisioning of this technical support of victims referred to it by the Commonwealth because of a lack of funding, arguably at a time when it is needed most.

Supporting law enforcement to investigate and act upon cybercrime

We acknowledge that the Australian government has mechanisms in place to facilitate cooperation and coordination in responding to cybercrime issues, including the NCWG and the AeCWG and Electronic Evidence Specialist Advisory Group (EESAG), which allow for collaboration between Australian cybercrime investigators and digital evidence specialists. This section is limited to describing IDCARE's existing coordination with law enforcement and ways that we believe better coordination could assist law enforcement capabilities to respond to cybercrime.

IDCARE is placed in a unique position being able to receive threat actor details through first-hand individual's experiences, identify trends and tactics from our significant data holdings, and view the

threat actor behaviour on the dark and clear web, giving us a bigger view over the practices and techniques employed by scammers. This community intelligence can be better leveraged by law enforcement. Unlike ReportCyber, IDCARE specialist services engage victims multiple times and are not constrained by pre-formatted reporting templates. But to advance, 'the system' needs to also acknowledge the needs of the victim and accommodate not just law enforcement reporting, but system signalling back to victims to aid their (and our) detection, protection and response priorities.

Each victim of a cybercrime often wonders whether other crimes are already being committed in their name. They want to know whether they can trust their device. They are desperate to protect their accounts and protect against the creation of new ones. All of this is on the victim to do. It is our mission to walk in the shoes of these victims and look for opportunities to improve the system. This is why we strongly advocate for better ways to not just leverage the consumer intelligence, but work with IDCARE to place the consumer at the centre of our national resilience and response efforts. This requires investment, an acknowledgment of the role of victims, and innovation.

Prevention and education approaches and strategies

IDCARE's community education and outreach programs include:

- Cyber resilience at local community centres and libraries,
- Scam awareness and disruption sessions with Westpac St George bank staff,
- Fact sheets and information brochures on our website and distributed in pamphlets.

In partnership with Westpac in 2021, we set up a Cyber Resilience Outreach Clinic program to do in-person outreach at the 50 most scam vulnerable communities in Australia. We identified the 50 communities through a number of vulnerability factors. The genesis of the program was seeing in our data holdings a 136% increase in regional and remote client support demand and most worryingly, we saw that remote clients incurred:

- 88% higher average losses from email scams than those reported by metropolitan clients,
- 43% higher financial losses from relationship scams,
- 29% higher losses from online shopping scams compared to metropolitan clients,
- Remote clients take 10% more time to respond to these events than metropolitan counterparts due to significantly reduced local service access and connectivity issues.

Our work has enabled IDCARE to conduct 201 cyber resilience outreach clinics across metropolitan, regional and remote communities since November 2021, including over 20 remote First Nations Communities, engaging over 16,000 Australian community members. A priority of this work has been to engage communities to better understand their attitudes and opinions about scams prior to victimisation and juxtapose this with those who experience such crimes to engage our specialist services. The insights are revealing and almost directly point to the need for prevention, detection and response to have a consumer focus.

To test community resilience within the locations we visited, we developed an interactive 'Scambulance' test that assesses resilience. Results show that only 9.6% of participants demonstrated sufficient skills and knowledge to detect and prevent scam attempts.

The rate at which organisations can enact preventative measures correlates to reducing exposure for the individual and subsequent financial losses following scam detection. IDCARE provides a proximity value via a presence in these regional and remote locations. It was a common reflection among community attendees that they wish they had known about IDCARE earlier due to a distressing scam experience they, or someone they knew, had previously experienced.

A sustained understanding of IDCARE's available services, and access to prevention and awareness messaging, amplifies the speed at which individuals detect and organisational responses can occur to minimise losses.

Providing much greater specificity of the response journey relating to financial institutions, such as details about the process, role expectation management, and timeframes, were common enhancement themes captured from community members. This theme was consistent across Australia.

Account and personal information custodians were evident across many remote communities. Their role is largely ignored or not understood in many of the response system requirements of victims – this further exacerbates the challenges confronting victims in remote communities responding to these crimes. The ability to leverage these key community points has yet to be realised in terms of both prevention and response across many of the remote communities engaged.

We saw that First Nations cultural practices and the practical limitations of living on country are not adequately accommodated in many of Australia's established cybercrime response processes imposed by governments and businesses (such as presenting to a branch or station in person). We also continue to see a lack of access to culturally appropriate, in-language information about foundation concepts including cybercrime prevention, device protection, personal information, identity documents, accounts and scams. As an example, telephone engagement was often the only option available to people to complete relevant processes, yet for many in the communities English is a third or fourth language, and their traditional languages did not have words for identity credentials, identity theft, scams and cybercrime. Some community representatives indicated that a person would often simply end the call because they could not comprehend or even hear the representative.

We saw that the reality of many Government and corporate services moving online and reducing their physical presence in remote and regional communities actually has the effect of amplifying the cybercrime and scam risks to these communities.

Concluding remarks

There are many aspects of policing cybercrime that IDCARE could contribute towards, but we have selected only those we believe are most relevant to our community work and experiences. We applaud the Parliamentary Joint Committee for its inquiry and would welcome the opportunity to engage further.